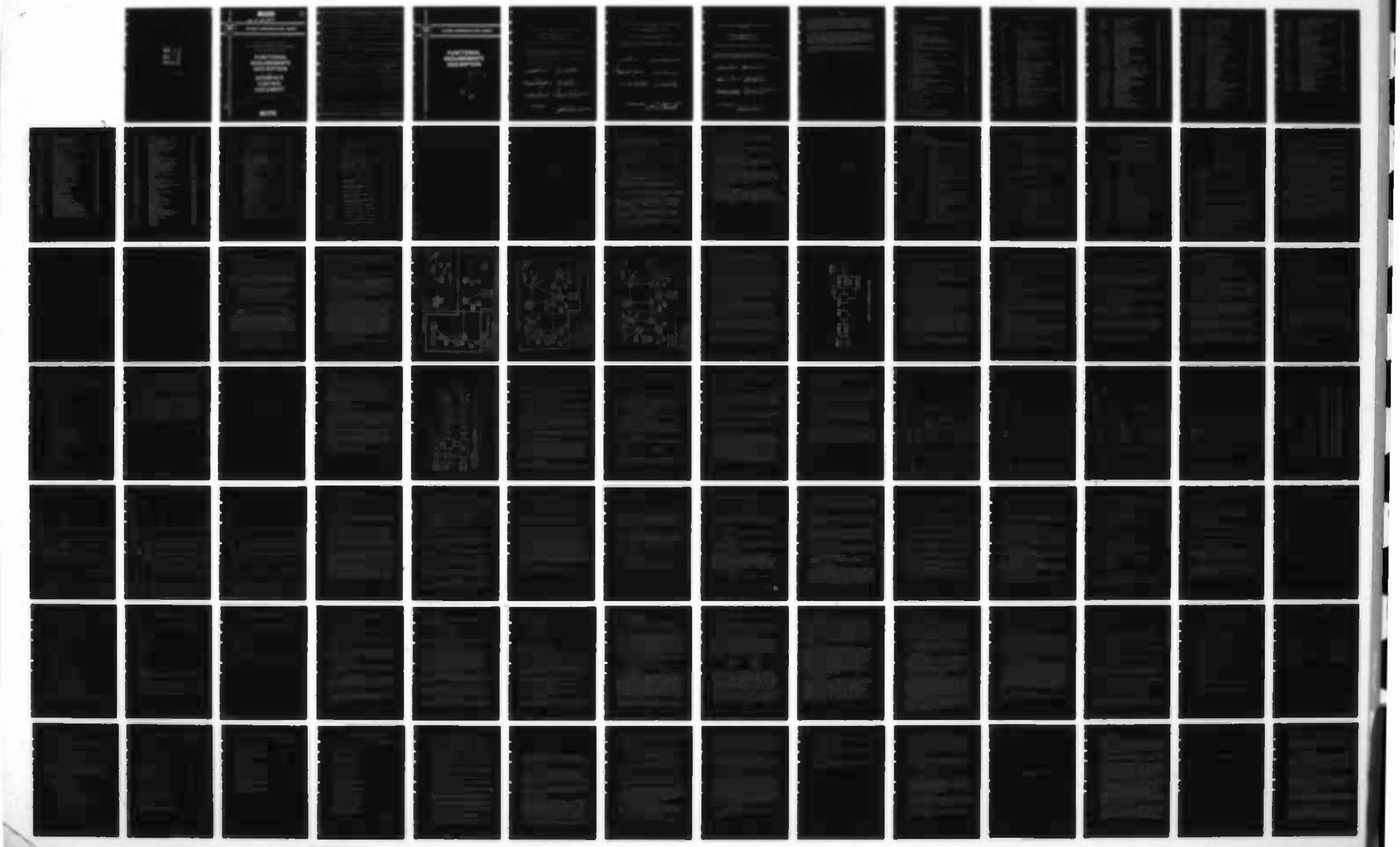
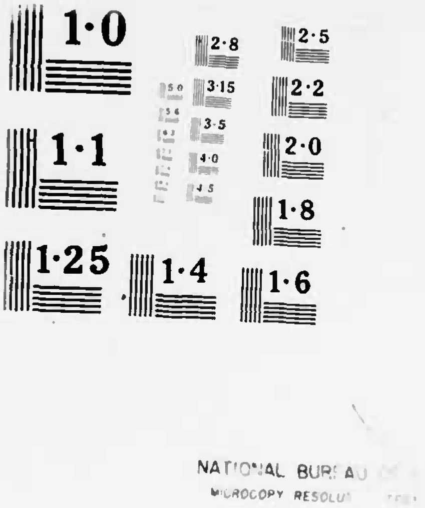
AD-A134 884 INTER-SERVICE/AGENCY AUTOMATED MESSAGE PROCESSING EXCHANGE PROGRAM FUNCTI..(U) DEFENSE COMMUNICATIONS AGENCY ARLINGTON VA 01 NOV 83 1/7

UNCLASSIFIED F/G 17/2 NL




1·0
2·8
2·5
3·15
2·2
3·5
1·1
2·0
4·0
1·8
1·25
1·4
1·6
NATIONAL BUREAU OF
MICROCOPY RESOLU

UNCLASSIFIED

(2)

AD-A134884

DEFENSE COMMUNICATIONS AGENCY

INTER-SERVICE/AGENCY
AUTOMATED MESSAGE PROCESSING
EXCHANGE PROGRAM

FUNCTIONAL REQUIREMENTS DESCRIPTION

AND

INTERFACE CONTROL DOCUMENT

(WITH CROSS REFERENCE MATRICES)

APPROVED FOR PUBLIC RELEASE
DISTRIBUTION UNLIMITED

DTIC
1983
E
D

AD-A134884

DTIC FILE COPY

UNCLASSIFIED

83 11 21 018

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION
UNCLASSIFIED

1b. RESTRICTIVE MARKINGS
NONE

2a. SECURITY CLASSIFICATION AUTHORITY
Various Sources

2b. DECLASSIFICATION/DOWNGRADING SCHEDULE
N/A

3. DISTRIBUTION/AVAILABILITY OF REPORT
A. APPROVED FOR PUBLIC RELEASE
DISTRIBUTION UNLIMITED

4. PERFORMING ORGANIZATION REPORT NUMBER(S)

5. MONITORING ORGANIZATION REPORT NUMBER(S)

6a. NAME OF PERFORMING ORGANIZATION
DATA NETWORK ACCESS DIVISION

6b. OFFICE SYMBOL *(If applicable)*
B662

7a. NAME OF MONITORING ORGANIZATION
same

6c. ADDRESS *(City, State and ZIP Code)*
Defense Communications Agency
8th & So. Courthouse Roads
Washington, D. C. 20305

7b. ADDRESS *(City, State and ZIP Code)*

8a. NAME OF FUNDING/SPONSORING ORGANIZATION
same

8b. OFFICE SYMBOL *(If applicable)*
B662

9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
n/a

8c. ADDRESS *(City, State and ZIP Code)*

10. SOURCE OF FUNDING NOS.

PROGRAM ELEMENT NO.	PROJECT NO.	TASK NO.	WORK UNIT NO.
33126 K			

11. TITLE *(Include Security Classification)*
See Block 16

12. PERSONAL AUTHOR(S) n/a

13a. TYPE OF REPORT
Final

13b. TIME COVERED
FROM 31Oct 81 TO 31 Oct8

14. DATE OF REPORT *(Yr., Mo., Day)*
1983 NOV 01

15. PAGE COUNT
634

16. SUPPLEMENTARY NOTATION Title: "INTER-SERVICE/AGENCY AUTOMATED MESSAGE PROCESSING EXCHANGE PROGRAM FUNCTIONAL REQUIREMENTS DESCRIPTION AND INTERFACE CONTROL DOCUMENT"

17. COSATI CODES

FIELD	GROUP	SUB. GR.

18. SUBJECT TERMS *(Continue on reverse if necessary and identify by block number)*
a. Data Communications b. AUTODIN C. Formal Message
d. DDN Host e. Inter-Service/Agency Automated Message Processing Exchange

19. ABSTRACT *(Continue on reverse if necessary and identify by block number)*

The Inter-Service/Agency Automated Message Processing Exchange(I-S/A AMPE) will provide a standardized replacement for existing Service/Agency AMPEs, and will provide a functional replacement for existing AUTODIN Switches. This "Inter-Service/Agency Automated Processing Exchange Functional Requirements Description and Interface Control Document" represent user agreed characteristics for the I-S/A AMPE. These documents will be used in part as an exhibit in the Statement of Work for procurement of the I-S/A AMPE

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT
UNCLASSIFIED/UNLIMITED ☒ SAME AS RPT. □ DTIC USERS □

21. ABSTRACT SECURITY CLASSIFICATION
UNCLASSIFIED

22a. NAME OF RESPONSIBLE INDIVIDUAL
Mr. Charles Eislminger

22b. TELEPHONE NUMBER *(Include Area Code)*
(202) 692-2042

22c. OFFICE SYMBOL
B662

EDITION OF 1 JAN 73 IS OBSOLETE.

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE

DEFENSE COMMUNICATIONS AGENCY

FUNCTIONAL REQUIREMENTS DESCRIPTION

Accession For
NTIS GRA&I ☒
DTIC TAB □
Unannounced □
Justification

By
Distribution/
Availability Codes
Dist Avail and/or Special
A-1

DTIC COPY INSPECTED 2

Inter-Service Agency Automated Message Processing Exchange
(I-S/A AMPE)

FUNCTIONAL REQUIREMENTS DESCRIPTION (FRD)
and
INTERFACE CONTROL DOCUMENT (ICD)

Integrated AUTODIN System (IAS) Requirements Panel Coordination Sheet

Coordination indicates IAS Requirements Panel-level approval of the incorporation of all Service/Agency comments to this document received to date with the exception that the following sections of the FRD/ICD have not been completed at this time:

Section 20, I-S/A AMPE Message Format Validation (Included)

Section 30, Security Appendix

ARMY

Ron Elliott
NAVY

AIR FORCE

NATIONAL SECURITY AGENCY

William E Howell
DEFENSE INTELLIGENCE AGENCY

Thomas A
DEFENSE LOGISTICS AGENCY

Date: 28 JAN 83

Jack C. Lane, Lt Col USAF
DEFENSE COMMUNICATIONS AGENCY

Inter-Service Agency Automated Message Processing Exchange
(I-S/A AMPE)

Functional Requirements Description (FRD)
Section 30.0

Integrated AUTODIN System Requirements Panel
Coordination Sheet

Coordination indicates IASRP-level approval of the incorporation of all Service/Agency comments to this document received to date.

ARMY

Mary Jo Beckman, LCDR
NAVY

AIR FORCE

NATIONAL SECURITY AGENCY

Douglas A Brothers
DEFENSE INTELLIGENCE AGENCY

DEFENSE LOGISTICS AGENCY

Date 13 October 1983

DEFENSE COMMUNICATIONS AGENCY

Inter-Service Agency Automated Message Processing Exchange
(I-S/A AMPE)

FUNCTIONAL STATEMENT DOCUMENT (FSD)
APPENDIX 3B
I-S/A AMPE MESSAGE FORMAT VALIDATION

Integrated AUTODIN System (IAS) Requirements Panel Coordination Sheet

Coordination indicates IAS Requirements Panel-level approval of the incorporation of all Service/Agency requirements to this document. Appendix 3B will also become FRD (Section 20) upon approval. (Included)

George Gross
ARMY

CDCorman, LT, USN
NAVY

AIR FORCE

NATIONAL SECURITY AGENCY

Douglas A Brothers
DEFENSE INTELLIGENCE AGENCY

Thomas A Twitchell
DEFENSE LOGISTICS AGENCY

Date: 3MAY83

Jerry A Swint
DEFENSE COMMUNICATIONS AGENCY

PREFACE

The Inter-Service/Agency Automated Message Processing Exchange (I-S/A AMPE) Functional Requirements Description (FRD) is an intermediate step in the documentation and specification of the requirements of Military Services, Defense Agencies, Joint Chiefs of Staff and the Department of Defense for a common-user communications automation facility which will be a follow-on and replacement of existing Service and Agency AMPE programs and the AUTODIN Switching Centers (ASCs).

The FRD and its companion Interface Control Document (ICD) are an outgrowth of earlier documentation; the Functional Statement Document (FSD) in three sections (Section I - Base Level, Section II - ASC Residual, and Section III - Network Interface). The FRD and ICD organize the FSD statements in a logical, system-oriented manner; expand and extrapolate them to provide the basis for technical specifications; and fill in requirements (e.g., system performance and sizing) dictated by system needs.

The validated baseline for the FRD and ICD is the three section FSD. When validated, the FRD and ICD become the baseline for the preparation of the solicitation package by the Air Force Automated Systems Project Office, Gunter AFS, Alabama.

ABBREVIATED TABLE OF CONTENTS

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF TABLES (CONT.)

SECTION 1

SCOPE

1.0 SCOPE

This is the functional requirements description for the Inter-Service/Agency Automated Message Processing Exchange (I-S/A AMPE), a service processing element of the Integrated AUTODIN System (IAS). The I-S/A AMPE will perform the following functions:

a. Message processing currently done by Service/Agency (S/A) AMPEs.

b. Message processing currently done by the AUTODIN Switching Centers (ASCs).

c. Information interchange between AUTODIN and Defense Data Network (DDN) subscriber communities.

d. Secure information processing and transfer, to include compartmented information.

1.01 Basis

This document forms the basis for the development and preparation of the following I-S/A AMPE specifications:

a. Type A Specification - System Specification. This type of specification will state the technical and mission requirements for the I-S/A AMPE (See Appendix I of MIL-STD-490).

b. Type B Specification - Development Specifications. These specifications will state the requirements for the design or engineering development of the I-S/A AMPE. Two types of these specifications will be prepared.

(1) Type B2 - Critical Item Development Specification (See Appendix III of MIL-STD-490). Type B2 specifications will be prepared for I-S/A AMPE items which are engineering critical or logistics critical.

(2) Type B5 - Computer Program Development Specification (See Appendix VI of MIL-STD-490). This type of specification will be prepared for development of the I-S/A AMPE computer programs, and it will describe in operational, functional, and mathematical language all the requirements necessary to design and verify the required computer programs in terms of performance criteria.

c. Type C Specification - Product Specifications. These specifications will be applicable to I-S/A AMPE items which are functional (performance) requirements or fabrication (detailed design) requirements. Two types of these specifications will be prepared.

(1) Type C2 - Critical Item Product Specification. These specifications will be prepared for engineering or logistic critical I-S/A AMPE items. They may be prepared as function or fabrication specifications (See Appendices IX and X of MIL-STD-490).

(2) Type C5 - Computer Program Product Specification (see Appendix XII of MIL-STD-490). This type of specification will be prepared for the production of the I-S/A AMPE computer programs. When two-part specifications are used, B types shall form Part I and C types shall form Part II.

1.1 Interface Control Document

This document is complemented by the Interface Control Document (ICD), which serves as the repository for environmental, mechanical, electrical, protocols, format, and human interface criteria controlling or constraining the development of the I-S/A AMPE.

1.2 Standard Definitions and Terminology

To insure consistent, accurate and concise application of terminology, this document contains a glossary of terms and acronyms (Section 10.0). References may be made to the applicable documents in Section 2.0 for information to supplement that contained in Section 10.0.

1.3 Pre-Planned Product Improvement

The I-S/A AMPE is being implemented in two parallel and interlocking tracks. Track I involves the development of a system incorporating those required functions which can be implemented using current state-of-the-art practices. Track II will implement the I-S/A AMPE interface to the Defense Data Network and provide full consolidation of DSSCS and GENSER facilities. Sub-section 3.12 provides a more detailed discussion of the intended Pre-planned Product Improvements (P^3I).

1.4 Change Procedure

All changes to this document will be processed in accordance with Appendix II of the Management Engineering Plan, I-S/A AMPE Functional Requirements Change Process. All Services and Agencies that utilize the AUTODIN will be members of the Integrated AUTODIN System Requirements Panel (IASRP). This panel will have the responsibility for obtaining ratification of all proposed changes to requirements documents associated with the I-S/A AMPE program and will operate according to the provisions of the IASRP charter.

SECTION 2

APPLICABLE DOCUMENTS

2.0 REFERENCED DOCUMENTS

2.1 Military and Federal Standards

FED-STD-1031	Telecommunications, General-Purpose 37 Position and 9 Position Interface Between Data Terminal Equipment and Data Circuit Terminal Equipment
FED-STD-1037	Telecommunications Terms and Definition
MIL-STD-188-100	Common Long Haul and Tactical Communication System Technical Standards
MIL-STD-188-114	Electrical Characteristics of Digital Interface Circuits
MIL-STD-188-124	Grounding, Bonding and Shielding
MIL-STD-188-310A	Subsystem Design and Engineering Standards for Technical Control Facilities
MIL-STD-470	Maintainability Program Requirements (for Systems and Equipments)
MIL-STD-483	Configuration Management Practices for Systems, Equipment, Munitions, and Computer Programs
MIL-STD-490	Specification Practices
MIL-STD-785A	Reliability Program for Systems and Equipment Development and Production
MIL-STD-756A	Reliability Prediction
MIL-STD-781C	Reliability Tests, Exponential Distribution
MIL-STD-1472	Human Engineering Design Criteria for Military Systems, Equipment and Facilities
MIL-STD-1521A	Technical Reviews and Audits for Systems, Equipment, and Computer Programs
MIL-STD-1679	Software Development
MIL-E-4158E	General Requirements for Ground Electronic Equipment
MIL-H-232	(C) RED/BLACK Engineering-Installation Guidelines (U)
MIL-H-46855B	Human Engineering Requirements for Military Systems, Equipment, and Facilities

2.2 DoD Directives, Instructions, and Manuals

DoD 5000.29	Management of Computer Resources in Major Defense Systems
DoD 5200.28	Security Requirements for Automatic Data Processing (ADP Systems)
DoD 5200.28-M	ADP Security Manual
DoD 5200.1-R	Information Security, Program Regulation
DoD 5220.22-M	Industrial Security Manual for Safeguarding Classified Information
DoD C-5030.58M	(C) Defense Special Security Communications System, Security Criteria and Telecommunications Guidance (U).
DoD Manual 7935-1-5	Automatic Data System Documentation Standard

2.3 Joint/Allied Communications Publications

ACP 100, US SUPP 1	(C) Address Indicator Groups (U)
ACP 112	(C) Task/Type Organizations (U)
ACP 117, CAN-US SUP 1	US Routing Indicator Book
ACP 117, US SUPP-3	Defense Communications System Routing Doctrine General Purpose Networks
ACP 121, US SUPP-1	(C) Communications Instructions - General (U)
ACP 122	(C) Communications Instructions - Security (U)
ACP 126	(C) Communications Instructions - Teletypewriter (Teleprinter) Procedure (U)
ACP 127, US SUPP-1 and NATO SUPP 3	(C) Communications Instructions - Tape Relay Procedures (U)
ACP 131 ( )	Communications Instructions - Operating Signals
ACP 167 ( )	Glossary of Communications-Electronic Terms
ACP 198 US SUPP-1	Instruction for the Preparation of Communications - Electronics Publications
JANAP 128( )	Automatic Digital Network (AUTODIN) Operating Procedures

DOI 101	(Secret Compartmented Document) Defense Special Security Communications System (DSSCS) Address Groups (DAG) (U)
DOI 102	(Secret Compartmented Document) Defense Special Security Communications System Operating Instructions - Routing Indicators (U)
DOI 103	(Confidential Compartmented Document) Defense Special Security Communications System Operating Instructions System/Data Procedures (U)

2.4 Service/Agency Telecommunications Instructions and Procedures

AFM 10-4	Air Force Directory of Unclassified/Classified Addresses
AR 105-32	Authorized Addresses for Electrically Transmitted Messages
JDOD PLAD	Joint Department of Defense Plain Language Address Directory
NTP 3 SUPP-1( )	Plain Language Address Directory
NTP 4	Modifications to ACP-126
NAVELEX INST 5200.23	Computer Software Life Cycle Management Guide
DCAC 300-175-9	DCS Operation-Maintenance Electrical Performance Standards
DCAC 310-55-1	Status Reporting for the DCS
DCAC 310-D70-30	DCS AUTODIN Switching Center and Tributary Operation
DCAC 310-D70-55	(C) DCS AUTODIN Defense Special Security Communications System Routing Doctrine (U)
DCAC 310-130-1	Submission of Telecommunications Service Requests
DCAC 310-D130-3	Approved DCS AUTODIN Terminal Systems
DCAC 370-D95-1	System Description DCS-AUTODIN
DCAC 370-D175-1	Interface and Control Criteria
DCAC 370-D195-1	DCS AUTODIN Interface Category I Testing
DCAC 370-D195-2	DCS AUTODIN TEMPEST Category II Testing

DCAC 370-D195-3	DCS AUTODIN Category III Operational Acceptance Test
DoD CSEC	Trusted Computer System Evaluation Criteria, 24 May 1982 (Draft)
USSID 307	(Secret Compartmented Document) SIGINT Product Distribution (U)
USSID 309	(Secret Compartmented Document) Manual of Authorized SIGINT Product Recipients (U)
USSID 505	(Secret Compartmented Document) Directory of SIGINT Organizations (U)
USSID 519	(Top Secret Compartmented Document) Delivery Distribution Indicators (U)
DIA Publication	(Secret Compartmented Document) Compartmented Address Book (U)

2.5 Other References

a. Draft AUTODIN I System Functional Specification, DCA B652, August 1982

b. I-S/A AMPE Functional Statement Document (Section I, II and III), DCA 23 SEP 82

c. Jensen, Randall W. and Tonies, Charles C., "Software Engineering", Prentice Hall 1979.

d. NAVELEX Software Management Guidebook Vol. I "Software Acquisition Monitoring."

e. Defense Data Network Program Plan, DCA, January 1982 with changes.

f. Nibaldi, G.H., "Proposed Technical Evaluation Criteria for Trusted Computer Systems," M79-225, The MITRE Corporation, Bedford, MA, 25 October 1979

g. E. T. Trotter & P. S. Tasker, "Industry Trusted Computer System Evaluation Process," The MITRE Corporation, Bedford, MA, 1 May 1980

h. Nibaldi, G. H. "Specification of A Trusted Computing Base (TCB)," M79-228, The MITRE Corporation, Bedford, MA, 30 November 1979

i. M. H. Cheheyl, M. Gasser, G. A. Huff, J. K. Millen "Secure System Specification and Verification: Survey of Methodologies," MTR-3904, The MITRE Corporation, Bedford MA, 20 February 1980

j. Nomenclature internationale des bureaux de poste - Universial Postal Union - Bern Edition 1977 w/changes Index Printers, Dunstable, Bedfordshire, England

2.6 Selected Papers on Secure Systems Development

The following is a partial list of papers in the area of secure systems development.

(Ames78), Ames, S. R., "Design of a Message Processing System for a Multilevel Secure Environment," MTR-3449, The MITRE Corporation, Bedford, Massachusetts, (June 1978).

(Anderson72), Anderson, J. P., "Computer Security Technology Study," ESD-TR-73-51, Volumes I and II, James P. Anderson & Company, Fort Washington, Pennsylvania, (October 1972).

(Bell73), Bell, D. E. and LaPadula, L. J., "Secure Computer Systems," ESD-TR-73-278, Volumes I and II and III, The MITRE Corporation, Bedford, Massachusetts, (November 1973-June 1974).

(Biba75), Biba, K. J., "Integrity Considerations for Secure Computer Systems," MTR-3153, The MITRE Corporation, Bedford, Massachusetts, (June 1975).

(Burke76), Burke, E. L., "Secure Minicomputer Architecture," MT76-224, The MITRE Corporation, Bedford, Massachusetts, (October 1979).

(Cheheyl79), Cheheyl, M. H., Huff, G. A., Gasser, M., Millen, J. K., "Secure System Specification and Verification: Survey of Methodologies," MTR-3904, The MITRE Corporation, Bedford, Massachusetts, (20 February 1979).

(Lampson73), Lampson, B. W., "A Note on the Confinement Problem," CACM, Volume 16, No. 10, 613-615, (October 1973).

(Lipner75), Lipner, S. B., "A Comment on the Confinement Problem," MTR-167, The MITRE Corporation, Bedford, Massachusetts, (November 1975).

(Parnas72), Parnas, D. L., "A Technique for Software Module Specification with Examples," CACM, Volume 15, No. 5, (May 1972).

(Schroeder72), Schroeder, M. D., "Corporation of Mutually Suspicious Subsystems in a Computer Utility," Ph.D. Thesis, MIT, (1972), Project MAC Report MAC-TR-104.

(Smith74), Smith, L., "Architecture for Secure Computing Systems," MTR-2772, the MITRE Corporation, Bedford, Massachusetts, (June 1974).

(Tangney78), Tangney, J. D., "Minicomputer Architecture for Effective Security Kernal Implementation," ESD-TR-78-170, Electronic System Division, AFSC, Hanscom Air Force Base, Massachusetts, (October 1978).

(NBS80)-NBS, Proceedings of the Second Seminar on the DoD Computer Security Initiative Program, January 1980, W-1 to W-11.

2.7 Industry Specifications, Instructions and Manuals

ANSI Standard S1.2-1971 Noise

SECTION 3

REQUIREMENTS

3.1 OBJECTIVES AND CONCEPTS

3.0 REQUIREMENTS

3.1 General I-S/A AMPE Objectives and Concepts

This document establishes the functional and performance requirements for the development of the I-S/A AMPE for use by all Services and Agencies. The multi-level secure I-S/A AMPE is a key element in the Integrated AUTODIN System (IAS) and will be comprised of three functional modules; network communications, service processing and user terminal. The I-S/A AMPE will be a host subscriber of the Defense Data Network (DDN) and as such needs the host-to-host protocol structure required to directly interface a Packet Switching Node (PSN) of the DDN, thus the network communications module. The service processing module provides the Formal Message Service (FMS), while the user terminal module provides the requisite man machine interface (e.g., keyboard, video display and printer). Current state-of-the-art technology shall be exploited in the construction of the I-S/A AMPE equipment. The I-S/A AMPE shall fulfill the following requirements:

- Provide a multi-level secure certified and accredited, standard automated telecommunications message processing system with capabilities based on validated Service/Agency requirements. The developed baseline system will provide the minimum essential functional capabilities currently existing in DoD automated telecommunications message processing systems.

- Provide a functional replacement for the current AUTODIN Switching Centers (ASCs) retaining only the functions required to support AUTODIN users.

- Provide an interface to the Defense Data Network (DDN).

3.1.1 The I-S/A AMPE as an Element of the Integrated AUTODIN System Architecture

The major objective of the Integrated AUTODIN System (IAS) is to provide system commonality and compatability in record and data processing within the Defense Communications System (DCS). The IAS Architecture (IASA) is the plan defining the types of systems (in terms of processing and interface capabilities) required to support the IAS objectives, while enhancing the capabilities of the current DCS structure. As a key element in the IASA, the I-S/A AMPE will be the standard system which will replace the automated message processing exchange of all DoD Services and Agencies. In this regard, the prime objectives in the development and implementation of the I-S/A AMPE are as follows:

- To standardize the telecommunications services performed.

- To identify and standardize interface capabilities.

- To decrease overall operating and maintenance costs.

- To eliminate duplicate efforts in the development and maintenance of message processing systems and subscriber terminals.

The evolution of the IASA is divided into three time frames keyed to the deployment of I-S/A AMPE and the phase out of ASCs. The Near-Term is defined as that time prior to fielding of the I-S/A AMPE. The Mid-Term begins with the fielding of the I-S/A AMPE and concludes with the phasing out the last ASC. The Far-Term is defined as the time frame following phase out of all ASCs.

3.1.2 The Near-Term IAS Architecture

The major Near-Term activity will be the implementation of the Defense Data Network (DDN). The DDN is a secured packet switching network designed to provide a packet transport backbone capability for the IAS.

In the Near-Term, as depicted in Figure 1, the PSNs will support only the DDN subscribers and will not interface with the AUTODIN community. During this time frame, AUTODIN should not experience major changes or enhancements except for urgent mission requirements and those necessary to maintain ASC viability through the IAS mid-term. The following Automated Message Processing Exchanges (AMPEs) will be operational in the near-term IAS: Army's AMME, Navy's LDMX, Air Force's AFAMPE, NSA's STREAMLINER, and DLA's AMPE. In the near-term, the interface for the TRI-TAC AN/TYC-39 switches and the NICS TARE switches to AUTODIN will be via the ASCs. In this period, the I-S/A AMPE will be developed, implemented and prototype tested.

3.1.3 The Mid-Term IAS Architecture

With the advent of I-S/A AMPE Initial Operational Capability (IOC) the Mid-Term IAS begins and it lasts until the Goal IASA has been achieved (the last of the ASCs has been phased out). Each I-S/A AMPE will initially serve either the DSSCS or the GENSER community. The DSSCS I-S/A AMPE will be accessed only by Top Secret and Special Compartmented Intelligence (SCI) cleared personnel and traffic between them will be End-to-End Encryption (E^3) protected. As trusted computer base technology matures, segregation of DSSCS and GENSER facilities will be eliminated. During the Mid-term IAS, initial deployment of the I-S/A AMPEs will be undertaken and the I-S/A AMPEs will be required to assume the terminal support functions of the ASCs. The I-S/A AMPEs will be the element that will ultimately allow members of the Formal Message Service (FMS) community to exchange message traffic with members of the Virtual Connection Service (VCS) community. These changes are illustrated in Figure 2. Once the Goal Architecture is fully achieved, the I-S/A AMPEs and PSNs will fully replace the ASCs. Further the I-S/A AMPE, in its role as an ASC functional replacement, will provide the interfaces to TRI-TAC, other non-DoD U.S. networks (State's Diplomatic Telecommunications Service (DTS) and GSA's Advanced Record System (ARS)), specified allied networks, and the NATO alliance NICS TARE switches as do ASCs.

3.1.4 The Goal and Far-Term IAS Architecture

The Goal Architecture is illustrated in Figure 3. During the Transition Phase, the I-S/A AMPEs will be replacing existing AMPEs. Certain of these AMPEs will have economic service

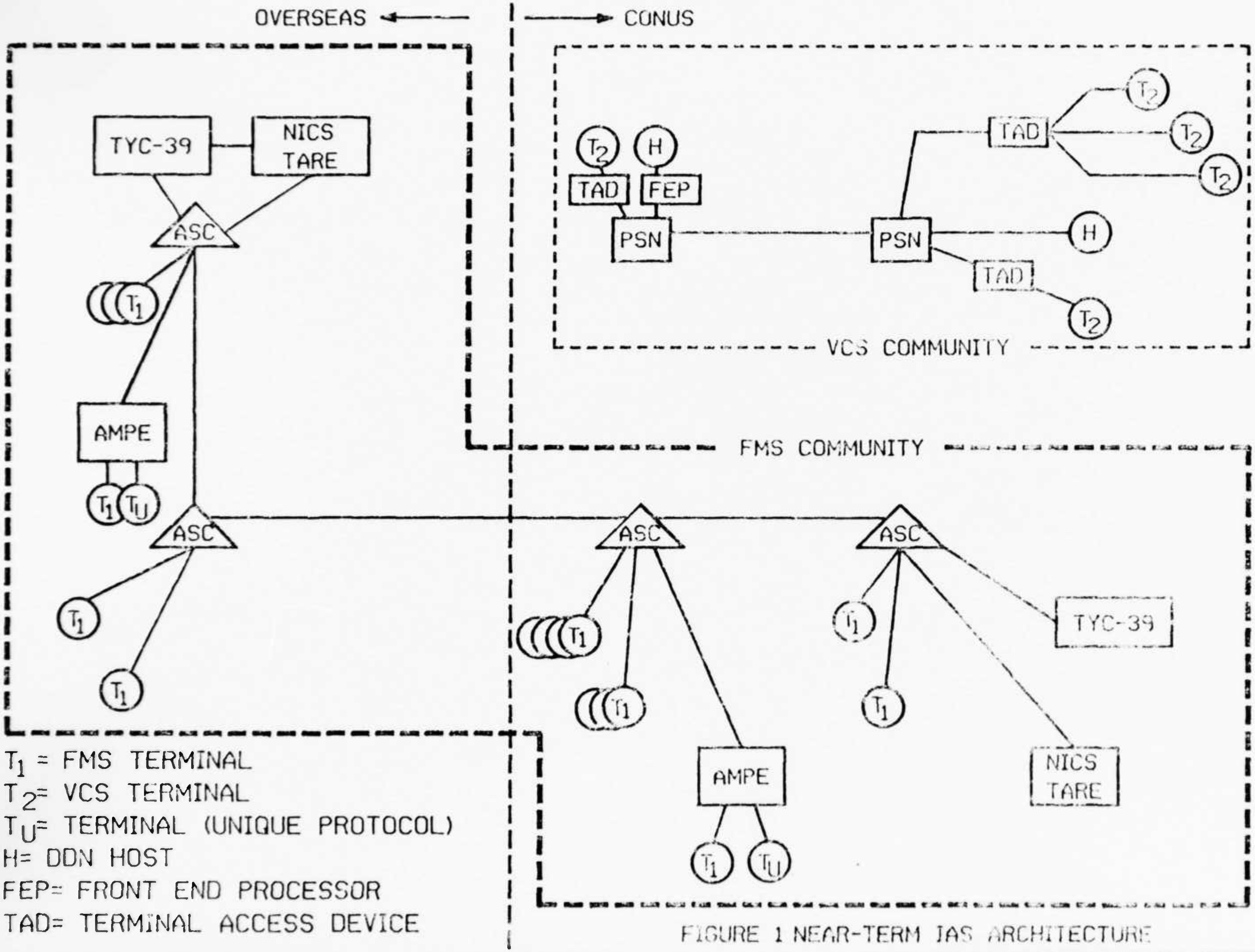
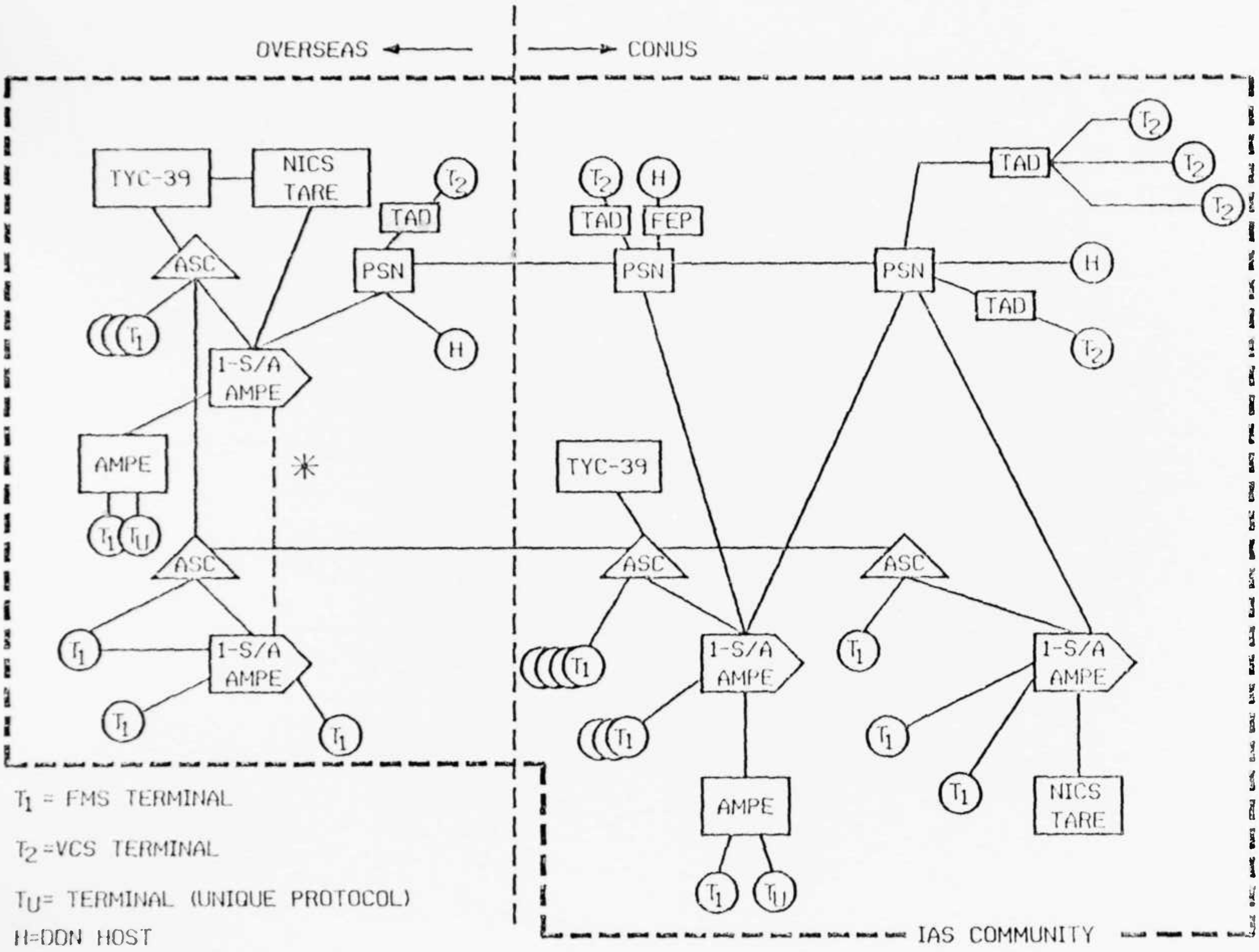


FIGURE 1 NEAR-TERM IAS ARCHITECTURE



T_1 = FMS TERMINAL

T_2 =VCS TERMINAL

T_U= TERMINAL (UNIQUE PROTOCOL)

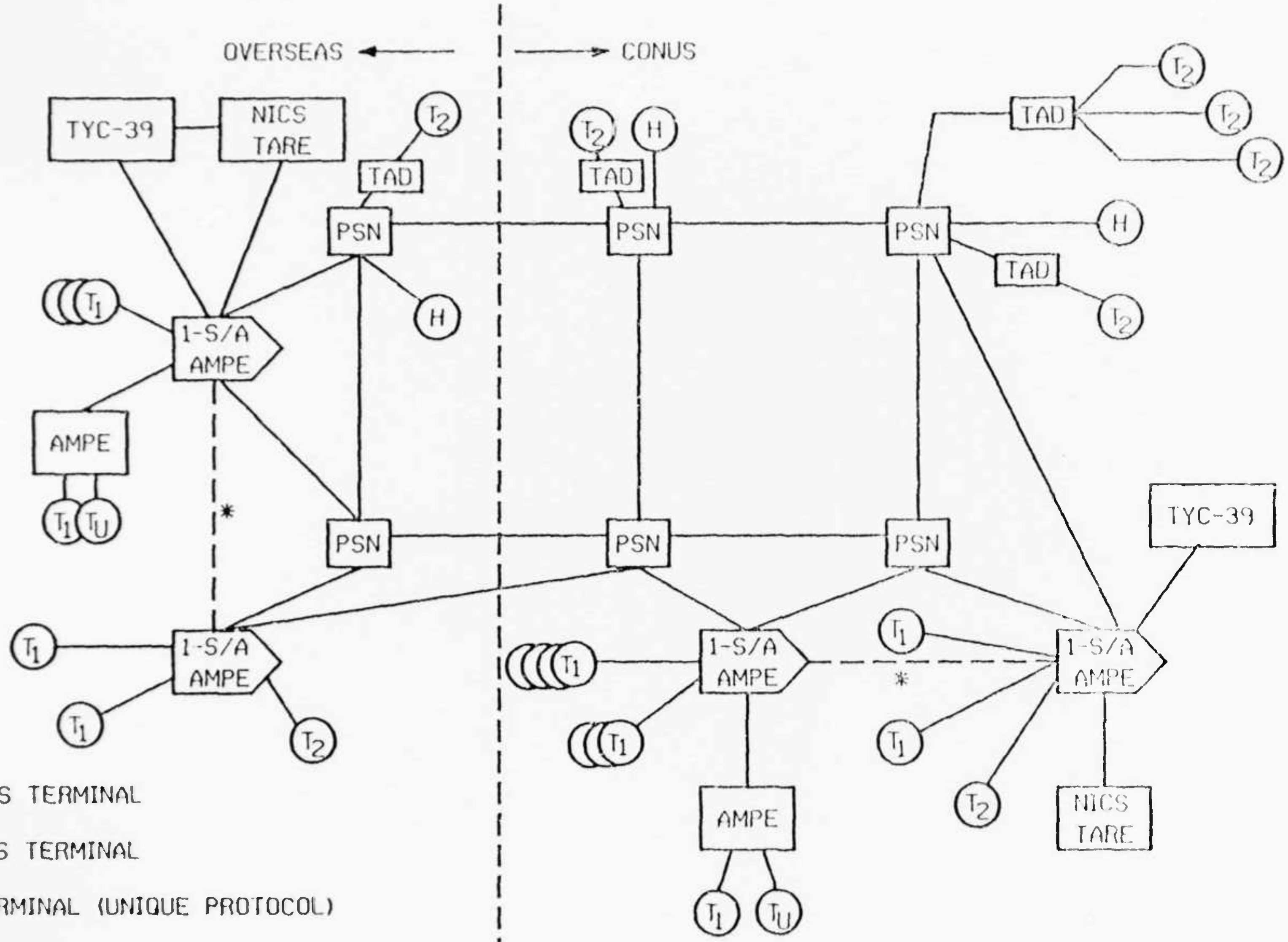
H=DDN HOST

*= CONTINGENCY CONNECTION

FEP= FRONT END PROCESSOR

TAD= TERMINAL ACCESS DEVICE

FIGURE 2 IAS TRANSITION AT I-S/A AMPE IOC



T_1 = FMS TERMINAL

T_2 = VCS TERMINAL

T_U = TERMINAL (UNIQUE PROTOCOL)

H=DDN HOST

*= POST IOC IF VALIDATED

FEP= FRONT END PROCESSOR

TAD= TERMINAL ACCESS DEVICE

FIGURE 3 GOAL IAS ARCHITECTURE

lifetimes which will extend beyond the Mid-term and are, therefore, included in the Goal Architecture. The I-S/A AMPE, in its role as the integrator of FMS and VCS, will ultimately provide network value-added services to selected DDN subscribers in addition to current AUTODIN FMS terminals. For example, the I-S/A AMPE provides an FMS similar to the current AUTODIN narrative/data message service to directly connected subscriber and ultimately to selected remote subscriber who access the I-S/A AMPE through the network. Further details on the interface, network service and data flows to be provided by the I-S/A AMPE are contained in paragraph 3.1.5 and its subparagraphs.

The Far-Term IAS looks to a complete integration of narrative, record and data communications services worldwide. There is expected to be a continuing evolution of the Integrated AUTODIN System as the DCS continues to mature toward a World Wide Digital System Architecture (WWDSA). New IAS services are expected to be developed in response to user requirements. The initial I-S/A AMPE, as an IAS network element, may be required to provide some of the new AUTODIN services such as improved message profiling and retrieval, message processing workload sharing, teleconferencing and mail box service. The design of the IOC I-S/A AMPE shall allow for expansion of services such that the incremental addition of new features within the basic IOC I-S/A AMPE can be accomplished with minimal impact on the existing software after taking into account security constraints. Paragraph 3.1.5.4, I-S/A AMPE Design Requirements, discusses this requirement in more detail. This document specifies the requirements for the I-S/A AMPE for the Goal IASA (See Figure 3).

3.1.5 I-S/A AMPE Concept of Operations

The I-S/A AMPE is the element of the IAS Goal Architecture providing Formal Message Service (FMS) including a Message Editing and Preparation Service (MEPS), and network access to both the FMS and VCS community of terminals (See Figure 4). In this role, the I-S/A AMPE views all other I-S/A AMPEs as directly connected. For example, in Figure 4 I-S/A AMPE #1 views terminals A and B as directly connected to itself and terminals C and D directly connected to I-S/A AMPE #2. I-S/A AMPEs also view other I-S/A AMPEs as directly connected. In Figure 4 I-S/A AMPE #1 and #2 view each other as directly connected.

There are two types of paths to users that are understood by the I-S/A AMPE. These are: 1) paths to users physically connected to the I-S/A AMPE (in Figure 4 I-S/A AMPE #1 views terminals A and B in this manner) and 2) virtual paths which connect users (or other I-S/A AMPEs) to the I-S/A AMPE via the backbone network. For example, based on Figure 4, I-S/A AMPE #2 can establish virtual paths through the DDN backbone to Terminal C, I-S/A AMPE #1, and the Host.

The Goal IAS Architecture provides two distinct and separate addressing schemes, the AUTODIN Routing Indicator (RI) addressing and the DDN logical addressing. The I-S/A AMPE shall be capable of translating from one addressing scheme to the other. Specifically, the I-S/A AMPE shall be capable of maintaining both the AUTODIN and DDN addresses for all appropriate IAS

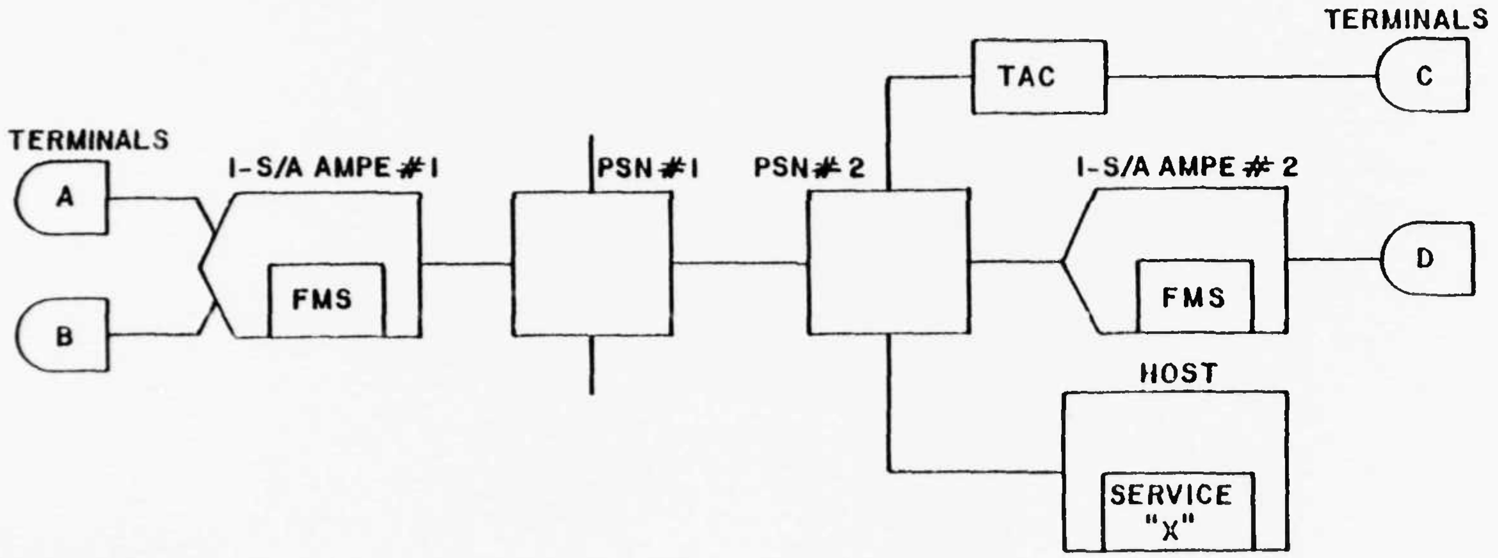


FIGURE 4 - IOC I-S/A AMPE DATA FLOW PATHS

subscribers, and it shall be capable of using that information to effect the delivery of traffic to any affected IAS subscriber.

3.1.5.1 I-S/A AMPE Services

The definition of the IAS has led to the identification of several network services designed to meet both existing and anticipated DoD user requirements. The service provided during the Mid-Term by the IOC I-S/A AMPE shall be Formal Message Service (FMS) with its Message Editing and Preparation Service (MEPS). Additional services such as improved message profiling and retrieval, message processing workload sharing, teleconferencing, and mail box service are intended to be provided in the Far-Term. The architecture of the I-S/A AMPE (hardware and software) will be sufficiently flexible to allow the introduction of new functions as they become validated and available, and the modification of existing functions as necessary throughout the service life of the system.

3.1.5.1.1 Formal Message Service (FMS)

FMS provides the capability for subscribers to create, send, and receive formal messages. FMS can be regarded to be a continuation of the current AMPE functions and the AUTODIN message sevice. Formal messages are defined as messages based on the 16 line military message format that are prepared, released, handled, and recorded for storage in accordance with Service/Agency procedures. The I-S/A AMPE FMS shall support both DSSCS and GENSER traffic in all but not limited to, the following formats: JANAP 128 (narrative and data), DOI-103, ACP 127, and ACP 126 (modified) formats, as well as Joint Message Form (DD Form 173) input. The FMS will perform those message processing and routing functions necessary to replace AMPE and ASC message functions. Detailed requirements for FMS are specified in 3.2.1.

3.1.5.1.2 Message Editing and Preparation Service (MEPS)

The I-S/A AMPE will provide the capability to guide the message preparer through the process of entering a message. This function includes automatic supervision of message preparation, including message mask call-up and message editing capabilities. Messages entering the I-S/A AMPE via an Optical Character Reader (OCR) will conform to the standard DD 173 format (ACP-121 US-SUPP-1). An editing capability will permit the message preparer to make corrections and changes to a message both during and after entry but prior to release. Editing will permit additions, deletions, and replacement of characters, words, and lines. Detailed requirements for MEPS are specified in 3.2.2. MEPS will validate the applicable portions of the DD 173 entries and if correct will perform format conversion to either JANAP 128 or DOI 103.

3.1.5.1.3 Future IAS Services

The IOC I-S/A AMPE is to be designed and implemented so new functions & capabilities can be incrementally added within the basic IOC I-S/A AMPE without requiring major modifications to the existing hardware or software. Improved Message Profiling and Retrieval, Message Processing Workload

Sharing, Informal Message Service (IMS), Teleconferencing Service (TCS) and Data Base Transaction Service (DBT) are candidate services which might be added to the I-S/A AMPE in the future. (See section 3.12 for P^{3}I).

3.1.5.1.4 Virtual Connection Service (VCS)

VCS provides the basic transport capability of the DDN to the I-S/A AMPE via the protocol structure (i.e., the set of protocols from TCP through and including the DDN interface). At IOC the VCS shall provide the reliable movement of packets from I-S/A AMPE FMS to I-S/A AMPE FMS and from terminals connected to other IAS elements (e.g., multilevel secure Terminal Access Controller) to the FMS of an I-S/A AMPE. VCS is to be used by all other services in the IAS to obtain DDN long haul trunking.

3.1.5.2 I-S/A AMPE Interfaces

The IOC I-S/A AMPE is to implement a standard set of interfaces and protocols to communicate with standard subscriber terminals and the IAS network. In order to meet specific subscriber requirements, variations to these standard interfaces will also be accommodated. The details of these interfaces are specified in the Interface Control Document (ICD), paragraphs 4.2.2 and 5.1.2. Additional interfaces may be added post-IOC as new requirements are validated.

3.1.5.3 I-S/A AMPE Data Path Control

The I-S/A AMPE provides services to its subscribers via the establishment of data flow paths. The I-S/A AMPE establishes data flow paths between subscribers, between subscribers and services, and between services. The service management function of the I-S/A AMPE, see paragraph 3.2.3, controls the establishment, use and termination of these data flow paths. The data flow paths the I-S/A AMPE shall support are described below. The following definitions apply:

User: An I-S/A AMPE user is any organization or activity that obtains service from the I-S/A AMPE. A user may obtain this service by use of its own equipment connected to the I-S/A AMPE or by obtaining "over-the-counter" service from a telecommunications center.

Subscriber: An I-S/A AMPE subscriber is an IAS "user" that uses its own equipment homed to an IAS element. The term "subscriber " means either a terminal with its associated operator or a host. Subscribers are further catagorized as local subscribers and remote subscribers. A local subscribers circuit terminates on the I-S/A AMPE. A remote subscriber's circuit terminates on another IAS element (e.g., TAC), and the remote subscriber accesses the I-S/A AMPE through the network to obtain service.

Terminal: An IAS terminal is a piece of subscriber equipment capable of handling only one logical channel at a time to the IAS.

Host: An IAS Host is a piece of subscriber equipment connected to the IAS backbone, the DDN, and is capable of simultaneously processing multiple logical connections to the IAS.

3.1.5.3.1 Data Flow Paths

There are four distinct basic paths for data to flow between the I-S/A AMPE, its subscribers, and the IAS network. These data paths are described below and specified in paragraph 3.2.3.1. The security related attributes are prescribed in Section 3.4.

3.1.5.3.1.1 Local Subscriber to Local Service

The local subscriber to local service data flow path allows subscribers directly connected to an I-S/A AMPE to access the service functions available within that I-S/A AMPE. For the IOC I-S/A AMPE these services are the Formal Message Service (FMS) and Message Editing and Preparation Service (MEPS). However, additional services will be provided in the Far-Term (See FRD 3.1.5.1). Thus, the design and implementation of the IOC I-S/A AMPE (specifically in the service management function area) shall permit data flow paths to additional services.

3.1.5.3.1.2 Local Subscriber to Local Subscriber

The local subscriber to local subscriber data flow path allows a subscriber directly connected to an I-S/A AMPE to access another directly connected subscriber. This capability will be offered post IOC, however, the design and implementation of the IOC I-S/A AMPE shall permit this data flow to be implemented later.

3.1.5.3.1.3 Local Subscriber to Network

The local subscriber to network data flow path allows a subscriber directly connected to an I-S/A AMPE to access the network and vice-versa. The capability for local Subscriber to the DDN to be implemented later shall be included in the IOC design and implementation.

3.1.5.3.1.4 Service to Service via the DDN

A local service in the I-S/A AMPE shall have the ability to establish a data flow path to a service or process located in a remote host(s) of the DDN, e.g., another I-S/A AMPE. Specifically, the IOC I-S/A AMPE FMS will require a data flow path to the FMSs located throughout the IAS network in order to pass message traffic. Post IOC when other services are resident in the I-S/A AMPE the design and implementation shall ensure their ability to use VCS to transit the DDN.

3.1.5.3.2 Access Control

The I-S/A AMPE shall maintain positive access control on behalf of all subscribers it serves. Access control is accomplished as described in the following paragraphs and in Section 3.4.

3.1.5.3.3 Physical Line Security Validation

The I-S/A AMPE is to monitor the security levels of the traffic on all access lines. All transactions received or transmitted on an access line must be validated to assure they do not exceed the security level of the line.

3.1.5.3.4 Subscriber Identification Validation

The I-S/A AMPE is to assure positive identification of all subscribers (terminals and hosts) accessing the I-S/A AMPE. The security level requested by a subscriber shall be validated against a pre-determined, maximum authorized security level for that subscriber to ensure the maximum has not been exceeded. Security requirements are prescribed in Section 3.4.

3.1.5.3.5 Data Path Requests

Each validated subscriber or service requesting data paths in the I-S/A AMPE shall require further validation to access either a subscriber directly connected to the I-S/A AMPE, a service provided by the I-S/A AMPE (e.g., Formal Message Service), or a remote network element located elsewhere in the IAS network (e.g., a TAC, another I-S/A AMPE, or a subscriber Host). The types of services and data paths a subscriber or entry service is authorized to request shall be predefined by a table (classmark) and the I-S/A AMPE shall verify that the subscriber request is authorized prior to granting access. Security requirements are prescribed in Section 3.4.

3.1.5.3.5.1 Access to a Local Subscriber

Permission for a validated subscriber or service to establish a data path to a local subscriber shall be granted if the request meets pre-established authorization criteria. As a minimum, the subscriber must satisfy criteria relating to physical line security and subscriber validation as described in 3.1.5.3.3 and 3.1.5.3.4, respectively. The capability shall also be provided to classmark subscribers as a means to limit subscriber-to-subscriber data paths to a closed user group or groups within the IAS subscriber population.

3.1.5.3.5.2 Access to a Service

Permission for a validated subscriber or service to access a service executing under control of the I-S/A AMPE shall be granted if the request meets pre-established authorization criteria. The capability shall be provided to classmark services to limit access to those services to a closed subscriber group or groups within the IAS subscriber population.

3.1.5.3.5.3 Access to a Remote Network Element

Permission for a validated subscriber or service to request a data path to an element located elsewhere in the IAS network shall be granted if the request meets pre-established authorization criteria. The capability shall be provided to classmark subscribers and services to limit remote data paths to those authorized for specific subscribers and services.

3.1.5.3.6 Data Path Error Processing

Unauthorized requests for data paths shall be reported as they occur to the I-S/A AMPE operator position for resolution. Security breaches or attempted security breaches detected by the I-S/A AMPE shall cause immediate interruption or termination of traffic on the affected data path. Traffic exchange on unaffected data paths shall continue uninterrupted.

3.1.5.4 Message Validation

The I-S/A AMPE is the replacement for ASCs and Service/Agency AMPEs. The I-S/A AMPE will process messages in the formats that are currently in use to permit a smooth transition for subscriber terminals as these terminals are cut over from the ASCs and Service/Agency AMPEs to the I-S/A AMPEs. Additional design requirements are prescribed in Section 3.4 and Section 20.0.

3.1.5.5 I-S/A AMPE Design Requirements

3.1.5.5.1 Modularity Concept

An important requirement in the design and development approach for the I-S/A AMPE is the concept of functional modularity. Functional modularity, as used here, means the grouping of all resources, (hardware and software) required to perform a function such that the resources may be added, modified or removed without affecting other functions or their interfaces. The I-S/A AMPE shall be designed and implemented using functional modularity as defined above to support the addition, modification, and deletion of I-S/A AMPE interfaces, protocols, and services.

3.1.5.5.2 Interoperability & Survivability

Interoperability can have a significant impact on survivability by providing the necessary wartime telecommunication needs even when a significant number of transmission paths and telecommunications nodal switching capabilities are destroyed. Interoperability between the DCS and publicly available communication facilities can provide immense reserve capacity and high flexibility in times of crisis or natural disasters, and can also enhance command and control functions by facilitating message exchange among organizations which currently cannot communicate directly. In order to interoperate with DCS and publicly available communications equipments and networks, the I-S/A AMPE shall incorporate all of the protocols and interfaces specified in the ICD.

3.1.5.5.3 Security

Security is of major importance in DCS networks. The I-S/A AMPE shall be designed and implemented to meet the security requirements specified in 3.4.

3.1.5.5.4 I-S/A AMPE System Objectives

The I-S/A AMPE will be one of the most important elements of the IAS. The design objectives of the I-S/A AMPE include:

- Serving as a basis for replacing existing AMPEs
- Serving as a basis for phasing out ASCs
- Interfacing the FMS and VCS Communities (Post-IOC)
- Providing flexibility for growth (in function, in throughput and in the ability to terminate customers) by expansion of its systems functions, features, and services.

In its initial configuration the I-S/A AMPE shall contain the following network functions:

- Communications Interface
  - Standard Subscriber Protocols
  - ASC and DDN interface Protocols
  - ICD identified Unique Link Protocols
- Communications Processing
  - Internet Protocol (IP)
  - Transmission Control Protocol (TCP)
  - Formal Message Protocol (FMP)
- Message Processing
  - Formal Message Service (FMS)
  - Message Editing and Preparation Service (MEPS)
- Transfer and Control
  - Service Management Function
  - Link Selection for Network Traffic
  - Link Selection for Local User Traffic
- Input/Output Internal Services
  - Traffic Management
  - Intransit Storage
  - Statistical Data Collection
  - Automatic Report Generation

The design approach adopted for the IOC I-S/A AMPE shall be sufficiently robust to permit secure incremental modular enhancement of the IAS through the addition of new functional modules and the transportability of the hardware/software modules to other implementation configurations. The specific I-S/A AMPE design shall be proposed by the contractor and may be composed of a family of computer processors, a multiprocessor, a set of microprocessors, or some combination thereof. The main requirements are the ability to meet security requirements, assurance that the software can be executed on the range of designs proposed without modification, and that all hardware and support software (e.g., compilers) be completely operational and sufficiently supported to provide for the initial deployment of the system and for future expansion.

A complete analysis of the effects and maximum limits of expanding the design (hardware and software) shall be provided. Each type of relevant component must be covered including, for example, main memory, I/O controllers, processor(s) bandwidth, local and remote terminal communication support, and number of terminals supported. Any limitations of the software to utilize the hardware (e.g., the inability of a vendor supplied operating system to utilize all the processor features) shall be identified. A complete description of the requirements for implementing additions to the I-S/A AMPE within the maximum limits shall be provided and when the addition of equipment requires the addition of other support equipment (e.g., when adding another terminal interface requires the addition of a terminal concentrator) it shall be identified. Analyses depicting the effect of expansion on performance features such as throughput and delay shall be provided.

3.2 I-S/A AMPE FUNCTIONS

3.2 I-S/A AMPE Functions

The I-S/A AMPE shall provide standard services and connection functions for subscribers located throughout the Integrated AUTODIN System (IAS). Figure 5 shows a block diagram with modules and their interconnections for illustrative purposes. Figure 5 is not binding on the contractor; however, the functional connection capabilities prescribed herein are. Message Editing and Preparation Service (MEPS) and Formal Message Service (FMS) are the standard services provided at IOC by all I-S/A AMPEs. The connection functions provide the interconnection between subscribers, services, and remote network elements and are subject to security considerations prescribed in Section 3.4 and access validation as specified herein. These connection functions include modules that implement the following protocols: DDN interface (network and link layers), IP, TCP, THP, and FMP. The control of the above functions and services is provided by the Service Management Function (See Figure 5).

3.2.1 Formal Message Service (FMS) Functions

3.2.1.1 Message Processing Overview

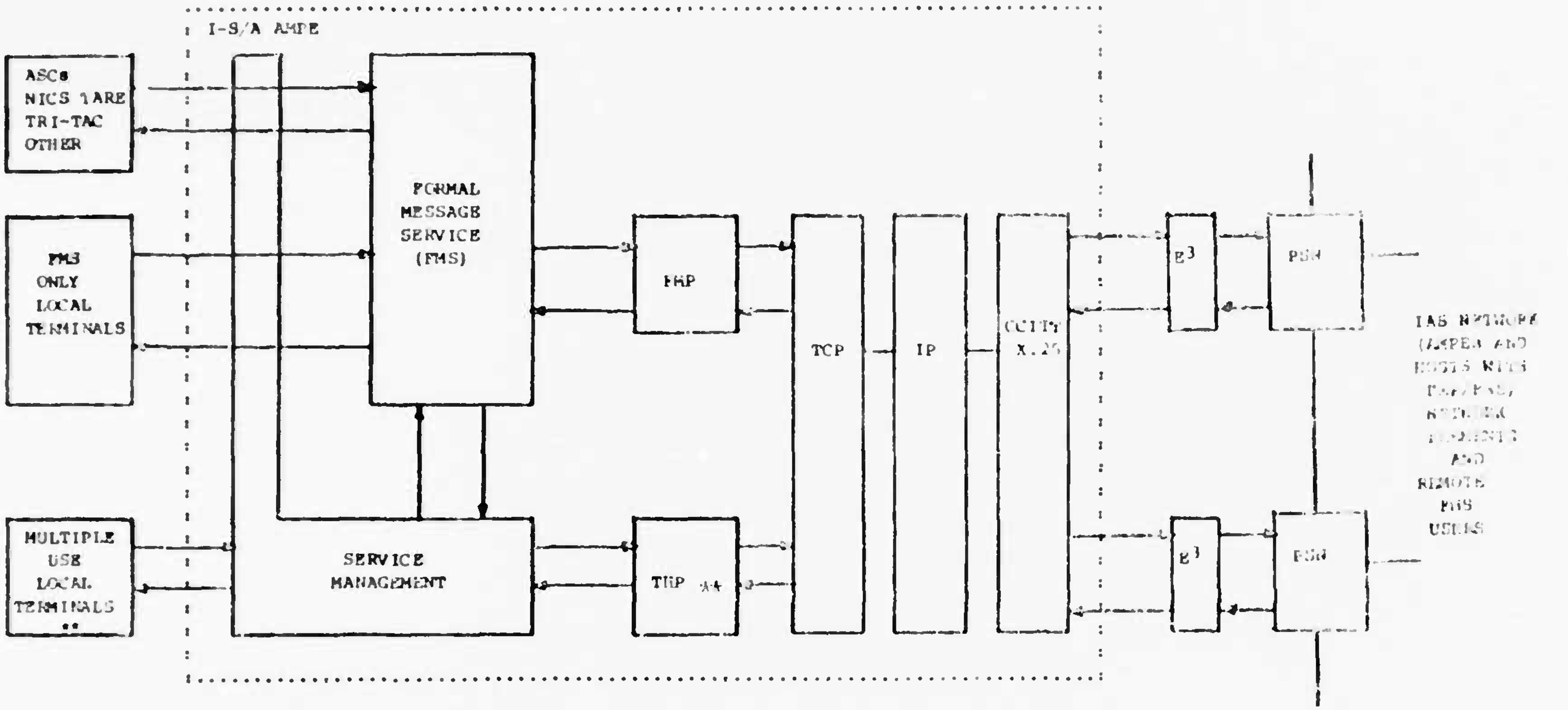
The I-S/A AMPE shall operate and process messages in accordance with ACP 121, Communications Instructions - General and the US Supp-1 thereto; DOI-103, DSSCS Operating Instructions - System/Data Procedures; JANAP 128, AUTODIN Operating Procedures; and ACP 127, Communications Instructions - Tape Relay US Supp-1 and NATO Supp-3. The FMS shall process message formats as specified in JANAP 128, ACP 127, Modified ACP 126 (NTP 4), DOI 103, abbreviated and abbreviated SI. The FMS shall support the OPINTEL Fleet Broadcast (Post-IOC, details to be provided by NSA). The processing of messages by FMS shall be as specified herein.

Once the FMS accepts a message from a subscriber or a network element as a valid message, delivery shall be guaranteed to the appropriate subscriber or network element based on the information contained in the message heading.

All DSSCS traffic that does not undergo Language Media Format (LMF) conversion shall be provided end-to-end character and bit count integrity. No technique for transmission, processing or switching shall be employed that violates this integrity. Character count integrity is required for all letters, numbers and functions in DSSCS traffic; bit count integrity is required for binary stream data traffic.

3.2.1.1.1 Input Message Processing Overview

Messages that are input to the FMS are of two categories:



** - POST-IOC REQUIREMENT

ASC - AUTODIN SWITCHING CENTER   FMP - FORMAL MESSAGE PROTOCOL   THP - TERMINAL TO HOST PROTOCOL (TELNET)

TCP - TRANSMISSION CONTROL PROTOCOL   IP - INTERNET PROTOCOL   X.25 - IAS PROTOCOL LAYERS 1, 2, & 3

NICS TARE - NATO TELEGRAPH AUTOMATIC-RELAY EQUIPMENT   TRI-TAC - TRI-SERVICE TACTICAL COMMUNICATIONS

E^3 - END-TO-END ENCRYPTION

FIGURE 5 - I-S/A AMPE FUNCTIONAL BLOCK DIAGRAM

- Originating traffic transmitted to the I-S/A AMPE by terminals.
- Network traffic transmitted to an I-S/A AMPE via the Formal Message Protocol (FMP).

Traffic from other networks interfaced in the terminal mode (e.g., the AUTODIN, NICS TARE and TRI-TAC Networks) shall be categorized as originating or terminal traffic. The only traffic that shall be considered network traffic is the traffic received from other I-S/A AMPEs via the FMP.

All categories of input messages shall be subjected to validation of the required format (See Section 3.2.1.2). The heading of all traffic shall also be checked to verify that the message has not been transmitted previously and looped back.

3.2.1.1.2 Control and Routing Overview

Throughout the message processing cycle, messages shall be processed by precedence and on a first-in-first-out (FIFO) basis within precedence except as specified in 3.2.1.5.1.

All messages shall be subject to routing determination. There are two levels of message routing within the I-S/A AMPE. A determination is made as to whether the addressees are served by the I-S/A AMPE or not. Messages destined for addressees served by the I-S/A AMPE are categorized as terminating traffic and are subject to further delivery (output to subscriber terminal) and distribution (messages annotated with distribution list for manual distriution to users) processing. Messages for addressees not served by the source I-S/A AMPE shall be categorized as messages that need to be output to the IAS network. These network outgoing messages shall be routed to the appropriate I-S/A AMPE(s).

The I-S/A AMPE operator shall be provided the status of traffic flowing through the I-S/A AMPE. The operator shall have the capability to control the flow of traffic via intercept and alternate routing methods (See Sections 3.3 and 3.2.1.5).

3.2.1.1.3 Output Message Processing Overview

Output messages consist of terminating traffic and network outgoing traffic. Terminating traffic shall be subject to distribution and delivery processing. The distribution (see Section 3.2.1.4.2.1) and delivery (see Section 3.2.1.4.2.2) process shall determine whether any users served by the I-S/A AMPE should receive the message in addition to the formal addressees of the message. The distribution and number of copies for each served addressee shall also be determined. Format and code conversion shall be provided for terminating traffic as required (See ICD 4.4). Network outgoing messages shall be routed to the appropriate I-S/A AMPE.

3.2.1.2 Input Message Processing

Each message received by the FMS shall be subject to a set of input processing functions comprising message and format identification, subscriber verification, message validation, and security validation, as well as any associated error processing. Specific actions of the FMS regarding input processing of messages shall depend on a combination of factors including, but not limited to:

- Message format
- Input line or circuit
- Characteristics of transmitting terminal
- Community of interest of the received message (i.e., GENSER/ DSSCS)
- Severity of detected errors.

The remainder of this overview describes the broad requirements and purpose of message and format identification, message validation, and security validation processing of messages input to the FMS. Subsequent sections describe those aspects of input message processing common to all input traffic, those aspects of input message processing unique to terminal traffic, and those aspects of input message processing unique to network traffic.

3.2.1.2.1 Input Message Processing (General)

Aspects of input message processing common to both terminal and network traffic are discussed below.

3.2.1.2.1.1 Message and Format Identification

The FMS shall analyze all incoming traffic to identify the boundaries of all received messages. This shall include identification of message delimiters, for example, start-of-message (SOM) and end-of-message (EOM) sequence. The FMS shall also identify and analyze, for each message, any format lines required to properly identify the message format or community of interest.

3.2.1.2.1.1.1 Acceptable Formats

The I-S/A AMPE shall be capable of identifying and accepting for processing a variety of message types, each with its own characteristics. These shall include:

- JANAP 128
- ACP 127
- Modified ACP 126 (NTP 4)
- DD Form 173
- DOI-103 CRITIC
- DOI-103
- DOI-103 Special
- Abbreviated SI
- Abbreviated

Terminal traffic may be received in any of the above formats, while network traffic will be constrained to a subset of the listed formats (e.g. - ACP-126, Abbreviated SI, etc. are processed into network formats such as JANAP 128 and DOI-103 prior to delivery or transmission to the network).

Message formats are described in terms of Format Lines (FL), which are numbered. The FL numbers used herein are those used for describing JANAP 128, ACP 127, and all DOI 103 formats. Details of all the above formats are described in their respective controlling documents (See ICD 4.3).

3.2.1.2.1.1.2 Message Integrity

The I-S/A AMPE shall perform checks to ensure that messages being received and transmitted are complete entities capable of being processed and that no messages are lost.

The I-S/A AMPE shall perform straggler and interlace checking on all incoming subscriber messages. Any message failing the straggler and interlace check shall be rejected and the subscriber shall be notified. A straggler message is one which either trails or is attached to a preceding message. An interlaced message is one in which the content of two or more messages have been intermixed. I-S/A AMPE straggler processing shall conform to JANAP 128, paragraphs 315 and 316; DOI-103, paragraphs 530 and 534; and DOD C-5030-58-M, Chapter 3, paragraph 3f(5).

The I-S/A AMPE shall also perform SOM-SOM (without intervening EOM); EOM-EOM (without intervening SOM), and Channel Designator (CD) and Sequence Number (SN) (where appropriate) continuity checks. These checks are intended to detect conditions where one or more messages or portions thereof either have been lost or may have been lost (See DOD C-5030-58-M, Chapter 4, paragraph 8).

Further the I-S/A AMPE shall protect against the interleaving of portions of two or more messages in the process of outputting messages. Related security requirements are further described in Section 3.4.

3.2.1.2.1.2 Message Validation

The I-S/A AMPE shall perform message format validation in accordance with Section 20.0, I-S/A AMPE Message Format Validation, of this document and as specified herein. Tables 3.2.1.2.1.2-1 and -2 specifically identify the procedures and format rules by reference document and paragraph in use by subscribers entering messages into AUTODIN. The I-S/A AMPE shall validate each message to assure that the heading, text, and ending are in accordance with the specified referenced paragraphs of Tables 3.2.1.2.1.2-1 and -2. In interpreting the reference paragraphs, the I-S/A AMPE shall take on the mission and functions of the type items it replaces. That is, any action required by an ASC, a Service/Agency AMPE or an Automatic Relay shall be accomplished by the I-S/A AMPE. For example: Table 3.2.1.2.1.2-1 JANAP 128/DOI 103 Message Processing Requirements, Format Line 15, EOM Validation Number refers to Paragraph 315, 316, and 404 of JANAP-128 for narrative messages. Paragraph 315 addresses Straggler Messages and Subparagraph e therein states: "ASCs detecting a suspected straggler message will notify the input station by service message..."; therefore, the I-S/A AMPE shall, upon detecting a suspected straggler message, notify the input station by service message.... The I-S/A AMPE shall process CRITIC messages and validate that they are in accordance with paragraphs 201-204 of DOI-103. Reference 2.5.a, paragraphs 302 through 306 and 310, describe how input message processing requirements are implemented in ASCs and may be used as a guide.

3.2.1.2.1.3 Security Validation

The I-S/A AMPE shall validate the security classification and special handling instructions of all input messages and shall assure the security of each message throughout all phases of message processing. DSSCS messages shall be subjected to the security validation procedures specified in DoD Manual C-5030-58.M, Chapter 3, paragraph 3f(6). The message security shall be compared against the security level of the particular connection. Security error processing shall be initiated whenever a message security classification and/or special handling designators (SHD) and/or transmission control codes (TCC) exceed that of the connection. Further security requirements are contained in Section 3.4. and Section 20.0.

3.2.1.2.1.4 Error Processing

FMS reaction to errors detected during message and format identification, message validation, or security validation of input messages will depend on the severity of the error. In general, errored messages shall be rejected by the I-S/A AMPE and appropriate system generated notifications shall be communicated to I-S/A AMPE operating personnel and to the message originator. The errors for which a system generated message shall be produced are specified in 3.2.1.5.8.1. Further details of error processing procedures are listed in Section 20.0.

3.2.1.2.2 Input Message Processing (Terminal)

The FMS shall be capable of accepting formal message traffic from peripheral terminal devices, directly connected terminals, and, as a possible P^3I initiative, remote terminals selectively "homed" to the FMS through the DDN. The I-S/A AMPE shall also accept messages from and transmit messages to the ASCs, TRI-TAC, NATO and Allied Countries in a terminal mode. That is, the I-S/A AMPE shall treat these network interfaces as terminals whether they are in fact an automated processor of a network or a simple terminal. The remainder of this section describes those aspects of input message processing unique to input traffic from terminals.

Table 3.2.1.2.1.2-1 JANAP 128/DOI 103 MESSAGE PROCESSING REQUIREMENTS

FORMAT LINE	CONTENTS		ELEMENTS	JANAP 128 REFERENCE PARAGRAPHS		DOI 103	OTHER REFERENCES	COMMENTS NOTES
				NARRATIVE	DATA PATTERN			
1	TRANSMISSION IDENTIFICATION & PILOTS		TI LINE	403, 334 464, 469		303, 130 306, 313 509, 604	(A) 302	
			PILOTS	302, 328	302, 328 504, 542	313, 332 513		(1)
2	HEADER		ALL	412-426	520-537	306, 311 337		
	FL 2 POSITION	1	PRECEDENCE	413	521	308, 313 337	(C) 328	
		2-3	LMF	414 ANNEX A	522, 503 640 ANNEX A	313, 325 347, 337 ANNEX A	(A) 304.1.b	(3) HIGH PRECEDENCE
		4	CLASSIFICATION	415	523	313, 337		
		5-8	CIC	416 ANNEX B	524, 615 ANNEX B	313, 531 337 ANNEX B		(2) JOAC, DOCK, DOAA & DOOR placed at front of FLASH Queue
		9	SEPARATOR	417	525	313, 337		
		10-16	OSRI	418	526	313, 337		
		17-20	OSSN	419	527	313, 304 548, 549 337		(3) HIGH PRECEDENCE

Table 3.2.1.2.1.2-1 JANAP 128/DOI 103 MESSAGE PROCESSING REQUIREMENTS

FORMAT LINE	CONTENTS		ELEMENTS	JANAP 128 REFERENCE PARAGRAPHS		DOI 103	OTHER REFERENCES	COMMENTS NOTES
				NARRATIVE	DATA PATTERN			
2	HEADER (Con't.)							
	FL 2 POSITION	21	SEPARATOR	420	528	313, 337		
		22-28	TOF	421,422	529,530	120, 313, 337		
			SEPARATOR	NOT USED	531	337		
			RECORD COUNT	NOT USED	532,610	332, 337, 347		
			SECURITY SENTINEL	423	503,533	313, 337		
			CLASSIFICATION REDUNDANCY	423 701-705	503,533	124, 308 313, 337	(A) 304.1.1.	
			START OF ROUTING SIGNAL	424	534	313, 337		
			ROUTING INDICATORS	331,424	331,534	301, 313 317	(D) Ch. 9 Para. 3	
			END OF ROUTING SIGNAL	425	535	313, 337		

Table [illegible] JANAP 128/DOI 103 MESSAGE PROCESSING REQUIREMENTS

FORMAT LINE	CONTENTS	ELEMENTS	JANAP 128 REFERENCE PARAGRAPHS		DOI 103	OTHER REFERENCES	COMMENTS NOTES
			NARRATIVE	DATA PATTERN			
3	CALLING STATION AND FILING TIME	DE OSRI, OSSN TOF	ANNEX C		NOT USED	(C) 114.1 & Appendix B	NOT USED IN JANAP 128/DOI 103 ORIGINATED MESSAGES. WILL BE RECEIVED IN MESSAGES ORIGINATED IN ACP 127/DOI-103 SPECIAL FORMAT
4	TRANSMISSION INSTRUCTIONS	SECURITY WARNING, CLASSIFICATION,	405,407 409,411 310, 314 701-705	405,407 409,411 310, 314 701-705	124,140 307,308 313,531	(A) 304.3.d	
		PROSIGN T, OTHER OPERATING SIGNALS	318 425	318 425			
5	PREAMBLE	PRECEDENCE DTG OPERATING SIGNALS	ANNEX C	ANNEX C	313,531 513		
6	ADDRESS	ORIGINATOR	ANNEX C	ANNEX C 505	313,402		
7		ACTION ADDRESSEE(S)	ANNEX C 406,408 409	ANNEX C 505,406 408,409	313,402 404	(B) ANNEX C	
8		INFORMATION ADDRESSEE(S)	ANNEX C 406,408 409	ANNEX C 406,408 409	313,402		
9		EXEMPT ADDRESSEE(S)	ANNEX C 409	ANNEX C 409	NOT USED	(B) ANNEX F Para.4.d.1	
10	PREFIX	ACCOUNTING SYMBOL	449 ANNEX C APP. I	449 ANNEX C APP. I	313		

Table 3.2.1.2.1.2-1 JANAP 128/DOI 103 MESSAGE PROCESSING REQUIREMENTS

FORMAT LINE	CONTENTS	ELEMENTS	JANAP 128 REFERENCE PARAGRAPHS		DOI 103	OTHER REFERENCES	COMMENTS NOTES
			NARRATIVE	DATA PATTERN			
10	PREFIX (Con't.)	GROUP COUNT	402		313		
11	SEPARATION	PROSIGN	ANNEX C	ANNEX C	313		
12	TEXT	CLASSIFICATION	111, 111	111	313		
		TEXT	401, 402	501, 503 506, 510 601-624	313, 328 331, 346		NTTS – SPECIAL DATA PATTERN MESSAGE – SEE CHAPTER 6, JANAP 128.
13	SEPARATION	PROSIGN	ANNEX C	ANNEX C	NOT USED		
14	PROCEDURE	CONFIRMATION			NOT USED		NOT USED IN AUTODIN AND TAPE RELAY OPERATIONS
15		CORRECTION	ANNEX C		111		NOT USED IN DATA PATTERN MESSAGES
		EOM VALIDATION NUMBER	315, 316 404		305, 313 530	(E) Ch. 2, Para. 6.d. (6)	
16		EOM	404, 427		119, 305 313		
		EOT		404, 538 539, 610 502	119, 331 338-341 347, 530		

REFERENCES

(A) DCA B652 Draft AUTODIN I System Functional Specification, August 1982

(B) ACP-121 US SUPP-1

(C) ACP-127 US SUPP-1

(D) DCAC 370-D175-1, DCS AUTODIN Interface and Control Criteria

(E) DCAC 370-D95-1, System Description - DCS AUTODIN

NOTES

(1) Pilots indicating that a message is a suspected duplicate, see JANAP-128 paragraphs 328 and 547, shall be stripped by the destination I-S/A AMPE prior to delivering the message to subscribers that are appropriately classmarked, for example; all GSA subscribers.

(2) Flash message with a CIC of DGGC, DGGE, NGGC, or JGGC are not processed FIFO but are placed at the front of the FLASH Queue.

(3) On high precedence messages (flash and above), messages shall not be rejected if only this field is invalid; messages shall be forwarded to addressee and originator shall be serviced advising of invalid field and that message was forwarded.

Table 3.2.1.2.1.2-2 ACP 127/DOI 103 SPECIAL, MESSAGE PROCESSING REQUIREMENTS

ORMAT LINE	CONTENTS	ELEMENTS	ACP 127 REFERENCE PARAGRAPHS		DOI 103	OTHER REFERENCES	COMMENTS - NOTES
			BASIC AND U.S. SUPP-1	② NATO SUPP-3			
1	Handling Instructions	Transmission Identification	103, 131, 202, 203, 402, 412, 413, 147, 429-433 436	136, 137, 138, 202, 403, 412, 413, 414, 430, 432, 433	007.a. (1) 045 ①		① All paragraphs below 100 refer to paragraphs in Supplement 1 to DOI 103, SPECIAL FORMAT ② See Appendix B to ACP-127 NATO SUPP-3 for additional requirements
		Pilots	135, 305, 425-427	129, 145, 426, 427	007.a. (1) 040		
2	Called Station(s)	Precedence	150-152, 407, 304, 420	161, 162, 163, 207, 420	007.a. (2)		
		Routing Indicators	204, 206, 207, 303, 406, 147	205, 303, 305, 306	007.a. (2) 150		
3	Calling Station and TOF	OSRI	147		007.a. (3) 019		
		OSSN	129, 434, 147, 203	139	007.a. (3)		
		TOF	115, 138, 147		007.a. (3)		
4	Transmission Instructions	Security Warning	124, 138, 203, 212	133, 203			
				204, 401, 406			

Table 3.2.1.2.1.2-2 ACP 127/DOI 103 SPECIAL, MESSAGE PROCESSING REQUIREMENTS

FORMAT LINE	CONTENTS	ELEMENTS	ACP 127 REFERENCE PARAGRAPHS		DOI 103	OTHER REFERENCES	COMMENTS NOTES
			BASIC AND U.S. SUPP-1	NATO SUPP-3			
4	Transmission Instructions (continued)	PROSIGN T, other operating signals	203, 205-207 222,507, 508		029,034, 035,038, 124,140 307,308 313,531		
5	Preamble	Precedence	150-152		313		
		Date-Time Group	113		313		
		Message Instructions	206,438		014,023, 039,313, 511,531		
6	Address	Originator	205		313,402		
7		Action Addressee(s)	205,502, 503,507, 222,508	206	012,013 313,402, 104,158		
8		Information Addressee(s)	205,206		313,402, 404		
9		Exempted	205,205		Not Used		
10	Prefix	Accounting Symbol	509-511 App. 1 to Annex B		113		
		Group Count	208		313		

Table 3.2.1.2.1.2-2 ACP 127/DOI 103 SPECIAL MESSAGE PROCESSING REQUIREMENTS

FORMAT LINE	CONTENTS	ELEMENTS	ACP 127 REFERENCE PARAGRAPHS		DOI 103	OTHER REFERENCES	COMMENTS NOTES
			BASIC AND U.S. SUPP.1	NATO SUPP.3			
11	Separation	PROSIGN	Annex B		313		
12	Text	Classification	209,402 403,405 212	403	313		
		Internal Instructions	405	101	015,019 023,313 328		
		Text	138,208 210,415	143,209	015,019 023,313 328		
13	Separation	PROSIGN	Annex B		Not Used		
14	Ending	Confirmation	Annex B	212	Not Used		
15		Correction	211		313		
		EOM Validation Number	114,203 405	119	014,305 313,530		
16		End of Message Functions	114,203 405	118,119, 423,424	119,305 313		

3.2.1.2.2.1 Message and Format Identification

For input traffic the FMS shall be capable of accepting, identifying, and validating and verifying all message formats introduced in 3.2.1.2.1.1.

3.2.1.2.2.2 Message Validation

All input traffic shall be subject to the message validation requirements specified in 3.2.1.2.1.2.

3.2.1.2.2.3 Security Validation

The FMS shall perform security validation processing on all input traffic in accordance with the objectives stated in 3.2.1.2.1.3. When required, each logical terminal connection via the IAS network shall be subjected to the same level of security processing as terminals directly connected to an I-S/A AMPE.

3.2.1.2.2.4 Error Processing

FMS response to errors detected in terminal input traffic during message and format identification, message validation or security validation processing shall be governed by all the factors introduced in 3.2.1.2 (message format, input circuit, terminal characteristics, community of interest, and error severity) in conjunction with system settable parameters. Messages containing errors described in 3.2.1.2.1.2 above shall be displayed at an I-S/A AMPE service position. All detected errors existing in the message shall be indicated on the display. The I-S/A AMPE shall process detected errors in accordance with Section 20. If the message is rejected, the I-S/A AMPE shall automatically generate a service message to the originator. CRITIC messages with errors shall be forwarded, and the originator shall be serviced at the Flash precedence level.

On a line selectable basis, based on predesignated parameters, messages failing format or header validation shall be automatically rejected, in which case the FMS shall automatically generate a service message to the originating station. Any automatically generated service message shall be of the same precedence as the rejected message except CRITIC and ECP which shall be of FLASH precedence. Messages with invalid precedence characters shall receive an automatically generated service message with a precedence of Immediate.

Processing of errored messages detected during security validation shall be selectable on a line by line basis at the I-S/A AMPE. Two options shall be available for use on controlled and uncontrolled lines. On uncontrolled lines, the I-S/A AMPE shall receive the complete message in which the error was detected but not process the message for delivery to the addressees indicated on the message. The I-S/A AMPE shall automatically notify the originating terminal of the error. On controlled lines, the I-S/A AMPE shall automatically reject the errored message and provide notification of the error. Messages or partial messages with security errors shall be retained on history files until purge date.

3.2.1.2.2.5 Message Editing and Preparation Service (MEPS)

Message Editing and Preparation Service (MEPS) shall be available to all FMS users whose traffic is not initially entered already in one of the following final formats: JANAP 128, ACP 127, DOI-103, or DOI-103 Special. The output of MEPS shall be a complete and correct message in either JANAP 128 for GENSER or DOI-103 for DSSCS. All Plain Language Address (PLA) to Routing Indicator (RI) assignment shall be accomplished by MEPS portion of FMS (MEPS is a subset or module of FMS). All MEPS requirements are prescribed in 3.2.2, except PLA to RI Assignment prescribed in 3.2.1.2.2.6.

3.2.1.2.2.6 Plain Language Address (PLA) to Routing Indicator (RI) Assignment

The FMS shall process all originating traffic to perform plain language address-to-routing indicator assignment when required.

3.2.1.2.2.6.1 Formulation of Plain Language Addresses

PLAs are formulated as follows:

a. A PLA will consist of an activity and geographical location (city, base, camp, etc., and the state and country), except as noted in 3.2.1.2.2.6.2.

(1) Activity Title: An activity is a unit, organization or installation performing a function or mission. The activity title can be abbreviated in the PLA. The abbreviations and acronyms used in the PLAs are contained in the PLA Directory of the appropriate service or agency.

(2) Geographical Location:

(a) Cities will be spelled out as they appear in the "International List of Post Offices", (Reference 2.5.j). See 3.2.1.2.2.6.2 for exceptions.

(b) Base, camp, station, etc., will be abbreviated, e.g., AFB for Air Force Base, CP for Camp, FT for Fort.

(c) The two letter state and country abbreviations as authorized in Annex C of ACP 198 US SUPP-1( ) will be used when geographical locations are required.

b. A PLA will not exceed 55 characters, including spaces. Office codes/symbols and parentheticals appended to a PLA are not considered a part of the PLA. Commercial addresses are exempt from the 55 character limitation. The only punctuation authorized in PLAs are the hyphen (-) and decimal point (.).

3.2.1.2.2.6.2 Use of Plain Language Addresses

a. The PLAs contained in the appropriate service or agency Plain Language Address Directory are the only PLAs authorized for use in message addressing for activities listed. Deviations in spelling, spacing, or formatting are not authorized and shall either be corrected if possible by the I-S/A AMPE operator or rejected back to the originator.

b. If an activity to be addressed is not contained in any PLA directory, the message with only that addressee shall be sent to the service position of the I-S/A AMPE. The addressee's title and geographic location will be included in lieu of a PLA, except in the DSSCS community. An I-S/A AMPE operator will make a determination as to the further electrical processing of the message thus ensuring protection to all addressees.

c. DSSCS, Mobile and afloat commands are exempt from using geographical locations on their PLAs.

d. Activities which move to an Emergency Relocation Site (ERS) during emergency situations and activities which for security reasons - a tactical consideration, are not associated with a specific location are exempt from using geographical locations in their PLAs.

e. The FMS shall provide the capability to assign RIs to all valid PLAs, including Address Indicator Groups (AIG) (See ACP 100), Collective Address Designator (CAD) (See NTP 3 Supp-1), Task/Type organizations (See ACP 112), general message titles (See ACP 121 US SUPP-1), DSSCS Address Groups (DAG) (See DOI-101), and product distributions (See NSA Document USSID 307 SIGINT Product Distribution). If a PLA is not contained in the data base the message shall be referred to an I-S/A AMPE routing management position for manual lookup and routing assignment. PLAs on a given message are either all GENSER community or all DSSCS community PLAs, and DSSCS and GENSER PLAs shall not be mixed in the same message. A single PLA can, however, correspond to both a GENSER and a DSSCS RI. Such a PLA is termed a "duplicated PLA." When processing a duplicated PLA from an R/Y capable channel, the I-S/A AMPE shall check the other PLAs of the message and process the message as a DSSCS message if any DSSCS-only PLAs are present. If the message contains only duplicated PLAs, the message shall be processed as a DSSCS message if the caveats in format line 12 so dictate (see DOI-103). If caveats are not present, the message shall be handled as a DSSCS message. DSSCS processing includes the assignment of a "Y-community" RI rather than an "R-community" RI. The I-S/A AMPE shall prevent routing a message to a local addressee not cleared for the security level of the message by crosschecking the classification and special handling instructions of the message with the authorized security level of the addressee.

3.2.1.2.2.6.3 Automated PLA Directory Maintenance

The I-S/A AMPE operator shall be able to make on-line update entries in the Plain Language Address Directory file.

3.2.1.2.2.5.4 PLA Directory Files

The PLA directory files shall be in standard format and contain only PLA entries from directories listed in paragraph 3.2.1.2.2.6.6.

3.2.1.2.2.6.5 File Maintenance

The PLA directory files require the capability to be constructed, added to, deleted from and otherwise modified in an on-line environment. Provisions shall be available to introduce these updates into the system either for immediate on-line modifications or batched. Update parameters may be provided within specially formatted text. An update audit file shall be maintained at each site to record all pertinent data (e.g., Time of Receipt for each update, Actual Time of Site Update, etc.). The data base maintenance procedures shall not have an adverse effect on system performance (e.g., degrading message throughput) and shall consider site unique attributes (e.g., peak traffic times, number of subscribers, etc.). Local PLA data base updates will be the responsibility of the I-S/A AMPE operation personnel, and therefore shall not be available to remote subscribers.

3.2.1.2.2.6.6 Data Base Sizing For PLAs

It is estimated that the maximum number of PLAs contained in the PLA directories will be seventy-five thousand at IOC, and the PLA data base shall be designed to accommodate this maximum and not to preclude expansion up to 256,000. The actual number of PLAs in each I-S/A AMPE directory will vary from site to site and will be determined by operations at each site. The following is a listing of authorized Plain Language Address Directories:

a. Army Regulation 105-32, Authorized Addresses for Electrically Transmitted Messages.

b. Naval Telecommunications Publication (NTP) 3 SUPP-1( ) Plain Language Address Directory.

c. Air Force Manual 10-4, Air Force Directory of Unclassified/Classified Addresses.

d. USMCEB Book, Joint Department of Defense Plain Language Address Directory (JDOD PLAD).

e. For information concerning DSSCS Plain Language Addresses, refer to USSID 505, USSID 309 and DIA Compartmented Address Book.

3.2.1.2.3 Input Message Processing (Network)

The I-S/A AMPE shall be capable of accepting IAS network traffic from the formal message processing service of other I-S/A AMPEs. Such traffic shall consist of messages received and processed by those network elements and then subsequently transmitted to the I-S/A AMPE for delivery.

The FMSs of any two I-S/A AMPEs shall communicate via logical connections established by the Formal Message Protocol (FMP) through the IAS network.

3.2.1.2.3.1 Message and Format Identification

Network traffic shall be passed between I-S/A AMPEs via the FMP. The FMP is to be a host-to-host protocol that contains the necessary elements to prevent shuttling or looping of messages, provides a means for efficient transmission of single and multiple addressed messages throughout the IAS network, and indicates the format and character set in which each message was originated.

3.2.1.2.3.2 Message Validation

The FMS shall perform message validation on all messages received from the other I-S/A AMPEs. The validation process shall be as specified by the requirements of paragraph 3.2.1.2.1.2.

3.2.1.2.3.3 Security Validation

The FMS shall perform security validation processing on all messages received from other I-S/A AMPEs. The validation process shall be as specified by the requirements of paragraph 3.2.1.2.1.3. All logical connections between I-S/A AMPEs shall be subjected to security validation.

3.2.1.2.3.4 Error Processing

The I-S/A AMPE shall have an error processing scheme for message traffic received from other I-S/A AMPEs that is consistent with paragraph 3.2.1.2.1.4. The objective shall be to automatically reject to the originator for correction any errored messages received from other message processing systems, with the exception that CRITIC shall not receive any message validation beyond WW YEKAAH and is not rejected. Other high precedence traffic (FLASH and ECP) shall be delivered if at all possible; if not, it shall be brought to the immediate attention of an I-S/A AMPE operator position for the resolution of errors.

3.2.1.2.3.5 Looping Protection

The I-S/A AMPE shall protect against the looping of message traffic.

PREVIOUS PAGE
IS BLANK

The I-S/A AMPE shall contain a looping protection scheme which encompass all the I-S/A AMPEs of the IAS. The scheme is to protect against all potential looping contingencies that might result from a richly connected IAS network. The maximum number of nodes to be considered shall be 256 nodes. The I-S/A AMPE shall have the capability to notify the operator upon receipt (from any channel) of a message that has been previously delivered to the same output destination(s). As a minimum, the operator notification shall contain identification of the message input and output channels and message destination delivery information (Routing Indicators, PLA, etc.).

3.2.1.3 Routing

Routing, as prescribed herein, applies to the routing determination for a single copy of a message to each intended recipient of the message. Subsequent distribution and multiple deliveries that can be made locally by the I-S/A AMPE are a user service prescribed in 3.2.1.4.2, Terminating Message Processing.

3.2.1.3.1 Routing Parameters

Formal routing determination shall be based on the routing indicators of the addressees. The I-S/A AMPE shall prevent misrouting and mislabeling as specified in DOD C-5030.58M, Chapter 2, para 8 and 10 and JANAP 128 ( ). Messages received by the I-S/A AMPE routed and addressed to R---SCC will automatically have routing look-up performed for the R---SCC addresses. The I-S/A AMPE will automatically generate a ZOV for the R---SCC addresses.

3.2.1.3.2 Routing Determination

The I-S/A AMPE shall use a routing table to determine the destination for each message. The routing table shall contain the full routing indicator for all subscribers served by the I-S/A AMPE and four or more letter routing indicators to cover all other valid routing indicators.

3.2.1.3.3 Special Routing Considerations

Messages containing a Collective Address Designator (CAD), CRITIC messages, and multiple addressed messages shall be provided special routing considerations:

3.2.1.3.3.1 Collective Routing

CADs consist of approved General Message titles (ACP 117 CAN-US Supp-1, Section III), Address Indicator Groups (AIG - ACP 100), DSSCS Address Groups (DAG - DOI 102), and those approved titles or designators which are assigned to messages in format line seven. Each CAD will have a cognizant authority responsible for the administration of the CAD to include addition or deletion of an activity in the CAD, changes to the PLA of an activity in the CAD, changes to the activities in the CAD authorized to originate messages addressed to the CAD, and advising all concerned of any changes to the CAD. Special processing considerations shall include:

a. A unique RI, R---SUU, may be the same RI used for obtaining PLA to RI assignment (see Section 2.4, NTP 4) and for obtaining CAD to RI assignment. Messages containing a CAD received from an authorized subscriber shall have the CAD to RI assignment performed and be processed as a multiple addressed (multiple RIs in format line two) message for delivery to all RIs associated with the CAD in format lines seven and eight.

(1) Addressee RIs can be local I-S/A AMPE subscribers, remote I-S/A AMPE subscribers, or ASC subscribers.

(2) The I-S/A AMPE shall support both GENSER and DSSCS CADs. The assignment of GENSER RIs to DSSCS CADs and vice versa shall be prohibited.

(3) A CAD may contain more than five hundred routing indicators, however, for any one delivery the message shall be limited to five hundred RIs.

b. The capability for the I-S/A AMPE to classmark users (as designated by the cognizant authority through the DCA) as authorized to input a particular CAD, and the capability to recognize and reject all unauthorized inputs.

c. The capability to generate TARE instructions and to perform multiple delivery for collective routing indicators and those based upon TARE line information specified in format line 4 of JANAP 128( ) formatted messages.

d. The capability to recognize collective routing indicators (RUCR or YECR in the first four positions of the RI) received from an ASC during the transition period. These messages will contain a valid CAD in format line seven and eight and will require the same CAD to RI assignment as described in a. above with the following exceptions:

(1) The CAD to RI assignment shall result in the assignment of only RIs for the local I-S/A AMPE subscribers except as described in d.(2) below. Local implies all activities in a CAD which are serviced directly by the I-S/A AMPE in question.

(2) The assignment may include certain distant I-S/A AMPE subscriber RIs. This will only occur during the transition period in the event that the distant I-S/A AMPE is not directly connected to an ASC.

(3) The assignment shall never include ASC subscriber RIs. Since the message containing the CAD was received from an ASC, it can be assumed that delivery has been accomplished to all appropriate ASC subscribers.

e. CADs received from a distant I-S/A AMPE will already contain the addressee RIs and will require no special processing by the receiving I-S/A AMPE.

f. A capability to recognize and prohibit the multiple re-entry of a CAD by a local authorized subscriber for which delivery responsibility has been accomplished. Re-entry, when necessary, will require use of a pilot.

General Discussion: During the phase out of ASCs and the phase in of I-S/A AMPEs, CAD management will be critical in both systems to insure that all deliveries are properly accomplished and that multiple deliveries of the same message to a single subscriber are precluded.

3.2.1.3.3.2 CRITIC Routing

CRITIC messages shall be processed in accordance with Chapter 2 of DOI-103. The CRITIC Identification, WW YEKAAH, in format line 2 shall be detected on input and the message shall be routed without further validation. CRITIC acknowledgments shall be processed in accordance with Chapter 2 of DOI-103.

3.2.1.3.3.3 Multiple Addressed Messages

Multiple addressed messages, required to be transmitted to more than one I-S/A AMPE in the IAS network shall be given special consideration. The I-S/A AMPE routing methodology shall be based upon an investigation of alternate methods to route multiple addressed messages to other I-S/A AMPEs. It is possible for an I-S/A AMPE to open a separate logical connection through the DDN directly to each other I-S/A AMPE that must receive the message. For output delivery the I-S/A AMPE shall make deliveries based on the terminal receiving one (1) only, up to fifty (50), or up to five hundred (500) routing indicators per transmission at the option of the subscriber. This requirement shall be part of the per line parameters set at system initiation.

3.2.1.4 Output Message Processing

After the routing determination, messages shall be queued for output message processing as either terminating messages or as network outgoing messages, or both. Network outgoing message processing is prescribed in 3.2.1.4.1; terminating message processing is prescribed in 3.2.1.4.2.

3.2.1.4.1 Network Outgoing Message Processing

Network outgoing messages shall be queued to the Formal Message Protocol module for transmission through the IAS network (see ICD 4.2 Protocols) to other I-S/A AMPEs. Each transmission of a message to a distant I-S/A AMPE shall include only those Routing Indicators (RIs) for which the destination I-S/A AMPE has delivery responsibility.

3.2.1.4.2 Terminating Message Processing

Terminating Message Processing consists of message distribution determination, message delivery determination, security validation, and message format and code conversion as required.

3.2.1.4.2.1 Message Distribution Function

Local distribution of messages consists of locating the distribution parameters in a message (e.g., office symbol, subject identifier, content indicator code); determining the organizational units and offices which are to receive the message; determining the number of copies required for each recipient: and affixing the distribution information to the beginning of the message (See ACP 121 US SUPP-1). The I-S/A AMPE shall automatically determine distribution for originating and terminating traffic.

3.2.1.4.2.1.1 Distribution Determination Parameters

The determination of units and offices which shall receive distribution of a particular message shall be based on the following parameters:

a. Destination Station Routing Indicator (DSRI)

b. Plain Language Address (Guarded and Protected)* including AIGs, etc.

c. Office Symbol/Number

d. Content Indicator Code (CIC)

e. Identifier Code : NATO Subject Identifier (NASIS), Standard Subject Identification Code (SSIC),

f. Flagword/Keyword in first eight lines of text

g. Message references, both incoming and outgoing, (in first seven lines of text or down to first paragraph on JANAP 128)

h. Status of message recipient - Action or Info Addressee

i. Drafter Designators for local distribution

j. Source (Incoming channel - e.g., Optical Character Reader)

k. Precedence

l. Classification

m. Reference Routing

n. Originating Station Routing Indicator (OSRI)

o. Delivery Distribution Indicator (DDI)

*The term "Guard" means the I-S/A AMPE shall determine internal office distribution to specified organizations. "Protect" means the I-S/A AMPE shall provide a set number of copies to an organization, which in turn arranges for its own internal distribution.

NOTE: Office and unit determination shall not be performed for data pattern messages.

3.2.1.4.2.1.2 Distribution Determination

Each unit shall have the capability to specify any or all of the parameters in 3.2.1.4.2.1.1 that shall be used in determining distribution. These parameters represent minimum criteria and may be used individually and/or collectively to determine distribution. Additionally, each unit shall have the capability to prioritize the use of these parameters. Table 3.2.1.4.2.1.2 illustrates the use of these parameters for GENSER and DSSCS formats. Delivery Distribution Indicators (DDI) are specified in USSID 519. At IOC the I-S/A AMPE shall support the existing Service and Agency distribution schemes.

3.2.1.4.2.1.2.1 Comeback-Copies of Messages

The I-S/A AMPE shall provide the automatic capability, invoked at the I-S/A AMPE at the option of the subscriber, for either no comeback copy or for one of the following:

a. Providing to the originating subscriber a comeback copy of each originated message in the transmitted format including the unique message identifier.

b. Providing to the designated terminal position an acknowledgment, to include the date-time-group and unique message identifier, rather than a display or printed copy of the entered message.

3.2.1.4.2.1.2.2 Multiple Copy Determination

The number of copies of each message to be distributed to each unit and office shall be determined automatically, based on message subject, classification, and status (either action or info). Each unit and office shall be able to specify the number of copies that each combination of the aforenamed parameters dictates. The number of copies and the distribution shall be annotated on the first page of the copy delivered.

3.2.1.4.2.2 Message Delivery

The I-S/A AMPE shall deliver messages to local subscribers. For each message the I-S/A AMPE shall determine what deliveries are to be made, how to make each delivery, and what format is required for each delivery. The I-S/A AMPE shall automatically deliver each message to the appropriate interface, based on the parameters specified below. If the I-S/A AMPE is unable to deliver a message automatically, the message shall be sent to an operator position to allow for operator intervention.

Table 3.2.1.4.2.1.2 Distribution Criteria

CRITERIA	GENSER NARRATIVE	DSSCS NARRATIVE
PLA (Guarded)*	X	X
PLA (Protected)*	X	X
AIG	X	
Office Symbol	X	X
NASIS	X	
SSIC	X	
DDI		X
Keyword	X	X
Reference Routing	X	X
Action/Info	X	X
Drafter Designators	X	X
Source	X	X
Precedence	X	X
Classification	X	X

*NOTE: Office and unit determination shall not be performed for data pattern messages.

3.2.1.4.2.2.1 Message Delivery Parameters

The following items are used to determine the delivery destination of a message:

a. Destination Station Routing Indicator

b. Plain Language Address (Short Title)

c. Office Symbol

d. Content Indicator Code

e. Identifier Code (See 3.2.1.4.2.1.1.e)

f. Flagword/Keyword in first eight lines of format line 12

g. Source

h. Language Media Format

i. Precedence

j. Action/Info Addressee Status

k. TARE Line

l. Operating Signals

m. Classification

n. Transmission Release Codes (TRC)

o. Transmission Control Codes (TCC)

p. SPECAT Release codes (SPECAT Handling)

q. Delivery Distribution Indicator

r. Orginating Station Routing Indicator

s. Special Handling Designators (SHD)

3.2.1.4.2.2.2 Message Delivery Determination

Based on the parameters identified in paragraph 3.2.1.4.2.2.1, messages shall be electrically delivered to any or all of the following: a communications center local device, a remote terminal(s), and/or a service position. Tables 3.2.1.4.2.2.2-1 and 3.2.1.4.2.2.2-2 illustrate the

Table 3.2.1.4.2.2.2-1 Delivery Criteria for GENSER & DSSCS Narrative Messages

DELIVER TO:

CRITERIA	IAS NETWORK	LOCAL DELIVERY	SUBSCRIBER TERMINALS	ADVANCE COPY	SERVICE POSITION
Routing Indicator	X	X	X	X	X
PLA (Guarded)		X	X	X	
PLA (Protected)		X	X	X	
Office Symbol		X	X	X	
Communications Action Identifier		X	X		X
Classification		X	X	X	
Flagword/Keyword		X	X		X
Precedence		X	X	X	
Action/Info				X	
TARE Line		X	X	X	X
Operating Signal		X	X		X
Delivery Determination Indicator		X	X	X	X

NOTE: To obtain office symbol for guarded PLAs, search must be conducted on other fields (i.e., Flagword, ID code, etc.)

DEFINITIONS

Local Delivery - Position/Station within the confines of the I-S/A AMPE Telecommunication Center (e.g., printer, Video Display Terminal)

Subscriber Terminal - Hardware device located outside of the I-S/A AMPE Telecommunication Center

Service Position - Station located within the I-S/A AMPE Telecommunication Center used to correct, edit, or verify messages.

Table 3.2.1.4.2.2.2-2 Delivery Criteria for GENSER & DSSCS Data Pattern Messages

DELIVER TO:

CRITERIA	IAS NETWORK	LOCAL DELIVERY	SUBSCRIBER TERMINALS	SERVICE POSITION
Routing Indicator	X	X	X	X
Content Indicator Code	X	X	X	X
Source	X			X
Precedence		X		
Language Media Format		X		
Special Handling				X
Flagword/Keyword (TXTHDR)		X		
Security Classification	X	X	X	

combination of delivery parameters for GENSER narrative and data pattern messages, as well as DSSCS narrative and data pattern messages. These parameters represent the criteria needed to effect delivery. They may be used individually and/or collectively to determine delivery.

3.2.1.4.2.2.3 Security Validation

The I-S/A AMPE shall assure that each device is authorized (according to security level) to receive a message prior to delivery of that message to the device (See 3.2.3.2 and 3.4). Delivery of SPECAT messages shall be in accordance with paragraph 332, ACP 121, US SUPP-1(E).

3.2.1.4.2.2.4 Format Conversion

The I-S/A AMPE shall be capable of converting messages to any of the formats described in ICD paragraph 4.3. These formats shall be selectable for each input or output device or line.

3.2.1.4.2.2.5 Media Conversion

The I-S/A AMPE shall be capable of converting messages for output to card, hardcopy, paper tape (Navy requirement), magnetic tape, or any combination, for over-the-counter delivery, or electrically delivering the information to a remote device using the language media formats described in Annex A to JANAP 128(H), DOI-103 and DCAC 370-D175-1. Reference 2.5.a, Chapter 4 Section II describes format and media conversion as currently implemented in ASCs, and may be used as a guide.

3.2.1.4.2.2.6 Message Media Services

These services encompass those areas which format a message in accordance with user requirements. These capabilities shall be individually selectable by each user terminal. The I-S/A AMPE shall provide each of the following services automatically.

3.2.1.4.2.2.6.1 Distribution Identification

Each message delivered to the collocated Telecommunications Center terminal for over-the-counter delivery shall list the offices that have been identified as message recipients and the number of copies of the message they are to receive. As an operator selectable option, individual deliveries shall include only the distribution information pertinent to the users served by that delivery.

3.2.1.4.2.2.6.2 Message Identification

The following shall also appear on each page of the message: Time of receipt; Ordinal date, hours and minutes; message precedence at the top and bottom; unique message identifier; and Classification, Special Handling Designations, and Message Handling Instructions delimited by asterisks on the top and bottom center.

3.2.1.4.2.2.6.3 Editing

The I-S/A AMPE shall have the capability, selectable by channel, to strip communications information by format line (FL) beginning with FL1 running through 11 and from FL13 running through 16 from the message and to double or single space the message.

3.2.1.4.2.2.6.4 Print Expansion of Reports

The I-S/A AMPE shall have the capability to perform print expansion for Army SIDPERS reports as specified in the ICD Appendix B.

3.2.1.4.2.2.6.5 Classification Display

The I-S/A AMPE shall label all display screens with the classification of the message or data being displayed. This shall also apply to information associated with messages or data when it is displayed.

3.2.1.4.2.2.6.6 Special Print Out Requirements

Where required (determined on a site-by-site basis) the I-S/A AMPE shall print out messages in both edited and unedited format as follows: messages printed on the "Message Center" printer shall be in edited format; messages on the "Service Center" printer shall be in unedited format. Both formats have some things in common. The classification and special handling instuctions (caveats and codewords) shall be printed at the top and bottom of each page. Operating signals and content indicator codes are indicated at the top of the first page, beneath the classification. Above the classification at the bottom of the first page are printed the local distribution lines (OTC delivery, if any), a chop line indicating routing method and controlled routing for TS and SPECAT classification messages, and a control line containing UMI, input CSN, page count (_____ of _____ pages), and DTG. The remainder of each format is described below.

(1) Unedited. Unedited format consists of each line of the message printed exactly as received. No attempt shall be made to clean up the printout. In addition to the text and lines described above, the unedited format shall include any service lines generated by the processing routines. These lines shall be printed on the first page between the chop line and the control line.

(2) Edited. In edited format, message format lines 1, 2, 3, 4, 4A, 10, 11, 14, 15, 16, and any paging lines shall be deleted. The precedences shall be printed as words above format line 5. Format lines 7 through 9 shall be printed as two addressees per print line with RIs deleted, if the addressee short titles are short enough. Blank lines shall be printed between the precedence, format lines 5 through 9, format line 12, and any paragraphs.

3.2.1.4.2.2.7 Data Pattern Delivery Processing

Data Pattern messages shall be identified by destination Language Media Format (LMF) codes B, C, D or I. The I-S/A AMPE shall have the capability to either queue the data pattern traffic for subsequent delivery (e.g., retained for 72 hours) selectable by one of the parameters specified below or process for immediate delivery.

3.2.1.4.2.2.7.1 Data Pattern Delivery

The subscriber shall be able to specify that the I-S/A AMPE will select bulk data pattern traffic via the following parameters:

a. Routing Indicator (RI)

b. Language Media Format (LMF)

c. Content Indicator Code (CIC)

d. Text Header (TXTHDR)

e. Classification

Any mix of card punch, magnetic media and line printer shall be able to be specified for the output device(s).

3.2.1.4.2.2.7.2 Data Pattern Sections

The I-S/A AMPE shall provide four options for the receipt of data pattern messages that are sectioned (see paragraph 501 JANAP 128). The options shall be selectable by each subscriber. The options are:

a. Option 1 - (default option) Message sections are released for delivery to the subscriber as soon as received.

b. Option 2 - Message sections are released for immediate delivery to the subscriber if received in the correct sequential order; if received out of order, the message section(s) shall be held until the previous message section(s) are received, the sections shall then be released in message section number order.

c. Option 3 - All message sections shall be held until all sections are received; the sections shall then be released for delivery to the subscriber in message section number order.

d. Option 4 - It shall be possible to hold the data pattern traffic for delivery on a designated time schedule or released by the I-S/A AMPE operator at the request of the terminal.

The I-S/A AMPE operator shall have the capability to override options 2 and 3 and release individual message sections for delivery.

3.2.1.4.2.3 Output RI Classmarking

For output delivery, I-S/A AMPE subscribers shall have the classmark option of receiving 1, 50, or 500 RIs per transmission; e.g., should a message containing 10 RIs be destined for a subscriber classmarked to receive one (1) RI per transmission, the AMPE must make 10 transmissions, one for each RI.

3.2.1.5 Message Processing Control

3.2.1.5.1 Precedence Processing

Messages shall be processed First-In-First-Out (FIFO) within each precedence category (See 3.2.3.2.4) with the following exceptions:

a. Service messages shall be placed at the head of the appropriate precedence queue.

b. The AMPE shall have the capability to manage the strict FIFO by precedence message processing such that no one community of users (DSSCS, GENSER) can monopolize the available transmission media. To prevent such monopolization on dual community, channels, a 4-to-1 channel allocation ratio shall be applied such that at least one DSSCS flash and above precedence message is transmitted on a given dual community channel for every four GENSER flash and above messages transmitted. Another 4-to-1 channel allocation ratio shall apply to these same channels for immediate precedence messages. DSSCS messages will not be delayed to achieve the 4-to-1 ratio. FIFO within each precedence will apply unless enough GENSER messages are on queue ahead of the DSSCS messages to bring the channel allocation ratio into effect. Operator notification of high precedence DSSCS traffic shall be performed in accordance with DoD C-5030-58M, Chapter 4, paragraph 7 and DOI-103.

c. For GENSER traffic only, the I-S/A AMPE shall process messages with designated Content Indicator Codes (CICs) (not to exceed ten different codes) prior to other messages of the same precedence.

d. Overflow conditions as specified in para 3.2.1.5.4.

e. Queue Management as specified in para 3.2.1.5.6.

3.2.1.5.2 Message Preemption

Message preemption means ceasing to process the current message on the output queue and commencing to release the preempting message. The I-S/A AMPE shall have the capability to preempt the output of a message to allow transmission of a specified higher precedence message; preemption shall not cause the loss, modification, or segmentation of a message. ECP, CRITIC and Flash messages shall automatically preempt lower precedence messages. If a message is preempted during transmission, the I-S/A AMPE shall cancel the message and place the preempted message at the head of that precedence queue. If a message with a channel sequence number is preempted during transmission, a CANTRAN shall be sent and a new channel sequence number shall be assigned prior to reinitiating transmission of the preempted message. For DSSCS traffic all messages cancelled shall be terminated with a CANTRAN sequence. The message shall not be preempted if the end of message process is active.

3.2.1.5.3 Automation Assisted Traffic Management

This function encompasses all those automatic and I-S/A AMPE operator interfaced operations which control flow and processing of message traffic through the I-S/A AMPE. These operations include traffic loading, generating and processing service messages, altrouting, intercept processing, overflow protection and precedence processing.

3.2.1.5.3.1 Traffic Loading

The designated system operator shall have the capability to visually inspect the status of the queues on any specified channel. When the queue of messages for any channel reaches a predefined threshold (set by the I-S/A AMPE operator), the system shall generate a notice of the queue condition and display this notice at the designated operator position. Additionally, system status information, see 3.3, shall be available to the operator.

3.2.1.5.3.2 Message Timing and Overdue Notification

The system shall perform message auditing beginning at the time of receipt of the message EOM and shall notify the system operator if the time the message has been in the system exceeds a predetermined time threshold. A message is considered to be in the system as long as the I-S/A AMPE has delivery responsibility, i.e., until the I-S/A AMPE has completed transmission of the message to all required channels and an acknowledgment has been received for messages requiring it. (Exception: messages on intercept are excluded from this overdue notification until they are returned to active processing.) A message is considered overdue when the following time limits are exceeded:

Precedence	Time In System
a. Flash and above	1 minute
b. Immediate	5 minutes
c. Priority	30 minutes
d. Routine	80 minutes

If any of the time limits noted above are exceeded, the system shall provide an operator notification to the system operator. The overdue notification shall include the message OSRI-OSSN, system assigned unique message identifier, precedence and destination channel designator. The operator shall be notified of high precedence messages every five minutes until delivery. If multiple messages of the same precedence are overdue only the oldest message for the precedence shall be identified. The operator will be responsible for the action to be taken, i.e., altroute, reset overdue threshold, ignore, etc. The overdue time limit shall be able to be reset by the operator for immediate, priority or routine messages to a maximum of 99 minutes. Flash, ECP and CRITIC thresholds shall not be able to be reset.

The I-S/A AMPE shall be capable of generating an I-S/A AMPE-to-I-S/A AMPE receipt for each CRITIC received from a distant I-S/A AMPE indicating that the CRITIC message has been received and delivered. The I-S/A AMPE shall also be capable of suspensing receipts expected from a distant I-S/A AMPE following CRITIC transmissions, and when not received within specified time periods (software selectable not to exceed 60 seconds maximum), automatically select secondary or tertiary routes for delivery.

3.2.1.5.3.3 Intercept Processing

Intercept processing shall provide operator-initiated interim storage for messages whose delivery is delayed by an inoperative or backlogged output channel. Using intercept the I-S/A AMPE shall be able to temporarily hold messages for a destination which is partially or completely out of service or which operates on a part-time basis. The I-S/A AMPE shall provide the capability to invoke and revoke intercept by system operator specification of combinations of the following criteria: PLA, precedence, routing indicator, channel, security classification, and language media format. ECP, CRITIC and Flash and service messages shall not be intercepted but shall be delivered to the operator for further processing that will result in the delivery to the required PLA. Immediate precedence and below shall be intercepted, when initiated, with notification printouts for each occurrence. FIFO within each precedence level shall be maintained for the selected intercepted messages being returned to the I-S/A AMPE output queues.

3.2.1.5.4 Overflow Protection

An overflow condition exists when the combined message input load exceeds the capacity of the I-S/A AMPE to process that message load. When an overflow condition occurs, the most recently received and lowest precedence messages shall be automatically stored in an overflow storage file. When the message load permits, messages stored in the overflow file shall be automatically reintroduced for processing in accordance with FIFO criteria (See 3.2.1.5.1). The operator shall be notified automatically of message movement to and from overflow storage. CRITIC, Flash, and Emergency Command Precedence messages shall not be stored in overflow storage. The operator shall have the capability to manually reintroduce messages from the overflow file for processing, and to inhibit input from designated input channels. Criteria for message overflow shall be channel activity, queue load by addressee, precedence, or a combination of these. Message processing shall continue on active channels during the overflow condition. Adherence to the provisions of 3.4 shall continue during overflow conditions.

3.2.1.5.5 Alternate Routing

The I-S/A AMPE operator shall be able to invoke an automatic altroute for traffic destined to one of the I-S/A AMPEs local subscribers. The I-S/A AMPE shall automatically generate a pilot consistent with the message format, with the appropriate Routing Indicator, and forward the message to the new destination. The I-S/A AMPE operator shall have the capability to further identify messages to be altrouted by designating the addressee and any combination of one or more of the following: precedence, classification, language media format, and content indicator code. See 3.4 for security restrictions and 3.3.3 for additional requirements. The I-S/A AMPE shall automatically generate and transmit a service message notifying the destination of its altroute status prior to transmitting the first altrouted message. It shall also automatically generate and transmit a service message upon terminating the altroute condition.

3.2.1.5.6 Queue Management

The I-S/A AMPE operator shall have the capability to inspect and manipulate message queues as a means to alleviate processing backlogs. The operator shall be able to transfer entire queues to alternate channel queues for delivery, move individual messages to alternate queues or different positions within their current queues, or remove messages from the processing flow entirely by placing them on intercept. In addition the operator shall be provided the capability to purge a specific message (causing malfunction due to data sensitive software errors) from the queue. The additional capability to purge the entire system message files shall be provided, including safeguards that prevent accidental purging or purging by an unauthorized individual. Message identification shall be provided to the I-S/A AMPE operator to allow for subsequent recovery action on the purged message(s).

3.2.1.5.7 Automated Routing/Distribution File Maintenance

The I-S/A AMPE shall be able to semi-automatically process changes received for the routing and distribution files. The changes shall not be made to the file until the I-S/A AMPE operator has reviewed the change and made a positive manual action to enable the change to be posted.

3.2.1.5.8 Service Messages

Service messages are concise, and normally precisely formatted, messages used by communications personnel to exchange information and instructions concerning conduct of communications. In all cases, service messages shall be processed to preclude the possibility of compromise of classified information. The I-S/A AMPE shall automatically generate and deliver service messages in accordance with formats specified in JANAP 128, ACP 127 and DOI-103 upon detection of errors and as otherwise appropriate (e.g., on invoking and revoking alternate routing). A list of the service messages to be involked by the I-S/A AMPE are specified in Section 21.0.

3.2.1.5.8.1 System Generated Service Messages

System generated service messages are those originated within the I-S/A AMPE system itself, rather than being entered from a terminal or prepared manually by an I-S/A AMPE operator and entered through a terminal. System generated messages shall be initiated by either operator command or automatically in response to the following types of conditions: invalid channel designator, invalid channel sequence number, open channel sequence number, invalid routing field, invalid security field, invalid transmission release code, invalid header, invalid end-of-message sequence, invalid transmission control code, overlength message, suspected stragglers, input message timeout, acceptance or transmission of a high precedence message and an excessive number of routing indicators in the routing field. A complete listing of required service messages is detailed in Section 21.0, Service Message Appendix. The I-S/A AMPE shall automatically generate a channel continuity verification (JANAP 128 para. 329.e.(16)) when 30 minutes have elapsed with no receipt of traffic from a Mode II subscriber. Additionally, messages which require receipt of acknowledgment by the communications center (as opposed to acknowledgment by the user, which must be done only by the user) shall be automatically processed by the I-S/A AMPE to include acknowledgment. The I-S/A AMPE shall also automatically acknowledge receipt by routine precedence message for Flash, ECP and CRITIC messages. See Section 21 for a listing of service messages, their description and use. [Reference 2.5.a, Appendix B, Section I describes how this requirement is satisfied by ASCs and may be used as a guide.]

The I-S/A AMPE operator shall receive a copy of system generated messages. In addition, the system shall be so designed that all system generated messages are recorded on the history record.

3.2.1.5.8.2 Automated Processing of Service Messages

Service messages received from subscribers which require retransmission of messages stored online shall be automatically processed by the I-S/A AMPE, to include automatic retrieval and retransmission of the requested message(s). The automatic response to service messages will require close control due to security and privacy considerations; that is, the subscriber requesting the retransmission of a message must be authorized to act as an originator of such a message as well as being either the originator or an addressee on the subject message. The I-S/A AMPE shall also automatically process requests for retransmittal by Channel Sequence Number and time period. If a retransmission request is for more than 10 messages, it shall be forwarded to the I-S/A AMPE operator for approval. If a message cannot be retrieved automatically, the I-S/A AMPE operator shall be notified of all information to permit manual retrieval of the message if required.

3.2.1.5.8.3 Manual Processing of Service Messages

All incoming service messages which are not automatically processed by the I-S/A AMPE shall be delivered to the designated service position for manual intervention except that service messages destined for designated terminals (e.g., a Navy RIXT or Army IRT) shall be delivered to the designated terminals. The service position shall have the capability to perform message editing of service messages, attach pilots to the messages, readdress messages and call service message masks (JANAP 128, DOI-103, ACP-127) to the display for insertion of variable information and release of messages. The I-S/A AMPE shall also provide the capability (option) to send modified text of service messages to terminals manned by non-communications personnel. This option shall be selectable on a terminal-by-terminal basis and the text modification shall be such that the service message is easily understandable to the non-communications trained personnel. Additionally, the I-S/A AMPE shall be designed so that at least two operator/service positions can support processing of service messages if the primary service position becomes overloaded.

3.2.1.6 Accountability and Recordkeeping

The I-S/A AMPE shall insure that messages are accounted for during processing through the system and shall maintain history logs and files to record this accountability.

3.2.1.6.1 Message Accountability

Message accountability involves actions to guard against loss of traffic once it is accepted by the system. Techniques specified in DoD C-5030.58M for message accountability shall be used. Additionally, the following functions shall be implemented.

a. A global Unique Message Identifier (UMI) shall be assigned to each message accepted by the origination I-S/A AMPE and shall include positive identification of the originating subscriber's port and the originating I-S/A AMPE. This identifier shall be printed on all pages of the message.

b. An audit trail shall be maintained within each I-S/A AMPE, tracing all actions performed on the message as a whole. (Ref DoDC-5030.58M)

c. The storage of message and system status information shall preclude loss of stored information.

d. The system shall have the capability to annotate on-line message files to be nonretrievable. When the system or an operator requests retrieval of that message, a notification shall be sent to the operator position stating the message cannot be retrieved.

e. The I-S/A AMPE shall prevent intermixing of portions of two or more messages. The I-S/A AMPE shall prevent the interlacing of messages during processing. See DOD C-5030.58M, page 23, para 3f(5).

3.2.1.6.2 History Logs and Files

The I-S/A AMPE shall provide for storage of messages and system status information. This stored information is used to recover from a malfunction, to support retrievals and searches, to trace the progress of messages through the I-S/A AMPE, and to support the statistics function. The I-S/A AMPE shall provide on a site by site selectable basis the storage for either of the following:

a. All messages (including service messages, but excluding the text of AUTODIN Limited Privacy System (ALPS) messages) processed by the I-S/A AMPE.

b. All narrative messages (including service messages, but excluding ALPS messages) as well as the text of selected data pattern messages.

The retention period of on-line stored messages is specified in 3.5.

3.2.1.6.2.1 Incoming and Outgoing Journal Entries - System Status Information

The I-S/A AMPE shall provide the capability to store and access information regarding events which occur during the processing of a message, as well as information which describes the I-S/A AMPE configuration and events which change the configuration. The information in Tables 3.2.1.6.2.1-1 and -2 shall be stored for each message or system event as appropriate. The I-S/A

Table 3.2.1.6.2.1-1 Journal Entries - Messages

1. Start of message input.

2. End of message input and input channel and CSN if applicable.

3. Start of message output.

4. (Final) End of message output.

5. End of transmission for each output terminal, to include terminal identifier and channel number.

6. End of message acknowledgment for each delivery to include CSN if applicable.

7. Unique Message Identifier.

8. Routing indicator and channel number of each output message.

9. Error summary for each message to include date and time of the message.

10. Format line three OSRI (if applicable).

11. Input LMF pair and actual delivery media for each message.

12. Message status table.

13. Retrieval and retransmission actions.

14. Security, TCC, TRC, and SHD.

15. Message length data.

16. Statistical data (necessary to support requirements of paragraph 3.3.3).

17. Message Identification of all messages scrubbed by the system, time and reason.

18. Precedence.

19. Unsuccessful attempts by a subscriber to input message traffic to include date and time of each occurrence and reason.

20. Processing time in system.

Table 3.2.1.6.2.1-2 Journal Entries - System Events

1. Initiation and termination of input and output to overflow and intercept storage.

2. System configuration, to include status of peripherals and channels, software release identification and software patches or options installed.

3. Channel going into/out of service.

4. System state, to include failure times, restart times.

5. A record of all input from and output to the system operator position to include day and time.

6. A record of all system error conditions or abnormal events affecting message traffic processing to include day and time of each.

7. A record of all automatic system actions taken that affect message traffic flow or overall I-S/A AMPE operation to include day and time of each action.

AMPE shall provide the storage and access functions of the DoD Manual C-5030.58M, Chapter 3, paragraph 3f(2).

3.2.1.6.2.2 Reference Entries

Stored information on each message and each section of a multisectioned message shall support system restart and reload, statistics requirements (See 3.3.3), the trace of all actions taken on each message processed, and the search of message files for message data.

3.2.1.6.3 History Data Interrogation

The I-S/A AMPE shall provide the system operator the means to interrogate history data (see Tables 3.2.1.6.3-1 and 3.2.1.6.3-2). Interrogation criteria included in Table 3.2.1.6.3-3 shall be accommodated.

3.2.1.7 Message Search, Retrieval, Readdressal and Retransmission

All files and logs maintained by the I-S/A AMPE shall be accessible in support of the search and retrieval functions. Search is the process of obtaining message data from both online and offline files in order to determine which messages should be retrieved. Retrieval is the process of obtaining messages from I-S/A AMPE online and offline storage files. Retrieved messages are then processed for readdressal and/or retransmission. The operator shall have the capability to initiate or terminate search, retrieval, readdressal and retransmission operations

3.2.1.7.1 Message Data Search

In general, the I-S/A AMPE shall support searches of the following types and combinations of the following types:

a. Search by day and time.

b. Search by originating station routing indicator and station serial number.

c. Search for data between two given points in time, defined by Ordinal date and time of day.

d. Search by unique message identifier.

e. Search by Channel Sequence Number (CSN).

f. Search by precedence.

g. Search by classification.

h. Search by originator and date-time-group (DTG).

i. Search by Destination Routing Indicator

j. OSRI and SSN and File Time

Table 3.2.1.6.3-1 Message Status Information to be Stored

INFORMATION	DATE AND TIME OF OCCURRENCE RECORDED
Start of message input	YES
End of message input acknowledgement to include input channel and input CDSN if applicable	YES
Complete copy of message as received to include UMI	NO
Start of message ouput for each addressee channel	YES
End of message acknowledgement received for each output delivery to include CDSN if applicable	YES
Occurrence of each cancellation of an output transmission to include reason	YES
Delivery to intercept or overflow storage	YES
Receipt from intercept or overflow storage	YES
(Final) end of message output	YES
Error summary for each message	YES
Record of retrieval action to include output delivery data for each message	YES
Unsuccessful attempt by a subscriber to input message traffic to include reason for each occurrence	YES
Input and output message length for each message processed	NO
Information concerning message retransmitted and recieved from an error correction device	YES

Table 3.2.1.6.3-2 System Status Information to be Stored

INFORMATION	DATE AND TIME OF OCCURRENCE RECORDED
System Configuration to include status of peripherals and channels	YES
Record of channel going into or out of service	YES
Statistical data necessary to support the requirements of 3.3.4.2	NO
Message queue status	YES
Alternate routing status	YES
Overflow and intercept file status	YES
Journal files sufficient to support the system restart and reload requirements of 3.3.8.2 and 3.3.8.4	YES
A record of all input from and output to the system operator position	YES
A record of all system error conditions or abnormal events affecting message traffic processing	YES
A record of all automatic system actions taken that affect message traffic flow or overall AMPE operation	YES

Table 3.2.1.6.3-3 History Data Information Interrogation

Interrogation Criteria	Average* Access Time	Volume of Information* Available Within Access Time
Time of Receipt (TOR) of all messages received on a given channel		
TOR of all messages received on a given channel a specific OSRI, PLA, or LMF		
TOR of all messages received on a given channel following a specified CSN, OSRI/OSSN or PLA/DTG		
Time of Transmission (TOT) of all messages transmitted on a given channel		
TOT of all messages transmitted on a given channel with specified delivery RI, delivery PLA, or LMF		
TOT of all messages transmitted on a given channel (with a given LMF if applicable) following a specified CSN, OSRI/OSSN or PLA/DTG		
TOR or TOT of message with a specified input CDSN, OSRI/OSSN, PLA/DTG or UMI		
All activity (input and output) on a given channel between specified times		
All system restarts, reloads or error conditions between specified times		
All input from or output to the system operator between specified times		
Information on messages scrubbed or rejected by the system or the operator between specified times		

*(To be determined)

Table 3.2.1.7.1-1

Searches Provided by the I-S/A AMPE to the Operators

1. Search 01 prints all system restart entries and all monitor printer printouts that are on the history files.

2. Search 02 prints message information and time of receipt of all messages received with a particular security classification or preceoence.

3. Search 03 prints message information for all messages with tne specifieo Unique Message Ioentifiers.

4. Search 04 prints message heaoer and time of transmission of all messages transmitted to a given channel.

5. Search 05 prints message heaoer ano time of transmission of all messages transmitteo on a given oestination.

6. Search 06 prints message information ano time of receipt of all messages with a particular security classification received on a given channel.

7. Search 07 prints message icentification of all messages purged by the system on output.

8. Search 08 prints all message information that has been storeo in a specifieo area of the storage media.

9. Search 09 prints message identification of all messages purged by the system due to a storage failure.

10. Search 10 prints message information and time of receipt of all messages received with a given originating station routing indicator after a giver time.

11. Search 11 prints message information and time of receipt ano time of transmission of a Mode II, Mode I optional Transmission Identifier line users by channel sequence number and input channel number.

12. Search 12 prints message heaoer and time of transmission of all messages transmitteo to a given Mooe II, Mode V or Mode I optional Transmission Identifer line users, following a given channel sequence number.

13. Search 13 prints message identification of all messages receiveo with a given format line three originating station routing inoicator (OSRI) after a given time.

14. Search 14 prints message heaoer ano time of transmission of all messages transmitteo on a given channel to a given destination.

15. Search 15 prints message information ano time of receipt of all messages received on a given input channel, following a specified time.

k. ORSI and DTG

l. OSRI and DTG and Unique Message Identifier

m. PLA and DTG

n. CSN and time period

o. Content Indicator Code

p. Delivery Distribution Indicator (DDI)

Each search has the option of printing all the message information or abbreviated, journal information only. The I-S/A AMPE shall perform all searches specified in Table 3.2.1.7.1 upon operator initiation. Access times are specified in 3.5.3.4. ZULU time shall be used for message storage and retrieval operations.

3.2.1.7.2 Message Retrieval

The I-S/A AMPE shall support the retrieval of message parameters stored on-line as specified in 3.2.1.7.1. Access times are specified in 3.5.3.4. The I-S/A AMPE system or its operator shall be able to request message retrieval. System requests shall be the result of service messages. These service requests for retrieval may be made only by the originator or an addressee of the message to be retrieved. A retrieval request from a subscriber shall be honored only if the subscriber is either the originator or an addressee of the message to be retrieved and then only if the subscriber is homed to that I-S/A AMPE.

It shall be possible to retrieve up to 10 messages with a single request. The I-S/A AMPE shall allow retrieval of messages which contain two sets of originating station routing indicators, station serial numbers, and file times by either such set.Channel Designator (CD), Channel Sequence Number, or unique Message Identifier.

3.2.1.7.3 Message Readdressal

The I-S/A AMPE shall provide a message readdressal function defined as those actions necessary to cause a message to have a new set of addresses assigned which differ from the original set. Readdressal shall be capable of being initiated by a request entered (by message originator or original addressee) at the service position or by use of a DD Form 173. The DD 173 message form shall be accommodated by the I-S/A AMPE for the preparation, release, and input of readdressal requests. The form will be identical to that for a message origination except the text portion shall be replaced with the identification of the message to be readdressed. Message readdressal shall also be accomplished via operator entries via VDT. Readdressals shall be accomplished in accordance with JANAP 128, ACP 127 and DOI 103.

All messages for which new addressees are so inserted shall be routed to the service position for final review and editing of the header. The service position shall be prohibited from editing the text of any messages. The readdressed message shall then be routed through the I-S/A AMPE as if it were a new message, with security checks, internal distribution, and comeback copies included as appropriate. If the message fails to pass input message processing (see 3.2.1.2) the requestor shall be notified.

3.2.1.7.4 Message Retransmission

Retransmission is the resending of a message previously transmitted. The I-S/A AMPE shall automatically accomplish retransmission when a service message requests retransmission and the following conditions are met:

a. The retransmission request service message is originated by the originator or an original addressee of the requested message.

b. The retransmission request is for 10 or less messages.

c. The service message identifies the messages to be retransmitted by: the originating station routing indicator, station serial number and file time; channel designator and channel sequence number; Date Time Group; or Unique Message Identifier.

d. The requested messages are contained on the on-line message storage file.

e. The requested message has not been previously retransmitted a certain predefined number of times, set by the I-S/A AMPE console operator.

The retransmission capability shall allow the I-S/A AMPE operator to perform retransmission of multiple messages based on the message retrieval capability of FRD 3.2.1.7.2.

If any of the above conditions are not satisfied, then the request shall be sent to the I-S/A AMPE operator for resolution. The I-S/A AMPE operator shall have capability to override conditions b through e. The requestor shall be notified if the retransmission cannot be accomplished. Retransmission restrictions are specified in 3.2.1.5.8.2. All retransmitted messages shall indicate that the message is a retransmission in accordance with the procedures in JANAP 128, ACP 127 or DOI 103 as appropriate.

3.2.1.8 Automatic Formatting, Paging and Sectioning

The I-S/A AMPE shall format messages to include paging (assigning sequential page numbers) and sectioning (scanning the message for length and appending logical segments based on the analysis) of originated messages according to JANAP 128 and DOI-103 for each user requiring such. Each subscriber shall be classmarked at initialization.

3.2.2 Message Editing and Preparation Service (MEPS)

The FMS of the I-S/A AMPE shall provide automatic assistance to operators in the process of message entry. This capability includes automatic supervision of message preparation, message mask call-up from remote terminals, and editing capabilities. MEPS shall be available to all users who do not deal solely in fully formatted JANAP 128, ACP 127, DOI-103 and DOI-103 Special messages. For terminal subscribers the transactions shall be in messages, vice characters or lines. For local terminals (those colocated with the I-S/A AMPE) the editing capability shall permit the subscribers to make corrections and changes to his message both during and after entry but prior to release. Editing shall include insertion, deletion, and replacement of character(s), word(s), and line(s). MEPS also includes conversion from DD 173 message form to JANAP 128 and DOI 103 format and PLA to RI assignment.

3.2.2.1 Automatic Supervision of Message Preparation

The I-S/A AMPE shall have the capability to automatically guide the message writer through the process of entering a message into the I-S/A AMPE through the use of leading questions (e.g., format desired, security classification desired, addresses desired, examples of possible responses, menus, alternative replies and prompters, community, DSSCS or GENSER, as a minimum). Diagnostic messages in language easily understood by noncommunications oriented personnel shall be sent to the originators automatically when an error is made during the entry process.

3.2.2.2 Message Preparation Masks

A mask is an outlined message or form with variable fields left blank on the VDT, to be filled out by the user. The I-S/A AMPE shall provide a standard mask (DD 173 form) for general message preparation, a CRITIC mask, and certain canned formats (operational and deployment orders, services messages and emergency action messages) for specialized usage. The I-S/A AMPE shall have masks for the Standard Message Form (DD173) in accordance with ACP-121 and the CRITIC masks in accordance with DOI-103. The I-S/A AMPE shall make provision for 18 other masks to be prescribed by the users. These masks shall be able to be entered or changed by the local I-S/A AMPE operator. A page of a preformatted message shall be displayed on the screen within five seconds of the user request for the message mask. When a mask is displayed, the user shall have the capability to enter variable information (some fields will have default values, for routine precedence, while others must have valid data, e.g., from/to info.), create and edit text material, and release the message. Controls shall be exercised to restrict a private library of masks from being received by the general community (i.e., masks for CRITIC messages would only be permitted at designated I-S/A AMPEs).

3.2.2.3 Message Editing and Review

The I-S/A AMPE subscriber shall be able to edit messages during entry and after entry but prior to release by inserting, deleting, and/or replacing characters, words and/or lines.

3.2.2.3.1 Line Editing

Through editing, the message writer shall have the capability to insert new lines, delete existing lines, or replace any specified line with a new line then entered.

3.2.2.3.2 Character and Word Editing

The I-S/A AMPE editing capabilities shall allow character or word deletions, replacements and insertions in a line that has been identified for editing, or in the last line just entered if editing is being done during message entry.

3.2.2.3.3 Copy Review

The I-S/A AMPE shall provide a review copy of the message in either a hardcopy format, or as an edited display at the VDT. With the display feature, the I-S/A AMPE shall have the capability to scroll the message either forward or backward to aid the proofreader.

3.2.2.4 Format Conversion and PLA to RI Assignment

The MEPS shall perform all actions required to transform messages not ready for transmission (e.g., messages read from DD Form 173/3) to either JANAP 128 formatted messages for GENSER users or DOI 103 formatted messages for DSSCS users, suitable for transmission via the FMS. In addition to properly organizing the message, FMS shall ensure that precedence LMF, classification, CIC, OSRI, OSSN, TOF, security sentinel, redundant classification, start of routing, RI(s) and the end of routing, as well as all other required format lines are properly included. This shall require a PLA to RI assignment (see 3.2.1.2.2.6).

3.2.3 Service Management

At IOC the I-S/A AMPE shall provide management of FMS with its MEPS, conrol of subscriber connections and the VCS connection to the DDN. The I-S/A AMPE shall provide the variety of subscribers termination modes listed in paragraph 4.2.2.2 of the ICD. At IOC the I-S/A AMPE shall provide and manage the following subset of the Data Flow Paths of paragraph 3.1.5.3.1:

- o Local terminal subscriber to local FMS (3.1.5.3.1.1).
- o Local FMS to distant FMS via the DDN (3.1.5.3.1.4).

3.2.3.1 Terminal to FMS Connection

The I-S/A AMPE shall provide fixed connection depending on prestored classmarks for each terminal either to FMS directly or to FMS via MEPS. The direct FMS connection is to be used by terminals transmitting Modified ACP 126, ACP 127, JANAP 128, Navy's Abbreviated SI, DOI 103 or DOI 103 Special fully formatted messages. The MEPS connection is to be used by terminals transmitting DD 173, NSA's Abbreviated SI, or other less than fully formatted traffic. Note the Modified ACP 126 and Navy's Abbreciated SI formats both require PLA to RI assignment, a MEPS function.

3.2.3.2 Local FMS to Distant FMS

At IOC the I-S/A AMPE shall provide and manage a VCS capability to interconnect the FMS modules of the various I-S/A AMPEs. Note that the I-S/A AMPE is to be a host user of the DDN. In addition to the VCS protocols TCP and IP (see ICD, 4.2.4 and 4.2.5) a new protocol FMP (ICD 4.2.6.2) is required which is the interfacing protocol between the routines of FMS and those of TCP.

3.2.3.3 Management Flexibility

The I-S/A AMPE design shall accomodate a robust Service Management Function controlling all the 3.1.5.3.3.1 data flow paths and multiple services, see P^{3}I, paragraph 3.12.

PAGE 3-65 INTENTIONALLY LEFT BLANK

3.3 System Control

3.3.1 System Control Concept

Within the DCS, system control is the function whereby communications assets are used to maintain and restore maximum system performance under changing traffic conditions, natural or manmade stresses, disturbances, and equipment disruptions. Basic aspects of system control include (1) timely acquisition of system performance data, facility and traffic load status, an service quality indications; (2) rapid analysis, processing, and display of information; (3) decision-making and control execution; and (4) support of longer range system management and engineering.

The Integrated AUTODIN System (IAS), as a subsystem of the DCS is requir to include control functions as part of its design and implementation. That design and implementation must also consider the interaction of the IAS with other DCS elements.

The I-S/A AMPEs and the DDN are sub-elements of the IAS. The I-S/A AMPE can be viewed as a number of subscriber hosts, each with multiple terminals, interconnected via a backbone packet switched network (DDN). The DDN consis of approximately 175 Packet Switching Nodes (PSNs). Each PSN will be programmed to examine itself and its environment periodically and to report the results of these examinations to a processor designated as the System Monitoring Center (SMC), also referred to as a BLACK Monitoring Center. The term Monitoring Center (MC) will be used to refer to that functional portion of the control process responsible for the I-S/A AMPE subnetwork.

Each host subscriber to the DDN will operate at its own specified system high security level (the design allows for subnetworks consisting only of a specific compartment). Separation of each subnetwork is provided by the use of End-to-End Encryption (E^3). There will, therefore, be at least one E^3 cryptographic key for each different subnetwork. The E^3, in effect, prevents anyone not included in the subnetwork from communicating with the host behind the E^3 device, including the SMC. This security separation protection leads to the requirement for separate I-S/A AMPE MC functions. These MC functions may be viewed, like the SMC, as a processor attached via host interface to a PSN, however, final design may dictate another approach. The MC, supporting the I-S/A AMPE subnetwork, will be behind an E^3 device with appropriate key variable(s). This will allow the MC function to communicate with each I-S/A AMPE. The concept for control of the I-S/A AMPE subnetwork can be summarized as follows:

Each I-S/A AMPE will be responsible for monitoring itself and its environmer (including its associated terminals) and periodically reporting the results the MC function. Each I-S/A AMPE will also broadcast certain control and status messages to the DCA Operations Center (DCAOC) and all other I-S/A AMI in the subnetwork to advise them of various traffic controls such as temporarily inhibiting other I-S/A AMPEs from transmitting low precedence traffic to it. In effect, two levels of network control will exist, both under the overall control of the DCAOC. One level within the backbone is tl

3.3 SYSTEM CONTROL

responsibility of the DDN. The second level is within the I-S/A AMPE subnetwork and will be the subject of discussion in the remainder of this section.

It is important to note that the terms SMC and MC refer to the hardware and software type functions to be used in an integrated control process that supports the overall system control function of the IAS. Although the SMC ar MC functions/computers are important components of the network, their operation must not be essential to either the DDN backbone or to the I-S/A AMPE subnetwork.

3.3.1.1 System Control Evolution

The I-S/A AMPEs in conjunction with the DDN will provide the capability t phase out the AUTODIN Switching Centers (ASCs) currently serving Formal Message Service (FMS) subscribers. Initially, the I-S/A AMPE will connect tc both ASCs and PSNs. During this initial stage, the present AUTODIN control centers will be responsible for the total combined ASC and I-S/A AMPE subnetwork, with the I-S/A AMPE MC providing necessary monitoring and control functions for the I-S/A AMPE subnetwork. As subscribers are rehomed to I-S/ AMPEs and the I-S/A AMPEs are interconnected via DDN, the ASCs will be phasec out. During all phases of the transition, coordination and cooperation with the DDN SMC will be required.

3.3.1.2 Connectivity Requirement for System Control

Each I-S/A AMPE will use DDN service for its primary system control communications. In addition, the system control design will allow for the us of dial up service for backup system control communications to send and receive system control data and directives. All system control data transmissions will be encrypted and have authentication policies and safeguards to prevent malicious or accidental modifications. Further, I-S/A AMPE operators will be provided with dial up voice service.

3.3.2 Subnetwork Management and Control

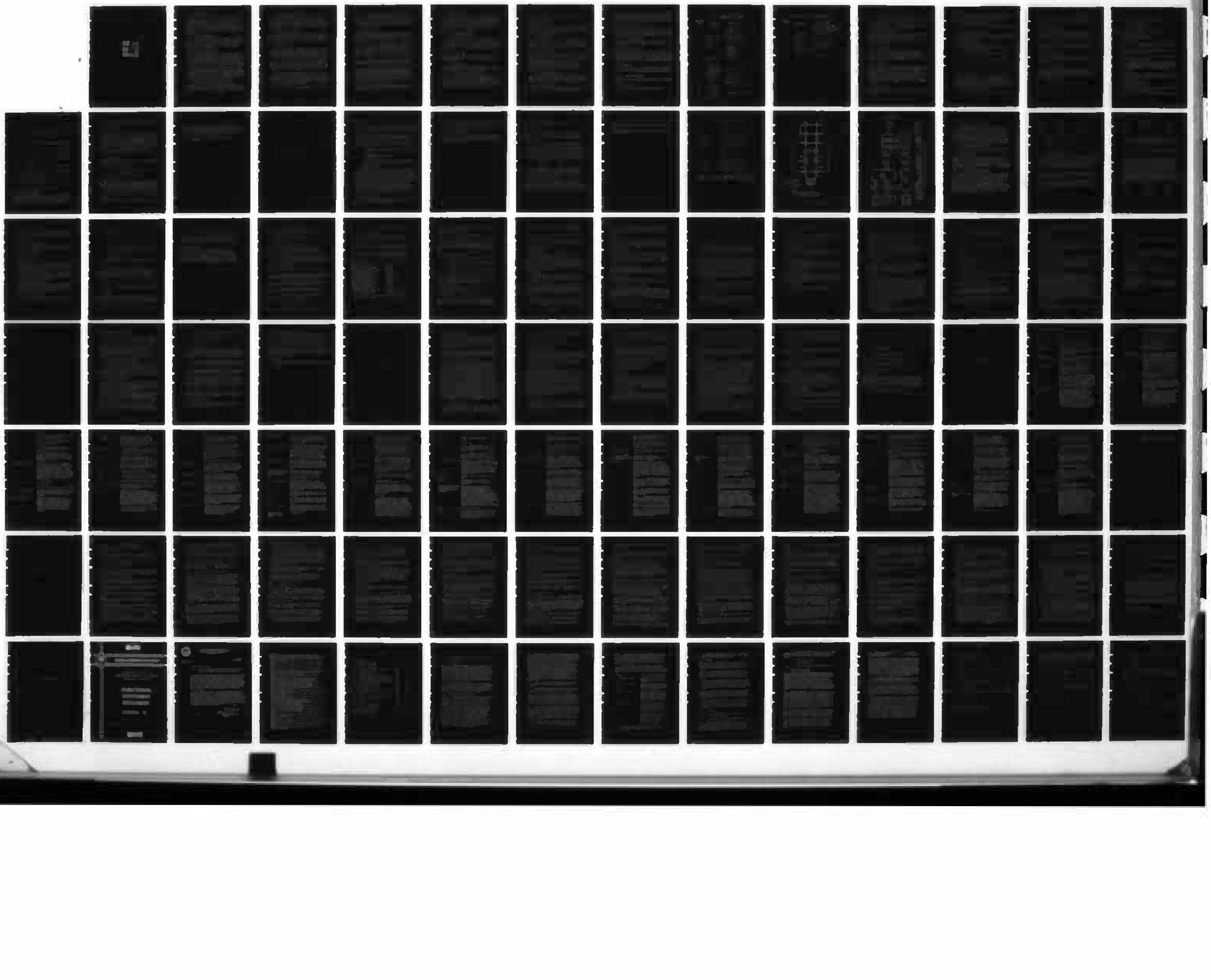
Monitoring Center functional interfaces will be extended to the geographically separated AUTODIN Control and Operations Centers (ACOC). In this way, network management and control will be supported by the Monitoring Center function. Control and operations centers in the CONUS will be backed up by subordinate regional monitoring centers located in the Pacific and Europe.

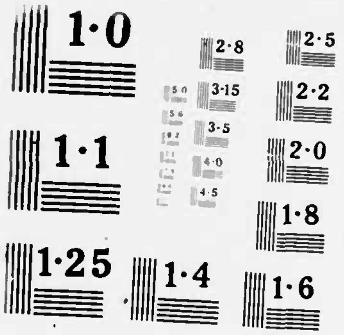
3.3.2.1 Integrated AUTODIN System Control Process

The Integrated AUTODIN System control process will utilize elements for the AUTODIN, DDN, and I-S/A AMPE; and will include the hardware, software, personnel and procedures necessary to perform the assigned functions. The I-S/A AMPE MC functions which will take control inputs from each I-S/A AMPE and compile, store, and present information. The information will be used f developing responses to routing problems, unanticipated subnetwork problems, long-term planning for network configuration management, and billing.

AD-A134 884 INTER-SERVICE/AGENCY AUTOMATED MESSAGE PROCESSING 2/7
EXCHANGE PROGRAM FUNCTI.. (U) DEFENSE COMMUNICATIONS
AGENCY ARLINGTON VA 01 NOV 83

UNCLASSIFIED F/G 17/2 NL





NATIONAL BUREAU

MICROCOPY RESOLUT TEST

3.3.2.1.1 Crisis Management

A major function of the MC will be to support the management of crises or contingency conditions. This will be accomplished by providing the MC function associated with the I-S/A AMPEs the capability to selectively apply control measures before the subnetwork capability is unacceptably degraded. However, as discussed earlier, the ability must be provided to continue expeditious network control under wartime conditions, without an operational MC. The I-S/A AMPE operator, or the MC, will be able to provide destination code cancellation, or to block access by selected users or precedence levels. Adequate authentication and verification procedures must be provided to preclude either inadvertent or malicious disruptions to the operation of the subnetwork.

3.3.2.1.2 Network Modification Control

The I-S/A AMPE operator will review network modification control changes prior to implementation in order to ensure that improper changes cannot be made as a result of accidental access, deliberate attempt, or communications failure. (The MC will be capable of directing and controlling the implementation of I-S/A AMPE software changes and routing table updates. These changes will be transmitted to the I-S/A AMPE via secure means and subject to a verification process.)

3.3.3 Configuration Monitoring and Control

Configuration monitoring and control is concerned with maintaining current records of the network access and connectivity to the backbone. Each I-S/A AMPE shall maintain status information on its connected user locations and transmission links, and temporary records of reroutes and subsequent restorals up to the point of connection to the backbone. The MC function will maintain records of all connected users and their locations, servicing I-S/A AMPE, and user characteristics. The I-S/A AMPE shall automatically (as an operator selectable option) transmit to the ACOC and DCAOC changes of this information.

3.3.3.1 Activations/Deactivations of Subscribers and Transmission Links

The I-S/A AMPE operator shall be provided the capabilities to coordinate and implement the activation and deactivation of subscribers and supporting transmission links. In addition, each I-S/A AMPE operator shall be provided the capability to review and either accept or reject updates in routing. In the event the MC function is disabled the I-S/A AMPE shall have the capability to broadcast the update information to all other I-S/A AMPEs.

3.3.3.2 Subscriber and DDN Access Line Reroute and Restoral

Each I-S/A AMPE shall support the reroute and restoral of failed subscriber lines, ASC access lines, and the I-S/A AMPE's DDN access lines. This capability shall be provided as part of the I-S/A AMPE's Fault Isolation and Correction (FI&C) function. (See Section 3.3.6) All circuit reroutes and subsequent restorals shall be monitored and automatically reported to the MC.

3.3.3.3 Network Configuration Engineering

The configuration engineering function of the I-S/A AMPE subnetwork will use the latest network configuration and resource availability data together with historical information concerning line, trunk and equipment utilization and performance monitoring measurements to plan and maximize the I-S/A AMPE sub-network performance. This information will reside in the MC to be used for configuration engineering purposes. The I-S/A AMPE role in performance of this function shall be to automatically provide the information required by the MC, and to respond to directives or requests for additional data as specified in Section 3.3.4.

3.3.4 Traffic Flow and Routing Control

The DDN backbone provides for flow control, and dynamic routing to hosts (I-S/A AMPE) connected to the backbone. The I-S/A AMPE (and associated MC) shall provide traffic flow and routing control for individual I-S/A AMPEs and their terminal elements. The I-S/A AMPE shall be capable of supporting these control capabilities, and the MC will have the capability to provide directives to the I-S/A AMPE.

3.3.4.1 Traffic Flow Control

The I-S/A AMPE shall provide flow control mechanisms, specified below, to permit the I-S/A AMPE operator to alleviate problems associated with traffic congestion at individual I-S/A AMPEs. Congestion can result from failed hardware or software modules, error prone transmission channels, insufficient storage resources, or unusual surges in incoming message traffic. Flow control shall be implemented without denying subscribers access to the Formal Message Service. The I-S/A AMPE shall provide the following controls:

a. A traffic intercept control to direct messages -- up through Immediate -- to a mass storage device upon direction from the I-S/A AMPE operator. Once implemented, traffic intercept shall remain in effect until cancelled by the operator. The effect of intercept is to temporarily remove traffic from the I-S/A AMPE. Intercept would normally be employed in the event of a subscriber line outage or high traffic volumes destined for subscribers.

b. An automatic dial-up capability to obtain a temporary path to a terminal, an ASC, or another I-S/A AMPE shall be provided. This has the effect of enhancing network availability and will be used in the event of a circuit failure or for relief of high volume to a specific circuit. This control shall be under operator control. Automated dial-up capability shall be provided such that no operator involvement is required beyond initiation, or approval, of the dial-up. Any dial-up connection so obtained shall be the operational equivalent of a permanent connection.

c. The capability to automatically generate reports of congestion, intercept status, and queue status and transmit these reports to the MC shall be provided.

d. The capability to issue and respond to I-S/A AMPE congestion control commands to temporarily inhibit other I-S/A AMPEs from attempting to transmit lower than FLASH precedence traffic to the I-S/A AMPE. The congestion control commands shall be automatically implemented. For control in crises each I-S/A AMPE shall automatically command other I-S/A AMPEs to cease sending traffic to user terminals connected to the commanding I-S/A AMPE which have terminated operations. The I-S/A AMPE operator shall have the capability to override these commands and shall have the capability to implement the control.

3.3.4.2 Routing Control

The I-S/A AMPE shall provide routing control capabilities to respond to line and subscriber outages or relocation of a subscriber. The I-S/A AMPE which implements a routing control shall notify the MC of the action. Provision shall be made to permit all appropriate routing tables or data bases at PSNs and other I-S/A AMPEs to be notified by an operator of routing controls, without the aid of the MC. Different types of routing actions shall be provided and the control shall include as a minimum:

a. A control to automatically, or upon operator demand, route messages to predefined alternate addresses (terminals). This control shall be implemented automatically in the event of a subscriber line or terminal failure or serious impairment. The capablility shall be provided to permit the operator to specify (as the parameters which initiate the automatic control): (1) A degree of circuit impairment, and; (2) A time period (operator selectable from zero to 30 minutes) during which this impairment exists. In addition, the I-S/A AMPE shall be capable of storing an alternate address for each subscriber.

b. A subscriber line routing control to transfer messages to the alternate path of dual-homed subscribers upon operator command. This control would be employed in the event of subscriber line failure. The primary serving I-S/A AMPE shall send the routing change to the MC.

c. An alternate routing control in the event of a destination I-S/A AMPE or user failure/relocation. In the case of failure of a destination I-S/A AMPE or user, the source I-S/A AMPE shall be capable of utilizing "prestored" routing table updates. These tables shall be capable of being electrically transmitted utilizing the MC function. Such transmission will be encrypted and will have authentication policies and safeguards to prevent malicious or accidental modifications of routing tables. Each I-S/A AMPE shall, upon operator command, be capable of redirecting all traffic originally destined to the failed I-S/A AMPE or user to a specified alternative.

3.3.5 Status Monitoring and Performance Assessment

Status monitoring and performance assessment provides data on the I-S/A AMPE, subscribers, transmission media, and network to determine the status of the system as it is currently operating and the performance over an extended period of time.

3.3.5.1 Status Monitoring

The I-S/A AMPE subnetwork is composed of individual facilities where improper operation may cause network disruptions. Improper operation results in two categories: impaired operation, in which the sub-network or element is capable of operation but not within its rated operational parameters; and an outage, in which the sub-network or element is not operable. Status monitoring is intended to detect such conditions and, in addition, provide information on the operational status of redundant equipment. Change of status events shall be reported immediately to the I-S/A AMPE operator. The capability shall be provided to have these reports automatically forwarded to the MC.

3.3.5.1.1 I-S/A AMPE Status Monitoring

3.3.5.1.1.1 Impairment/Outage Condition

The status monitoring function shall provide the capability to identify when the I-S/A AMPE is in an impaired or outage condition. I-S/A AMPE status shall be considered to be impaired when the I-S/A AMPE fails to serve all connected subscribers, is not capable of maintaining its rated throughput, or cannot provide all services. The impairment monitoring and reporting shall be based on a setable threshold, adjustable over the range from 70 to 100 percent. The I-S/A AMPE shall be in an outage condition when it cannot pass traffic.

3.3.5.1.1.2 Equipment Status

The status monitoring function shall provide the capability to identify outages in I-S/A AMPE equipments. Examples of typical equipment items for which status is required are: Processing Units, Memory, Disk, Console, I/O Devices, and Scanners.

3.3.5.1.1.3 Hazardous Condition

The status monitoring function shall provide the capability to identify hazardous operating conditions. A hazardous operating condition exists when an I-S/A AMPE equipment failure occurs and any further failure of this type of equipment will result in I-S/A AMPE failure or impairment.

3.3.5.1.2 Subscriber and DDN Access Line Impairment and Outage

The status monitoring function shall provide the capability to detect when subscriber and access lines are in an impaired or outage condition. A subscriber or access line is defined as the transmission media and all line hardware associated with it, (e.g., cryptographic equipment and modems). A subscriber or access line shall be considered impaired when it fails to operate at rated speed and/or rated error rate. The subscriber or access line is considered out of service when it is incapable of passing any traffic.

3.3.5.1.3 Equipment Status

The status monitoring function shall provice the capability for the I-S/A AMPE to identify outages in the subscriber and access line equipment. Examples of typical equipment items for which status is required are: cryptographic equipment and modems.

3.3.5.1.4 Subnetwork Status

The MC will continuously monitor subnetwork status from a combination of operator and automatically generated reports from the I-S/A AMPE operator to the MC. The sub-network status reports will include I-S/A AMPE and subscriber outage or impairment status, congestion reports, traffic alternate routes in effect and detected sub-network error conditions.

3.3.5.2 Performance Assessment

The I-S/A AMPE shall provide a capability to assess its performance and that of all connected lines. The I-S/A AMPE shall be capable of reporting substandard performance characteristics to the local operator and to the MC. This shall be accomplished in real time on an exception basis, i.e., when thresholds are exceeded. The thresholds shall be setable for each channel and parameter. Upon request from the operator or the MC, individual parameters or predetermined groups of parameters, shall be reported.

3.3.5.3 Traffic Header Statistics

The I-S/A AMPE shall be capable of providing a complete record of traffic activity from its history records. This capability shall not interfere with the throughput capability of the on-line I-S/A AMPE. This capability shall be available to produce, within a two day time period from request, an extract of any 24 hour period of history files. This capability shall not have a significant impact upon the workload of the I-S/A AMPE personnel (i.e., require no more than five minutes of any one hour period dedicated to accomplishing this task). The traffic statistics to be extracted shall be modeled after the ASCs Header Extract Program, the contents of which are shown on Table 3.3.5.3. This extracted information shall be transmitted to the MC for further processing.

3.3.5.3.1 Traffic Statistics Processing

A traffic statistical program package shall be developed and contain all the applicable data presently contained in the DCS Switch Profile, Record Communications Report (see Section 40.0). These programs will be run on the processors at the MC. The traffic statistical package will, in addition to the above, satisfy the requirements outlined in 3.3.5.3.1.1 through 3.3.5.3.3.

3.3.5.3.1.1 Total Traffic Volume

Data on subscriber access lines are received and transmitted in units of messages, line blocks, or characters. This data shall be listed and shall include the total number of incoming and outgoing data units for each subscriber line by R or Y community and for DDN access line(s). DDN access line units shall be packets and the total number of bits transmitted and received. The statistical program package shall record the number of messages and lineblocks that are received and transmitted over a specified time period, broken out by channel, classification, precedence, language and media format, format or media conversions, PLA/RI/LA conversion or any combination of these breakouts.

3.3.5.3.1.2 Busy Period Traffic Volume

The statistical program package shall determine each I-S/A AMPE's busy hour based on the traffic sent and received by its subscribers. It shall include the peak volumes for each trunk and subscriber access line and busy hour total for each destination I-S/A AMPE. Totals shall include traffic on queue for output delivery and on intercept and overflow storage as appropriate.

3.3.5.3.1.3 Multiple Addressing Factor

The average multiple addressing factor for any predefined message category or combination of categories (defined in Section 3.3.5.3.1.1) shall be computed for each I-S/A AMPE or group of I-S/A AMPE's for any time period specified up to 24 hours.

3.3.5.3.2 Speed of Service Data

Speed of service (SOS) data shall be computed for each message delivery and included in a report for each precedence level. SOS is defined as the time at which a message starts into a I-S/A AMPE until the time of delivery at the destination I-S/A AMPE. The time frame covered by the report shall be specified by the operator. The mean SOS shall be reported for each I-S/A AMPE pair by precedence. The messages that had the maximum SOS and the minimum SOS shall be listed. The Header Extract Records for these messages shall also be reported.

3.3.5.3.2.1 Network Delay

The MC is to report the same data for Network Delay that is reported for SOS. Network Delay is defined as the elapsed time between an EOM received at an I-S/A AMPE until the message is queued for output at the destination I-S/A AMPE.

3.3.5.3.2.2 SOS & Network Delay Matrix

The MC will report for any specified time period, up to 24 hours, both the mean SOS and the mean Network Delay experienced between each I-S/A AMPE pair by precedence.

3.3.5.3.3 Message Length

The average message length, by precedence, of all Formal Message Service (FMS) traffic during the 24 hour sample shall be determined.

Table 3.3.5.3. Header Extract Record Format

CHARACTER POSITION	DESCRIPTION	NORMAL CONTENTS

1	Message Precedence	Y,W = [Y = Emergency Command Precedence,]
		[W = CRITIC]
		Z = Flash
		O = Operational Immediate
		P = Priority
		R = Routine

2	Input Language Media Format	Teletype = A, F, G, Q, R, or T Data Pattern = C or S Mag Tape = B, D, or I
3	Output Language Media Format	Same as character position 2

4	Message Security	M = Special
		T = Top Secret
		S = Secret
		C = Confidential
		R = Restricted
		E = EFTO
		U = Unclassified

5	Originating Switch Designator	ASC Entry Switch
6	Blank	--
7	Input Channel Type	
8-14	Originating Station Routing Indicator	See AMIE Tributary Listing
15-18	Originating Station Serial Number	Numeric value, zeros for test messages
19-21	Message Length	Length in line blocks
22-28	Time of File	Ordinal date and time received from originator
29-35	Time of Transmission	Date and time of entry into AUTODIN
36-42	Start of Message In	
43-47	End of Message In	These fields give start and stop times of message processing
48-54	Start of Message Out	
55-59	End of Message Out	

Table 3.3.5.3. Header Extract Record Format for ASCs

CHARACTER POSITION	DESCRIPTION	NORMAL CONTENTS
60-61	Routing Indicator Count	If more than one destination is processed by a single transaction, there is one record for each destination and this field is numbered consecutively from 01 to n.
61-68	Destination Routing Indicator	See AMIE Tributary Listing
69-71	Input Channel Number	Numeric or codes, SVM, ICI or IMI
72-74	Destination Number	ASCs code for destination
75	Reporting Switch Designator	Designator for switch making the transaction.
76-78	Output Channel Number	Numeric, ICO, or IMO
79	Output Channel Type	
80	Content Indicator	Type of transaction

3.3.5.3.4 I-S/A AMPE Load and Throughput Data

Load data shall be gathered on a regular and as required basis (regular interval to be established by operator console command). Occurrences of established thresholds being exceeded shall be forwarded to the MC. The purpose of this data is to provide real-time statistics on the utilization of the I-S/A AMPE resources and to surface throughput problems as they occur. This data shall be reported to the operator and the MC. The peak 15 second period in each hour, amount of traffic throughput in each hour, and the average throughput per hour, shall be reported when requested by the MC.

3.3.5.3.5 Access Line Backlog Data

Access line backlog thresholds shall be adjustable and shall be determined based on an analysis of network performances and operational procedures. When the traffic threshold for a line is exceeded, the operator shall receive notification messages which include number of messages, volume, and time of occurrence. This data shall be accessible to the operator by line, precedence, and Language Media Format (LMF).

3.3.6 Reporting

3.3.6.1 DCAC 310-55-1 Reporting

The I-S/A AMPE is to be designated as a DCS Reporting Station as defined in DCAC 310-55-1, Status Reporting for the Defense Communications System. In this capacity, the I-S/A AMPE subnetwork, equipment, trunk and subscriber outages shall be reported to DCA in accordance with DCAC 310-55-1. This reporting by the I-S/A AMPE shall be automated. Report preparation shall be computer assisted to minimize operator workload and participation in all but the decision making process.

3.3.6.2 MC Reporting

The I-S/A AMPE shall transfer performance assessment and status data to the MC for system control, billing, and planning purposes. This data shall be reported real time, at operator specified periods and on request depending on the nature of the data. For example, real-time reporting would be associated with threshold violations. Periodic reports would be the transfer of statistical data at regular time intervals, depending on the collection method and information requirements. On request reporting shall be provided to accommodate MC special requests for additional information or transfer of statistical data on a real-time rather than a periodic basis for purposes of operational direction and control under crisis conditions. The I-S/A AMPE shall notify the MC of changes in status of the access lines and I-S/A AMPE major equipments.

3.3.6.3 Subscriber Reporting

The I-S/A AMPE shall be responsible for reporting subscriber status to the MC. Subscriber utilization data shall be collected continuously and forwarded by statistical report message daily to the MC. The data, based on all message deliveries for each radio day (Raday) and sorted by Originating Station Routing Indicator (OSRI), shall include: reporting I-S/A AMPE, originating I-S/A AMPE, total number of messages, total number of lineblocks, total number of high precedence messages, total number of high precedence lineblocks. Multiple deliveries of the same message shall be counted once for each delivery.

Subscribers will provide reports to the connected I-S/A AMPE on outages and changes in equipment status which affect the transmission of message traffic to or from the I-S/A AMPE. The I-S/A AMPE shall forward these reports to the MC.

3.3.6.4 DCS Message Quality Control Data

The I-S/A AMPE shall record and report statistics on messages rejected for specified reason codes and other data necessary to implement the DCS Message Quality Control Program as prescribed by ACP 121 US Supp-1. It shall also be responsible for generating Communication Improvement Memoranda (CIMs) to subscribers for rejected messages.

3.3.7 Fault Isolation and Correction (FI&C)

An integral part of each I-S/A AMPE facility shall be a FI&C Capability (FICC) to monitor, test, and substitute circuits or equipments connected to the I-S/A AMPE. The FICC shall include:

a. A circuit configuration data base containing the circuit identification number and identifying the various components comprising the circuit.

b. Circuit quality monitor and alarm indication of circuit degradation or outage.

c. Rapid, remote access to circuit segments for loopback and testing.

d. Automatic fault isolation using loopback, remote test equipment and software routines.

e. Semi-automated switching for replacing defective equipment or circuits.

The goal of the FICC is to create an environment which will maximize circuit and access trunk reliability, quality and speed of restoration while minimizing personnel requirements. The I-S/A AMPE FICC function shall provide both automated and manual operations on all circuits connected to the I-S/A AMPE. All security requirements shall be maintained during these operations. The operator will be provided 4-wire AUTOVON access and other switched voice networks as appropriate to establish coordination with other I-S/A AMPEs, PSNs, ASCs, subscribers, and the MC as required.

3.3.7.1 Circuit Configuration Data Base

The circuit configuration data base shall be accessible from the I-S/A

AMPE operator console and shall depict the terminal to I-S/A AMPE circuit configuration including identification of: the subscriber, critical parameters, each major equipment item in the circuit, and test points or loopback points in the circuit. The purpose of the circuit configuration data base is to provide a ready reference for the operator in performing fault isolation and in directing repair activities. Spare assets shall also be described in the data base.

3.3.7.2 Circuit Quality Monitor

Each circuit shall be provided with both local and remote monitoring capability to detect abnormal conditions and equipment alarms. Each malfunction shall be displayed at the operator console and shall identify the condition by circuit number. Greater detail regarding the status of the equipment in the malfunctioning circuit shall be displayed upon request by the operator.

3.3.7.3 Remote Access to Circuit Segments

Remote access to circuit segments shall be provided either through inherent capabilities of the circuit elements (cryptographic equipment, modems, terminals, etc.) or via auxiliary components under control of the operator. This access shall provide for loopbacks and the connection of requisite test equipment.

3.3.7.4 Automatic Fault Isolation

Upon receipt of a fault indication on a circuit, the operator shall be able to activate automatic fault isolation routines which initiate a series of loopbacks toward the I-S/A AMPE, and, in conjunction with remotely controlled test equipment, isolate the circuit segment or equipment causing the malfunction.

3.3.7.5 Semi-Automated Switching

Each I-S/A AMPE facility shall be provided with semi-automatic switching which will allow rapid restoration of service once a fault is located. Upon command from the console operator, spare equipment or circuits can be put on-line to replace the faulty element. All operational circuits shall be accessible and permit switching, monitoring and testing. In particular, the semi-automated switching shall support:

a. Channel swapping (Red or Black)

b. Equipment swaps (modem, crypto, timing source)

c. Circuit testing (new subscriber acceptance)

d. Spare channel capability

(1) Between the I-S/A AMPE and the serving Primary Technical Control Facility (if applicable)

(2) For software testing

e. Phase III rehome capability (DCA OPLAN 1-79)

f. AUTOVON and Public Telephone and Telegraph (PTT) dial-up and restoral capability

g. Subscriber community separation.

3.3.7.5.1 Red/Black Isolation

The requirements of MIL-HDBK-232 and of DoD manual C-5030.58M, Chapter 3, paragraph 3b(6), shall be met for Red/Black isolation.

3.3.7.5.2 Subscriber Community Separation

Provision shall be made to provide appropriate separation of subscriber communities. For example:

a. Red Patch Frame: GENSER U.S. and Allied subscribers with the capability to preclude inadvertent cross connection of U.S. and Allied channels.

b. Yellow Patch Frame: DSSCS subscribers only with the capability to preclude inadvertent cross connection of selected compartmented DSSCS subscribers.

c. Red and Yellow Frame Separation: No cross connection capability.

3.3.7.6 Interface with Technical Control

The I-S/A AMPE will be provided an interface with appropriate elements of the DCS serving Technical Control where applicable. This interface shall be used by the I-S/A AMPE to monitor fault alarms, threshold violations, and circuit, trunk and communications equipment failures and HAZCONs that may affect the I-S/A AMPE connectivity to the ASC, PSN, or subscribers.

3.3.8 Billing Data

The I-S/A AMPE shall maintain data to support both billing by connection and billing by utilization. (The Government will select one or the other scheme. Even if not selected for billing purposes, utilization data will have engineering and management value.)

3.3.9 I-S/A AMPE Internal Control

3.3.9.1 Operator Control Function

The operator control functions provide the I-S/A AMPE with all operational services and man-machine interfaces. The I-S/A AMPE console operator control functions shall provide for the following:

a. Control of programs, 1) system start-up, and 2) system loading procedures.

b. Display, print, and/or modify data base entries.

c. Control network operating parameters such as message routing, traffic thresholds, time-out values and reroute plans.

d. Display and recording of I-S/A AMPE performance, status condition alarms, and switchover to backup facilities.

e. Placing units on or off-line and forcing change-over to redundant units.

f. Monitoring status of the I-S/A AMPE, backbone access line(s), subscriber lines, and initiating required action in response to status changes including:

(1) Channel out of service both send and receive immediately.

(2) Channel out of service either send or receive immediately.

(3) Channel out of service receive following receipt of current transmission.

(4) Channel out of service receive following receipt of current message.

(5) Channel in service send, receive or both.

(6) Display and set input and output Channel Sequence Numbers (CSNs).

(7) Generate by command a cancel (CAN) or reject message (RM) control on any connected channel.

g. Display of current FICC connection configuration.

h. Control of local test initiation.

i. Report generation in response to local requests and requests from the MC.

j. Display of current traffic controls.

k. Coordination with other IAS Network Elements.

3.3.9.2 Failure Recovery Management

Failure recovery management is the ability of the I-S/A AMPE to perform recovery from a system outage and includes initialization, reload, restart, and reconstruction of system files to a secure state. Initialization capability shall be provided which will establish all control measures for the correct operation of the equipment. The I-S/A AMPE shall maintain a backup for the reconstruction of system files. For restart or reload the I-S/A AMPE shall securely provide for reload of the system generation software and applications programs, including the data base or files, to enable a restart of failed equipment or complete startup. Security attributes are prescribed in Section 3.4.

3.3.9.2.1 Automatic Recovery

The I-S/A AMPE shall have a secure graceful degradation of services and/or speed as failures occur, with automatic transfer of critical functions to reserve processor capability. If the on-line system sustains a failure all appropriate peripheral devices and communications terminating equipment shall be automatically switched to remaining processor capability. All security requirements shall be maintained during the above procedures. The I-S/A AMPE shall maintain in non-volatile memory the information describing the configuration data to securely support system restart and reload, to maintain performance statistics, and to support message tracing actions. The I-S/A AMPE shall be capable of reloading and performing an on-line recovery of undelivered traffic automatically. Notification of software failures, hardware failures, and peripheral devices failures shall be automatically directed to the I-S/A AMPE operator or to the MC, or both. Security requirements are further defined in Section 3.4.

3.3.9.2.2 Manual Recovery

The capability for similar actions to those specified in 3.3.8.2.1 shall be available with human intervention. Typical processes requiring manual intervention are:

a. Enter bootstrap loader program.

b. Enter system software from an external storage medium.

c. Enter applications programs.

d. Update all files with data from last checkpoint.

3.3.9.3 Data Base Management

Data base management includes maintaining, updating and displaying the data base. Examples of data bases include routing tables, security tables, procedure lists, subscriber or user classmarks, connectivity and configuration data, historical logs, and status data. The I-S/A AMPE shall provide the capability to securely process data base updates upon receipt from the MC, other I-S/A AMPEs and the local system control operator. A capability shall be provided to maintain data base integrity. Initiated data base changes shall be made from clearly understood input.

Data base changes shall be subjected to cross reference and validation before being made.

Data base information shall be accessible by the operator in readily understood and useful format(s). It shall be possible to provide an individual I-S/A AMPE the capability to securely restrict data base changes to either on-line or off-line changes. New information entered at the MC shall be distributed and incorporated throughout the network to all affected I-S/A AMPEs. In addition, update information entered at a particular I-S/A AMPE shall be capable of being broadcast to all other I-S/A AMPEs when the MC is disabled or disconnected. The I-S/A AMPE operator shall be notified of all data base updates prior to local implementation.

The I-S/A AMPE shall have the data base and reports generation capabilities presented in Section 50.0.

PAGE 3 - 83 INTENTIONALLY LEFT BLANK

3.4 I-S/A AMPE Security

3.4.1 General

This section establishes the security design criteria for the I-S/A AMPE hardware and software. The goal of the I-S/A AMPE is to field a system that will be accredited for the consolidated handling of Defense Special Security Communications System (DSSCS) and General Service (GENSER) message traffic now processed through AUTODIN.

The messages and data processed by the I-S/A AMPE will be of varying security levels and security compartments. Thus the I-S/A AMPE must be certified as Multilevel Secure (MLS). In order to meet this certification, the I/S-A AMPE hardware and software shall meet the criteria specified here.

As a minimum, the I-S/A AMPE shall include a trusted computing base (TCB) capable of Class "A1" certification (See Section 30) consisting of the following capabilities:

- A secure operating system and an appropriate access control mechanism certified for use in an MLS environment that provides requisite protection from:
  - unauthorized disclosure,
  - unauthorized denial of service, and
  - unauthorized alteration.
- Hardware isolation mechanisms complementary to the secure operating system and providing the requisite security necessary to meet the criteria specified in this section.

3.4.2 DSSCS/GENSER Integration

At IOC the I-S/A AMPE will be fielded as two deployments, one a GENSER only deployment for the "R" community and second, a DSSCS deployment for the "Y" and "R/Y" community. [Note that "R/Y" terminals are in fact "Y" terminals allowed to pass "R" traffic in addition to their normal "Y" traffic.] It is intended that these be two deployments of a single I-S/A AMPE development. On the network side of the I-S/A AMPE the ASC will provide "R" and "Y" separation until transition to the DDN, at which time the Blacker Program technology will be used to maintain the "R" and "Y" separation. Each deployment of the I-S/A AMPE shall be multilevel secure. The I-S/A AMPE will be subjected to extensive design proofs and testing as part of the certification and accreditation process. The Director, DCA is the GENSER accreditation authority. DIA and NSA have the accreditation responsibility for Special Intelligence (SI) handling and JCS for Single Integrated Operations Plan (SIOP) handling. Preceding the accreditation of the system, NSA will make recommendations to the accrediting authorities based on NSA's analysis and verification of the I-S/A AMPE system security.

3.4.3 Security Certification

The I/S-A AMPE shall meet the criteria of Class A1 as described in Section 30. Class A1 requires that formal methods be employed to verify the design of the trusted computing base. For details see Section 30.

It is not mandatory that the I/S-A AMPE meet the criteria of Class A2 as this class is currently considered beyond the state-of-the-art. However, aspects of Class A2 that can be accomplished should be considered for incorporation into the I-S/A AMPE. [Note: To meet Class A2, a formal analysis of the object code is required to prove that the implementation software fulfills the requirement of the security model. Also, formal methods of verification are applied to the hardware design.]

3.4.4 Cryptographic Security

The I-S/A AMPE will interface with the link encryption equipment currently fielded and in use in the DCS for subscriber terminals; this includes the KG-13, KW-7, KG-34, KW-26, and KG-84 systems. The I-S/A AMPE shall also interface with the end-to-end encryption (E^3) equipment being developed for NSA under the BLACKER program.

3.5 Performance Requirements

All performance requirements of the I-S/A AMPE specified herein shall be satisfied simultaneously unless specifically exempted.

3.5.1 Traffic Processing

The I-S/A AMPE shall process the traffic, with those characteristics and traffic load specified in paragraph 3.5.1.1. The total traffic load is specified in paragraph 3.5.1.3. The maximum allowable delay for processing an individual message or data transaction through the I-S/A AMPE is specified in paragraph 3.5.1.2. The derivation of the expected I-S/A AMPE input traffic from connected terminals is detailed in Table 3.5.1. Total traffic is derived in Figure 6(a).

3.5.1.1. Formal Message Service Traffic Characteristics and Traffic Loads

The input from Formal Message Service traffic the I-S/A AMPE shall be able to process on a sustained basis is 12.2 KBPS (19.0 line blocks per second). The length of messages is expected to be negative - exponentially distributed with a mean length of 2075 characters, (26 line blocks) (the maximum length of a message is 44,000 characters). Therefore the I-S/A AMPE shall be expected to process .73 input messages per second on the average. Twenty-five percent of input messages are expected to be multiple addressed; and given that it is a multiple addressed message the expected average of the number of addressees per message is 4.2. The expected message distribution by precedence is:

Flash and above	1%
Immediate	12%
Priority	38%
Routine	49%

The expected expansion factor for local delivery and distribution is 5 (for each message having at least one local addressee, the message must be delivered to 5 local channels). The resultant output from Formal Message Service the I-S/A AMPE shall process on a sustained basis is 50 KBPS (77 line blocks per second) which is expected to equate to 3 output messages per second.

3.5.1.1.1 Input Traffic Processing Capability

The I-S/A AMPE shall process input traffic at the sustained rate of at least 12.2 KBPS (19.0 line blocks) per second with a total connected input line load of 192,000 bits per second. After operating at the sustained input and output rates for 30 minutes processing the expected load with full input and output line capabilities, the I-S/A AMPE shall be capable of handling the following surge conditions without denying input of Formal Message Service traffic at its sustained input rate of 12.2 KBPS (19.0 line blocks per second):

a. Loss of all output availability for ten (10) minutes.

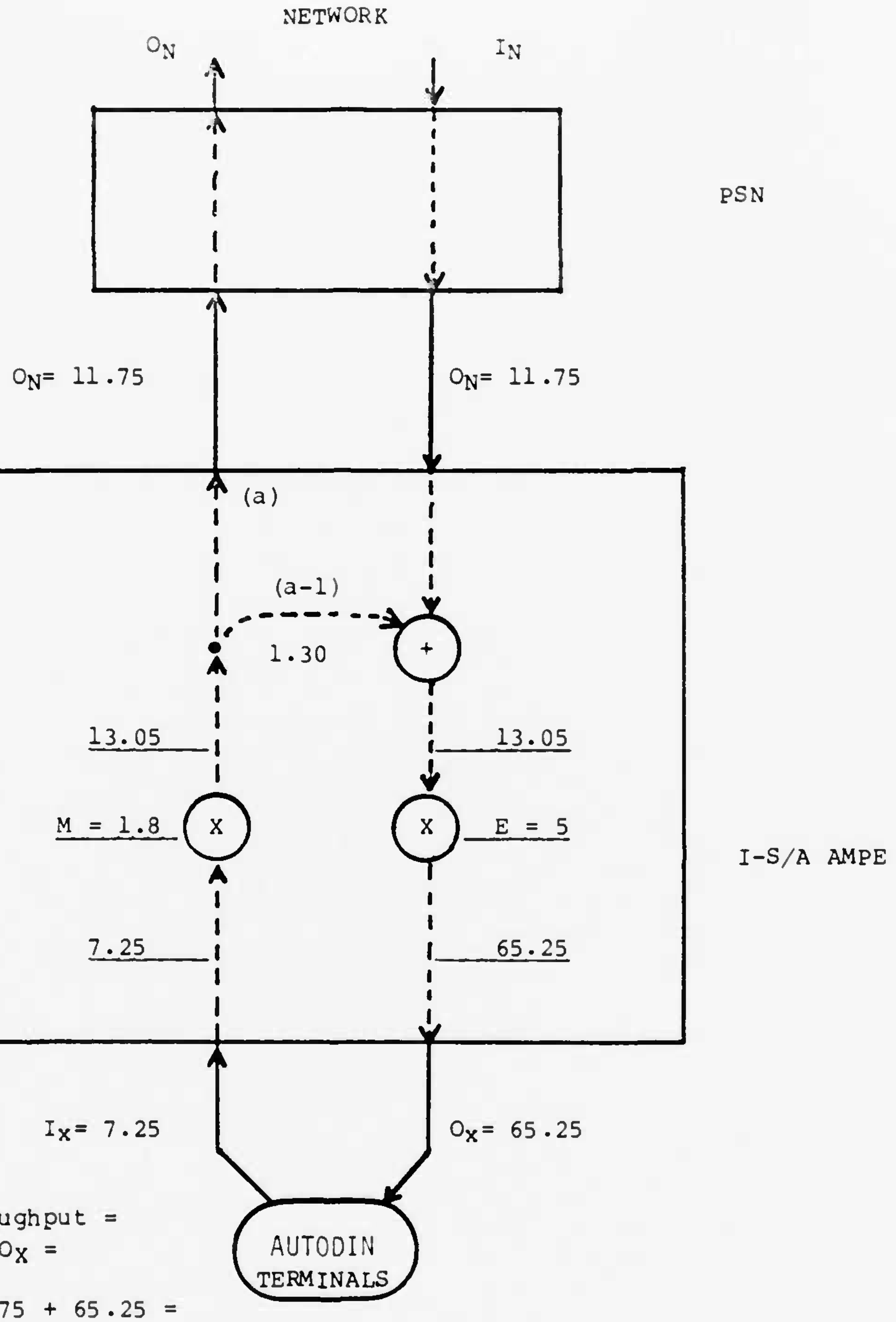
b. Surge of input load to 192,000 bits per second for 20 seconds, output line capability not impaired. All input data in this 20 seconds shall be processed and not lost.

After either surge condition the I-S/A AMPE shall be able to recover to the presurge conditions within one hour while continuing to process data at the normal specified sustained rate.

TABLE 3.5.1 DERIVATION OF TRAFFIC LOADS FROM SAMPLE DATA

1.2×10^9	Lineblock handlings per month in CONUS, end of 1980
$/ 3.45$	handlings per lineblock
$= 347.8 \times 10^6$	Originated lineblocks per month
$/ 30$	Days per month
$= 11.59 \times 10^6$	Lineblocks per average day
$\times 1.275$	Ratio of peak day to average day
$= 14.78 \times 10^6$	Lineblocks per peak day
$\times 8\%$	busy hour percent of daily traffic
$= 1.18 \times 10^6$	Lineblocks per busy hour peak day
$/ 3600$	sec/hr
$= 328$	Lineblocks/sec - 1980
$/ 72$	AMPEs
$= 4.55$	Lineblocks/sec/AMPE - 1980
@ 6%	increase per year (1.59) for 8 years
$= 1.88 \times 10^6$	Lineblocks per busy hour - 1988
$(= 1.2 \times 10^9$	(bits per busy hour - 1988)
=522	Lineblocks per sec IAS - 1988
$(= 3.34 \times 10^5)$	(bits per sec IAS- 1988)
$= 7.25$	Lineblocks per sec per AMPE - 1988

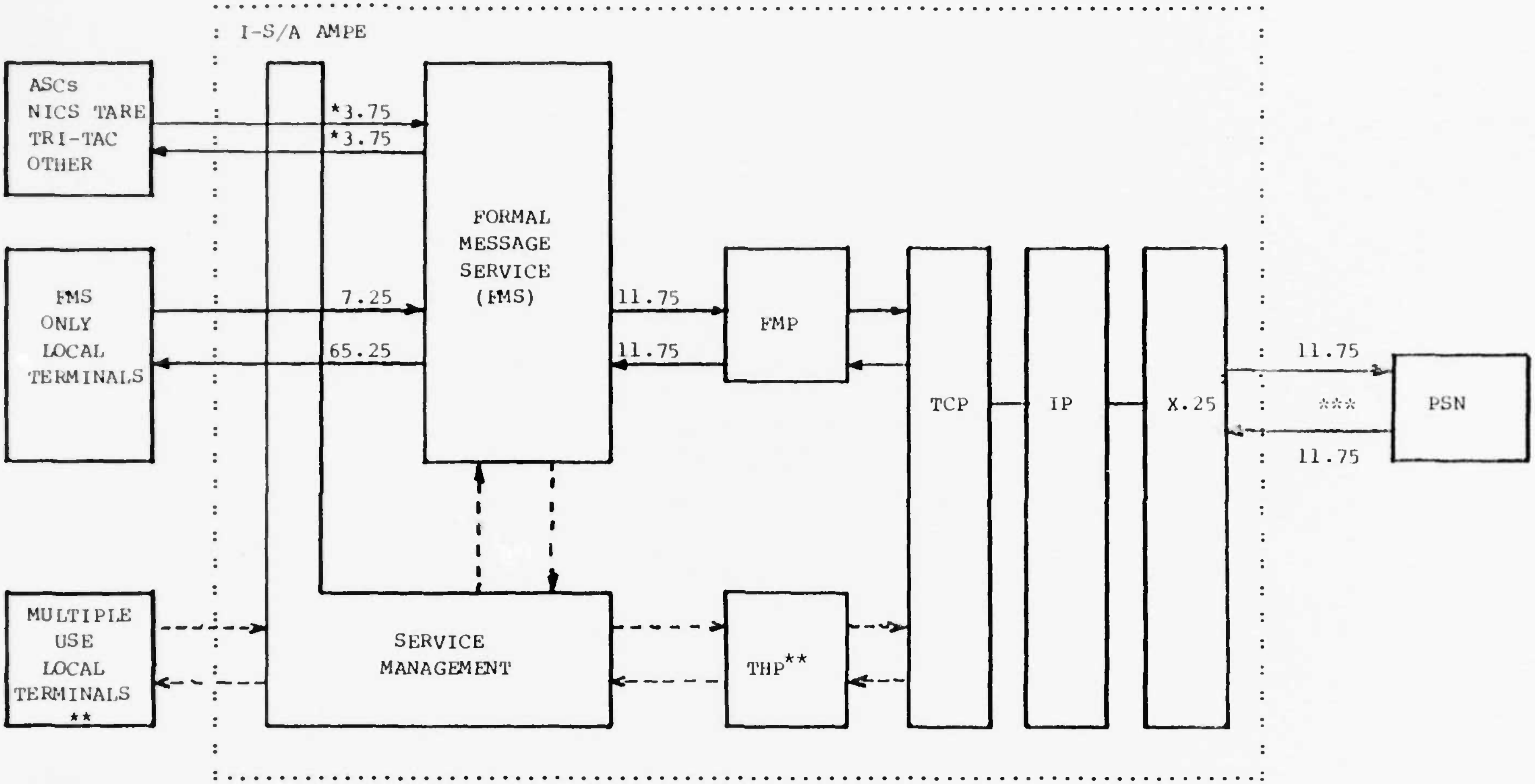
Therefore it is expected that the average connected terminal population will generate 7.25 lineblocks per second of traffic to the serving I-S/A AMPE. This figure is used as Ix, the expected terminal input load in Figure 6(a).



I-S/A AMPE Throughput =
$I_X + O_N + I_N + O_X$ =
7.25 + 11.75 +
11.75 + 65.25 =
96 Lineblocks/second

NOTE:
M = 1.8 ; Multiple Addressee Factor
E = 5.0 ; Expansion For Distribution Factor
a = .9 ; Traffic-to-Network Factor

Figure 6 (a) - I-S/A AMPE Traffic Load Handling Requirements



** - POST-IOC REQUIREMENT

ASC - AUTODIN SWITCHING CENTER   FMP - FORMAL MESSAGE PROTOCOL   THP - TERMINAL TO HOST PROTOCOL (TELNET)

TCP - TRANSMISSION CONTROL PROTOCOL   IP - INTERNET PROTOCOL   X.25- NETWORK LAYER PROTOCOL

* - FMS SHALL BE ABLE TO SEND THE INDICATED TRAFFIC TO THE ASC IN LIEU OF OTHER DESTINATIONS, THEREFORE THIS REQUIREMENT DOES NOT ADD TO THE TOTAL. *** E^3 DEVICE BETWEEN I-S/A AMPE AND PSN

I-S/A AMPE FORMAL MESSAGE SERVICE REQUIREMENTS IN LINEBLOCKS PER SECOND

FIGURE 6 (b) - I-S/A AMPE FMS TRAFFIC LOAD HANDLING REQUIREMENTS

3.5.1.1.2 Output Traffic Processing Capability

The I-S/A AMPE shall process and output traffic at the sustained rate of at least 50,000 data bits per second (77 line blocks per second) with a total connected output line capacity of 192,000 bits per second. Reduction of output line capability shall not impact on the I-S/A AMPE capability to process traffic and queue it for output at the above sustained rate (See 3.5.3 Storage Requirements). If traffic has queued up for all output lines for any reason and all output lines become available to accept traffic at their maximum rate, then the I-S/A AMPE shall be able to output traffic at the rate of the sum of the output line capabilities up to a rate of at least 200,000 bits per second while still processing new data for output at the sustained rate of at least 50,000 data bits per second (77 line blocks per second).

3.5.1.2 Throughput Traffic Processing Capability

Throughput is defined as the sum of input plus output. The I-S/A AMPE shall throughput traffic at the sustained rate of at least 61,500 data bits per second (96 line blocks per second).

3.5.1.3 Traffic Processing Delays

Traffic Processing Delay is defined as the elapsed time from time of receipt of the last element of an incoming message by the I-S/A AMPE until the message is processed and transmission is initiated for output on all applicable output lines. The transmission time into or out of the I-S/A AMPE is not considered part of the processing delay time. The individual traffic elements shall be processed within the time delays specified in the following subparagraphs while processing the total sustained input and output traffic loads specified in 3.5.1.1 above.

3.5.1.3.1 Formal Message Service Processing Delays

The processing delay for formal messages is defined as the elapsed time from the receipt of the end-of-message sentinel on input of a message until all required copies of the message are queued for output and transmission of the first data bit (if the output lines are available and not queued up). This includes all message format and heading validation, PLA to RI conversion, RI to logical address conversion as required, routing segregation, distribution and delivery determination, placement in all output queues, establishment of internal I-S/A AMPE connections where required, and start of transmission of all copies of the message (on output lines that are available and not queued up with equal or higher precedence traffic). The allowable traffic delays are specified for each precedence as follows: the maximum value of the mean processing time E(t) and the elapsed time at which the probability of completion shall be 0.95, Prob ($t \leq T = 0.95$).

PRECEDENCE	MEAN PROCESSING TIME E(t)	PROB (t=T)=0.95 T
ECP & CRITIC	0.75 Sec	1.25 Sec
Flash	1 Sec	1.7 Sec
Immediate	5 Sec	8 Sec
Priority	30 Sec	50 Sec
Routine	80 Sec	135 Sec

The I-S/A AMPE shall meet or better the above processing delays while processing the sustained load of 3.5.1.2, and while processing a message with the following characteristics:

- Message length 5,400 characters
- Two addressees - One remote (terminated on another I-S/A AMPE) and One local (directly terminated)
- Local delivery distribution expansion of 4 (i.e., to be output on 4 local channels).

3.5.1.3.2 Data Transactions to the IAS Network

Post IOC non-FMS traffic shall be exchanged with the IAS Network as data transactions. A data transaction shall consist of the receiving of a block of data from a local terminal and the conversion of the block of data to packets and the transmission of the packets through the PSN backbone. The receiving of a group of packets, combining into a block of data and the transmission of this block of data to a local terminal is also a data transaction. The I-S/A AMPE shall process data transactions FIFO by precedence. The type of traffic shall not be considered in meeting processing requirements. The internal delay for the I-S/A AMPE to process a data transaction shall be measured as follows:

a. For a block of data to be transmitted to the network: from the receipt of the last bit of data to fill the input buffer or a receipt of a request to transmit from the local terminal to the start of transmission of the first packet to the network.

b. For a group of packets from the network to be combined and transmitted to a local terminal as a block of data: from the receipt of the last packet or enough packets to make a complete block of data until the first bit of that block is transmitted to the terminal. The maximum allowable expected traffic processing delays for data transactions are specified by precedence as follows:

PRECEDENCE	MEAN PROCESSING TIME E(t)	PROB (t=T)=0.95 T
Flasn & above	100 millisec	150 millisec
Immediate	200 millisec	300 millisec
Priority	300 millisec	500 millisec
Routine	400 millisec	700 millisec

3.5.2 Connection Service

Connection time is measured from the time when the originating user of service completes tne initiation of the connection request until the connection is completeo and tne aovisement to the originator is placeo on the line. The times apply to completion of the connection internal to the I-S/A AMPE; that is, the times are for total completion of:

- Local suoscriber to local subscriber connection
- Local subscriber to local service connection

but apply only to the internal connection between the local user or local service ana the THP (TELNET) for those connections to remote network elements. The connection time includes the time requireo to verify the connection is authorizeo.

In the event the connection cannot be completea because the oestination user is busy at an equal or higher preceoence level, then the originator of the request shall be provioeo with the busy inaication within the same time as specified for tne connection completion. In the event a request for a connection is received in which the oestination user is busy at a lower preceaence level than the requestea connection, then the new connection shall not be establisheo unless the request is of flash or higher precedence; in which case the lower precedence connection shall be preempteo ano the new (higher precedence level) connection established. The connection times specified ao not incluoe the time for preemption notification. There are two oifferent preemption notifications oepending on whether the connection is for Formal Message Service or Data Transactions. If the connection being preempted was carrying Formal Message Traffic then the preemption notification shall be the cancel transmission (CANTRAN) sequence specified in JANAP 128 (H) paragraph 330, Cancelling Transmissions. The contractor shall develop the preemption notification message for Data Transactions. The I-S/A AMPE shall satisfy the following connection requirements:

PRECEDENCE	MEAN PROCESSING TIME	TIME LIMIT P(t=T)=0.95 T
Flash & above	500 Millisecongs	1 Second
Immediate	1 Secono	2 Seconds
Priority	2 Seconos	4 Seconos
Routine	2 Seconds	4 Seconds

3.5.3 Storage Requirements

The I-S/A AMPE shall have the capability to store on-line data to support Plain Language Address to RI tables, RI to Logical Address tables, formal message service traffic and other possible storage requirements in order to meet all I-S/A AMPE performance requirements simultaneously. The contractor shall calculate and define the different storage media based on the requirements specified herein and the contractor's system design and submit for government approval.

3.5.3.1 Plain Language Address (PLA) to RI Table

The PLA to RI table shall be capable of holding seventy-five thousand (75,000) entries minimum, expandable to 256,000 entries. An entry shall have an expected length of 40 characters and a maximum length of 62 characters.

3.5.3.2 RI to Logical Address Table

The RI to Logical Address table shall be capable of holding 5000 entries. Entries shall be 15 characters in length.

3.5.3.3 On-Line FMS Storage

The expected number of messages per day is thirty thousand (30,000) with an expected length of 2075 characters (26 line blocks) each. Additional data elements are required to be stored with each message to meet the requirements of 3.3 System Control and 3.2.1.6.2 History Logs and Files. The on-line storage capability of the I-S/A AMPE shall be a total of 10 days on-line traffic with the capability to expand to hold up to sixty (60) days of FMS traffic by the simple addition of more storage media. 'Simple' means there shall be no changes required to the operating system or software to accomplish the expansion. Storage media shall be removable to facilitate extended storage in an off-line manner. The contractor shall demonstrate in the design the method to expand on-line storage for government approval.

3.5.3.4 Search and Retrieval Access Times

The I-S/A AMPE shall support searches of the kinds specified in 3.2.1.7.1 as applied to the on-line FMS storage described in 3.5.3.3. While processing the sustained load specified in 3.5.1.2, a search or retrieval of any kind shall not require more than 30 minutes to be accomplished, measured from the time of operator initiation or service request until the last unit of information is queued for output.

3.5.3.5 General Storage Requirements

The contractor may deem it necessary to provide other storage capability in order to meet system performance requirements. The contractor shall specify in the system design all the different storage media and their specific use(s).

3.5.4 Processing Error Rates

The I-S/A AMPE shall meet the following processing error rate requirements:

- The probability of introducing a data error within the I-S/A AMPE shall be less than one occurrence in 10^{12} characters.
- The probability of transmission of errors originating within the I-S/A AMPE shall be less than one occurrence in 10^{12} characters.
- The probability of messages being misrouted by action of the I-S/A AMPE shall be less than one occurrence in 10^{12} messages.
- The probability of messages being lost by action of the I-S/A AMPE shall be less than one occurrence in 10^{12} messages.

3.5.4.1 Undetected Error Rate

The probability of any of the above errors occurring without detection and notification of supervisory personnel shall be less than one occurrence in 10^{12} events.

3.5.5 Availability

Availability shall be considered of prime importance in the design and manufacture of the I-S/A AMPE. The I-S/A AMPE shall automatically receive, process, and transmit user transactions in accordance with the functional requirements specified herein, and shall be capable of performing these functions concurrently 24 hours per day, 7 days per week. Availability requirements shall meet or exceed collectively the following quantitative values:

- Availability to operate without loss of service to a specific circuit of at least 0.9995
- Availability to serve 75% or more of all circuits of at least 0.9995
- Availability to process traffic on any non-failed circuit of at least 0.9995.

3.5.5.1 Recovery

The I-S/A AMPE shall provide secure automatic restart and recovery procedures (see Section 3.4) following a hardware malfunction or failure condition. The expected recovery time of the I-S/A AMPE shall have a mean of at most 5 minutes and probability of at least 0.95 completion of recovery in 10 minutes or less. During this recovery period, the I-S/A AMPE shall automatically perform the functions necessary to:

- Replace or restore hardware as necessary to configure an operational system

- Reconstruct active processing files to their status prior to failure

- Restore all other software to its status prior to failure

No Formal Message Service traffic that has been accepted for processing prior to the time of I-S/A AMPE failure or malfunction shall be allowed to be lost. There is no requirement for protection of Bulk Data Transfer Traffic during recovery. All directly connected users of the I-S/A AMPE shall be automatically advised of any failure and recovery wherein there was a possible denial of service or loss of data.

3.5.6 Degraded Operation

In the event of a hardware failure, unavailable output circuit, or other condition that decreases the processing capability of the I-S/A AMPE or reduces throughput, a degraded mode of operation shall be available. The degraded mode of operation shall process input data according to precedence (as described in 3.2.1.3.4 and 3.2.2.5.1) and capability, with processing of lower precedence traffic being denied as processing capability decreases. In this degraded mode of operation, the I-S/A AMPE shall process the highest precedence incoming traffic to the maximum extent possible. Any degration operation shall not violate the requirements of Section 3.4.

3.6 Requirements for Software and Firmware Development

All software and firmware developed for the I-S/A AMPE shall meet the requirements specified below. Software and firmware shall encompass operational programs, diagnostic programs, operating test, emulation firmware, and all support software.

All software and firmware the contractor develops or uses for the maintenance, operation, and testing of the I-S/A AMPEs shall be delivered to and become the property of the Government.

All security-related software and firmware shall be classified in accordance with the Security Classification Guidelines.

If the I-S/A AMPE is implemented using firmware developed by the contractor, the contractor shall provide an assembler and simulator as software deliverable items. The assembler, simulator, and any other micro support software develcped or used shall be host independent.

All software and firmware shall be designed and developed in accordance with MIL-STD-483, supplemented by MIL-STD-1679, and the security requirements, Section 3.4. In addition, the requirements set forth below shall apply. Any deviation from these requirements shall require approval by the I-S/A AMPE Program Manager. The following paragraphs apply to specific wording or requirements of MIL-STD-1679.

3.6.1 Modifications to MIL-STD-1679 (Navy)

The contractor shall comply with all requirements of MIL-STD-1679, as modified below.

a. To improve readability and clarity, the contractor may replace the phrase "weapon system" with the phrase "communications system" throughout MIL-STD-1679. Note, however, that Section 3.1 of MIL-STD-1679 includes communications systems within the scope of the definition of "weapon system".

b. Page 6 Section 4.3: delete first sentence and replace with the following: "Communication system software shall be coded in a high order programming language (HOL) approved by the procuring agency."

c. Page 10 Section 5.3.6: replace sentence with the following: "Recursive procedures or routines shall not be used unless approved by the government on an individual basis."

d. Page 15 Section 5.5.3: replace sentence with the following: "Communication system software shall be coded in a high order programming language (HOL) approved by the procuring agency."

e. Page 16 Section 5.5.4: Add the following at the end of the paragraph: "The use of patching shall be minimized."

f. Page 16 Section 5.5.5: Delete section.

g. Page 16 Section 5.5.6.1 line 4: delete the phrase ", if available."

h. Page 21 Section 5.10.2.2: delete the last sentence.

i. Page 22 Section 5.10.3.1: replace section with the following: "There shall be zero unresolved software errors."

3.6.2 Software and Firmware Management

a. The contractor shall institute a software and firmware quality assurance program in accordance with MIL-STD-1679 (See Section 4).

b. The contractor shall perform configuration management in accordance with MIL-STD-1679 (See 4.1.1).

c. The contractor shall perform sufficient development testing to realistically measure program performance and development progress (See Section 4).

d. The contractor shall produce documents to substantiate security verification prior to the Program Design Specification (PDS) DI-E-2138 specified in paragraph e. Required documents are specified in Section 3.4.

e. The contractor shall produce the following documents in accordance with MIL-STD-1679:

Contract Data Requirement	DID	Document Order
Software Development Plan	DI-A-2176	1
Software Quality Assurance Plan	DI-R-2174	1
Software Configuration Management Plan	DI-E-2175	1
Program Performance Specification (PPS)	DI-E-2136	2
Program Design Specification (PDS)	DI-E-2138	3
Program Description Document (PDD)	DI-S-2139	3
Data Base Design Document (DBD)	DI-S-2140	3
Computer Program Test Plan	DI-T-2142	4
Computer Program Test Specification	DI-E-2143	5
Operator's Manual (OM)	DI-M-2145	5
System Operator's Manual (SOM)	DI-M-2148	5
Preliminary Program Package Document	DI-S-2141	5
Computer Program Test Procedures	DI-T-2144	6
Computer Program Test Report	DI-T-2156	7
Software Change Proposal(SCP)/Software Enhancement Proposal (SEP)	DI-E-2177	as needed
Computer Software Trouble Report (STR)	DI-E-2178	as needed
Final Program Package Document	DI-S-2141	8

f. The contractor shall provide step-by-step operating instructions for message preparation, retrievals, traffic management and all facets of on-line and off-line system operations.

The above items shall be produced and delivered in the order specified. Program design documentation (PDS, PDD, DBD) shall be completed prior to initiation of coding. See 4.7 for security related quality assurance.

3.6.3 Programming Requirements

In addition to the programming requirements of MIL-STD-1679 and the Security Section 3.4., the following shall apply:

a. I-S/A AMPE software shall be written in a high order language in accordance with DoDI 5000.31. The high order language selected by the contractor shall be approved by the Government Program Manager prior to its use. Minimal use of assembly language is permitted when absolutely necessary due to software dependencies on target machine architecture; however, no more than 10 percent of the I-S/A AMPE software written in assembly language is a goal.

b. Software and firmware design requirements shall be developed by a systematic, top-down methodology.

c. The contractor shall implement code in a top-down manner that permits incremental development and test of software.

d. The contractor shall utilize structured programming techniques.

e. The contractor shall utilize common code and common procedures to the maximum extent practical.

f. Software procedures and routines shall be serially reusable.

g. Instruction modification during execution shall be prohibited.

h. In-line documentation shall be included in software and firmware and shall follow those guidelines set forth in 3.6.4

i. Software procedures and routines shall use the general registers (or other conventional methodologies) in a uniform manner for procedure and routine linkage, parameter passing, and error information.

3.6.4 Documentation Requirements

In addition to the documentation requirements of MIL-STD-1679 and the security Section 3.4., the following shall apply:

a. The contractor shall document software and firmware in a clear and concise manner.

b. Each software and firmware module shall contain a preamble of comments describing its function, interfaces, inputs, outputs, number of lines of code and any other information deemed necessary to the understanding of the module. In addition, the preamble shall contain a list of those modules which call the described module and those modules called by the described module.

c. Software and firmware shall use block comments wherever appropriate to amplify the meaning of sections of code. Block comments should not merely restate in-line comments but should explicate the meaning of the commented code.

d. Block comments and preambles shall be delineated from the software and firmware by special character sequences for increased readability and possible later extraction.

e. In-line comments shall be clear and informative, and they shall not simply restate the instruction. In the case of assembly and firmware assembly language programs, an in-line comment shall be placed on each line of code.

3.7 Hardware System Requirements

3.7.1 Hardware Definition

The I-S/A AMPE hardware shall consist of data processing equipment and peripherals necessary to perform message storage and switching, operator and service position controls and displays, fault isolation and correction capability and required connectivity among these elements to meet the description and requirements specified in this document. The I-S/A AMPE development shall not include cryptographic, terminals, or transmission multiplex equipment. Except where otherwise stated, the I-S/A AMPE equipment shall meet the requirements of MIL-E-4158E, General Requirements for Ground Electronic Equipment, MIL-STD-188-114, Electrical Characteristics of Digital Interface Circuits, and MIL-STD-188-100, Common Long Haul and Tactical Communication System Technical Standards.

3.7.2 Modularity

The I-S/A AMPE equipment shall be modular in nature to permit a fully functional I-S/A AMPE to be installed at each location that will be efficient in utilization of resources, be a readily expandable facility, and permit gradual degradation in the event of component failure(s).

3.7.2.1 Reliability Through Modularity

The modularity of the I-S/A AMPE equipment shall be implemented in a manner that will enhance the reliability of the overall performance. Failure of a module shall not cause either other modules performing the same function or other modules interfacing the failed module to become inoperable. Sufficient modules shall be used to duplicate functions so failure of a single module shall not cause a complete I-S/A AMPE outage.

3.7.2.2 Sizing

The I-S/A AMPE, with its modular nature, shall be implemented in such a manner that an installed I-S/A AMPE can change sizing in terms of subscriber connectivity and/or throughput capability without replacing or grossly modifying existing equipment. Further the I/S-A AMPE shall have an inherent growth reserve of 25% (percent) at IOC. The contractor shall demonstrate how the design provides for; increase in subscriber terminations, increase in throughput, and the 25% inherent growth reserve. The minimum number of subscriber terminations shall be thirty-two (32) expandable in increments of 16 up to 64 subscribers.

3.7.3 Memory

Criteria of interest for the I-S/A AMPE memory are maximum expansion size of physical memory, maximum addressability capability of virtual memory, increment size, nominal cycle time, and cost per bit. The hardware structure of the I-S/A AMPE memory shall provide for protection against errors and memory loss of critical data (program, routing tables, etc.). For example, this may be implemented with nonvolatile memory.

3.7.3.1 In-Transit Storage

In-transit storage for the I-S/A AMPE shall be developed such that there will be no loss of messages due to a hardware or software failure. The storage is to be multi-tiered to permit rapid access for current messages being processed and a secondary storage for preserving traffic on queues while a circuit is busy and not loading the main memory or processor, and some form of off-line storage which does not require rapid access for historical purposes.

3.7.3.2 Message Storage for Retrieval

Sufficient capacity of storage or capability in terms of off-line storage shall be developed for the I-S/A AMPE to preserve for a period of up to 60 days (determined on a site-by-site basis) the traffic processed by the I-S/A AMPE. This storage shall be in a form that is usable on-line as specified in 3.5.3.3.

3.7.3.3 Memory Access

The I-S/A AMPE hardware implementation shall be of a nature which enhances the capability to restrict access to certain portions of memory, such as a ring architecture.

3.7.4 Fault Isolation and Correction Capability

The I-S/A AMPE FICC shall provide automatic testing and a default manual testing capability, circuitry termination and rerouting, and reporting. The FICC shall be designed and implemented as an integral part of the I-S/A AMPE. An objective of the FICC is to minimize the human actions required. The FICC shall comply with MIL-STD-188/310, Subsystem Design and Engineering Standards for Technical Control Facilities. The I-S/A AMPE FICC shall provide on a per termination basis:

- o Circuit configuration data base;

- o Immediate alarm indication of circuit degradation or outage;

- o Rapid, remote access to any circuit segment for loopback and testing;

- Automatic fault isolation using loopback, remote test equipment and software routines;

- Keystroke speed of patching (replacing individual defective equipment or facilities);

- Positive verification of repaired operation;

- Generation of necessary logs and performance data to facilitate network management.

3.7.4.1 Connection Capability

The I-S/A AMPE FICC shall provide for the secure termination of communications circuits, associated cryptographic, modem and other related communications hardware associated with per line communications circuits and shall provide "normal through" and reconnection capabilities for routine and failed hardware situations. See paragraph 3.3.6 for further requirements.

3.7.4.2 Testing

The I-S/A AMPE FICC shall provide automatic testing with manual testing fallback capability. Automatic testing shall enable the operator to perform automatic line testing (e.g., to specify the line and test to be performed) and obtain the results of that test from a console position. The console shall provide the capability of selecting a circuit in the Red, Black, or modem area for testing; however security concerns require strict segregation of Red and Black, thus the design shall ensure that the FICC is working Red or Black but never both simultaneously. Manual Testing provides the operator the capability and test equipment to physically access lines and perform appropriate tests. Test equipment shall meet minimum performance standards of DCAC 300-175-9. The I-S/A AMPE FICC shall have rapid, remote access to circuit segments for loopback and testing, and automatic fault isolation using loopback, remote test equipment and software routines.

3.7.4.3 Reporting

The FICC will be responsible for reporting as required by DCAC 310-55-1. Therefore, the FICC shall provide a semi-automated capability to provide required reports (See paragraph 3.3.5).

3.7.5 Operational Characteristics (See additional discussion in Section 3.4, Security)

3.7.5.1 Availability

The capability of the I-S/A AMPE system to perform traffic handling functions shall be a minimum of 99.95 percent with the I-S/A AMPE in continuous operation. This may be accomplished by redundancy of processors. Redundant processors may be implemented using one processor for communications functions while another performs background, statistical and other 'housekeeping' functions, operating processors in parallel, or splitting processing among multiple processors.

3.7.5.2 Reliability

The I-S/A AMPE equipment shall have features to maintain high levels of reliability in terms of both maintaining operation and maintaining correct functioning. This will be implemented through mechanisms for detecting failures such as a watchdog timer, automatic restarts and recovery, capability to automatically reconfigure and operate in a degraded mode, internal data checks for data transfers, and sufficient I/O channels and checking. Failure of a single peripheral shall not stop operations.

3.7.5.3 Maintainability

The I-S/A AMPE shall be modular in both logic and hardware implementation. This will assist in providing a capability to perform maintenance on a portion of the equipment while the remainder is still in operation. Maintainability features shall be provided to maintain a Mean Time to Repair (MTTR) for any failure of less than 1 hour.

3.7.5.4 Interrupt Structure

Due to the multilevel precedence nature of traffic, the processor should possess a multilevel vectored priority interrupt mechanism with context switching handled in hardware under control of the trusted computer base. There shall also be a secure capability to inhibit interrupts to prevent erroneous operations during operations such as updating routing tables. See Section 3.4, I-S/A AMPE Security.

3.7.5.5 Instructions in Hardware

To improve reliability and minimize operation times, implementing operations in hardware or firmware shall be implemented where it is feasible and does not detract from system flexibility, such as code conversions, recognition of special characters, parity or CRC checking, flag detection, and operations with bit transparent protocols.

3.7.5.6 Cycle Times

A significant criteria is the instruction operation time for operations which will be used repetitively in the I-S/A AMPE software.

3.8 Design and Development (Also see Section 3.4, I-S/A AMPE Security)

3.8.1 Modularity

The concept of modularity shall be considered of prime importance in the design and development of the I-S/A AMPE. Modularity of software, hardware, and functional performance shall be required to permit tailoring of each I-S/A AMPE to the requirements of both the supported community of interest and the IAS network at large, and to permit smooth transition of future IAS services. At the same time, it shall assure simplicity of development and standardization of functional performance among all I-S/A AMPEs. A given I-S/A AMPE configuration shall be required to include only those service processing functions necessary to support the network services provided, those communications processing functions necessary to support the user community and the service functions provided, and those communications interface functions necessary to support the communications lines and user terminal devices connected to the I-S/A AMPE. The functional structure of a given I-S/A AMPE shall be tailorable to the requirements of the I-S/A AMPE users. However, the performance or provision of each function included in that I-S/A AMPE shall be accomplished in accordance with the requirements of the functional specification.

3.8.2 Software Design

The software design for the I-S/A AMPE shall be developed under disciplined, top down, structured programming techniques in accordance with MIL-STD-1679 and DoD Directive 5000.29. Standard software shall be developed using an approved High Order Language (HOL) (See 3.6.3) or give sufficient justification to the Program Manager for using a non-approved HOL. The software shall be designed to be expandable and, to the maximum extent practical, independent of the vendor hardware.

3.8.3 Hardware Design

Design and construction of the I-S/A AMPE shall demonstrate a quality commensurate with the best commercial design practices. The hardware shall be modular in nature allowing graceful growth and enhancements and minimizing field maintenance. The hardware shall also be designed to minimize the amount of hardware modification needed to satisfy any required I-S/A AMPE packaging configurations (e.g., rack-mounted, stand alone, or transportable units). Maximum use shall be made of state-of-the-art technologies available at the time of procurement in order to fully exploit the performance, reliability, cost, size, weight, logistics, and maintenance advantages those technologies may offer. Replacement modules shall be utilized whenever practical to promote ease of maintenance, reduce downtime, and lower costs. The I-S/A AMPE shall be provided with a computer power center compatible with the I-S/A AMPE hardware proposed at each site. The computer power center shall include as a minimum an isolation transformer, circuit breakers, panelboards, computer Automated Data Processing Equipment (ADPE) branch circuits, shunt trip breakers, transient protection, and meters.

3.8.4 Commonality/Standardization

The I-S/A AMPEs shall be developed with a maximum degree of commonality in hardware and software and with a degree of standardization required to insure commonality without compromising operational effectiveness.

3.8.5 Human Performance/Human Engineering

Relevant human factors which can be identified in the context of the man/machine interface functions shall be defined and applied in accordance with the techniques described in appropriate paragraphs of MIL-H-46855. All Human Engineering inputs shall meet the applicable criteria of MIL-STD-1472 and other criteria specified in the Interface Control Document.

3.9 Maintainability and Logistics

Maintainability shall be considered of prime importance in the design and manufacture of the I-S/A AMPE. Maintainability requirements shall comply with MIL-STD-470. Maintainability requirements shall adhere to the following guidelines:

- Maintenance procedures shall be designed to be as simple and efficient as possible.

- A maintenance concept shall be developed whereby maintenance responsibility is assumed by on-site personnel to the fullest extent possible.

- Secure maintenance procedures shall be emphasized.

- A preventive maintenance program shall be defined and quantitative limitations shall be established on the frequency of required preventive maintenance.

- The Mean Time to Repair failures which would cause loss of service to all circuits shall not exceed one (1) hour.

An Integrated Logistic Support (ILS) Plan shall be prepared as part of the I-S/A AMPE development process. The ILS Plan shall adhere to the following organizational and conceptual guidelines.

3.9.1 Hardware Maintenance (Also see Section 3.4, I-S/A AMPE Security)

The I-S/A AMPE equipment shall be readily installed and maintained. It shall be subject to repair at three levels as follows:

a. Organizational Level Maintenance. This level of maintenance is defined as the maintenance which is the responsibility of and performed by organizational personnel with assigned equipments. It shall consist of inspecting, servicing, lubricating, adjusting, and replacing printed circuit cards, subassemblies, and assemblies.

b. Intermediate Level Maintenance. Intermediate level maintenance shall consist of the repair of faulty components and assemblies not considered repairable at the organizational level. It shall include printed circuit board component replacement, calibration, adjustments, soldering, and any required/scheduled preventive maintenance actions.

c. Depot Level Maintenance. Depot level maintenance shall consist of all repairs and overhaul not considered or designated as repairable at lower maintenance levels. This service shall be performed by designated depot repair facilities.

3.9.2 Maintenance Concept

Module replacement at the organizational level shall be the maintenance concept to be applied to the I-S/A AMPE. Module repair and parts replacement shall be accomplished in accordance with 3.9.1 of this specification. A level of repair analysis shall be performed in a later phase of program development and shall be used to justify a decision to repair or discard a defective module, printed circuit board or component for each maintenance action at each level of maintenance. Built-in-Test and diagnostics shall be used, where feasible, for rapid fault isolation. Fault isolation shall be achievable to the lowest replaceable module. Use of multipurpose test equipment shall be emphasized to reduce number and types of on-site inventory.

3.9.3 Software Maintenance Concept

After IAS Phasing Group processing, software changes will be forwarded to the LMD/PMO for action. Through the Configuration Control Board (CCB), the LMD/PMO will establish procedures for handling all aspects of proposed system software modifications, testing and certification of approved software changes. These procedures will include initial review and approval or disapproval. Responsibility for implementation of approved changes will reside with a centralized authority to be included in the Program Management Responsibility Transfer (PMRT) and Systems Operational Concept.

3.9.3.1 I-S/A AMPE Test Bed

Experience with AUTODIN has clearly demonstrated the need for centralized life-cycle software management and control, the need for a software development and testing facility, and the advantages of proximity between the software support staff, the management staff, and the test facility. This permits maximum responsiveness to operational needs regarding development and test efforts and reduces costs associated with travel and time. A centralized engineering and software development test bed facility is definitly required for life-cycle support of fielded I-S/A AMPE installations and will be provided by the LMD/PMO as part of the I-S/A AMPE Program. This facility will be referred to as the AMPE Support Facility (AMPE S/F). The LMD/PMO, through the contractor, will be expected to provide the first year's support. How the final life-cycle support in this area is accomplished will be decided by the LMD through coordination with DCA and the S/As. The decision will be reflected in the PMRT and must include a trade-off concerning contractor versus government support and must consider possible LMD delegation of this responsibility to other Services and Agencies. O&M planning figures and an organizational concept plan will be provided by the LMD/PMO as an input to the DCA Five Year Plan (FYP).

3.10 Design Priorities

While all requirements levied on the I-S/A AMPE are important and must be fully complied with, the following requirements should receive first priority in design and implementation.

3.10.1 Security

The DoD Manual C-5030.58M security design is vital to the DSSCS/GENSER accreditation/certification process.

3.10.2 Flexibility

The modularity of the I-S/A AMPE, both hardware and software, should be such that the I-S/A AMPE is capable of a secure, smooth, easy, evolutionary change and/or growth (see Section 3.4, I-S/A AMPE Security). Further, the I-S/A AMPE design should lend itself to both fixed and relocatable applications.

3.10.3 Performance

The design should explicitly address performing service functions and features in a way that least impacts the ability of the I-S/A AMPE to perform its total set of requirements. Aspects such as overflow and routing should be performed with minimal human intervention. To the maximum extent practicable functions and features should be performed via computing power vice human intervention.

3.11 Government Furnished Property (GFP)

3.11.1 Design Assistance

The government has available a number of computer based tools, such as simulation programs. Prior to either procuring or designing software tools, the contractor shall consult with the government. However, it is not the intention of the government to provide computer time for the use of any software tools.

3.11.2 Hardware and Software

For the effort to prepare Type B development specifications, the government does not anticipate providing any GFP. However, depending on the design approach adopted, GFP could be required for the implementation phase; thus the contractor shall interact with the government to generate a listing of GFP, as appropriate. The listing shall identify the property by reference to its nomenclature, specification number and/or part number or other appropriate identification.

3.12 Pre-Planned Product Improvements

3.12 Pre-Planned Product Improvement

The I-S/A AMPE is being implemented in two parallel and interlocked Tracks. Track I is the functional replacement and implementation of validated base-level telecommunications requirements, and the replacement of certain AUTODIN Switching Center functions. Track I will employ trusted computing base (TCB) technology in the design and implementation phases with test and evaluation (T&E) to the [A1] level. Rigorous mathematical proof down to the coding, not yet state-of-the-art, is deferred to Track II. Thus, during Track I separate DSSCS and GENSER systems will be deployed. The DSSCS systems will accommodate DSSCS-only and DSSCS-also-allowed-to-pass-GENSER subscribers. Track II provides the I-S/A AMPE interface(s) to the Defense Data Network (DDN), other as yet unvalidated enhancements, and the TCB T&E to allow full consolidation of DSSCS and GENSER facilities. Track II efforts will be accomplished by pre-planned product improvement (P^3I) techniques. Pre-planned product improvements are life cycle techniques to provide features which are not presently included in Track I (based on, e.g., lack of technology, immediate mission need, and excessive risk).

3.12.1 Pre-Planned Product Improvement Implementation

Since telecommunication research and development is ongoing, the need to implement P^3I features could come at any point during the I-S/A AMPE life cycle. Consequently, the I-S/A AMPE design shall explicity include a means of incorporating new capabilities such as P^3I. Once the technology is state-of-the-art, recomendations for implementing a validated feature will be assessed based on cost, schedule, and performance impacts the contractor shall provide during the Formal Review Process. As P^3I features are approved and validated, they will be incorporated into the I-S/A AMPE. The following paragraphs outline P^3I requirements.

3.12.2 Additional I-S/A AMPE Services

Since the telecommunications environment is constantly evolving, future I-S/A AMPE subscribers will recognize and document the need for additional services. For planning purposes, it is estimated that several services will be required in addition to the Formal Message Service (See para 3.2.1) with its Message Editing and Preparation Service (See para 3.2.2). The following services are examples of those which may be required:

a) Informal Message Service (IMS). Informal Message Service provides two capabilities: "interactive" and "mailbox". Interactive Informal Message Service implies a near real time "electronic note pad" capability between two users. "Mailbox Service" implies the ability to defer delivery (analagous to "overnight telegrams"). Such service might be provided without the rigor of the FMS (e.g., lesser degrees of assured delivery, traceability, recovery).

b) Teleconference Service (TCS). This service provides capability for groups of subscribers to use the IAS network to engage in interactive group transactions. That is, an "electronic blackboard" might be established at each of several "conference" locations for group sized briefings, lectures, and so on.

c) Data Base Transaction Service (DBTS). This service provides subscribers with the capability to generate, modify, and retrieve data from their own or other subscriber data bases world wide.

The I-S/A AMPE design shall allow for the addition of validated new services and the enhancement of existing functions and services throughout the service life of the system.

3.12.3 Data Path Requests

Each subscriber or service requesting "data paths" through the I-S/A AMPE shall require validation to access either a subscriber directly connected to the I-S/A AMPE, or a service provided by the I-S/A AMPE (e.g., Formal Message Service). The types of services and connections that a user or service is authorized to invoke shall be predefined (e.g., by a classmark or a table) and the I-S/A AMPE shall verify that the subscriber request is authorized prior to granting access. The following examples illustrate potential applications for data paths.

a) Directly Connected Subscriber to Another Directly Connected Subscriber. The I-S/A AMPE shall have the capability to allow a subscriber directly connected to the I-S/A AMPE to communicate with another subscriber who is also directly connected to the same I-S/A AMPE, without requiring processing by the FMS.

b) Directly Connected Subscriber to Network. The I-S/A AMPE shall allow a subscriber directly connected to the I-S/A AMPE to establish a connection to the network. This type of connection will provide access to such services as the Informal Message Service and the Teleconferencing Service.

c) Remote Subscriber to Local Service Connection. The I-S/A AMPE shall provide the capability for a Terminal Access Controller (TAC) subscriber (a subscriber not directly connected to an I-S/A AMPE) to establish a connection, through the network, to an I-S/A AMPE for local service (e.g., MEPS). The connection request shall be subject to access control to determine whether or not the TAC subscriber is allowed access to that particular service.

3.12.4 Preamble Format

The I-S/A AMPE shall have the capability to identify and accept for processing messages in Preamble format. Preamble is a format used by Army data processing installations in lieu of JANAP-128 format (See Appendix D of the I-S/A AMPE Interface Control Document).

3.12.5 Routing Table Update

The I-S/A AMPE shall be capable of receiving alternate routing table update information from the IAS Monitoring Center. The receipt of this information shall include safeguards to prevent malicious or accidental modifications of the routing tables.

3.12.6 DSSCS and GENSER Consolidation

During Track I the state-of-the-art in providing trusted computing base software restricts security to the [A1] level of the DoD Computer Security Center's, Trusted Computer System Evaluation Criteria; thus the I-S/A AMPE will be deployed either as a Multilevel Secure (MLS) GENSER or a MLS DSSCS facility, dependent on operational requirements. It is not mandatory that the I/S-A AMPE meet the criteria of Class A2 as this class is currently considered beyond the state-of-the-art. However, aspects of Class A2 that can be accomplished should be considered for incorporation into the I-S/A AMPE. [Note: To meet Class A2, a formal analysis of the object code is required to prove that the implementation software fulfills the requirement of the security model. Also, formal methods of verification are applied to the hardware design.] In addition to the security T&E, this Track II effort shall include the design, implementation and installation of any modification necessitated by the security T&E.

3.13 Training

Establishment of a comprehensive life-cycle oriented training program shall parallel development of the I-S/A AMPE. The initial training increment shall be completed in time to support the IOC deployment of the I-S/A AMPE.

SECTION 4

QUALITY ASSURANCE

4.0 QUALITY ASSURANCE PROVISIONS

An extensive I-S/A AMPE Test and Evaluation program shall be conducted to insure the acquired system meets its operational requirements. Review and testing of the software, hardware, and functional operation shall be performed continuously throughout the development and implementation phases. This effort shall be divided into a number of evolutionary steps as prescribed in the following paragraphs and Section 3.4, I-S/A AMPE Security. The contractor's proposal shall fully describe how the mandatory review and testing requirements described herein shall be met, optimized, and integrated into management, and security programs.

The government intends to have an independent verification and validation effort covering the full life cycle of the program. General guidelines are provided in the following publications (See Section 2.0) reference 2.5c, MIL-STD-1521, and NAVELEX INST 5200.23. The contractor shall also produce a Software Quality Assurance Plan in accordance with MIL-STD-1679 (see 3.6.2).

4.1 Contractor Configuration/Development Reviews

The contractor shall conduct configuration management meetings and audits throughout the contractual period and provide configuration management data to the Government. The configuration management program for software and software related equipment functions shall ensure that when the software is transitioned for Government control, the records and data are in detail, format, and status to allow Government use for future modification recommendations such as reviews and approvals. Formal design reviews shall be conducted by the contractor for the Government as an integral part of the software, hardware, and security design, development and test phases. Formal security design review will be conducted by the Government during design, development, and testing phases. At each review, the contractor shall conduct a system/software walkthrough using, as a baseline, the latest approved revision of the computer software specification and design plan. As a minimum, design reviews shall be conducted to support the Government's review of major design data (e.g. software specifications). Further, the contractor shall schedule and conduct management progress/status reviews at each key decision point during the design development and testing of the I-S/A AMPE program. The contractor shall identify proposed scheduling, location and special requirements of the above meetings and reviews in his proposal, and where appropriate, in planning data required by applicable DD Form 1423s. In addition, the contractor shall support requirements for unscheduled meetings called for by either the Government or the contractor to discuss special problems requiring early resolution. Proposed agenda of subjects to be covered in Government/contractor reviews and meetings, and minutes thereof, shall be provided.

4.1.1 Configuration Management

Total system configuration management shall be employed in the I-S/A AMPE program. Configuration management emphasis shall be placed on the developed software, firmware , and any specialized hardware, as these areas have the greatest technical and security accreditation risks (see Section 3.4). The functions of the I-S/A AMPE configuration management are to identify, control, provide status accounting for and verify the software configuration as it is developed. This connotes formal life cycle baseline definition and control, formal reviews and audits, and formal change status accounting. "Formal" is defined in this case as documented and agreed to by the offeror and the Government.

4.1.1.1 Configuration Management Baselines

The contractor shall produce a Software Configuration Management Plan in accordance with paragraph 3.6.

4.1.1.2 Engineering Change Proposals

Engineering Change Proposals (ECPs) shall be the only means by which the functional, allocated, or product baseline may be changed. ECPs shall be prepared and processed as specified in the CDRL. Each ECP shall include all necessary specification change notices (SCNs) to correct/revise all documents, to include the system performance specification and the FRD/ICD, which have been incorporated into the contract. It is important to note that control of each baseline continues throughout the life cycle of the contract. Thus, a change late in the implementation effort may impact the entire hierachy of baselines engendering changes to corresponding documents.

4.2 Development Teat and Evaluation (DT&E)

The contractor shall perform necessary development testing on all hardware units and subsystems, and associated software of the I-S/A AMPE in order to: validate his equipment selection and its condition upon receipt from vendors; insure this design and security features meet specified operational performance; verify his testing procedures; and provide the Government a high level of confidence that operations testing will be accomplished with minimum delays and/or retesting. Test plans and procedures supporting contractor development testing shall be provided the Government. Contractor development testing may be conducted in the contractor's plant, subcontractor's facility, the hardware/software test facility and/or other approved testing area. Development testing shall include, but not be limited to, any testing requiring Government approval. The Government will retain the right to witness All contractor testing; however, such witness shall not constitute Government acceptance, or reduce Government formal operational testing requirements. The development testing cycle shall include complete integrated testing of all hardware units, subsystems, and applicable software modules prior to release for installation.

4.2.1 Software Testing

Comprehensive and integrative testing of software shall be performed by the contractor in accordance with and Sections 3.4 and 3.0 at critical points, as defined below, in development of the system software. This testing shall be conducted sequentially as software modules are developed, followed by integration testing of functional sets of modules with final hardware/software testing of all modules required to control the complete I-S/A AMPE. Software testing shall conform to modular development under the approved structured programming methods. The Government shall be invited to witness and/or participate in all contractor software testing. Software testing and the reporting and approval of test results shall be accomplished. The contractor shall insure that specific and detailed testing of security module(s) is accomplished. Software and software security testing, described herein, shall be completed and approved prior to the start of the operational testing specified in 4.3.

Software test plans and procedures shall be prepared by the contractor in accordance with MIL-STD-1679 and Section 3.4 and submitted to the Government for approval. Further, software testing shall be defined in the Test Program Outline/Plan required by 4.4. These plans shall provide for the levels of testing described herein; separate test procedures shall be provided, as necessary, to support individual module and integrative testing.

This testing shall use a building block approach with full testing at each iteration. First, the individual software modules shall be tested. Then, these tested modules shall be integrated on a functional basis and tested. Finally, the complete software program for the I-S/A AMPE shall be integrated with associated hardware and fully tested.

4.2.2 Electromagnetic Testing Requirements

The I-S/A AMPE shall be tested to demonstrate full compliance with the requirements of the ICD.

4.3 System Testing

System testing for the I-S/A AMPE system shall include site testing in at least one mutually selected location. Although systems software/hardware may be tested at the module, unit, subsystem or even site level in the various phases of testing prior to system and Government testing, successful completion of preliminary testing will constitute conditional acceptance only (for contract milestone purposes). Final system acceptance will be subject to: the successful completion of all system testing and Government conducted operations testing, and the approval of test results by the Government.

4.3.1 Site Acceptance Testing

Site testing shall be designed and conducted in accordance with Sections 3.6 and 3.4. Formal testing shall be conducted under the direction of a Government provided test director at each site. During site testing, each site shall be individually tested. This testing will be considered the initial phase of acceptance testing and shall include all hardware/software in its final design configuration unless specifically waived by the Government Test Director.

This testing shall verify that; the installation and facility performance meets all requirements of the specification/contract except those requiring complete network integration (as required for system testing in 4.3.2); the site hardware/software is properly interconnected and operationally compatible with connected GFE, multiplexers, and subscriber modems/interface equipments, as appropriate; the site meets all requirements for interface, formats and codes; proper operational techniques have been developed for processing traffic under normal and stressed conditions; performance requirements are met under both normal and stressed conditions, and the requirements of software and security testing are met. Testing of subscriber interface hardware and software shall include full operational compatibility and security testing of all access area components. Site testing shall be conducted in accordance with the contractor provided, Government approved Installation and Checkout Test Plan and Procedures. Sufficient equipment for each site testing terminals, traffic generators, network simulators shall be provided by the contractor so that all operational requirements can be fully tested.

4.3.2 System Tests

Upon successful completion of an initial off-line system test, the I-S/A AMPEs shall be connected to both the AUTODIN, DDN, TRI-TAC Equipment, and NICS/TARE in preparation for full system testing. Successful performance of this system test and Government testing specified in 4.3.3 and Section 3.4 must be demonstrated prior to further installation of follow-on I-S/A AMPEs. The follow-on units shall be integrated, tested and accepted on a site-by-site basis. The system test shall consist of sequences of events to exercise and test all areas of system software, and verify that the I-S/A AMPE hardware and software meets the total requirements of the specification/contract. The test shall demonstrate that the I-S/A AMPE, operating with AUTODIN, DDN, TRI-TAC Equipment, and NICS/TARE provides message integrity and protection with reliable security provisions under all operating conditions while at the same time meeting traffic, speed, throughput, reliability and availability requirements. The interconnection of different user types shall be specifically tested. All users operating with standard protocols and interfaces as well as users operating with unique link protocols (See ICD 4.2.2) or variations to FMS (See paragraph 3.2.1) shall be tested to insure that: (1) all user types can exchange message traffic through FMS; and (2) all local user types who have the capability to select connection to other local users shall be able to intercommunicate with each other. System testing shall be conducted by the contractor under the direction of a Government test director in accordance with contractor provided/Government approved System Implementation Test Plan and Procedures.

4.3.3 Operational Test and Evaluation (OT&E)

As a final phase of system testing, the Government will conduct formal testing of the I-S/A AMPE. The Government will prepare all necessary test plans and procedures, test configuration and test data, and provide for documentation and analysis of test results. The contractor shall not have access to these test plans, procedures, test configuration, or test data prior to Government testing. This Government testing will include, but not be limited to, operational, performance, and security testing. The contractor shall support this effort to the same extent as required for the system testing discussed in paragraph 4.3.2. Sufficient time and resources to support this testing shall be identified in the contractor's proposal. The Government will have a minimum of 90 uninterrupted testing days in order to perform this testing. The term "uninterrupted testing days" is defined as the time period during which there are no outstanding (open) deficiency reports. Should deficiency reports develop, the testing time period will be restarted.

4.4 Test Documentation

The contractor shall prepare detailed test plans and procedures in accordance with Sections 3.4 and 3.6 to insure all contractor conducted testing, outlined above, will be accomplished. The contractor shall provide test results to the Government for all tests and evaluations performed as required (See 3.6.2).

4.4.1 Test Program Outline/Plan

An overall Test Program Outline and Plan integrating all phases of testing shall be prepared and submitted to the Government for approval. The Test Program Outline/Plan shall describe the beginning-to-end testing concept, phasing and integration of testing, test objectives, planning factors and scheduling, facilities required, description of individual tests and basis for acceptance for all contractor testing.

4.4.2 Test Plans and Procedures

Test Plans and Procedures shall be prepared by the contractor to detail resources and assets required, test requirements, test data, procedures, test limits, layouts, and acceptance/rejection and retesting criteria of all development and operational testing. These shall be prepared for unit, subunit, and subsystem level testing; for site testing; for overall I-S/A AMPE system testing; and for the special testing requirements of TEMPEST and EMI/EMC. These test plans and procedures shall provide for adequate testing of system design, hardware and software, system security, and installation.

4.5 Responsibilities for Contractor Conducted Testing

4.5.1 Contractor Test Procedures

Once the development test plans and procedures have been accepted by the Government, the contractor is responsible for implementing and documenting the tests and inspections as necessary to demonstrate acceptable performance. The contractor shall:

a. Prepare and forward to the Government for approval an overall system test program outline and plan, functional area test plans and procedures, and acceptance test plans and procedures.

b. Inform the Government (Test Director) in writing at least 30 days prior to desired start date of any testing which is subject to Government witness or approval.

c. Conduct validation, functional and acceptance testing and support Government security testing, as required in test plans and procedures.

d. Document test results in coordination with the Government Test Director.

e. Maintain complete records of inspections and test results for review by Government representatives and submit test reports to the Government.

4.5.2 Government Responsibilities

The Government will:

a. Review and accept, provide recommended changes, or reject test plans and procedures submitted by the contractor.

b. Be prepared to witness/conduct testing within 30 days after receipt of written notification from the contractor.

c. Direct and participate in formal acceptance testing in accordance with approved test plans and procedures, and with the support of the contractor.

d. Provide acceptance or rejection of test(s) results within time frames specified in DD Form 1423.

4.6 Equipment

The contractor shall furnish all equipment, services, and facilities required for testing except Government Furnished Cryptographic Equipment and Subscriber terminals. The contractor shall furnish transmission facilities to existing ASCs and PSNs, and to any subscriber terminals which may be utilized during the testing at the test facility. The contractor shall submit, subject to Government acceptance and amendment, the subscriber configuration necessary to meet the test requirements as part of testing prescribed in 4.3.1 and 4.3.2.

4.7 Quality Assurance Provisions - Security Design

Security requirements are described in Section 3.4, I-S/A AMPE Security.

SECTION 10

DEFINITIONS AND TERMINOLOGY

10.0 DEFINITIONS AND TERMINOLOGY

TERM MEANING

ACK (ACKNOWLEDGMENT): A control sequence sent either to or from the subscriber.

Access Control: Actions taken to permit or deny use of the components of a communications system. (NCS)

ACM (Access Control Mechanism): A hardware and/or software component that implements an object protection strategy.

Altroute (Alternative Routing): A process whereby alternate delivery stations are used when circuit failures, equipment outages, or backlogs develop which restrict delivery to primary addressees.

AMPE (Automated Message Processing Exchange): Equipment which automates the functions necessary to transmit, receive, and process messages to and from or within a telecommunications network. AMPEs may stand alone or provide service to remote terminals.

ASC (AUTODIN Switching Center): The switch node in AUTODIN that performs the store-and-forward message functions and includes the patch and test facility, power generation and distribution, modems, cryptographic equipment, and other peripheral or support functions.

Note: The leased and government-owned AUTODIN switching centers are operationally compatible, although they differ in capabilities, hardware, and software. They function as a common system and will be referred to by the common term "ASC'. The prefix "Leased" or "Government-owned" ASC is used when addressing or emphasizing a peculiar function of only one type of ASC.

AUTODIN (Automatic Digital Network): The Automatic Digital Network (AUTODIN) is a switched network of the Defense Communications System (DCS), which functions as a single, integrated, worldwide, high-speed, computer-controlled, general-purpose, store-and-forward communication network, providing record communications service to the Department of Defense (DoD) and other Federal Government Agencies. It consists of all AUTODIN Switching Centers (ASCs), interswitch trunks, and all subscriber stations connected thereto. This secure, fully automatic, switching network was designed, engineered, and programmed to provide continuous operation, minimal loss of service, and no loss of traffic; and has done so since 1964.

Blacker Program

An end-to-end encryption program with applicability to the I-S/A AMPE's connection to the Defense data Network (DDN).

CSN (Channel Sequence Number):

A three-digit number used to indicate the sequential number of the transmission on a channel between two stations. These numbers shall commence with number 001 and continue consecutively through 000 (1000).

CARP (Contingency Alternate Routing Program):

Inherent in all ASCs is a program identified as the Contingency Alternate Routing Program (CARP). This program provides an automatic capability of routing a message destined for an identified station to an alternate station not necessarily connected to the same ASC. CARP can be used to alleviate backlogs, for traffic management, or during a contingency condition, e.g., ASC failure. CARP cannot be applied to messages routed by a collective routing indicator.

Classification:

The security classification of the message.

Classmark:

Designators used to describe the service privileges and restrictions for lines accessing a switch, e.g., precedence level, security level, zone restriction.

Content Indicator Code:

The Content Indicator Code/Communication Action Identifier (CIC) is composed of four alphabetic or three alphabetic and one numeric character in format line two of a message which can be used to specify the content of the message. See JANAP-128 ANNEX B.

CRITIC:

The highest precedence message processed by the DSSCS. Critic messages in the DSSCS community are recognized by the Critic prosign of "WW YEKAAH". CRITIC messages are provided special handling in the AUTODIN system and require special operating procedures to ensure proper delivery. CRITIC messages preempt messages of any other precedence with the exception of ECP messages or another CRITIC message.

DCAC:

Defense Communications Agency Circular

DDN: Defense Data Network, packet switching backbone for the Integrated AUTODIN System.

DSSCS: Defense Special Security Communications System, DSSCS is the intelligence community record message portion of the AUTODIN.

Duplex: A communication system or equipment that can carry information in both directions between two points. See Full-Duplex and Half-Duplex.

EAM (Emergency Action Message): High precedence message that is transmitted at Emergency Command Precedence or Flash Precedence. An EAM of flash precedence with the appropriate CIC is queued to the front of the GENSER flash queue, but not ahead of a DSSCS flash message.

ECP (Emergency Command Precedence): Emergency Command Precedence is designated for use on certain time-sensitive command and control emergency action messages. ECP preempts all messages of lower precedence. Only the National Command Authority (NCA) and certain designated commanders of Unified and Specified Commands are authorized to use the ECP capability of the AUTODIN system and then only for certain designated emergency action command and control messages. ECP is the highest precedence in the GENSER community.

E^3 End-to-End Encryption

EOM: End of Message

Far-Term: The time frame after phase out of all of the ASCs.

FIFO (First-In-First-Out): The system where incoming messages are processed sequentially and transmitted at the end of their respective precedence queue when completely received.

FMS (Formal Message Service): FMS provides the capabilities for IAS subscribers to create, send, and receive formal messages. Formal message service can be regarded, in large part, to be a continuation of AUTODIN "official" message service. Formal messages are defined as messages that are prepared, handled, released, and recorded for storage in accordance with Service/Agency procedures.

FRD (Functional Requirements Description): Describes and baselines the functional requirements for the Inter-Service/Agency Automated Message Processing Exchange (I-S/A AMPE). This document provides a definitive description of the needs of the participating Military Services and Defense Agencies, and the Defense Communications Agency (DCA).

Full-Duplex Channel: A communications channel where the signals may flow in both directions simultaneously and independently. The signaling speeds used for the two directions of transmission on a full-duplex channel need not be the same.

Full-Duplex Transmission: A type of transmission where information is sent in both directions simultaneously and independently. Two-way simultaneous transmission.

Functional Requirements: Functional requirements are the actions needed to perform the Service/Agency mission, and the quantitative performance parameters needed to specify the extent of the action.

GENSER (General Service) Traffic: Traffic that includes all security classifications, excluding DSSCS traffic.

Guard: The telecommunications center provides internal office distribution to specified organizations.

Half-Duplex Channel: A circuit that affords communication in either direction but only in one direction at a time.

Half-Duplex Transmission: A type of transmission where information is sent in one direction or the other, but not both directions simultaneously.

History File: A complete, continuously maintained communications record to include the following information for each message processed by the AMPE: A complete copy of the message as received (with the exception of ALPS and SDS messages whose text shall not be recorded); a complete record of all message transactions beginning with the start of the message into the I-S/A AMPE and ending with receipt of the end of message acknowledgement from the last addressee terminal.

History Search Capability: The capability to search history files (on-line or off-line) based on varied criteria to extract message data for display or print.

Host: An IAS Host is a piece of user equipment that is connected to the IAS backbone (the DDN) and is capable of handling simultaneously multiple logical channels with the IAS.

IAS: The Integrated AUTODIN System (IAS) is the narrative record/data portion of the Defense Communications System. The IAS will evolve from the currently operational AUTODIN store-and-forward message switching network and the packet-switching Defense Data Network. The principal concept is that DDN will be the communications backbone and along with the I-S/A AMPE will provide the communications connectivity for all users.

IASA: IAS Architecture, see IASA Report (Part 3).

IAS Netework The I-S/A AMPEs and their connectivity to other I-S/A AMPEs. Initially for the I-S/A AMPE, the connection is through AUTODIN,then, as I-S/A AMPE deployment progresses, a combination of AUTODIN and DDN. Finally, as AUTODIN is phased out, it will be through DDN only.

ICD (Interface Control Document): Interface Control Document(s) serve as the repository for environmental, mechanical, electrical, protocol/format, and human interface criteria controlling or constraining the functional requirements described in the FRD.

Intercept Processing: Intercept processing provides operator initiated interim storage for messages whose delivery is delayed by an inoperative or backlogged output channel. Using intercept, the AMPE can temporarily hold messages for a destination which is partially or completely out of service or which operates on a part-time basis.

Interface: A boundary or point common to two or more systems or other entities across which useful information flow takes place. (It is implied that useful information flow requires the specification of the interconnection of the systems which enables them to interoperate.)

Interface Criteria: Interface criteria are the functional/ physical characteristics required to exist at boundaries between two or more equipments or computer programs provided by different DCS or Service/Agency subsystems or contracted (tariff/leased) subsystems.

Interoperability: The ability of systems, units or forces to provide services to and accept services from other systems, units or forces and to use the service so exchanged to enable them to operate effectively together.

In-transit Storage: In a store and forward message processing system, storage that is used to store messages that have been acknowledged on input but have not been delivered to all addressees on input, i.e., messages occupying intransit storage space are those currently undergoing input or output processing or currently on queue for output delivery. Messages on intercept or overflow storage do not occupy in-transit storage space.

IOC (Initial Operating Capability): The first attainment of the capability to employ effectively a weapon, item of equipment, or system of approved specific characteristics, and which is manned or operated by an adequately trained, equiped, and supported military unit or force.

I-S/A AMPE (Inter-Service/Agency Automated Message Processing Exchange: The standard element that will replace the individual message processing exchanges of the Services and Agencies and the ASCs.

LA: Logical address, binary address of host subscriber to the DDN.

Language Media Format: Language Media Format (LMF) is a single alphabetic character which describes message media and format, LMFs are used in pairs to indicate the source and preferred destination media format. NOTE: For more detail, see JANAP 128, paragraph 414.

Looping: A message passing through the same I-S/A AMPE more than one time before delivery to its final destination.

Message: Any thought or idea expressed briefly in a plain or secret language, prepared in a form suitable for transmission by any means of communication. (JCSI)

Message Accountability: A process utilizing a unique series of numbers used to ensure the known disposition of every message and to provide the bookkeeping associated with message handling.

Message Editing and Preparation Service [MEPS] See paragraph 3.2.2

Message Recovery: The ability to recover and protect delivery for messages that have been acknowledged on input but not delivered on output and have been temporarily lost due to AMPE equipment (processor or peripheral), software or total system failure.

Message Retransmission: Retransmitting of a message or group of messages that have previously been transmitted and receipt acknowledged by the addressee(s). Message retransmissions are normally performed at the request of the addressee(s). Messages to be retransmitted must be retrieved from AMPE history files and each retransmission shall be marked ZDK.

Message Retrieval: The ability to retrieve a previously delivered message or group of messages from history files (on-line or off-line) based on varied criteria for print, display or retransmission purposes.

Message Switching: The technique of receiving a message, storing it until the proper outgoing line is available, then transmitting. No direct connection between the incoming and outgoing lines is set up as in circuit switching.

Mid-Term: The time frame which includes the fielding of the I-S/A AMPE and concludes with the phasing out of all ASCs.

Misrouted Message: A misrouted message is one which contains an incorrect routing instruction.

Missent Message: A missent message is one bearing a correct routing indicator but transmitted to a station other than the one represented by the routing indicator. Altrouted messages contain the RI of the delivery station in Format Line 2 and are not in this category.

Modular: a. Software.

The goal of modular design is to build independent functional pieces of a computer program which can be separately developed, tested, and modified or replaced. Good modular design minimizes and allows easy modification. Software which employs modules must rely only on a limited, well defined set of properties for the modules. Nothing in the software should depend on the internal method by which the modules accomplish their job. Proper modularity will reduce code by collecting similar functions into one module. It increases the program's clarity by employing a small conceptual set of well defined properties to construct larger program elements.

b. Hardware.

(1) A degree of standardization of computer/communications system components to allow for combinations and large variety of compatible units.

(2) The determination of the design of the equipment such that components can be readily identified, altered, or augmented without replacements of particular units or sections.

Monitoring Center Function This function is to provide an automation assisted capability to maintain a current status as to the efficient operation of the I-S/A AMPE sub-network. The MC function is to be implemented on a regional basis (CONUS, Pacific, Europe) that will be collocated with major DCS systems operations centers and will support individual I-S/A AMPE status reporting as well as sub-network level.

Near-Term: A point in time prior to fielding of the I-S/A AMPE.

Network: An organization of stations capable of intercommunication but not necessarily on the same channel.

NICS/TARE (NATO Integrated Communications System/ Telegraph Automatic Relay Equipment): The NICS TARE System is an automatic store-and-forward message relay system. The automatic switching centers are interconnected with dedicated trunk circuits. They serve users via dedicated low speed (typically 50/75 baud telegraph) and medium speed subscriber circuits. The TARE Network will accept, process and retransmit messages in the formats specified in ACP 127, NATO Supplement 3, as well as in the basic ACP 127 (manual torn-tape relay) formats. No other formats will be accepted. The NATO versions of ACP 127 are somewhat different from those used in the AUTODIN.

NSA: National Security Agency

Off-Line: That condition wherein devices or subsystems are not connected into, do not form a part of, and are not suject to the same controls as an operational system. These devices may, however, be operated independently.

On-Line: That condition wherein devices or subsystems are connected into and form a part of, and are subject to the same controls as, an operational system.

Operating Signal: An operating signal consists of three alphabetic characters and a fourth position for a numeric or blank--used to convey message handling instructions, see ACP 131.

OSRI (Originating Station Routing Indicator): The routing indicator of the station that originated a message.

OSSN (Originating Station Serial Number): a. Station Serial Numbers are used for two purposes: (1) in combination with the originating station's routing indicator they provide positive identification for each transmission, and (2) as the EOM validation number appearing in format line 15 they provide a means by which ASCs check for the existence of straggler messages.

b. The OSSN is expressed in four numeric characters beginning with 0001 and continuing consecutively through 9999 . On completion of each series of numbers, a new series begins.

Overflow (Channel): This function is similar to system overflow except it is output channel oriented, e.g., when the specified traffic queue threshold for a given output channel is reached, the most recently received and lowest precedence messages destined for that channel are diverted to overflow storage. This function is also system controlled.

Overflow (Input): The purpose of this system controlled function is to return messages, previously placed on overflow storage due to system or channel overflow conditions, to the output channel queue when system and/or channel thresholds indicate that such action is warranted. The messages are returned to the output queue in such a manner that FIFO by precedence is maintained.

Overflow (System): When a specified threshold of system traffic has been reached indicating that the system in-transit storage capacity is near saturation, candidate messages are diverted to overflow storage. Candidate messages for overflow are determined by precedence, time in the system, queue load and channel activity. In general, the most recently received and lowest precedence messages destined for inoperative or backlogged channels are diverted to overflow storage. This function is system controlled.

PLA: Plain Language Address, an abbreviated or complete activity (organizational) title. The geographic location may or may not be included with the title.

Plain Language Address (PLA) Directory: A directory consisting of a compilation of Plain Language Addresses. (Often refered to as a PLAD.)

Plain Language Address (PLA) to Routing Indicator (RI) Assignment: Determination of the appropriate RI for a given PLA and its insertion in appropriate format lines of the message.

Precedence: A designation assigned to a message by the originator to indicate to communications personnel the relative order of handling and to the addressee the order in which the message is to be noted. NOTE: Precedence designations, in order of decreasing precedence, are ECP and CRITIC (same precedence level), FLASH, IMMEDIATE, PRIORITY, AND ROUTINE. These are defined as follows: (The letters indicate the corresponding prosign).

ECP Y Is designated for use on certain time-sensitive command and control emergency action messages. "Y" is designated Emergency Command Precedence (ECP) and has FLASH preemption capability and is used only in the GENSER community.

CRITIC WW Is designated for use on certain time-sensitive DSSCS messages and has FLASH preemption capability and is used only in the DSSCS community.

FLASH Z Reserved for initial enemy contact messages or operational combat messages of extreme urgency, and CRITIC messages originated in the GENSER community. Brevity is mandatory.

IMMEDIATE O Reserved for very urgent messages relating to situations which gravely affect the security of national/allied forces or populace.

PRIORITY P Reserved for messages concerning the conduct of operations in progress and for other important and urgent matters when routine precedence will not suffice.

ROUTINE R To be used for all types of messages which justify transmission by rapid means but are not of sufficient urgency and importance to require a higher precedence.

Preemption: The reallocation of services and equipment from a lower precedence use to a higher precedence use. That is, the AMPE shall have the capability to preempt the output of a message to allow transmission of a specified higher precedence message; preemption shall not cause the loss, modification, or segmentation of a message.

Preplanned Product Product Improvement (P^3I) Is an acquisition concept which programs resources to accomplish the orderly and cost effective phased growth or evolution of a system's capability, utility, and operational readiness.

Protect: The telecommunications center provides a set number of copies to an organization, which in turn arranges for its own internal distribution. NOTE: Office and unit determination is not performed for data pattern messages.

Protocol: The rules for communication system operation that must be followed if communication is to be effected.

R: Refers to the first character of the routing indicators (always an R) in the GENSER community.

Readdressal: Those actions necessary to cause a message stored on the message storage file to have a new set of addresses assigned which differ from the original set.

RED/BLACK: The concept that electrical and electronic circuits, components, equipments, systems, etc., which handle classified plain language information in electric signal form (RED) be separated from those which handle encrypted or unclassified information (BLACK). Under this concept, RED and BLACK terminology is used to clarify specific criteria relating to, and to differentiate between such circuits, components, equipments, systems, etc., and the areas in which they are contained.

RI (Routing Indicator): A group of letters assigned to indicate: a. the geographic location of a station; b. a fixed headquarters of a command, activity, or unit at a geographic location; and c. the general location of a type of relay or tributary station to facilitate the routing of traffic over the tape relay networks. (JCSI)

R/Y: Refers to communications facilities, e.g., lines and terminals, that process both GENSER and DSSCS traffic. Note that such facilities are "Y" and belong to the DSSCS community, but are allowed to also process "R" traffic.

Shall: Statements incorporating the verb "shall" are directive on the contractor(s).

SHD (Special Handling Designator) Symbol: A five character field consisting of one alphabetic character repeated five times. The SHD Symbol appears in the SPECAT field of the DD Form 173. In JANAP 128 format, SHD Symbols appear in format line four, immediately following the classification/transmission release code field (e.g., /AAAAA).

SOM (Start of Message): Sentinel indicating the message start (V or Ltrs ZCZC in format line 1).

SPECAT (Special Category) Messages: A subset of special handling designations which are recognized by the word "SPECAT" immediately following the classification in the first word of text. In addition, the appropriate SPECAT DESIGNATOR OR SHD repeated five times, preceded by an oblique (/) will immediately follow the security characters appearing in format line 4.

SSN (Station Serial Number): A message reference number assigned within a a communication/signal center. NOTE: It will normally consist only of a number allotted in sequence. However, in those instances where station serial numbers are alloted at more than one position, as prescribed by in-station procedure, a single letter designator can follow each number, e.g., 107A, 119B. SSN with an alphabetic character is not allowed in the DSSCS community. The message reference number is normally expressed in four numerical characters and is assigned within a communication center for two purposes, viz., in combination with the originating station's routing indicator, it provides positive identification for each transmission, and, as the validation function number appearing in format line 15, it provides a means by which the station can check for the existence of straggler messages.

Station and Channel Designator: Three letters which identify one or both of the stations and a specific channel between the two stations. These are used as follows:

(1) Either two letters to identify one or both of the stations and one letter to identify a specific channel, or

(2) Three letters to collectively represent one of the stations and a specific channel.

System Controlled Function: A function that is performed automatically by the AMPE system (hardware/software). Operator action is not required to initiate or terminate the function.

Subscriber: An IAS subscriber is an IAS user that uses its own equipment homed to an IAS element. The term "subscriber" means either a terminal with its associated operator or a host. Subscribefs are further categorized as local subscribners and remote subscribers. A local subscribers circuit terminates on the I-S/A AMPE. A remote subscribers circuit terminates on another IAS element (e.g., TAC), and the remote subscriber accesses the I-S/A AMPE through the network to obtain service.

TAC: Terminal Access Controller, a host subscriber of the DDN provides the Virtual Connection Service (i.e., TCP, IP, and DDN interface) via THP to terminal subscribers of the DDN. An FMS terminal can make use of a TAC for transport to its home I-S/A AMPE for Formal Message Service.

TARE Line: Transmission Instructions: Transmission instructions are preceded by the prosign "T" and indicate specific transmission responsibility not apparent in other components of the message heading. These instructions appear in format line four of the message heading.

TCC (Transmission Control Code): An alphabetic code in the security field of the message header which is verified against the destination parameter of the subscriber to ensure the terminal is authorized receipt of the message contents.

TEP: Traffic Engineering Practices (for the Defense Communications System) DCA CIRCULAR 300-70-1.

Terminal:

a. Terminals are usually, but not always, located with the ultimate addressee and may provide for send and/or receive operation. The terminal uses the automated capabilities of an AMPE to perform message processing functions which would normally be done manually.

b. In the Packet Processing System (DDN) terminals are defined as character oriented devices capable of conducting conversation with only one destination at a time. Terminal devices may be computer peripheral controllers and or intelligent or unintelligent input-output devices.

c. Message Processing Terminal: A terminal that provides a basic capability to process messages to and from AUTODIN directly. These terminals may be either leased or government owned. Detailed information concerning these terminals is contained in the following: DCAC 370-D175-1, DCAC 370-D195-3, DCAC 310-D130-3, and DCAC 370-D95-1.

d. Local Terminal: In the IAS a local terminal is a terminal connected directly to an I-S/A AMPE.

e. Remote Terminal: In the IAS a remote terminal is a terminal directly connected to another IAS element but is "homed" to an I-S/A AMPE for certain services.

Throughput:

The number of bits, characters or blocks which can pass through a data communications system (or portion of that system) when the system (or portion of the system measured) is working at saturation. The throughput will vary greatly from its theoretical maximum.

TRC (Transmisson Release Code):

The transmission release code is a two-letter element which is inserted in the message heading format in conjunction with the redundant security character group to indicate authorization for the transmission of any U.S. DoD GENSER message to a regional defense organization or foreign nation (international traffic). It is, essentially, a software check on the release of a message to non-U.S. subscribers.

TRI-TAC:

Joint Tactical Communications Office.

TRI-TAC Message Switched Network: The TRI-TAC message switched network is a common user network consisting of TRI-TAC developed store-and-forward switches (AN/TYC-39 and AN/TYC-11) and existing tactical inventory tape relays.

a. The TYC-39 is an automatic electronic store-and-forward message switch under processor control. The TYC-39 comprises the backbone of the TRI-TAC message switched network.

b. The smaller capacity TYC-11 is an automatic message switch configured for inclusion in the TRI-TAC Modular Tactical Communications Center (MTCC) to provide expanded external circuit termination capability. It may be used as a concentrator or access switch for subscribers requiring access to the TYC-39.

Unique Message Identifier: The global unique message identifier shall be assigned by the origination I-S/A AMPE and shall uniquely identify the message globally in the IAS.

User: An I-S/A AMPE user is any organization or activity that obtains service from the I-S/A AMPE. A user may obtain this service by use of their own equipment connected to the I-S/A AMPE or by obtaining "over-the-counter" service from a telecommunications center.

Virtual Connection Service: See paragraph 3.1.5.1.4.

Will: Statements incorporating the verb "will" are directive on the Government to satisfy in support of the contracted tasks.

WIN (WWMCCS Intercomputer Network): The WWMCCS Intercomputer Network (WIN) is a centrally managed information processing and exchange system designed to serve the corporate information needs of the NCA, the JCS, the CINC's and Services. The WIN consists of an aggregation of WWMCCS computers, WWMCCS standard applications, command unique applications, communications, reporting systems and procedures. The term WIN encompasses WWMCCS host computers, designated WIN terminals and interconnecting communications subsystem. The WIN communications subsystem consists of the Interface Message Processors (IMPs), inter-IMP trunks, host-to-IMP and WIN terminal-to-host access circuits together with associated modems, multiplexers, concentraters and cryptographic equipment.

WWDSA	World Wide Digital System Architecture
Y:	Refers to the first character of the routing indicators (always a Y) used in the DSSCS community.

SECTION 11

COMPUTER SECURITY GLOSSARY

Computer Security Glossary

The following terms and definitions are provided to achieve a better understanding of terms used in computer security as they relate to the I-S/A AMPE Program.

Access. The ability and the means necessary to store or retrieve data, to communicate with (i.e., provide input to or receive output from), or otherwise make use of any resource in a computer system.

Access Control. A strategy for protecting objects from unauthorized access.

Access Control List. A list of subjects which are authorized to have access to some object. See Subject, Object.

Access Level. See Security Level.

Access Mode. A distinct operation recognized by the protection mechanism as a possible operation on an object. Read, write, and append are possible modes of access to a file, while execute is an additional mode of access to a program. See Security Mode.

Access Policy. See Policy, DoD Security Policy.

Accreditation. The final acceptance of a system for operation in a specific environment. This is a subjective evaluation of a system based upon certification testing and environmental analysis.

Accountability. The property that enables violations or attempted violations of system security to be traced to individuals who may then be held responsible.

Activity. A security model rule stating that once an object is made inactive, it cannot be accessed until it is made active again. See Bell-LaPadula Security Model.

Address Space. The virtual memory that can be address by a process. The maximum size of a process address space is usually a function of the underlying hardware.

AFFIRM. A formal methodology developed at USC-ISI for the specification and verification of abstract data types, incorporating algebraic specification techniques and hierarchical development.

Aggregation. A circumstance in which a totality of small pieces of information must be classified at a higher level than any single piece of information which comprises it.

Attention Character. In TCB design, a character that, when entered from a terminal, tells the TCB that the user wants a secure communications path from the terminal to some trusted code, in order to provide a secure service for the user, such as logging in or logging out.

Audit. An independent review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with estaolished policy and operational procedures, and to recommend any indicated changes in controls, policy and procedures.

Audit Trail. A chronological record of system activity which is sufficient to enable the reconstruction, review, and examination of the sequence of environments and activities surrounding or leading to each event in the path of a transaction from its inception to output of final results.

Authenticate. To confirm the identity of a person (or other agent external to the protection system) making an access request.

Authentication. The act of identifying or verifying the eligibility of a station, originator or individual to access specific categories of information. The process by which the Government determines concurrence with specifications.

Authorize. To grant a subject access to certain information.

Bell-LaPadula Security Model. An "access control" type of security model based on state-machine concepts; sometimes called the MITRE Model. In this model, the entities in a computer system are abstractly divided into sets of subjects (active entities such as processes) and objects (information containers). The notion of a secure state is defined, and an inductive proof of system security can be given: the initial system state is shown to be secure, and every state transition is shown to preserve this property.

A system state is defined to be "secure" if the only permitted accesses of subjects to objects are in accordance with specified security level restrictions. For example, a subject is permitted to read data at its own level or at a lower level (simple security condition), and to write data at its own level or at a higher level (*-property). State transitions preserve the "secure state" property in accordance with tranquility, erasure and activity principles (q.v.).

Among several versions of the Bell-LaPadula Model is an integrity model, which is essentially the mathematical dual of the security model, incorporating a "simple integrity principle" and "integrity *-property." See Integrity.

Capability. In a computer system, an unforgeable ticket that is accepted by the system as incontestable proof that the presenter has authorized access to the object named by the ticket. It is often interpreted by the operating system and the hardware as an address for the object. Each capability also contains authorization information identifying the nature of the access mode (e.g., read, write).

Category. The unit into which security information is partitioned, corresponding roughly to an interest group or topic area, e.g., NATO, CRYPTO. Category information can exist at many levels, unclassified through top secret. A subject must be cleared to an adequate level and have access to the proper category or set of categories before access to classified data can be given. See Security Level.

Certification. The application of policy doctrine and technical evidence to a system to determine the prudence of its use in a particular secure application. This is a technical activity.

Channel. An information transfer path within a system. "Direct" or "overt" channels are those paths that are designed for data transfer; "indirect" or "covert" channels are not explicitly intended for data transfer, but can pass information through the selected use of system resources, that is, through "leakage" or "signalling." Indirect channels are generally categorized as "storage" and "timing" channels. Timing channels are those that exploit the system clock or system performance characteristics to pass information and are difficult to identify in a non-procedural system specification, while most storage channels can be identified by flow analysis techniques. Both types of indirect channels are exploitable only through interprocess cooperation.

Classification. The level of protection that must be afforded information. It is the information counterpart of Clearance in DoD security policy. It applies to such system objects as buffers and files, as well as to "real-world" security-related documents.

Clearance. An authorization allowing a person access to classified information. This is a "real-world" term used in connection with DoD policy, whose mathematical counterpart is security level (q.v.). A clearance typically consists of a level (unclassified through top secret) and a need-to-know category or categories.

Code Proof. See Implementation Verification.

Compartment. See Category.

Computer Program Component (CPC). A CPC is a functionally or logically distinct part of a Computer Program Component Item (CPCI) distinguished for purposes of convinience in designing and specifying a complex CPCI as an assembly of Subordinate elements. (Para 5.D MIL STD 483 of 31 Dec 70)

Computer Program Configuration Item (CPCI). An entity that will be tracked by configuration control. The aggregate of CPCIs is the software system.

Computer Security. See Security.

Compromise. The known or suspected exposure of clandestine personnel, installations or other assets, or of classified information or material to an unauthorized person. (JCS1)

Confidentiality. The status accorded to private data and the degree of protection that must be provided for such data. Data confidentiality applies not only to data about individuals but to any proprietary or sensitive data that must be treated in confidence. See Privacy.

Confinement. Allowing a process executing a borrowed program (in general, an arbitrary program) to have access to data, while ensuring that the data cannot be misused, altered, destroyed, or released. See Channel.

Confinement Channel. See Channel.

Container. A repository of data in a system. See Object.

Controlled Security Mode. A mode of system operation in which there are users who have legitimate access to the system but have neither a security clearance nor need-to-know for all classified material contained in the system. However, the separation and control of users and classified material is not essentially under operating system control as in the multilevel secure mode. Equivalent with compartmented mode (Ref D112M504). See Security Mode.

Correctness. Formally, the property of a system that is determined through formal verification activities. Correctness is not an absolute property of a system, rather it implies the mutual consistency of a specification and its implementation. See Verification.

Correctness Proof. A mathematical proof of consistency between a specification and its implementation. It may apply at the security model to formal specification level, at the formal specification-to-HOL code level, at the compiler level, or at the hardware level. For example, if a system has a verified design and implementation, then its overall correctness rests with the correctness of the compiler and hardware.

Once a system is proved correct, it can be expected to perform as specified, but not necessarily as anticipated if the specifications are incomplete or inappropriate.

Covert Channel. See Channel.

Data Security. Procedures and actions designed to prevent the unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional, of data.

Debug. Jargon meaning to detect, trace, and eliminate mistakes.

Dedicated Security Mode. In government installations, a mode of operation in which the computer system, its connected peripheral devices and remote terminal are exclusively used and controlled by specific users or groups of users who have a security clearance and need-to-know for all categories and types of classified material contained in the computing system. See Security Mode.

Denial of Service. The prevention of authorized access to computer resources, or the delaying of time-critical operations.

Design Verification. The use of verification techniques, usually computer-assisted, to demonstrate a mathematical correspondence between an abstract (security) model and a formal system specification. See Verification.

Discretionary Access Control. Access controls to an object that may be changed by the creator of the object. More generally, mechanisms that allow each subject, at its own discretion, to decide which of its own access rights are to be given to any other subject.

DoD Security Policy. The complete body of law, regulations and policy concerning the safeguarding of Defense sensitive information. DoD security policy includes all the espionage laws, the DoD regulations, and DoD authorized commercial classification for handling and access to information concerning national defense. The basic policy sets four levels and several categories on non-discretionary information control and requires that anyone accessing classified information have a "need-to-know" for the particular information in question. See Non-Discretionary Access Controls.

Domain (Hardware). A means by which hardware features can be restricted or nested. For example, the DEC PDP-11/45 or 11/70 has three execution domains: kernel, supervisor, and user. The kernel domain is the most privileged, and allows access to all hardware features including memory maps and I/O; the other domains do not allow these privileges. Another example is the Honeywell MULTICS architecture, which includes eight rings.

Domain (Software). An environment or context that defines the set of access rights that a subject has to objects of the system.

Downgrade. See Regrade.

Edit/Reasonableness Tests. A wide range of tests may be performed on items within the files from zero to excess balance. Thesetechniques are searches for conditions which should not exist if controls are effective.

Emulator. A combination of hardware and software that permits programs written for one computer to be run on another computer. In computer security terminology, the emulator is the portion of the system responsible for creating an operating system compatible environment out of the environment provided by the kernel. In KSOS, the emulator maps the kernel environment into the UNIX environment.

Encryption. The (usually) invertible coding of data through the use of a transformation key so that the data can be safely transmitted or stored in a physically unprotected environment.

Erasure. A security model rule stating that objects must be purged before being activated or reassigned. This ensures that no information is retained within an object when it is reassigned to a subject at a different security level. See Bell-LaPadula Security Model.

Error. An error is an item of information which, when processed by the system, produces a failure (of a non-reproducible type).

Failure. The termination of the ability of an item to perform its required function.

Fault. A malfunction that is reproducible, as contrasted to an error, which is defined as a malfunction which is not reproducible.

Fault Isolation. In testing, the process of searching for and locating a defect in a system.

Flow Analysis. See Security Flow Analysis.

Flow Control. A strategy for protecting the contents of information objects from being transferred to objects at improper security levels. It is more restrictive than access control. See Access Control, Non-Discretionary security.

Formal Specification. The unambiguous description of hardware or software in a language with a well-defined syntax and semantics. These specifications give a precise mathematical description of the behavior of the system being specified. Computer readability of these specifications allows for automation of various phases of the verification. Formal specifications for a system can be written at any level of detail. See Top Level Specification.

Granularity. The size of the smallest protectable unit of information. In a TCB system, this would be the size of the smallest protectable file or portion of virtual memory.

Human Interface Functions. TCB operations that require human intervention or judgement. Untrusted processes would not be able to invoke them. See Software Interface Functions, Trusted Computing Base.

Identification. The process that enables, generally by the use of unique machine-readable names, recognition of users or resources as identical to those previously described to the computer system.

Implementation Verification. The use of verification techniques, usually computer-assisted, to demonstrate a mathematical correspondence between a formal specification and its implementation in program code. See Verification.

Indirect Channel. See Channel.

Integration Testing. A technique used to test groups of components together, particularly in order to evaluate the correctness of shared interfaces.

Integrity. The assurance, under all conditions, that a system will reflect the logical correctness and reliability of the operating system; the logical completeness of the hardware and software that implement the protection mechanisms; and the consistency of the data structures and accuracy of the stored data. In a formal security model, integrity is interpreted more strictly to mean protection against unauthorized modification or destruction of information.

Interface. A boundry or point common to two or more similar or other entities against which or at which necessary information flow takes place.

Interprocess Communication (IPC). Communication between two different processes using system-supplied constructs, e.g., shared files.

Isolation. The containment of users, data, and resources in an operating system in such a way that users may not access each other's data and resources, and may not manipulate the protection controls of the operating system. See Confinement.

Level. See Security Level.

Mapping. The use of program analyzers to determine what special conditions lead to the execution of each program module. Use requires a basic understsnding of the application system's structure and application programming.

Mandatory Security. See Non-Discretionary Access Control.

MLS. The Multilevel Security flow analysis tool developed at SRI. See Hierarchical Development Methodology, Security Flow Analysis.

Multilevel Security Mode. A mode of system operation permitting data at various security levels to be concurrently stored and processed in a computer system where at least some users have neither the clearance nor the need-to-know for all classified material contained on the system. Separation of personnel and material on the basis of security level is accomplished by the operating system and associated system software. See Security Mode.

Need-to-Know. A job-related requirement for access to specific information. Need-to-know implies discretionary control of information--even though potential accessors may have the necessary clearance.

Non-Discretionary Security. The aspect of DoD security policy which restricts access on the basis of security levels. A security level is composed of a level and a category set restriction. To access an item of information, a user must have a clearance level greater than or equal to the classification of the information, and also have a category clearance which is a superset of the access categories specified for the information. See Discretionary Access Controls, Security Level.

Non-Kernel Security-Related Software (NKSR). Security-relevant software which is executed in the environment provided by a security kernel, rather than as part of the kernel. Processes executing NKSR software may or may not require special privilege to override kernel-enforced security rules. See Trusted Process.

Non-Procedural Language. A formal high-level language for the specification of program modules. Such languages express relations which hold between "input" and "output" values of program variables, without constraining the particular algorithms which implement the change. See HDM, INA JO.

Object. In a formal security model, an identifiable resource, data container or related entity of the system; the counterpart of Subject. Software-created entities such as files, programs and directories are objects, as well as hardware resources such as memory blocks, disk tracks, terminals, and tapes. See Bell-LaPadula Security Model, Subject.

Parallel Simulation. The application is tested by using the same input files and data and attempt to produce the same results. Unlike ITF, purging of files is not required because the simulation is run parallel to the "live" data and results are then compared to the "live" results confirming processing or identifying areas of discrepancies needing further analysis. All or parts of the system may be tested. An excellent verifier of controls.

Password. A protected word or string of characters that identifies or authenticates a user, a specific resource, or an access mode.

Penetration. The successful, repeatable, unauthorized extraction of recognizeable information from a protected data file or data set.

Penetration Testing. The use of special programmer/analyst teams to attempt to penetrate a system for the purpose of identifying any security weaknesses.

Periods Processing. In computer installations, a mode of processing in which a specific security mode is temporarily established during a specific time interval for processing sensitive information. For example, the computer system could process secret information in the dedicated security mode during one period, and unclassified material in a second period. The computer system must be purged of all information before transitioning from one period to the next whenever there will be new users who do not have clearance and need-to-know for information processed during the previous period. See Dedicated Security Mode.

Policy. Administrative decisions which determine how certain security-related concepts will be interpreted as system requirements. All such policy decisions must eventually be interpreted formally and implemented.

Privacy. The protection afforded to information in a communications system or network in order to conceal it from persons within the system or network.

Privileged Process. A process that is afforded (by the kernel) some privileges not afforded normal user processes. A typical privilege is the ability to override the security *-property. Privileged processes are trusted. See Trusted Process.

Process. The active system entity through which programs run. The entity in a computer system to which authorizations are granted; thus the unit of accountability in a computer system. A process consists of a unique address space containing its accessible program code and data, a program location for the currently executing instruction, and periodic access to the processor in order to continue.

Protection. Narrowly, the mechanisms used to control access of executing programs to stored data. See Security.

Quality Assurance. The planned and systematic pattern of actions necessary to provide adequate confidence that materiel, data, supplies, and services conform to established technical requirements and achieve satisfactory performance.

Recovery Procedures. In data communications, a process whereby a data station attempts to resolve conflicting or erroneous conditions arising during the transfer of data.

Reference Monitor. A security control concept in which an abstract machine mediates accesses to objects by subjects. In principle, a reference monitor should be complete (in that it mediates every access), isolated from modification by system entities, and verifiable. A security kernel is an implementation of a reference monitor for a given hardware base.

Regrade. A determination that classified information requires a different degree of protection against unauthorized disclosure than currently provided, together with a change of classification designation that reflects such different degree of protection. an "upgrade" results in a higher classification; a "downgrade" results in a lower classification.

Reliability. The probability that an item will perform its intended function for a specified interval under stated conditions.

Ring. See Domain.

Risk Analysis. The term applied to the systematic quantification of threats, loss exposures, and countermeasures benefits.

Secure Path. See Trusted Path.

Security (Computer Security). Used in the most general sense, this denotes the totality of mechanisms and techniques that protect resources (including data and programs) from accidental or malicious modification, destruction, or disclosure. The term includes the physical security of the computer installation, administrative security, personnel security, and data security. Used more narrowly in a verification context, it denotes protection of computer information from unauthorized disclosure.

Security Flow Analysis. A type of security analysis performed on a non-procedural formal system specification which locates potential flows of information between system variables. By assigning security levels to system variables, many indirect information channels can be identified. Security flow analysis defines a security model similar to the access control model (Bell-LaPadula) but with a finer protection granularity.

Security Kernel. A privileged supervisory operating system. A localized mechanism, composed of hardware and software, that controls the access of users (and processes executing on their behalf) to repositories of information resident in or connected to the system. The correct operation of the kernel along with any associated trusted processes should be sufficient to guarantee enforcement of the constraints on access. TCBs have been implemented using security kernels along with trusted processes. See Trusted Computing Base (TCB).

Security Level. In the context of formal security modeling, the fundamental security attribute of subjects and objects. Security levels combine a level (e.g., Unclassified, Confidential, Secret, Top Secret) and a set of need-to-know categories. A derived partial ordering of security levels is defined using a combination of the "less than" order on levels and the "subset" relation on category set. Thus (Secret, NATO) is less than both (Top Secret, NATO) and (Secret, [NATO, CRYPTO]). The security levels (Confidential, NATO) and (Top Secret, CRYPTO) are incomparable. This derived partial ordering on security levels is the basis on which all subject-to-object access is determined.

Security Mode. A Department of Defense term for "Authorized variations in the security environments and methods of operating ADP systems that handle classified data." DoD ADP security policy (DoD Directive 5200.28) defines four modes: dedicated, system high, controlled and multi-level security modes.

Security Model. See Correctness, Bell-LaPadula Security Model, Security Flow Analysis, Verification.

Security Policy. See DoD Security Policy, Non-Discretionary Access Controls.

Security Violation. See Violation.

Security *-Property (Star Property). A security model rule allowing a subject write-access to an object only if the security level of the object is the same or higher than the security level of the subject. See Bell-LaPadula Security Model.

Simple Security Condition. A security model rule allowing a subject read-access to an object only if the security level of the object is the same or less than the security level of the subject. See Bell-LaPadula Security Model.

Snapshot. A technique of capturing data at a particular point in time in the operations cycle, triggered by specific transaction types, that are identified by tags. An exellent method for very specific purposes.

Software Engineering. The establishment and use of sound engineering principles in order to obtain software that is reliable, efficient, understandable, maintainable, economical and functional.

Software Interface Functions. TCB operations that can be invoked by software, as opposed to a person at a terminal. See Human Interface functions, Trusted Computing Base.

Spoofing. The deliberate inducement of a user or a resource to take an incorrect action.

Specification. Generally, a description of the input, output, and essential functions to be performed by a system or by a component of a system. The specification is produced by the organization that is to develop the system; hence at the top level it can be thought of as the contractor's interpretation of the requirements.

Storage Channel. See Channel.

Structured Programming. An approach to programming the premise of which is the use of a small set of simple control and data structures. This method typically restricts the number of connections between program parts, clarifies module entry and exit points, limits module size, restricts arbitrary branching, and incorporates hierarchical design, thereby improving comprehensibility, reliability, and maintainability. See Software Engineering.

Subject. An active user of a computer system together with any other entity onbehalf of a user or on behalf of the system; for example, processes, jobs, and procedures may all be considered subjects. Certain subjects may also be considered to be objects of the system. See Bell-LaPadula Security Model, Object.

System Control Audit Review File (SCARF). An audit trail of specified transactions built into the program to tag or extract exceptional data into the audit files. During normal processing, the audit tests are performed on the processed data. The auditor can then examine the review file and draw the appropriate conclusions. If SCARF testing results are repeated, it may indicate that the controls should have been built in initially; a case of audit leading to improved internal program controls.

System High. The highest security level supported by a system at a particular time or in a particular environment.

System High Security Mode. The mode of operation in which the computer system and all of its connected peripheral devices and remote terminals are protected in accordance with the requirements for the highest security level of material contained in the system at that time. All personnel having computer system access have the security clearance and need-to-know for all material then contained in the system.

System Low. The lowest security level supported by a system at a particular time or in a particular environment.

System Testing. A series of exercises involving the test of the completed system by an outside group.

System Utility. Any software, not part of the verified operating system, used to perform various functions that are not directly part of the applications. Examples are compilers, debuggers, editors, and loaders.

Test data. Test decks are used to check results againstpredetermined values Little ADP knowledge is required for there use and they can provide a highly specific test of individual control features and exception conditions. The decks are difficult to maintain where program modifications are frequent. Usually a special computer run is requiredfor there use. Since they are oriented to known controls,their use will doubtfully detect the absence of any needed controls. Test Data Generator is an automated development of test transactions.

Testing. The controlled exercise of program code in order to expose errors. It consists of exercising the software and accumulating performance statistics on its operation.

Thread Testing. A technique of functional testing that can demonstrate the operation of key functional capabilities fairly early in testing activity. A thread is a string of programs that when executed, accomplishes a distinct processing function.

Timing Channel. See Channel.

Top-Down Design. The decomposition of system design decisions into a succession of refinements, from the more general to the more specific.

Top-Down Development. A technique for implementing hierarchically-structured programs in which top level routines are written first. For test purposes, lower level routines, called stubs, are written to interface with these. The system's correctness is assumed, not proved, until the last stub has been replaced.

Top Level Specification (TLS). In a verification context, a mathematical specification of system behavior at the most abstract level, typically a functional specification that omits all implementation detail. The formal top level specification of a security kernel precisely defines the behavior of the security kernel observable outside the kernel domain (at the kernel interface). See Formal Specification.

Trace. A technique identifying the sequence of actual exceptions of program code, triggered by specific transaction types identified by tags on conditions. Trace may also be used to document use of program modules or instructions to process specific transactions.

Tranquility. A security model rule stating that the security level of an active object cannot change. See Bell-LaPadula Security Model.

Trap Door. An entry point in a computer system that can be selectively accessed to allow unauthorized access to the system.

Trojan Horse. A borrowed program that performs actions unrelated to the caller's intent, subverting the security of the caller's data. It may disclose sensitive data either by hiding it in a file or other form of storage where it can be accessed later, or by communicating the information via a covert channel. The name Trojan Horse was given to this kind of problem because it involves a foreign or gift program which has unexpected or malicious side effects. Trojan Horses may be planted on a temporary or permanent basis. See Confinement, Channel.

Trusted Computing Base (TCB). The totality of protection mechanisms for an operating system. It provides both a basic protection environment plus additional user services required for a trustworthy turnkey system. TCBs have been implemented as security kernels and trusted processes.

Trusted Path. A reliable and unforgeable connection between a user at a terminal and a trusted process. A trusted path may be achieved through an attention character. Also call Secure Path. See Attention Character.

Trusted Process. A process in a position to affect system security. It is sometimes but not always endowed with privileges to override TCB-enforced rules. A trusted process requires reliable confirmation that its protection capabilities or characteristics comply with stated requirements (e.g., through formal verification). Trusted processes are sometimes used to execute NKSR software.

Unauthorized Disclosure. See Violation.

Untrusted Process. A process whose incorrect or malicious execution cannot affect system security. Verification is usually not applied to untrusted processes.

Upgrade. See Regrade.

Validation. The collection of evaluation, integration, and test activities carried out at the system level to ensure that the system being developed satisfies the requirements of the system specification.

Verification. Informally, a clear and convincing demonstration that software is correct with respect to well-defined criteria, such as a security model. In a formal context, verification refers to the mathematical demonstration of consistency between a formal specification and a security model (design verification) or between the formal specification and its program implementation (implementation verification). The phrase "formally verified" is now beginning to imply that computer-assisted techniques have been employed in the verification effort. See Correctness.

In testing, verification refers to the iterative process of determining whether the product of selected steps of the CPCI-developed process meets the requirements levied by the previous step.

Violation. Some form of security breach. "Compromise" carries the connotation that security-relevant data has "possibly" been exposed to uncleared persons (or processes), while "unauthorized disclosure" implies that the data has been exposed to cleared persons who do not possess a need-to-know.

Virtual Space. See Address Space.

Walkthrough. A management review to discover errors in the system.

*-Property. Pronounced "star" property. See Security *-Property.

SECTION 20

I-S/A AMPE MESSAGE FORMAT VALIDATION

UNCLASSIFIED

Section 20

DEFENSE COMMUNICATIONS AGENCY

INTER-SERVICE/AGENCY
AUTOMATED MESSAGE PROCESSING
EXCHANGE PROGRAM

FUNCTIONAL STATEMENT DOCUMENT

APPENDIX 3B

AMPE MESSAGE FORMAT VALIDATION

APPROVED FOR PUBLIC RELEASE
DISTRIBUTION UNLIMITED

UNCLASSIFIED

DEFENSE COMMUNICATIONS AGENCY
DEFENSE COMMUNICATIONS SYSTEM ORGANIZATION
WASHINGTON, D.C. 20305

12 MAY 1983

IN REPLY REFER TO: B660

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Appendix 3B, I-S/A AMPE Message Format Validation Criteria, to the I-S/A AMPE Functional Statement Document (FSD)

1. The purpose of this letter is to forward a copy of the final version of Appendix 3B, I-S/A AMPE Message Format Validation Criteria, the I-S/A AMPE Functional Statement Document (Enclosure 1). This document also serves as Section 20, AMPE Message Format Validation Criteria, of the I-S/A AMPE Functional Requirements Description/Interface Control Document (FRD/ICD) and should be inserted therein. This final document contains all of the Service/Agency provided requirements with respect to message format validation criteria. This concludes formal staffing of the FSD and all portions of the FRD/ICD with the exception of Section 30, Security Appendix.

2. The requirements contained in this document have been organized and presented in such a manner as to assist the Services and Agencies in identifying their input. The I-S/A AMPE Specification Working Group currently meeting at Gunter Air Force Station, Alabama, will review this document and may make revisions to reduce the amount of duplication which currently exists. If, upon review, there are conflicting criteria generated by these requirements which cannot be resolved by the on-site S/A representative, then a special meeting will be called at Gunter Air Force Station to resolve these issues.

for

1 Enclosure a/s

ROBERT O. PETTY
Brigadier General, USAF
Director

Distribution:
Director, Information Systems ODUSDRE(C^3I), Washington, DC 20301
Deputy Director, Tactical/Theater C3 Systems, OJCS, Washington, DC 20301
Director, Defense Logistics Agency, ATTN: DLA/ZT, Cameron Station,
ALexandria, VA 22314
Director, National Security Agency, ATTN: T41, Ft George G. Meade, MD
20755
Director, National Security Agency, ATTN: S86, Ft George G. Meade, MD
20755
Director, National Security Agency, ATTN: C21, Ft George G. Meade, MD
20755
Director, Defense Intelligence Agency, ATTN: RCM-4, Washington, DC 20301
Director, Defense Logistics Agency Systems Automation Center, ATTN:
DSAC-R, P.O. Box 1605, Columbus, OH 43216
Director, Joint Tactical Communications Office, ATTN: TT-E-SD, Ft
Monmouth, NJ 07703
Director, Command and Control Communications & Computers, ATTN:
DAMO-C4S-C, Department of the Army, Washington, DC 20310
Director, Command and Control Communications & Computers, ATTN:
DAMO-C4P, Department of the Army, Washington, DC 20310
Director, Command and Control Communications & Computers, ATTN:
DAMO-C4L, Department of the Army, Washington, DC 20310
Assistant Chief of Staff for Intelligence, Department of the Army, ATTN:
DAMI-CIC, Washington, DC 20310
Assistant Chief of Staff for Intelligence, Department of the Army, ATTN:
DAMI-AML, Washington, DC 20310
Commmander, US Army Communications Command, ATTN: CC-OPS-PR, Ft
Huachuca, AZ 85613
Director, Naval Communications Division, Department of the Navy, ATTN:
OP-941H, Washington, DC 20350
Commander, Naval Telecommunications Command, ATTN: Code 231C,
4401 Massachusetts Avenue NW, Washington, DC 20390
Commander, Naval Tactical Automation Support Center, Naval Communications
Unit Washington, Washington, DC 20390
Director, Command & Control & Telecommunications, Headquarters, US Air
Force, ATTN: XOKCR, Washington, DC 20330
Director, Command & Control & Telecommunications, Headquarters, US Air
Force, ATTN: RDSS, Washington, DC 20330
Commander, Air Force Communications Command, ATTN: XODN, Scott AFB, IL
62225
Commander, Air Force Communications Computer Programming Center, ATTN:
SKX, Tinker AFB, OK 73145
Commander, Air Force Automated Systems Project Office, ATTN: PGA, Gunter
AFS, AL 36114
Commander, Air Force Automated Systems Project Office, ATTN: DCA Liaison
Office, Gunter AFS, AL 36114
Commander, Defense Communications Agency-European Area, ATTN: E400, APO
NY 09131
Commander, Defense Communications Agency-Pacific Area, ATTN: P400,
Wheeler AFB, HI 96854

INDEX

I-S/A AMPE MESSAGE FORMAT AND SECURITY VALIDATION/VERIFICATION

1.0. Introduction.

1.1. I-S/A AMPE Channel Parameter Information. In this appendix on message validation/verification, it is always assumed that the actual characteristics of any subscriber terminal match those contained in the I-S/A AMPE channel parameters. At various points, reference will be made to these characteristics without discussing the problems which may be caused by incorrect parameter entries since any such conflicts should be resolved in testing and prior to use of the subscriber terminal for "live" message traffic. For example, it is always assumed that if the subscriber terminal is a Mode I using a Transmission Identifier line, the I-S/A AMPE is set to reflect that optional capability.

1.2. Maintenance of Message Integrity. I-S/A AMPE message processing shall be designed such that both the loss of message data within the I-S/A AMPE and the intermixing of data from different messages (interlacing) are prohibited. Garbling or changing any single character within the I-S/A AMPE shall be minimized by the use of normal internal computer verification techniques.

1.2. Navy LDMX Validation Philosophy.

1.2.1 Validation Philosophy. The LDMX message validation is performed to insure that a message contains all of the properly formatted data to allow precedence and security processing, addressee routing and distribution assignment, transmissijon to "backbone" or other networks (where appropriate) and data to allow LDMX file updates for message recall and statistical data gathering/audit trails. Most format errors detected by the LDMX are sent to an interactive service terminal to allow LDMX personnel to either correct the message (interactively), or, if appropriate, reject the message to an LDMX service position. See paragraph 1.4 for interactive error processing and LDMX service position processing. The general philosophy of LDMX error processing is to interactively correct all errors possible without compromising security or delivery intention assignment by the message originator. In this sense, the LDMX performs a base level service to it's subscribers. It is recognized that the I-S/A AMPE is both a replacement for the backbone switching centers (ASCs) and the base level AMPE's, and as such it may not be feasible or appropriate for the I-S/A AMPE to provide the same level of interactive error processing/correction as that of the LDMX.

1.3. Message Formats. The I-S/A AMPE shall accept and process a variety of message formats to satisfy the requirements of different subscribers. GENSER subscribers will utilize formats IAW the JANAP 128 ( ), ACP 127, or ACP 126 as modified by Naval Telecommunications Publications (NTP) 4 (4), hereafter referred to as Modified ACP 126. DSSCS subscribers will utilize formats IAW the DOI- 103, the unique DOI-103 Abbreviated format and the Streamliner unique Abbreviated format. DSSCS subscribers who have a requirement to communicate with GENSER subscribers will utilize R/Y channels and will comply with GENSER formats. It is noted here for factual purposes that DSSCS subscribers are directly connected to DSSCS I-S/A AMPEs only. There will be no GENSER subscribers connected to the DSSCS I-S/A AMPEs; however, there are some DSSCS subscribers having the capability to send and receive GENSER traffic. An R/Y channel/port can be likened to a system high security - all applicable elements (i.e. link, operating system, facility, and personnel) meet the stringent security requirements necessary for certification.

Note that with some limitations for special formats, the format employed by a subscriber is independent of the mode of operation.

1.4. Error Processing. When I-S/A AMPE input message processing detects unacceptable errors within those message format areas that are validated, the following procedures shall be followed:

1.4.1. The I-S/A AMPE shall record the error condition and if the detected error is of sufficient seriousness to cause immediate rejection of the message, a reject message (RM) control character shall be generated to the input subscriber terminal and a service message shall be generated and transmitted to the input subscriber citing the reason for the message rejection. See FRD Section 21 for system generated service message conditions, addressees and formats.

1.4.2. Upon the completion of the format error detection process and when at least one error has been detected, the I-S/A AMPE shall prepare a service message indicating the errors found and whether or not the message has been accepted or rejected and forward it to the subscriber terminal. On any message rejection by the I-S/A AMPE on a controlled line, the RM shall be generated at the time of occurrence so that a minimum amount of data is involved. If the error is in the EOM validation, the RM shall be generated at that time vice an EOM ACK.

1.4.3 Navy LDMX Interactive Error Processing. The heading analysis modules display unprocessable leading lines for operator review and correction or rejection. The first line displayed on the console screen is the line in error to be corrected. The operator will use the first three spaces preceeding the line in error to indicate the type of correction or response he has chosen. Line 2 provides the reason for line 1 being unprocessable. Lines 3-12 are 10 lines of the message which follow line 1. Lines 13-19 are filler. Lines 20-22 contain message identification, classification, and system control data.

The VDT operator enters a one-character Action Code, a period, and a space (example: P.); and corrects or rejects the displayed error line. As an example, the operator has the following response options in correcting an invalid short title in format line 7.

RESPONSE	ACTION OF HEADING ANALYSIS MODULE
L. RUEDNKA/U.S.S. BAINES	Accept corrected line for routing assignment but message test not corrected.
P. RUEDNKA/U.S.S. BAINES	Accept corrected line for routing and replace the incorrect message line with the corrected line as it appears in the response.
X. PROTECT FOR BAINES	Reject the message to the service printer with the annotation "PROTECT FOR BAINES" (or whatever message is appropriate to notify the Service Center of reason for rejection or action to be taken. (See Para. 1.4.4.)
Y. TEXT CLASS ERROR	Reject the message to the TS Control with the annotation, "TEXT CLASS ERROR" or whatever message is appropriate to notify TS Control of reason for rejection or action to be taken.
C. (SVC note)	Ignore processing of this message line and continue processing the message (not valid in some cases). If a note is included after the C., the message will also be sent to the service printer with the note.

The LDMX Operator Manuals OM-01B, Volume 3 and OM-02A, Volume 4 summarizes the allowable response options for various unprocessable format line errors.

1.4.4 Interactive VDT Options. The VDT operator may respond to an error with one of five different options. The type or response acceptable for each format line is validated.

1.4.4.1 Options.

1.4.4.1.1 "X." or "X. xxxx". This signifies that the VDT operator wants to reject the message to the Service Center. The VDT operator may attach a narrative to the response (xxxx). The narrative is appended to and printed with the message at a service position.

1.4.4.1.2 "Y." or "Y. xxxx" This signifies that the VDT operator wants to reject the message to the TS Courier. The VDT operator may attach a narrative to the response (xxxx). The narrative is appended to and printed with the message at the TS Courier.

1.4.4.1.3 "C." or "C. xxxx" (Continue). This response is used when the VDT operator does not want to correct the error. The line in error will be ignored and processing will continue with the next line of the message. The "xxxx" is an optional service line which can be either the line in error or a comment added by the VDT operator.

1.4.4.1.4 "P. xxxx" (Physical Change). This signifies that the VDT operator wishes to replace the entire line. Both the line in error and corrected line are properly identified for subsequent processing. All routing and distribution is done according to the corrected line.

1.4.4.1.5 "L.xxxx" (Logical Change). The VDT operator wishes to use the input argument (xxxxx) in reprocessing the line and wants the line to remain unchanged in the message. For a logical correction, the new data entered through the VDT will be used to process the line, but the original line will be saved for subsequent processing.

1.4.4.2 Exceptions.

1. No continuations (C.) are permitted on format lines 2 through 4 and 13 through 16.

2. No logical changes (L.) are permitted on format lines 7 and 8 for sideroutes or on format line 11.

1.4.5 LDMX Service Position Processing. The service position consists of a service clerk, a line printer to list messages rejected by the system or interactive operators, and an interactive display console for entering, recalling, or editing messages. Basically, the clerk has four approaches to processing messages received at this position:

a. Using his interactive terminal, recall the message in error and correct/pilot the error as required and re-enter the message for processing. The message is then treated as a new message.

b. Service the originator.

c. Both of the Above.

d. Deliver the message by alternate means (other than AMPE).

2.0. General Comments - GENSER

2.1. Format Line 1 - Transmission Identifier Line and Pilots. A Transmission Identifier (TI) line is transmitted ahead of each message on all asynchronous and some synchronous terminal channels. For asynchronous channels (Mode II and Mode V), the TI line incorporates a Start-of-Message Sequence (SOMS); the Channel Designator (CD), and a three-digit Channel Sequence Number (CSN). For synchronous channels, full channel controls make use of a TI line unnecessary but TI use is available as an option if terminal procedures make message accountability by CSN desirable. The CSN is initialized to 001 at terminal or I-S/A AMPE start-up, and normally continues to 999 at which point it "rolls over" to 000, then 001, etc.

2.2. Asynchronous Channels. A Transmission Identifier (TI) line is mandatory for all traffic sent to the I-S/A AMPE by a teletype (asynchronous) subscriber terminal. This line must consist of the Start of Message Sequence (SOMS), "ZCZC", followed by a three alphabetic character Channel Designator (CD) or Channel Identifier (CID). This is followed for five level (ITA2) terminals by the figure shift (FIGS), which in turn is followed by a three numeric character channel sequence number (CSN). For five-level terminals, the CSN is followed by the letters shift (LTRS) machine function and, in normal operations, by the End-of-Line (EOL) sequence of two carriage returns (CR) and one line feed (LF).

2.2.1. To avoid loss of the first SOMS character due to occasional signal path instability or terminal mechanical equipment start-up delay, the SOMS may be preceded by the letter "V" as a "throwaway character", but the I-S/A AMPE shall not require this letter for proper recognition of the SOMS if the "ZCZC" sequence is correct.

2.2.2. Detection of two consecutive SOMS by the I-S/A AMPE without an intervening EOMS shall result in rejection of the presumed incomplete message for "Two Consecutive SOMS." On a Mode II channel, the second message shall be accepted if it is otherwise valid. On Mode I and V channels, the second message shall also be rejected.

2.3. Synchronous Channels. While the TI line is mandatory on all asynchronous channels, it is an option for Mode I (synchronous) subscriber terminals.

2.3.1. Since the synchronous user employs line block framing with the SOH character as the first character of the message, the "ZCZC" sequence is not employed. Instead, the first character following the SOH-SEL framing characters is the letter "C". This is followed by the CD, the figures shift (if the select character is an "A" indicating message preparation in five-level paper tape), the CSN, and, again for "A" select, a letters shift. No EOL is necessary, but the TI line will occupy a block by itself with no header data in the TI line block. The TI line block may either be terminated with an EM character, or filled out to a full 80 data characters. No data past the CSN shall be validated, and any remaining characters in the line block shall be discarded by the I-S/A AMPE.

2.4. Message Header Validation - Introduction. The I-S/A AMPE shall perform validation on message headers not only to insure correctness for such purposes as security and precedence but also to ensure that the routing indicators are valid for delivery.

2.4.1. The I-S/A AMPE shall validate both the header and the trailer (either the End-of-Message Sequence (EOMS) or the trailer card) of all messages. This shall include checking of the header station serial number against that contained in the trailer to protect against a straggled message - that is, a message following one with a garbled trailer or EOMS as one transmission. (See para 4.3.5.)

2.4.2. Before discussing the specifics of header validation, here is some additional information on what are termed "combined R and Y Community channels". These are correctly termed Y Community (DSSCS) channels over which R Community (GENSER) traffic may be sent. It shall be permitted for these channels to use different formats for the two communities. That is, these R/Y channel subscribers may use either a pre-established format IAW JANAP 128 ( ), ACP 127, or Modified ACP 126 to transmit GENSER messages and a pre-established format IAW DOI-103 or the DSSCS Abbreviated formats to transmit DSSCS messages but, with the exception of CRITIC, formats cannot be mixed within the community. This point is brought forth here because proper processing of the message depends on determination of the community of the traffic. If the message is garbled and an error is made in this determination, the message shall always be rejected.

3.0 GENERAL – COMMENTS- DSSCS

3.1 Reference Documents:

3.1.1 DSSCS Operating Instructions – DSSCS Address Groups (DAG) DOI-101

3.1.2. DSSCS Operating Instructions – DSSCS Routing Indicators DOI-102

3.1.3. DSSCS Operating Instruction – System/Data Procedures DOI-103

3.1.4 United States Signals Intelligence Directive (USSID) 307 Product Distribution

3.1.5. United States Signals Intelligence Directive (USSID) 309 Manual of Authorized Recipients of Product.

3.1.6. Message Preparation for DD Form 173 in Defense Special Security Communications System (DSSCS)

3.2. OFFICE SYMBOLS

3.2.1. Office symbols are optional within the DSSCS community. When used in message format lines 6, 7 or 8, they are placed after the plain language address (PLA) without intervening spaces and are preceded and followed by 2 slant (//) signs. Example: //DCX//

3.2.2 When more than one office symbol appears in format line 7 or 8, each office symbol is separated by one slant (/) sign. Example: //DCO/DCX//.

3.3. ADDRESSING

3.3.1. Geographic locations are not authorized after the DSSCS community Plain Language Address (PLA). Addressees are limited to no more than 12 characters as listed in DOI-102, for exception see paragraph 3.3.2.3.1.

3 3.2. Routing Indicators are not used in Format Lines 7 or 8 preceeding the PLA, except when an addressee has been designated delivery responsibility. It is used to designate a specific activity as communications guard or cryptoguard for an addressee who has no assigned routing indicator. When such a procedure is used, the station routing indicator responsible for delivery is suffixed with a "C" and placed in format line 7 or 8 preceeding the activity with cryptoguard responsbility. Example "YXXXXXC/SITE TWO".

3 3.2.1. COLLECTIVE ADDRESSING

3 3.2.1.1. In the DSSCS community "DSSCS Addressing Groups" (DAGs), (Ref paragraph 3 1.1) and Product Distributions (PD) (Ref paragraphs 3 1.4. and 3 1.5) may be used in lieu of listing each PLA.

3 3.2.1.2. DAGs consist of 5 alphebetic characters and are general purpose addressing groups, which contain a minimum of 5 addressees. The majority of the DAG's contain from 15 to 75 addressees.

3 3.2.1.3. When a DAG is used, the originator can exclude one or more addressees from a DAG for a specific message. The exclusion address is indicated in the message as a "LESS" addressee, immediately following the DAG in the address portion of the message.

```
EXAMPLE    "TO ZORRO<<=
            LESS STATION 15<<=
            LESS STATION 21<<=
            ETC "
```

3 3.2.1.4. A DAG may be used with any number of additional "write-in" addressees. The following example shows the manner in which two addressees not represented by the DAG are inserted.

```
EXAMPLE    "TO OHHOO
            STATION 15
            STATION 25"
```

3 3.2.2 Two or more DAGs may be used for addressing a message, with either/or additonal or LESS addressees for each DAG. Following is an example.

EXAMPLE: "TO OHHOD
LESS STATION 21
RANOS
STATION 5"

3 3.2.3. PRODUCT DISTRIBUTION

3 3.2.3.1 Product distribution symbols are composed of two elements, each separated by a slant (no space). The first element is the PLA of the originating unit. The second is a letter or letters that equate to the specific addressees (for example: NSA/DELTA or NSA/ALFA CHARLIE). A PD may contain more than 12 characters as stated in paragraph 2.3.1.

3 4 PAGING OF TRAFFIC

3 2.4.1. Paging of message traffic within the DSSCS community is not authorized.

3 5 MESSAGE LENGTH

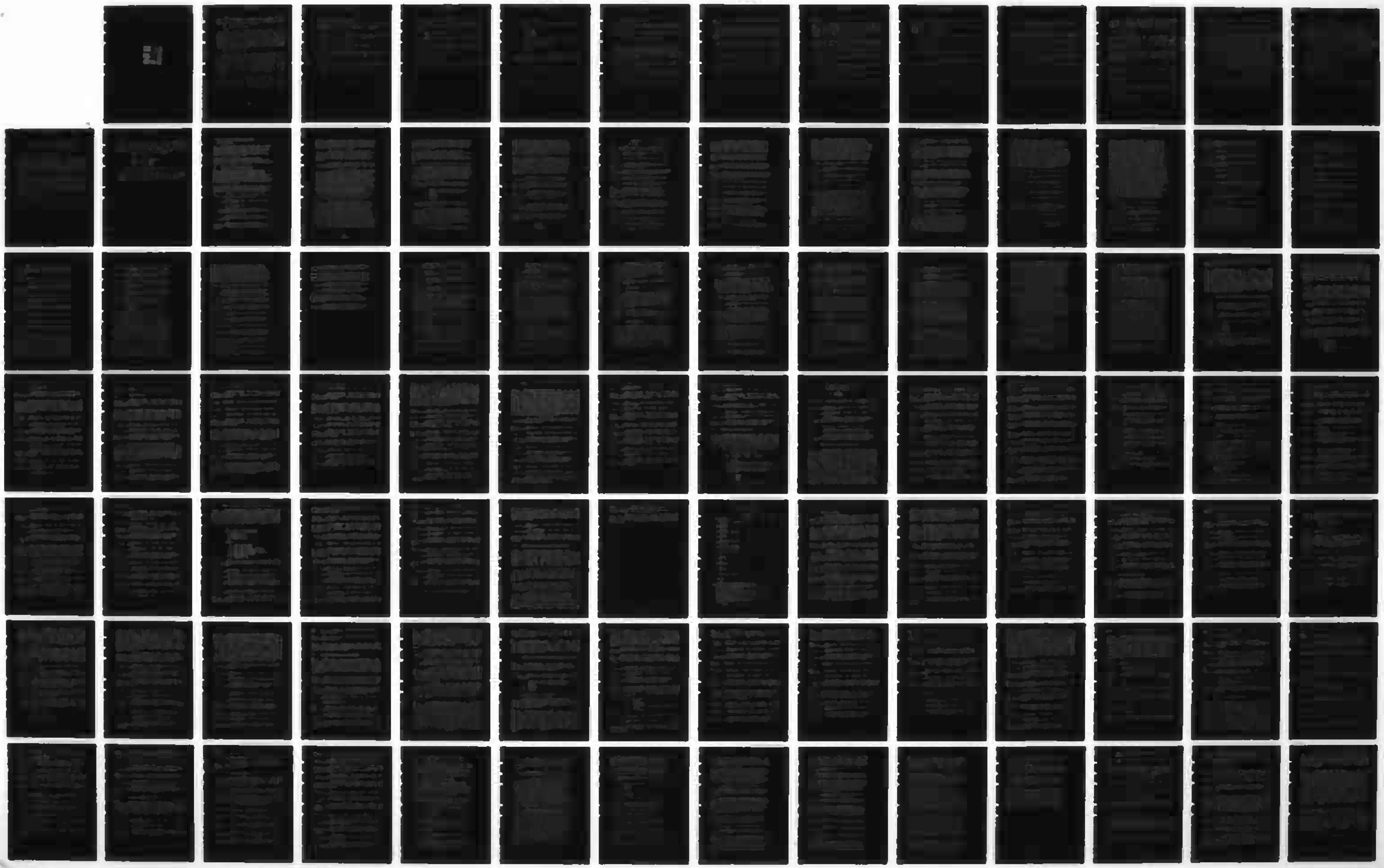
3 2.5.1. DSSCS message length is 40,000 characters, except for those messages that are routed to or through any collaborating communication center or mobile unit, which are limited to 5400 characters, per DOI-103.

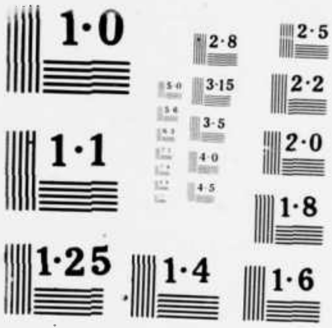
3 6 DUAL PRECEDENCE MESSAGES

3 6.1. On dual precedence messages, when the action precedence is FLASH and the information precedence is IMMEDIATE or lower, then two transmissions are required. One transmission will have the action precedence of FLASH in the message header and the second transmission will have the information precedence in the message header. The same procedures apply on collective addressing, i.e., DAG's and Product Distribtion, when action and information addressees are designated.

AD-A134 884 INTER-SERVICE/AGENCY AUTOMATED MESSAGE PROCESSING EXCHANGE PROGRAM FUNCTI..(U) DEFENSE COMMUNICATIONS AGENCY ARLINGTON VA 01 NOV 83 3/7

UNCLASSIFIED F/G 17/2 NL





NATIONAL BUREAU OF S

MICROCOPY RESOLUT TEST

3 6.2. On dual precedence messages in which both the action and information precedences are IMMEDIATE or lower, then the action precedence is placed in the message header and only one tranmission is required.

3 7. SECURITY PROCESSING

3 7.1. When the classification and special handling instructions do not dictate an output format the sytem shall use the addresses to determine the output format. If a addressee is duplicated across communities (GENSER and DSSCS), the I-S/A AMPE shall try to format the data according to other addressees in the data that can identify a specific community of interest. If the data contains only duplicate addressees and the classification (to include the message handling instructions) does not dictate and absolute community of interest routing, the I-S/A AMPE shall defer the formatting and routing to the DSSCS community.

3 8. SECTIONALIZATION

3 8.1. Message which exceed 40,000 characters (500 cards) for MODE I and MODE V terminals and 10,000 characters for MODE II terminals are considered long messages and will be divided into transmission sections. Messages routed to or through any collaborating communications facilities, or mobile units are limited to 900 groups (5400 characters) and must be divided into transmission sections. Those message originators having unique or special requirements for repeated preparation and transmission of messages containing 40,000 characters (500 cards) should coordinate with each addressee terminal for the continuous acceptance of long messages

3 8.2. Messages forwarded in transmission sections will be divided at a convenient point, but not beyond the number of characters prescribed. Immediately following the security classification, codeword, or restrictive handling instruction (if any) , insert "SECTION 1 OF __". Each additional transmission section will be identified as "SECTION __ OF __ ", and preceded by an identical message heading, except that it will contain a different station serial number for

each transmission section. The final transmission section will be identified as "FINAL SECTION OF __".

3 8.3. All information from format line 5 through the first full teletype line of the "SUBJ" line of format line 12 is carried over to all sections of a multi-section message.

3 9. END-OF-LINE FUNCTIONS

3 9.1. The normal end-of-line functions will be 2 carriage returns and 1 line feed, unless DSSCS operating signals, e.g., "ZZR" or "ZNZ1", appears in Format Line 5.

3 10. CANCELLING TRANSMISSIONS

3 10.1. The I-S/A AMPE and DSSCS terminals must be able to recognize and generate a cancel transmission (CANTRAN) sequence.

3 10.2. Input DSSCS terminals can cancel a transmission in one of two ways: 1) by depressing the "CANCEL" control button on MODE V and certain MODE I terminals; 2) MODE II terminals must use the CANTRAN sequence of SE's AR, optional for MODE I and V.

3 10.3. The I-S/A AMPE must detect and discard cancelled transmissions, by either a control character or CANTRAN sequence. A CANTRAN sequence is: "CC=E E E E E E E E AR CC=========NNNN", a minimum requirement: "CC=E E AR==NNNN".

3 10.3.1. The CANTRAN sequence generated by the I-S/A AMPE will be as follows: "CC=YXXXABC001 E E E E E E E E AR CC=========NNNN"

3 10.3.2. Following is a breakdown of the CANTRAN sequence.

3 10.3.2.1. "YXXX" is the Routing Indicator of the I-S/A AMPE which generated the CANTRAN.

3.10.3.2.2. "ABC" is the Channel Designator (CD) of the I-S/A AMPE generating the CANTRAN, if applicable.

3.10.3.2.3. "001" is the Channel Sequence Number (CSN) of the transmission that is being cancelled. If TI lines are not used the terminal, the I-S/A AMPE will "999" in this field.

3.10.3.2.4. "E E E E E E E E AR" is the prosign meaning "cancel this transmission".

3.10.3.2.5. All CANTRANS will be immediately followed by a valid EOM sequence of 2 carriage returns, 8 line feeds and four N's.

3.10.4. If the I-S/A AMPE must cancel an outgoing transmission currently in progress, it will send a cancel control character, always followed by the CANTRAN sequence.

3.10.5. On card messages, the cancellation is indicated by the eighth punch in the 81st column of the card.

3.11. COMEBACK COPY

3.2.11.1. The I-S/A AMPE shall provide the capability for the input terminal/originator of a message to receive: 1) a fully formatted copy of the outgoing message, or 2) the "as received" version including the M/R, distribution, and drafter/releaser information or both 1 and 2. The Option 2 comeback copy shall reflect the highest classification of either the message or the M/R.

3.12 FORMAT VALIDATION

3.12.1 The following precedences are authorized within the DSSCS community:

W - CRITIC
Z - FLASH
O - IMMEDIATE
P - PRIORITY
R - ROUTINE

3.12.2 The I-S/A AMPE shall recognize a CRITIC message in any one of four possible message formats.

DD-173 Joint Message Form Data
Abbreviated Message Format (AMF)
DOI-103 Special
JANAP 128

3.12.3 CRITIC Message - The I-S/A AMPE shall examine incoming transactions only to the extent necessary to verify that a transaction is a CRITIC message. No format or validation checks will be performed once a message has been recognized as a CRITIC.

EXAMPLE:

```
FORMAT LINE 1   ZCZCABC123
FORMAT LINE 2   WW YEKAAH
FORMAT LINE 16  NN========NNNN
```

3.12.3.1 The I-S/A AMPE shall handle a DD-173 Joint Message Form Data as a CRITIC if the following two criteria are met:

3.12.3.1.1 If a "W" appears in either the ACTION or INFO Addressee precedence block

3.12.3.1.2 The word "CRITIC" appears in the "Orig/Message Ident" block.

3.12.3.2 If either of the above criteria is met and the other is not, the I-S/A AMPE shall divert the data to an error correction console and notify the operator with a unique visual and audible alarm.

3.12.3.3 The I-S/A AMPE shall handle an AMF formatted message as a CRITIC if F/L 3 contains the following data:

3.12.3.3.1 The message precedence is "W".

3.12.3.3.2 The message precedence is followed by "space CRITIC".

3.12.3.4 For a JANAP 128 formatted message to be recognized as a CRITIC, the precedence must be "Z", the Routing Indicator must be "RUETIAA", and the word "CRITIC" must appear in F/L 12 followed by a space, carriage return, or line feed. If the word CRITIC is preceded or followed by "FOLLOW-UP" or "LATERAL" the message shall not be handled as a CRITIC. Upon recognition of a GENSER CRITIC, the I-S/A AMPE shall process the CRITIC as in Para 3.12.3

3.12.3.5 If either of the above criteria is met and the other is not, the I-S/A AMPE shall divert the message to an error correction console and notify the operator with a unique visual and audible alarm.

3.12.3.6 For a DOI-103 Special formatted message to be recognized as a CRITIC, the first nine characters of format line (F/L) 2 must immediately follow either the SOM sequence or F/L 1 and end of line sequence, or be within the first eighty (80) characters following a valid EOM sequence of the previous transaction.

3.12.3.7 The I-S/A AMPE shall separate CRITIC messages based on one of the following criteria which apply to formats listed in paragraph 3.12.2

3.123.7.1. A valid End-of-Message (EOM) indicator has been received. The End-of-Message sequence is defined in MIL-STD-188-C.

3.12.3.7.2. During the receipt of a CRITIC, if no activity exists on the communications line for sixty (60) seconds, the I-S/A AMPE shall generate a truncate indication, insert an EOM, and forward the CRITIC The I-S/A AMPE shall notify the input terminal that the CRITIC has been truncated and forwarded incompete. The service operator shall be alerted of the notification with a unique visual and audible alarm.

3.12.3.7.3. The I-S/A AMPE shall detect and resolve receipt of unpaired SOM bit sequences. The I-S/A AMPE shall insert an EOM if a second SOM is detected without an intervening EOM. The I-S/A AMPE shall continue processing the CRITIC and notify the service operator with a unique visual and audible alarm.

3.12.3.7.4. The I-S/A AMPE shall check for the SOM and EOM sequences. However, if an error is detected, the I-S/A AMPE shall continue processing the CRITIC and notify the service operator of the error.

3.12.3.7.5. The I-S/A AMPE shall detect an overlength (exceeding 5400 characters) CRITIC, generate a truncate indication, insert an EOM, continue processing the CRITIC, and notify the service operator with a unique visual and audible alarm and the originatir terminal via a service message.

3.12.3.8. The I-S/A AMPE shall acknowledge receipt of a CRITIC (R W) within two minutes of receipt.

3.12.4. DSSCS Messages

3.12.4.1. The I-S/A AMPE shall verify the Channel Designator (CD) to be the correct CD for the incoming line. When an invalid CD is detected, the I-S/A AMPE shall insert the proper CD, continue to process the message, generate a service message to the input terminal and notify the service operator.

3.12.4.2. The I-S/A AMPE shall verify the Channel Sequence Number (CSN) to be valid and in the proper sequence. The I-S/A AMPE shall send a ZFX as described in DOI-103 to the input terminal when an out of sequence CSN is detected and continue to process the message. If an otherwise invalid CSN is detected, the I-S/A AMPE shall record the message as the last good CSN received, continue processing, and notify the service operator and the input terminal.

3.12.4.3. Upon recognition of two consecutive SOM's without an intervening EOM, the I-S/A AMPE shall deliver all data preceding the second SOM to the error correction console for manual inspection and correction. The second SOM shall then be treated as the beginning of a new transaction.

3.12.4.4. The I-S/A AMPE shall recognize a DSSCS message by the presence of "Y" Routing Indicators (RI), i.e., RI's that begin with the letter "Y", in F/L 2 of the message

3.12.4.5. The I-S/A AMPE shall separate DSSCS messages on the basis of valid SOM and EOM sequences. The I-S/A AMPE shall perform the straggler checks described in DOI-103 and DOD Directive C-5030.58-M.

3.12.4.6. The I-S/A AMPE shall detect an EOM sequence and Station Serial Number mismatch, reject the message and notify the input terminal and the I-S/A AMPE operator.

3.12.4.7 The I-S/A AMPE shall detect an overlength message, generate a truncate indication, insert an EOM, continue processing the message, and notify the service operator and the originating terminal via a service message.

3.12.4.8. The I-S/A AMPE shall detect an idle line condition once a valid transaction has begun. If no activity occurs on the line for (3) minutes, the I-S/A AMPE shall notify the service operator

3.12.4.9. Following is an EXAMPLE of the format lines to be validated in in a DOI-103 message and validation checks that the I-S/A AMPE shall perform:

FORMAT LINE 2	PTTMZYUW YYOSRI 1234 1234567-MNSH--YYDEST YADEST.<<=
FORMAT LINE 4	ZNY MMNSH<<=
FORMAT LINE 15	#1234
FORMAT LINE 16	<<========NNNN

3.12.4.10. FORMAT LINE 1 - TRANSMISSION IDENTIFIER (TI) LINE.

3.12.4.10.1. For DSSCS MODE I terminals, the use of the TI is optional.

3.12.4.10.2. For those terminals using TI lines, the following rules apply.

3.12.4.10.2.1. For DSSCS MODE I terminals using a full TI Line and all MODE II and MODE V terminals, the TI line is as follows:

3.12.4.10.2.2. The first four characters are "ZCZC".

3.12.4.10.2.3. The fifth, sixth and seventh characters are the Channel Designator (CD). It must match the CD stored in the I-S/A AMPE for that channel.

3.12.4.10.2.4. The eighth character is a figure shift if the terminal operates in the ITA-2 code.

3.12.4.10.2.5. The next three characters are the Channel Sequence Number (CSN). A CSN is considered in error if it is either non-numeric, or if it is not the next expected CSN.

3.12.4.10.2.6. The 12th character is a letter function if the terminal operates in the ITA-2 code.

3.12.4.10.2.7. For DSSCS MODE I terminals using the the abbreviated TI line, the start of message "ZCZC" is abbreivated and only the "Z" is generated and sent to the I-S/A AMPE. The rest of the TI line processing is the same as paragraphs

3.12.4.10.2 thru 3.12.4.10.2.6.

3.12.4.10.2.8. Any error in Format Line 1 will not result in the message being rejected, except for duplicate CSN.

3.12.4.11. FORMAT LINE 2 contains the following:

3.12.4.11.1. FIELD 1 is the precedence. Only FLASH, IMMEDIATE, PRIORITY and ROUTINE are authorized. Any invalid character will require the I-S/A AMPE to process the message at IMMEDIATE preceaence, but leave the character as received.

3.12.4.11.2. FIELD 2 and 3 are the Language Media Format (LMF). The following LMF's are authorized in DSSCS; A, B, C, D, E, G, H, I, R, T and Y. Any character, other than these listed, will result in the message being rejected.

3.12.4.11.2.1. The first LMF character is the input station media of transmission. The second LMF character is the preferred output LMF.

3.12.4.11.2.2. The LMF's of E, H, and R can only be paired with A, C, and T respectively, and the LMF's of B, D, and I can only be paired with themselves. Any unauthorized pairing will result in the message being rejected

3.12.4.11.2.3. The LMF's of "G" and "Y" are generated by the I-S/A AMPE. The LMF's of "GT" and "YT" indicates that the I-S/A AMPE preformed format conversion on the message.

3.12.4.11.3. FIELD 4 is the DSSCS security sentinel "M". If there is any other character in this field, the message will be rejected.

3.12.4.11.4. FIELDS 5 thru 8 are the Content Indicator Code (CIC). The four character CIC field (also called the communications action identifier field when it contains communications instructions) contains information related to the type of message being processed. The CIC is validated to be either four alphabetic or three alphabetic and one numeric characters.

3.12. 4. 11. 4. 1. If the message has a SEL "A", indicating preparation in ITA-2 paper tape, and the CIC contains a numeric character in the fourth character position, the appropriate shift characters must precede and follow the character. If the shift functions are not present, the message will be rejected

3.12. 4. 11. 5. FIELD 9 is a space. If not present, the message must be rejected.

3.12. 4. 11. 6. FIELDS 10 thru 16 are the Originating Station Routing Indicator (OSRI). On DSSCS messages, the OSRI must start with the letter "Y" and are six characters long. However, a seventh character may be added to indicate . All characters must be alphabetic, or the message is rejected. If a six character OSRI is used, then the seventh position must be a space, or the message will be rejected

INSERT

indicator or by automated systems to indicate automatic generated service messages.

3.12.4. 11. 7. FIELDS 17 thru 20 are the Station Serial Number (SSN). If the station is operating in the ITA-2 code, then the SSN must be preceeded by a figure (upper case) function. The SSN must be all numbers or the message is rejected. The SSN also is used as the End of Message (EOM) validation number in message format line 15.

3.12.4. 11. 8. FIELD 21 is a space, or the message is rejected.

3.12. 4. 11. 9. FIELDS 22 thru 28 are the Time-of-File (TOF). This field must be all numbers. More then or less than seven numbers, or alphabetic characters will result in the message being rejected.

3.12. 4. 11. 10. FIELD 29 is a dash (-) which indicates the start of the security field. If not present, the message will be rejected.

3.12.4. 11. 11. FIELDS 30 thru 33 are the security field. Position 30 must be the DSSCS security sentinel of "M", or the message is rejected ⓤ Position 31 through 33 is the Transmission Control Code (TCC). The TCC is derived from information contained in message format line 12, that is the

ⓤ INSERT

For stations operating in ITA Code, Position 30 must be preceeded by a letters (lower case) function.

classification, codeword, caveats, and other data appearing in message Format Line 12.

3.12.4.11.11.1. The I-S/A AMPE must validate that the TCC in message format lines 2 and 4 match and are valid. Any error will result in the message being rejected.

3.12.4.11.12. FIELDS 34 and 35 are 2 dashes (--), which indicates the start of routing. Any invalid character or less than two dashes will result in the message being rejected. If a station operate in the ITA-2 Code, the two dashes must be preceeded by a figures (upper case) function and followe by a lette (lower case function.

3.12.4.11.13. FIELD 36 is the start of routing. All DSSCS RI's must start with the letter "Y", or the message is rejected. DSSCS RI's are six letters, but there can be a seventh letter. Each RI is separated by a space, or the message is rejected. A maximum of 4 RIs will appear on the first line of Format Line 2, with a maximum of 9 routing indicators on each successive line. A maximum of 500 RI's are authorized on a DSSCS message. If a message exceeds 500 RI's, the message is rejected. The message will be rejected if RI's are split across a line, such as the first 3 character on one line then end of line functions followed by the remainder of the RI. If any routing indicator begins with any character other then a Y, the entire message must be rejected and none of the remaining or valid routing indicators are processed ∧ A period (.) will be inserted following the last addressee's RI to indicate end-of-routing ∧ If the station is operating in the ITA-2 Code the period (.) must be [illegible]ceeded by a figure (upper case) function and should be followed by a letters (lower case) functio

3.12.4.12. FORMAT LINE 4, SECURITY LINE

3.12.4.12.1. The first three characters are the security warning operating signal. On DSSCS messages this will always be "ZNY", including unclassified and unclassified EFTO messages. Following the security warning operationg signal, there must be a space character, or the message is rejected. Following the space is the DSSCS security sentinel "MM", any other characters or only one "M" will result in the message being rejected. Following the "MM" is the DSSCS Transmission Control Code (TCC). The TCCs in Format Line 2 and 4 must match, or the message is rejected.

3.12.4.13. FORMAT LINE 15

3.12.4.13.1. This line has two separate functions. Each function must be on a line by itself. The first line(s) is the correction line. (If used, it must contain the prosign "C" followed by necessary corrections.) On the last line is the End Of Message (EOM) validation. It contains a number symbol (#) immediately followed by the four digit station serial number which appeared in format line 2, positions 17 thru 20. If the number symbol is missing; there is less then four numbers, or the EOM validation numbers do not match the SSN in message format line 2, the message is rejected.If the station is operating in the ITA Code, the numbers symbol (#) is preceeded by a figures (upper case) function and the last number the four digit number is followed by a letters (lo case) func

3.12.4.14. Format line 16, End of Message (EOM).

3.12.4.14.1 The EOM functions are "2 carriage returns (CR), 8 line feeds (LF) and 4 N's, e.g., "<<========NNNN". To allow for errors in the number of 'line feeds, the I-S/A AMPE shall accept as a minimum 2 line feeds and 4 N'.

3.12.4.15. Following is an EXAMPLE of an DOI-103 SPECIAL formatted message and the format validation checks that the I-S/A AMPE shall perform.

```
FORMAT LINE 1    ZCZCABC123
FORMAT LINE 2    PP YYDEST YYDEST<<=
FORMAT LINE 3    DE YYDSRI #1234 1231547<<=
FORMAT LINE 4    ZNY MMNSH<<=
FORMAT LINE 15   #1234
FORMAT LINE 16   <<========NNNN
```

3.12.4.15.1. Format line 1 - See paragraph 3.12.4.10.

3.12.4.15.2. Format Line 2 - Contains the dual precedence prosign and the destination routing indicators

3.12.4.15.3. Format line 3 - Contains the prosign DE, the originating stations routing indicator, the station serial number preceded by a hatch mark, and the file time of the message

3.12.4.15.4. Format line 4 - See paragraph 3.12.4.12.

3.12.4.15.5. Format line 15 - See paragraph 3.12.4.13.

3.12.4.15.6. Format line 16 - See paragraph 3.12.4.14.

3.12.5. DD-173 JOINT MESSAGE FORM DATA

3.12.5.1. The I-S/A AMPE shall recognize DD-173 transactions from various input devices, i.e., optical character readers, keyboard/display devices (cathode ray tubes, etc.). The I-S/A AMPE shall recognize a DD-173 transaction that contains one or more pages. The I-S/A AMPE shall validate the precedence, classification, a Message ID, a page number, and on the last page of the message the total number of pages. The I-S/A AMPE shall detect the start of the DD-173 message as a function of the line control procedures for the input line.

3.12.5.2. The I-S/A AMPE shall check the page number and Message ID of each incoming DD-173 form. If the Message ID field is missing or invalid (improper) alphanumeric format, inconsistent across pages, etc.), precedence character missing or invalid, classification missing or invalid, or if the page number number is in error (i.e., missing, non-numeric, out of sequence, etc.), the I-S/A AMPE shall route the message to the service operator. For messages delivered to the service operator, that are Flash precedence or above, the I-S/A AMPE shall alert the service operator with a visual and audible alarm.

3.12.5.3. The I-S/A AMPE shall detect an idle line condition once a valid transaction has begun If no activity occurs on the line for a three (3) minutes, the I-S/A AMPE shall notify the service operator.

3.12.6. ABBREVIATED MESSAGE FORMAT (AMF) RECORD MESSAGE

3.126.1. The I-S/A AMPE shall recognize Abbreviated Message Format (AMF) transactions by the presence of "QQQQ" in line 2 in positions 1 through 4. The I-S/A AMPE shall guard against interlaced messages by checking for duplicate "QQQQ" (NOTE: "QQQQ" also indicates end of classification line). If an error is detected, the I-S/A AMPE shall deliver the message to the service operator.

```
EXAMPLE:

FORMAT  LINE  1   ZCZCABC123
FORMAT  LINE  2   QQQQ
STUTTER LINE      QQQQ
FORMAT  LINE 16   NNNN
```

3.12.6.2. The I-S/A AMPE shall separate AMF messages on the basis of valid SOM and EOM sequences.

3.12.6.3. The I-S/A AMPE shall detect the following error conditions and process them as described above for DSSCS messages (see paragraph 3.12.4.1of this appendix): Overlength messages, Channel Designator (CD) errors, Channel Sequence Number (CSN) errors, and Idle line conditions.

4.0 JANAP 128 Message Processing Requirements.

4.1 General Comments.

4.1.1. This section details existing JANAP 128 format validation processing. The checks and validations currently performed and identified herein shall be performed by the I-S/A AMPE in such a manner that subscribers are provided the same service on an interface and interaction basis that they currently derive from existing ASCs and Service/Agency AMPEs.

4.1.2. There are two categories of JANAP format header - "teletypewriter" which is used with that input medium and "data pattern" which is used with all other media. The differences, where existing, will be described in this section.

4.2. Validation/Verification Requirements

4.2.1. Format Line 1 - Transmission Identifier (TI) Line. I-S/A AMPE validation of the TI line shall be identical for both asynchronous channels (Mode II and V teletypewriter terminals whose use of a TI line is mandatory) and synchronous channels (Mode I users who employ line block framing and whose use of a TI line is optional, but must be specified at the time the I-S/A AMPE sets the port/channel parameters). All TI lines through the CD-CSN fields shall be processed as follows:

4.2.1.1. The first characters of the TI line block must be a Start of Header (SOH) and a select (SEL) character. If the channel is asynchronous, these shall have been inserted by the I-S/A AMPE; if the channel is synchronous, the terminal has inserted them.

4.2.1.2. Check 1.1.a. The first data characters of the TI line must be a valid Start of Message Sequence (SOMS).

Error Condition - None - nothing can be recognized prior to receipt of the SOH.

Error Resolution - N/A

4.2.1.3. Check 1.1.b. The next three characters of the TI line must be the Channel Designator (CD) and must match the CD stored at the I-S/A AMPE for that port/channel.

Error Condition - A CD shall be considered to be in error if it does not match the CD stored in the I-S/A AMPE for its' associated channel.

Error Resolution - Except for messages of ECP or Flash precedence, messages having CD errors shall be rejected to the input port/channel. Precedence categories are explained later in this document.

4.2.1.4. Check 1.1.c. The next character of the TI line can be either a figures shift or the first character of the CSN field; the figures shift must be present for "A" Select (ITA 2) messages and may or may not be present for other selects. If the CSN is correct, TI line processing is complete at this point.

Error Condition - A CSN shall considered to be in error if it is either non-numeric or if it is not the next expected CSN; i.e., one greater than the last "accepted" from a Mode V port/channel or "received" from a Mode I or II port/channel. For this purpose, a CSN of 000 shall be considered to be one greater than 999.

Error Resolution - Messages of ECP or Flash precedence shall be accepted regardless of CSN errors detected. Other messages having CSN errors shall be processed as follows:

If the CSN is a duplicate of the last "accepted" (Mode V) or "received" (Mode I/II), the message shall be rejected to the input port/channel. This is the only instance of CSN error where a message shall be rejected by the I-S/A AMPE which shall generate an "INVALID CSN" message to the input port/channel and log the error condition for future compilations such as the existing Communications Improvement Memorandum (CIM) program. If the CSN is incorrect for any other reason including being non-numeric, the message shall be accepted. However, these errors shall cause the I-S/A AMPE to generate a service message to the input port/channel citing the CD and CSN as well as other pertinent message identification data. This service message shall indicate "INVALID CD", "INVALID CSN" and whether the message was accepted or rejected. A duplicate CSN shall cause generation of an additional service message, "DUPE CSN". When a CSN is received out of sequence, an open number (ZFX) service message shall be generated to the input port or channel detailing the missing CSNs.

4.2.1.5. Further I-S/A AMPE TI Line processing. To maintain CSN continuity between the I-S/A AMPE and the terminal, the I-S/A AMPE tables shall be updated based on the results of CSN and message processing. When a CSN is rejected (i.e., duplicate condition), no CSN updating shall be performed. When a CSN is accepted, even if it is out of sequence, the accepted CSN (or the expected CSN, if the received CSN is non-numeric) shall be made the last accepted CSN for processing of future messages. When the channel is Mode I or Mode II, this update shall be done immediately on receipt of the TI line whether the associated message is accepted or not, since the Mode I or Mode II terminal is assumed to update the CSN at the beginning of each message transmission. This is also consistent with a terminal transmitting a tape in which there are pre-cut CSN's preceding each message. Since Mode V procedures require that CSN's be updated on acceptance of the message, Mode V terminal equipment does not update its TI generator until the associated message has been acknowledged by the I-S/A AMPE. Consequently, the I-S/A AMPE also shall not update the last accepted CSN on a Mode V channel until the message has been validated and accepted, and the ACK for the message has been sent to the terminal.

4.3. Format Line 2 - Message Header. For I-S/A AMPE validation/verification purposes, the JANAP header shall be divided into three parts: Header data up to and including the Start-of-Routing Sequence (Format Line 2); the Routing Indicator Field (still a part of Format Line 2); and the Security Line (Format Line 4).

4.3.1. Header Validation/Verification Through the Start-of-Routing.

4.3.1.1. Precedence Field. The first header field to be validated shall be the precedence field. It should be noted that even though the TI line is the first data received from the port/channel, it shall not be the first message area to be processed. The precedence field shall be processed first since the precedence of the message affects the decision on whether to accept a TI line with errored fields. Once validated, the precedence shall be saved for later correlation with FL5 precedence(s).

4.3.1.1.1. Check 2.1.a. Precedence is a single character, the first character of the header and shall be validated to be one of five characters:

"Y" - Emergency Command Precedence (ECP) which may be input only on authorized ports/channels.
"Z" - Flash
"O" - Immediate
"P" - Priority
"R" - Routine

Error Condition - If the field is not one of the five precedence characters specified above or "Y" is received from a port/channel not authorized its use.

Error Resolution - An error in the precedence field of either an invalid or an unauthorized character shall result in message rejection on all except Mode II channels where the invalid precedence character shall be replaced by an "O" (immediate) and the message processed at that precedence level. Errors in the precedence field which cause rejection shall result in generation of an "INVALID HEADER" error condition except for attempted use of ECP by an unauthorized user, which shall cause generation of a separate "UNAUTHORIZED USE OF ECP" error condition.

4.3.1.2. Language Media Format (LMF). The next field to be validated in a JANAP format message shall be the Language and Media

Format (LMF) field. This is a two character field in which the first character (LMF1) indicates the medium in which the input message was originally prepared. It is sometimes also called the Input LMF or ILMF. The ILMF must be consistent with the select character (SEL). The second character (LMF2) indicates the medium in which the originator prefers the message to be delivered to the addressee. It is sometimes also referred to as the Output LMF (OLMF) or Preferred Output LMF (POLMF). Input header processing merely validates the SEL/LMF combination.

4.3.1.2.1. Check 2.2.a. In the I-S/A AMPE, the LMF pair shall never be validated separately. LMF Validation shall always be combined with validation of the SEL, and the three characters shall be validated together. If the message is from a TI user, the SEL shall be obtained from the second framing character of the TI line block. Otherwise, it shall be obtained from the second framing character of the header line block. Once the SEL-LMF combination passes validation, the LMF pair information shall be saved to determine whether a message of the specified LMF can be delivered to a given RI.

Error Condition - If the SEL/LMF combination does not match any I-S/A AMPE table entry, the SEL shall be validated separately.

Error Resolution - If the SEL is invalid, an error condition shall be recorded and the message shall be rejected with no exceptions. A "REPROTECT TO ALL ADDRESSEES" service message shall be generated.

If the message is high-precedence (Cat I) and not magnetic tape, the LMF field shall be corrected to make the invalid LMF(s) the most common ones for that SEL ("T" for "A" Select, "A" for "H" Select, "C" for "D" Select). If LMF1 is valid and is "H", "E", or "R", an invalid LMF2 shall be made "C", "A", or "T" respectively.

When the SEL is valid, but one of the LMF characters is invalid, a test shall be made of the message precedence and of the SEL. If the message has a SEL of "B" or "C" (magnetic tape), or is of low precedence, it shall be rejected, with an "INVALID HEADER" service message being generated.

4.3.1.3. Single Security Character Field. The next field to be validated shall be the single character security field. The single character which indicates the security, shall be one of the following characters:

"T" - Top Secret
"S" - Secret
"C" - Confidential
"R" - Restricted

"E" - Unclas E F T O -(encrypt for transmission only)
"U" - Unclas

A single card message (LMF of SC) is only authorized a security level of unclassified and this field shall be validated to be a "U".

4.3.1.3.1. Check 2.3.a. The single character shall be compared to the valid security characters above.

Error Condition - Detection of an invalid security character.

Error Resolution - An error shall cause rejection, with generation of an "INVALID SECURITY FIELD - SEC" service message. There shall be no exceptions.

4.3.1.3.2. Check 2.3.b. The security of the message as indicated by this character, shall also be tested against the security of the channel over which the message is being received.

Error Condition - If the message security is higher than the channel security, the message is in error.

Error Resolution - The message shall be rejected as above for security error. There shall be no exceptions.

4.3.1.4. Content Indicator Code (CIC) Field. The four character CIC field (also called the Communications Action Identifier field when it contains communications instructions) contains information related to the type of message being processed. See Appendix 19A for specific additional codes and required action.

4.3.1.4.1. Check 2.4.a. If the message has a SEL of "A", indicating preparation in ITA2 paper tape, and the CIC contains a numeric character in the fourth character position, the appropriate shift characters must precede (SO/FIGS) and immediately follow (SI/LTRS) that character.

Error Condition - Absence of the necessary shifts indicates that the message preparation medium does not conform to the select character.

Error Resolution - The message shall be rejected for "INVALID HEADER;" there shall be no exceptions in this case.

4.3.1.4.2. Check 2.4.b. The CIC shall be validated to be either four alphabetic or three alphabetic and one numeric characters.

Error Condition - Numeric character(s) in other than the fourth character position.

Error Resolution - Low precedence messages shall be rejected. Errors in the CIC field, such as numeric characters in the first three characters with other than an "A" select, shall be accepted if the message is high precedence (CAT I). When a high-precedence message is accepted with CIC field errors, the CIC field shall be changed to "WWWW." This shall be be transmitted to the receiving terminal in lieu of the original errored CIC field.

4.3.1.4.3. Check 2.4.c. Two special CIC's are used to provide special handling to Flash precedence Emergency Action Messages (EAMs). The I-S/A AMPE shall check to see if the CIC is in this category.

Action - Detection of these CIC's in a Flash message shall cause that message to take precedence for delivery over other Flash traffic. These CIC's shall be ignored in other than Flash messages.

4.3.1.5. Separator. The character following the CIC field must be a space (teletypewriter space, card no punch). Note that if the select is "A" and the fourth CIC character is numeric, the SI/LTR shift must precede the space separator.

4.3.1.5.1. Check 2.5.a. Check the character following the CIC field.

Error Condition - Any character other than a space character.

Error Resolution - Any other character shall cause rejection of the message for "INVALID HEADER." There are no exceptions.

4.3.1.6. Originating Station Routing Indicator (OSRI) Field. Following the separator is the seven character OSRI field. This must be a seven character RI in the JANAP format.

4.3.1.6.1. Check 2.6.a. The OSRI must be a valid RI and generally shall be validated in the same manner as a destination RI, i.e., all characters must be alphabetic; the relay portion of the RI (first four characters) must be valid; if the relay portion is the local I-S/A AMPE, the next two characters shall be checked for validity and the seventh character shall be verified to be an alphabetic character.

Error Condition - The OSRI is invalid.

Error Resolution - Any error in the OSRI field shall result in message rejection for "INVALID HEADER". There shall be no exceptions.

4.3.1.7. Originating Station Serial Number (OSSN) Field. Following the OSRI is the four-character OSSN field. After the alphabetic OSRI, an upshift (SO/FIGS) is required on "A" select messages No upshift shall be allowed with other selects. The OSSN shall be validated to be four numeric characters, and low precedence messages which fail this check rejected for "INVALID HEADER". Flash and ECP messages shall be accepted with four non-numeric characters other than space or hyphen and/or a variable number of shift characters. A valid OSSN shall be saved for later comparison with the Trailer Station Serial Number (TSSN) at the end of the message to insure that a "straggler" condition does not exist. Straggler checking is described in detail under End of Message validation.

4.3.1.7.1. Check 2.7.a. Check "A" SEL messages for an upshift (SO/FIGS) after the alphabetic OSRI.

Error Conditions - If an upshift (SO/FIGS) is not present on "A" select messages or if an upshift is present on any other type of message.

Error Resolution - An error shall cause message rejection for "INVALID HEADER" with no exceptions.

4.3.1.7.2. Check 2.7.b. The OSSN shall be validated to be four numeric characters.

Error Condition - The OSSN is not four numeric characters.

Error Resolution - When the message is ECP or Flash four non-numeric characters, other than space or hyphen (dash), shall be acceptable. The detection of a dash or a space before four non-shift characters are found shall cause rejection of the message for "INVALID HEADER". When a high-precedence message is accepted with an OSSN field containing non-numeric characters, the OSSN field shall be changed to "9999." In the case of such acceptable errors in either this field or in the following field, the fourth character of the Content Indicator Code field shall be changed to a "W" (provided the CIC field has not already been changed to 4 W's) to indicate to the receiving terminal the acceptance of an errored high-precedence message. These corrections shall be used to construct both the output header to a terminal and the "INVALID HEADER ACCEPT" service message, so that both the delivery terminal and the input terminal are aware of any changes made in these fields.

4.3.1.8. Separator. A space character separator (teletypewriter space, card no punch) must be present following the OSSN.

4.3.1.8.1. Check 2.8.a. Check for space character.

Error Condition - No space character following the OSSN.

Error Resolution - An error in the separator field shall result in message rejection for "INVALID HEADER". There shall be no exceptions.

4.3.1.9. Time-of-File (TOF) Field. Validation of the TOF field is the same as that for the OSSN field except that a seven-character field is involved rather than a four. Procedurally, the TOF field is composed of a three character ordinal date (001-365/366) and time (0000-2359). In a single card (LMF SC) message, the next three fields do not appear and the TOF field is followed immediately by the Start-of-Routing sentinel.

4.3.1.9.1. Check 2.9.a. Check for seven numeric characters.

Error Condition - Any condition other than seven numeric characters.

Error Resolution - ECP and Flash messages shall be accepted and processed under the same circumstances described in OSSN field errors in paragraph 4.3.1.7 and shall cause this field to be changed to "9999999". In all other instances, the message shall be rejected and an "INVALID HEADER" service message generated to the input port/channel.

NOTE: The next two fields, 4.3.1.10 and 4.3.1.11 pertain to data pattern messages but not single card (LMF SC) messages.

4.3.1.10. Separator. If the message is data pattern and not single card (LMF SC), this paragraph applies and a space character (no punch) separator must be present following the TOF field. Use of a space separator in this field on non-data pattern or single card data pattern messages shall result in the message being rejected and an "INVALID HEADER" service message generated to the input port/channel.

4.3.1.10.1. Check 2.10.a. Check for space character.

Error Condition - Any character other than a space following the TOF field.

Error Resolution - An error in the separator field results in message rejection for "INVALID HEADER".

4.3.1.11. Record Count Field. If the message is data pattern, and not single card, this paragraph applies. This field must be a four character Record Count Field. There shall be no exceptions. The record count is intended as a further safeguard against lost data. The Record Count field may consist of the letters MTMS, the letters PLTS, or a four digit number in the range 0003-0500. No other characters shall be permitted in a message received from a subscriber terminal. If the field is numeric, it must be a count of the actual number of records (cards or line blocks) in the message, including the header and trailer. Since this field does not appear in a single card (LMF SC) message, and a record count of two would indicate only a header and trailer, the minimum acceptable record count is 0003. The maximum record count which may be specified in this field is 0500. A Record Count field of MTMS indicates either that the message originator wishes to forego a record count check (MTMS also in trailer) or that the true record count will appear in the trailer card. Messages with a Record Count Field containing MTMS in both header and trailer or containing PLTS in the header may exceed the 500 line block limit, up to a maximum of 556 line blocks. The record count field shall be saved for later comparison with the record count field in the trailer card to ensure that the record count is correct. This is also described in detail under End-of-Message processing. Use of the Record Count field on non-data pattern or single card data pattern messages shall result in the message being rejected and an "INVALID HEADER" service message being generated to the input port/channel.

4.3.1.11.1. Check 2.11.a. If the field is numeric, the value of the field shall be checked.

Error Condition - A Record Count Field value which is less than 0003 or higher than 0500.

Error Resolution - Any error shall result in rejection for "INVALID RECORD COUNT". There shall be no exceptions.

4.3.1.11.2. Check 2.11.b. A Record Count field containing the letters PLTS or MTMS.

Error Condition - Any alphabetic characters other than PLTS or MTMS in this field. See para 4.3.7 for ASC pilot exceptions.

Error Resolution - The message shall be rejected and an "INVALID RECORD COUNT" service generated to the input port/channel.

4.3.1.12. Security Redundancy Field Sentinel. Following the record count field if the message is data pattern (excluding single card message), or following the TOF field if it is teletypewriter, must be the dash or hyphen (ITA2 uppercase "A", card "11" punch) signalling the start of the Security Redundancy field.

4.3.1.12.1. Check 2.12.a. Check for security sentinel.

Error Condition - Any character other than the dash.

Error Resolution - The message shall be rejected and an "INVALID HEADER" service message generated to the input port/channel. Use of this sentinel on a single card message shall also result in message rejection for "INVALID HEADER".

4.3.1.13. Security Redundancy Field. When the message is "A" SEL teletypewriter, the character following the dash must be a downshift (SI/LTRS). Since there is no record count field in this format, the upper case of the TOF field is continued through the dash, then the lower case is required for the security field. There is no provision for this field in a single card message and its use shall result in message rejection for "INVALID HEADER". In the JANAP format, the four character Security Redundancy field shall be validated in different ways. All four characters of the security redundancy fie]d must be identical to the single security character previously valiaated (the fourth data character of the header, paragraph4.3.1.3)provided the message is not addressed to an Allied destinarion or is not an AUTODIN Limited Privacy Service (ALPS) message. If ~~the~~ message is addressed to an Allied destination, the last two character positions of the Security Redundancy field must than be valid transmission release codes (TRCs). The TRC is a two character field which serves to ensure that a message can be transmitted to the Routing Indicators assigned. It is, essentially, a double check on the release of a message to non-U.S. subscribers, so that an erroneously inserted or garbled Routing Indicator will not cause release to an Allied destination of a message not intended for such release. If the characters in the TRC field of a JANAP format message being received on an Allied channel are not valid TRC characters, the message shall be rejected since an Allied JANAP user must employ a TRC. Two characters ("C" and "U"), may be either security or TRC characters; therefore, the TRC field, although a part of the Security Redundancy field, shall be validated separately. If the message is ALPS, the third character must be a "V" and the fourth character must be a valid community-of-interest designator. The last two characters (whether TRC, ALPS, or security) shall be used later to check against each routing indicator and also against the equivalent field in Format Line Four. Note that FL4 must be present whenever a TRC indication is present in FL2.

4.3.1.13.1. Check 2.13.a. For "A" select message, check for downshift character.

Error Condition - Absence of the downshift.

Error Resolution - The message shall be rejected, without exception, and an "INVALID HEADER" service message shall be generated to the input port/channel.

4.3.1.13.2. Check 2.13.b. Check the first two security characters against the single security character field (see Check 2.3.a.)

Error Condition - The first two characters are not identical to the single character security field.

Error Resolution - The message shall be rejected and an "INVALID SECURITY FIELD" service message shall be generated to the input port/channel.

4.3.1.13.3. Check 2.13.c. The last two characters of the Security Redundancy field shall be checked to see if they are valid TRC characters, ALPS designator and community-of-interest indicator, or security characters.

Error Condition - The two characters fail the validation check (not TRC characters, ALPS, or security characters).

Error Resolution - The message shall be rejected and an "INVALID SECURITY FIELD - TRC" service message shall be generated to the input port/channel.

4.3.1.13.4. Check 2.13.d. If more than one TRC is used in this field, (two is the maximum allowed per transmission) they are checked for alphabetical order.

Error Condition - The characters are not in alphabetical order.

Error Resolution - The message shall be rejected and an "INVALID SECURITY FIELD - TRC" service message shall be generated to the input port/channel.

4.3.1.14. Start of Routing (SOR) Field. Header validation then shall proceed to the SOR field. If the message is "A" select this is a four character field, upshift (SO/FIGS), dash, dash, downshift (SI/LTRS). If other than "A" select, the field is the two-character field, dash dash.

Error Condition - Any error in this field.

Error Resolution - The message shall be rejected and an "INVALID HEADER" service message is generated to the input port/channel. There are no exceptions.

4.3.2. Header Validation/Verification of the Routing Indicator (RI) Field.

4.3.2.1. Routing Indicator (RI) Field. The RI is the "address" of a message. In teletypewriter and single card messages this first character must immediately follow the SOR field. In teletypewriter messages ("A" or "H" SEL) with more than one RI, each successive RI must be separated by either one space or by a valid End-of-Line (EOL) sequence consisting of two carriage return (CR) functions and one line feed (LF) function. An RI may not be split by either spaces or by an EOL sequence in any instance (teletypewriter, card, or data pattern message). For multiple card and data pattern messages, spaces (no card punch) are allowed between RIs and between the last RI in a line block (card) and the end-of-line block.

4.3.2.1.1. Check 3.1.a. The first character must immediately follow the SOR field.

Error Condition - First character not found immediately following the start-of-routing field.

Error Resolution - The message shall be rejected for "INVALID ROUTING FIELD" with an automatic generated service to the input port/channel. There shall be no exceptions.

4.3.2.1.2. Check 3.1.b. No RI may exceed seven characters.

Error Condition - A routing indicator contains eight or more characters.

Error Resolution - The message shall be rejected for "INVALID ROUTING FIELD" with an automatic generated service to the input port/channel. No deliveries shall be made and there shall be no exceptions.

4.3.2.1.3. Check 3.1.c. No presence of shift characters or "lettering out" (except for the single upshift necessary before the EOR in an "A" select message.

Error Condition - Shift-in/shift-out function separating routing indicators.

Error Resolution - The message shall be rejected for "INVALID ROUTING FIELD" with an automatic generated service to the input port/channel. No deliveries shall be made and there shall be no exceptions.

4.3.2.1.4. Check 3.1.d. Presence of non-alphabetic or non-separator characters in this field.

Error Condition - Detection of a numeric character in this field.

Error Resolution - The message shall be rejected for "INVALID ROUTING FIELD" with an automatic generated service to the input port/channel. No deliveries shall be made and there shall be no exceptions.

4.3.2.1.5. Check 3.1.e. Mixture of GENSER and DSSCS community RIs on a Y or R/Y channel.

Error Condition - Any mixed "R" and "Y" routing indicators in this field on a Y or R/Y channel.

Error Resolution - The message shall be rejected for "INVALID ROUTING FIELD" with an automatic generated service to the input port/channel. No deliveries shall be made and there shall be no exceptions.

4.3.2.1.6. Check 3.1.f. Check for more than 500 RIs in this field.

Error Condition - 501 or more RIs in this field.

Error Resolution - The message shall be rejected for "EXCESSIVE ROUTING FIELD" with an automatic generated service to the input port/channel. No deliveries shall be made and there shall be no exceptions.

4.3.2.1.7. Check 3.1.g. No more than one RI on a single card (LMF SC) message.

Error Condition - Two RIs on a single card message.

Error Resolution - The message shall be rejected for "INVALID ROUTING FIELD" with an automatic generated service to the input port/channel. No deliveries shall be made and there shall be no exceptions.

4.3.2.1.8. Check 3.1.h. An RI may not be split by an end-of-line (EOL) sequence or End-Of-Line Block (EOLB).

Error Condition - A routing indicator is split by a valid EOL (2 CR, 1 LF) or EOLB (end of card).

Error Resolution - The message shall be rejected for "INVALID ROUTING FIELD" with an automatic generated service to the input port/channel. No deliveries shall be made and there shall be no exceptions.

4.3.2.1.9. Check 3.1.i. Each successive RI must be separated by one (and only one) space or by a valid EOL (2 CR, 1LF) sequence or EOLB.

Error Condition - Any character other than a single space character or a valid EOL (2CR, 1LF) sequence or an EOLB.

Error Resolution - The message shall be rejected for "INVALID ROUTING FIELD" with an automatic generated service to the input port/channel. No deliveries shall be made and there shall be no exceptions.

4.3.2.2. End-of-Routing Field. The JANAP format end-of-routing (EOR) consists of either the three character field upshift (SO/FIGS), period (.), downshift (SI/LTRS) for "A" select messages or the one character field of period (.) for other selects. For "A" and "H" select, the period must be immediately followed by a valid end-of-line (EOL) sequence (2 CR, 1 LF). For card format messages ("D" select), the remainder of the card following the EOR must be blank. Any characters between a card EOR and the end of the card shall cause message rejection. The only exception is a single card message (LMF SC) which shall be assumed to have both its text and EOM field following the EOR. For magnetic tape messages ("B" or "C" select) an end-of-medium (EM) character may be used immediately following the EOR. The EM character in any other position shall cause message rejection.

4.3.2.2.1. Check 3.2.a. Validate that there is a valid EOR.

Error Condition - Field contains more than three characters for an "A" select, or contains an invalid EOR sentinnel.

Error Resolution - The message shall be rejected for "INVALID HEADER" with an automatic generated service to the input port/channel. There shall be no exceptions.

4.3.2.2.2. Check 3.2.b. "D" select multiple card message must not have extraneous characters between EOR and end of the card.

Error Condition - Any punch falling between the EOR and the end of the card (Col 80).

Error Resolution - The message shall be rejected for "INVALID HEADER" with an automatic generated service to the input port/channel. There shall be no exceptions.

4.3.2.2.3. Check 3.2.c. Insure EM character, if used in a "B" or "C" select, is immediately following the EOR. If not used, the remainder of the line block must be spaced filled.

Error Condition - EM character does not immediately follow the EOR sentinnel.

Error Resolution - The message shall be rejected for "INVALID HEADER" with an automatic generated service to the input port/channel. There shall be no exceptions.

4.3.3. Header Validation/Verification of the Security Line.

4.3.3.1. Security Line (FL4). Following the EOR, the next field to be validated on all teletypewriter ("A" or "H" SEL) messages shall be the security line, format line four. FL4 is optional for data pattern messages having LMFs of BB, DD, II, CC, or HC, but must be present whenever a TRC or ALPS indication is present in FL2. Data pattern messages except single card messages, may have an optional pilot, identified by the letters "PLTS" in the record count field. If a pilot is present, it shall be validated as the header but the FL4 to be validated must follow the original header. There must not be a FL4 following the pilot header. For all teletypewriter and those data pattern messages using FL4, the first four characters following the EOR (original header on piloted card messages) must be the operating signal "ZNR" or "ZNY" followed by a space. When it has been determined that FL4 has been properly employed and the first four characters are valid, the security fields shall be processed. The first of these is five characters in length and may consist of five redundant security characters, three redundant security sharacters, one ALPS indicator ("V") and one ALPS community-of-interest character or three redundant security characters and two transmission release code (TRC) characters. If the fourth character of the security field is a "V" indicating ALPS protection is required, the next character shall be checked to insure that it is a currently valid ALPS community-of-interest indicator and that the terminal from which the message is being received is authorized use of this ALPS character. (When a valid ALPS code is found, special processing shall be entered so that no message data will be written to the history record past the point in FL4 where the ALPS code is detected.) Following the TRC field, separated by a slash ("/"), may be from one to four optional special handling designator (SHD) fields (separated by a slash), each of which consists of a five-character repetition of a SHD character.

4.3.3.1.1. Check 4.1.a. The first four characters of FL4 shall be checked to see if they are "ZNR" or "ZNY" and a space.

Error Conditions - The first four characters are not "ZNR" or "ZNY" and a space; "ZNY" and a space is used, but the security redundancy field in FL2 is "UUUU"; or "ZNR" and a space is used but the security redundance field in FL2 is other than "UUUU".

Error Resolution - The message shall be rejected and an "INVALID SECURITY FIELD" service message automatically generated to the input port/channel.

4.3.3.1.2. Check 4.2.a. The first three characters of the security field shall be validated to be redundant and must match the security redundancy field in FL2.

Error Condition - The characters are not redundant or do not match those in FL2.

Error Resolution - The message shall be rejected and an "INVALID SECURITY FIELD - SEC" service message automatically generated to the input port/channel.

4.3.3.1.3. Check 4.3.a. The next two characters shall be checked for security redundancy.

Error Condition - If the FL2 security redundancy field does not indicate ALPS processing or TRCs required, any characters in these two positions other than security redundancy characters are in error.

Error Resolution - The message shall be rejected and an "INVALID SECURITY FIELD - TRC" service message automatically generated to the input port/channel.

4.3.3.1.4. Check 4.3.b. The two characters shall be checked for valid, required TRC character(s).

Error Condition - The TRC characters are invalid, not redundant if only one TRC is required, or not in alphabetical order if more than one TRC is required.

Error Resolution - The message shall be rejected and an "INVALID SECURITY FIELD - TRC" service message automatically generated to the input port/channel.

4.3.3.1.5. Check 4.3.c. If the fourth character of the security field is a "V", ALPS processing is indicated. The next character shall be validated to insure that it is a currently valid ALPS community-of-interest indicator and that the terminal from which the message is being received is authorized use of this ALPS character.

Error Condition - Input station not authorized use of ALPS character or invalid community-of-interest indicator.

Error Resolution - The message shall be rejected and an "INVALID SECURITY FIELD - TRC" service message automatically generated to the input port/channel.

4.3.3.1.6. Check 4.4.a. After validation of the security redundancy/TRC/ALPS field, check shall be made for the Special Handling Designator (SHD) sentinel, a slash (/) or an end-of-line sentinel (CRCRLF).

Error Condition - Any character other than a slash (/) preceded and followed by the proper shift characters or a valid end-of-line sequence (CRCRLF) following the previous field.

Error Resolution - The message shall be rejected and an "INVALID SECURITY FIELD - SRC" service message is automatically generated to the input port/channel.

4.3.3.1.7. Check 4.4.b. If an SHD sentinel is found, the next five characters must be identical and must be a valid SHD category character as specified in ACP 117.

Error Condition - The five characters are not redundant, not valid SHD category characters, the classification of the message is UNCLAS or EFTO, or the input station is not authorized the SHD.

Error Resolution - The message shall be rejected and an "INVALID SECURITY FIELD - SRC" service message automatically generated to the input port/channel.

4.3.3.1.8. Check 4.4.c. If another SHD sentinel (/) is found, the next SHD field shall be validated in the same manner as the first. This shall be repeated for up to four SHD fields. If, after either the TRC field or after any SHD field except the fourth, a SHD sentinel is not found, there still exists the possibility that the message contains one, or another, SHD but that the sentinel is garbled or mispositioned. To reduce the possibility that a SHD message will be accepted without proper validation, the character immediately following the TRC of a valid SHD shall be validated to be a space or a carriage return.

Error Condition - A character other than a space or carriage return is encountered following the TRC or a valid SHD.

Error Resolution - The message shall be rejected and an "INVALID SECURITY FIELD - SRC" automatically generated to the input port/channel.

4.3.3.1.9. Check 4.4.d. If a space is encountered following the TRC or a valid SHD field, that character and 14 characters following it shall be examined in an attempt to find four redundant contiguous characters which would be considered a suspected SHD.

Error Condition - Any four contiguous characters (9999, SSSS, etc.) following the TRC or a valid SHD field.

Error Resolution - Message shall be rejected and an "INVALID SECURITY FIELD - SRC" service message automatically generated to the input port/channel.

4.3.3.1.10. Check 4.4.e. If a carriage return is encountered immediately following the TRC or a valid SHD field, it must be followed immediately by a second CR and one line-feed (CRCRLF).

Error Condition - A carriage return (CR) is encountered not immediately followed by a second and a line-feed.

Error Resolution - The message shall be rejected and an "INVALID SECURITY FIELD - SRC" service message automatically generated to the input port/channel.

4.3.4. Routing Indicator Validation.

4.3.4.1. General. If a message contains only one RI, and that RI is invalid, the message shall be rejected. If a message is input on a Y or an R/Y channel and contains a mixture of R and Y RIs, the message shall be rejected regardless of RI validity. If a similar message is input on an R channel, only the invalid RIs and those beginning with a character other than "R" shall be considered invalid and shall be rejected individually; the message shall be protected to those valid GENSER RIs.

4.3.4.2. Check 5.1.a. RI validation shall determine whether the RI is in the I-S/A AMPE RI tables. Each I-S/A AMPE's RI tables shall contain all directly connected tributaries' RIs, all other I-S/A AMPEs' RIs, and all Non Automatic Relay Centers' (NARCs) RIs. A GENSER RI may be from 4 to 7 characters but must contain 7 characters if addressed to an I-S/A AMPE subscriber. If the RI is a local I-S/A AMPE subscriber, the first six characters shall be checked for validity and determination of delivery destination, the seventh ignored. If the RI is a distant I-S/A AMPE subscriber or a NARC, local or remote, only the first four characters shall be checked for validity and determination of delivery destination. If the first four characters indicate a collective RI (RHCR), the last three characters determine the actual collective list for delivery destinations.

Error Condition - A routing indicator is not found in the RI tables.

Error Resolution - If the message contains only one RI or no valid RIs, it shall be rejected and an "INVALID ROUTING REPROTECT TO" service message automatically generated to the originating subscriber. If the message contains at least one valid RI, it shall be accepted and processed for delivery to the valid RI. An "INVALID ROUTING REPROTECT TO" service message shall be automatically generated to the originating subscriber advising of the invalid RI(s) requiring reprotection.

4.3.4.2.1. Check 5.1.b. When the RI has been determined to be valid, the message security shall be checked against the security of the destination RI. The destination RI security must be equal to or greater than the security of the message.

Error Condition - Security of the message is greater than the security assigned to the destination RI.

Error Resolution - If the message contained only one RI, or if all RIs failed the security check, the message shall be rejected and an "INVALID ROUTING - SEC" service message automatically generated to the originating subscriber. If the message contained at least one RI which passed the security check, the message shall not be rejected but shall be processed for delivery to the RI passing the check. The service message shall be automatically generated to the originating station advising of the remaining RIs requiring reprotection.

4.3.4.2.2. Check 5.1.c. The delivery of an EFTO message to an Allied RI shall be prohibited regardless of the security level assigned to the RI.

Error Condition - An EFTO message addressed to an Allied RI.

Error Resolution - If the message addresses only one RI, or if all RIs are Allied, the message shall be rejected and an "INVALID ROUTING - SEC" service message automatically generated to the originating subscriber. If the message contained at least one non-Allied RI which passed the security check, the message shall not be rejected but shall be processed for delivery to the RI passing the check. The service message shall be automaticallly generated to the originating subscriber advising the remaining RIs requiring reprotection.

4.3.4.2.3. Check 5.3.d. Each RI shall be checked to determine if it requires a validating TRC. All messages addressed to non-U.S. RIs require a TRC. Messages addressed to U.S. RIs are not checked against the TRC unless the message is from an Allied JANAP user.

Error Condition - Use of an invalid or incorrect TRC, or absence of a TRC when required.

Error Resolution - If the message is addressed to only one RI or if all RIs fail the TRC check, the message shall be rejected and an "INVALID ROUTING REPROTECT - TRC" service message automatically generated to the originating subscriber. If the message contained at least one valid RI which passed the TRC check, the message shall not be rejected but shall be processed for delivery to the RI passing the check. The service message shall be automatically generated to the originating subscriber advising of the remaining RIs requiring reprotection. If the message is a magnetic tape medium (LMF of BB, DD, or II) with an Allied RI, the service message shall be "INVALID ROUTING REPROTECT - LMF" instead of "TRC" since this media cannot be delivered to Allied users. (They do not have compatible equipment.)

4.3.4.2.4. Check 5.3.e. If the message is ALPS (U.S. RIs only), the destination associated with each RI shall be tested for ALPS community-of-interest authorization.

Error Condition - Invalid or absence of the community-of-interest designator.

Error Resolution - If the message is addressed to only one RI or if all RIs fail the ALPS check, the message shall be rejected and an "INVALID ROUTING REPROTECT - TRC" service message automatically generated to the originating subscriber. If the message contained at least one valid RI which passed the ALPS check, the message shall not be rejected but shall be processed for delivery to the RI passing the check. The service message shall be automatically generated to the originating subscriber advising of the remaining RIs requiring reprotection.

4.3.4.2.5. Check 5.3.f. If one or more special handling designator (SHD) codes are present, the destination RI shall be checked for authorization to receive each SHD.

Error Condition - Destination RI not authorized to received a particular SHD.

Error Resolution - If the message is addressed to only one RI or if all RIs fail the SHD check, the message shall be rejected and an "INVALID ROUTING REPROTECT - SRC" service message automatcally generated to the originating subscriber. If the message contained at least one valid RI which passed the SHD check, the message shall not be rejected but shall be processed for delivery to the RI passing the check. The service message shall be automatically generated to the originating subscriber advising of the remaining RIs requiring reprotection.

4.3.4.2.6. Check 5.3.g. Each RI shall be checked against the LMF of the message. Three LMFs indicate magnetic tape traffic (BB, DD, and II) and these messages shall not be delivered to a non-compatible destination RI. In addition, three LMFs (HC-Cards, EA-eight level paper tape, and RT-five level paper tape) indicate the originator's desire that medium exchange be prohibited, and these also shall not be delivered to a non-compatible terminal. Single card (SC) messages shall not be delivered to a teletypewriter terminal.

Error Condition - Any incompatibility detected as a result of the above check (e.g. addressing a SC message to a Mode II or Mode V).

Error Resolution - If the message is addressed to only one RI or if all RIs fail the LMF check, the message shall be rejected and an "INVALID ROUTING REPROTECT - LMF" service message automatically generated to the originating subscriber. If the message contained at least one valid RI which passed the LMF check, the message shall not be rejected but shall be processed for delivery to the RI passing the check. The service message shall be automatically generated to the originating subscriber advising of the remaining RIs requiring reprotection.

4.3.4.2.7. Check 5.3.h. Some multi-card and magnetic tape messges may not have a FL4 and delivery of these messages shall not be made to teletypewriter-only (narrative) terminals since both JANAP and ACP formats require FL4 on all teletype traffic. In addition, card and magnetic tape messages having a pilot shall not be delivered to an ACP terminal since format exchange would cause output of an ACP header with no FL4.

Error Condition - Any violation of the above check (e.g. card to card message with no FL4 addressed to a terminal who uses ACP format).

Error Resolution - If the message is addressed to only one RI or if all RIs fail this check, the message shall be rejected and an "INVALID ROUTING REPROTECT - MFE" service message automatically generated to the originating subscriber. If the message contained at least one valid RI which passed this check, the message shall not be rejected but shall be processed for delivery to the RI passing the check. The service message shall be automatically generated to the originating subscriber advising of the remaining RIs requiring reprotection.

4.3.4.2.8. Check 5.3.i. If the message contains a collective RI, the initial check shall be to determine if the CRI is valid.

Error Condition - Use of an invalid CRI.

Error Resolution - If the CRI is invalid and the message was only addressed to that RI or did not contain any valid RIs, the message shall be rejected and an "INVALID ROUTING REPROTECT TO" service message shall be automatically generated to the originating subscriber. If the message contained at least one valid RI which passed this check, the message shall not be rejected but shall be processed for delivery to the RI passing the check. The service message shall be generated to the originating subscriber advising of the RIs requiring reprotection. Detection of a CRI in an ALPS message shall result in message rejection and the automatic generation of an "INVALID SECURITY FIELD - TRC" service message.

4.3.4.2.9. Check 5.3.j. A check shall be made to determine if the input subscriber is authorized to introduce a CRI or a CAD. One exception to this check shall be that ports/channels authorized to input ECP messages may input CRIs in their ECP messages, but not in messages of other precedences unless they are also classmarked for this capability.

Error Condition - Attempted input of a CRI/CAD by a port/channel not classmarked for CRI/CAD input and not an ECP CRI by an authorized ECP port/channel.

Error Resolution - The message shall be rejected and an "UNAUTHORIZED USE OF CRI/CAD" service message shall be automatically generated to the input port/channel.

4.3.5. End-of Message (EOM) Processing. Upon completion of SOMS validation, a continual scan of each message for the end of message sequence (EOMS) shall be performed. The JANAP narrative format EOM procedurally consists of two carriage returns, eight line feeds, and the letters "NNNN" but the minimum required for recognition by the I-S/A AMPE shall be one line feed and four N's. In a·multiple block data pattern message it shall consist of the letters "NNNN" in columns 77 through 80 of the last line block/card. This scan and others that shall be performed for the detection of specific character sequences are described in this section.

4.3.5.1. Straggler Protection. A "straggler" is caused by a message without a valid start of message sequence (SOMS) following a message without a valid end of message sequence (EOMS) on an asynchronous channel, or two messages entered as one on a synchronous channel and framed SOH-ETX as a single message. To protect against straggler messages, the I-S/A AMPE shall validate the Originating Station Serial Number (OSSN) in the message header against the Trailer Station Serial Number (TSSN) found in the message trailer. Failure of straggler validation shall result in message rejection unless the message is Flash precedence, and the automatic generation of a "SUSPECTED STRAGGLER" service message to the input port or channel. Flash messages shall be accepted and the service message generated shall advise the input port or channel "HIGH PRECEDENCE MESSAGE ACCEPTED, REPROTECT SUSPECTED STRAGGLER".

4.3.5.1.1. Data Pattern Messages. The EOMS must be the "NNNN" sequence in columns 77 through 80. The EOM line block must contain the ETX character in the third framing character (FC3) and it is incumbent on the terminal to ensure that the EOM is properly recognized and the block properly framed. Receipt of an ETX framing character without a correct EOM shall result in message rejection and generation of an "INVALID EOM" service message to the input port/channel. Receipt of a valid EOM without the ETX shall result in non-recognition of the EOMS and an input message hiatus rejection of a following SOH lineblock, and the ultimate rejection of the errored message. Related to EOM processing shall be the check for a valid record count field in a multiple line block card or magnetic tape message. There is a relationship between this field and the record count field of the header. The trailer record count field must be either "MTMS", signifying a message from a magnetic tape terminal which does not count line blocks, or a four digit numeric field. The use of "PLTS" in the trailer shall be prohibited and shall result in message rejection and an "INVALID

RECORD COUNT" service message being automatically generated to the input port/channel. If "MTMS" appears in the record count field of both the header and trailer, no further checking of the actual line block/card count shall be performed. If a number appeared in the header and "MTMS" or a number in the trailer, the actual line block/card count received shall be checked against the header number, and the trailer record count field shall effectively be ignored. If "MTMS" appears in the header record count field and the trailer field contains a number, that number shall be compared to the actual count of the line blocks/cards received. Any disparity in the above two instances shall result in the message being rejected and an "INVALID RECORD COUNT" service message being automatically generated to the input port/channel. When the message header record count field contains the pilot indicator "PLTS", there shall be no check of either the header or trailer record counts against the actual number of blocks received.

4.3.5.1.2. Teletypewriter (Narrative) Messages. The minimum EOMS recognizable shall be one linefeed character and four N's in an uninterrupted sequence. More than eight line feeds, extraneous characters in the linefeed field, or extraneous characters between the TSSN and the required EOMS are acceptable provided that the straggler sentinel (#) falls within 23 characters of the required line feed and the required EOMS is not interrupted. If the EOMS does not fall within 23 characters of the TSSN, the message shall be rejected and a "SUSPECTED STRAGGLER" service message automatically generated to the input port/channel. On asynchronous channels, an invalid EOMS shall result in either an input message hiatus or a two consecutive SOM condition. Either shall result in message rejection. On synchronous channels, detection of the ETX framing character without prior detection of a valid EOMS shall result in message rejection and an "INVALID EOM" service message automatically generated to the input port/channel.

4.3.5.2. Cancel Transmission Sequence (CANTRANS). The I-S/A AMPE also shall scan for the presence of a CANTRANS which procedurally consists of 3 E's, each separated by a space, the letters "AR", and an EOMS of two carriage returns, eight line feeds, and four N's. The minimum recognizable by the I-S/A AMPE shall be two E's separated and followed by a space, "AR", one linefeed, and four N's. When a CANTRANS is recognized, the message shall be discarded by the I-S/A AMPE with a notification to the system I-S/A AMPE operator that the message has been discarded.

4.3.5.3. Excessive Message Length. An additional check that shall be performed during receipt of message text is a count of total line blocks/characters being received. Should this count exceed 556 line blocks (44,480 characters), the message shall be rejected and an "EXCESSIVE MESSAGE LENGTH" service message automatically generated to the input port/channel. Mode II channels shall be limited to 125 line blocks (10,000 characters).

4.3.5.4. Excessive Input Hiatus. Incoming messages shall be also monitored for any delay (hiatus) in receipt by the I-S/A AMPE. Wher no additional data is received for a non-CRITIC message in progress for a period of approximately three minutes, the message shall be rejected and a "NO EOM RECEIVED" service message automatically generated to the input port or channel.

4.3.5.5. Framing Character (FC) Processing. Framing characters shall be validated for all input messages. On asynchronous channels, these shall have been inserted and the message blocked and framed by the I-S/A AMPE itself so that FC validation shall be essentially a self-checking process by the I-S/A AMPE. On synchronous channels, FC validation shall ensure proper framing by the terminal device. Any framing character error shall result in message rejection with a "REPROTECT TO ALL ADDEES" service message being automatically generated to the input port/channel. In addition, notification of the FC error shall be provided to the system I-S/A AMPE operator so that any FC errors caused within the I-S/A AMPE itself may be detected and corrective action taken.

4.3.6 RI Processing Exception: Messages may be transmitted to a given I-S/A AMPE from a connected ASC (as the result of an ASC altroute action) that contain ASC pertinent destination RIs which are not normally pertinent to the given I-S/A AMPE. This is because, unlike the I-S/A AMPE, an ASC delivers an altrouted message with the destination RI intact (as received from the message originator) to the alternate delivery station. Each ASC altroute invoke or revoke action involving an I-S/A AMPE as an alternate delivery station will result in ASC transmission of alternate routing notification service messages (specified in the AUTODIN System Functional Specification, Appendix B, Section II) to the affected I-S/A AMPE preceding any altrouted messages (invoke) and upon termination or modification of the altroute action (revoke). The I-S/A AMPE shall accept these altrouted messages from directly connected ASCs for delivery to pre-determined alternate delivery subscribers. If a pre-determined alternate delivery subscriber is a distant I-S/A AMPE subscriber (because the distant I-S/A AMPE is not directly connected to an ASC) the I-S/A AMPE receiving the message from its connected ASC shall append an alternate routing pilot containing the RI of the distant alternate delivery subscriber and forward the message to the distant I-S/A AMPE. In no case shall the I-S/A AMPE return a message received from a connected ASC to the same ASC or another connected ASC based solely on the received destination RI.

4.3.7 AUTODIN System Generated Pilots. The I-S/A AMPE shall accept and process for delivery messages received from connected AUTODIN Switching Centers (ASCs) containing "pilots" as described in the AUTODIN System Functional Specification, Para 412. Note that a message containing an AUTODIN system generated pilot will not be accepted by an ASC.

generator until the associated message has been acknowledged by the LDMX. Consequently, the LDMX also does not update the last accepted CSN on a Mode V channel until the message has been validated and accepted.

4.4 <u>JANAP Message Format</u>. - For NAVY LDMX validation/verification purposes, the JANAP format is divided into fourteen parts: Header data up to and including the Start-of-Routing Sequence (Format Line 2); the Routing Indicator Field (still a part of Format Line 2); "DE" Line (Format Line 3); the Security Line (Format Line 4); Passing Instructions (Format Line 4 Extensions); Operating Signals; the Date Time Group (Format Line 5); the Message Originator (Format Line 6); the Action/Information Addressees (Format Line7/8); the Exempt Addressee (Format Line 9); the Accounting Symbol (Format Line 10); the End of Header (Format Line 11); the Message Classification (Format Line 12); and the End of Message (Format Lines 13 through 16).

4.4.1 <u>Format Line 2 Processing Through the Start-of-Routing</u>.

4. .1.1 <u>Precedence Field</u>. - The first header field to be validated is the precedence field. The precedence field is processed first. Once validated, the precedence is saved for later correlation with FL5 precedence(s).

4. .1.1.1 <u>Check 2.1.a</u>. - Precedence is a single character, the first character of the header and is validated to be one of five characters:

"Y" - Emergency Command Precedence (ECP) which may be input only on authorized channels.
"Z" - Flash
"O" - Immediate
"P" - Priority
"R" - Routine

<u>Error Condition</u> - If the field is not one of the five precedence characters specified above.

<u>Error Resolution</u> - An error in the precedence field of either an invalid or an unauthorized character results in the message being rejected to a service position with the error annotation "INVALID PRECEDENCE". See Message Error Processing for the appropriate response.

4.4.1.2 Language Media Format (LMF). - The next field to be validated in a JANAP format message is the Language and Media Format (LMF) field. This is a two character field in which the first character (LMF1) indicates the medium in which the input message was originally prepared. It is sometimes also called the Input LMF. The second character (LMF2) indicates the medium in which the originator prefers the message to be delivered to the addressee. It is sometimes also referred to as the Output LMF. Input header processing merely validates the Input Media/LMF combination. Further use of the LMF in input processing and in output message delivery will be discussed later.

4.4.1.2.1 Check 2.2.a. - LMF validation is always combined with the validation of the Input Media. If the message is from a TI user, the SEL is obtained from the second framing character of the TI line block. Otherwise, it is the second framing character of the header line block. Once the SEL-LMF combination passes validation, the LMF pair information is saved for RI processing, which must determine whether a message of the specified LMF can be delivered to a given RI.

Error Condition - If the Input Media/LMF combination does not match an LDMX table entry, the Input Media is validated separately.

Error Resolution - If the Input Media is invalid, an error condition is logged and the message is rejected with no exceptions. A "REPROTECT TO ALL ADDRESSEES" service message is generated.

When the Input Media is valid, but one of the LMF characters is invalid, it is rejected to a service position with an "INVALID LMF" error annotation. See Message Error Processing for the appropriate response.

4.4.1.3 Single Security Character Field. - The next field to be validated is the single character security field. Once validated, the security character is saved for further security checks in format line 2, 4, and 12 processing. The single character which indicates the security, must be one of the following characters:

"T" - Top Secret
"S" - Secret
"C" - Confidential
"R" - Restricted
"E" - Unclas E F T O (encrypted for transmission only)
"U" - Unclassified

4.4.1.3.1 Check 2.3.a. - The security character is compared to valid security characters above.

Error Condition - Detection of an invalid security character.

Error Resolution - The message is rejected to a service position, with the error annotation "INVALID SECURITY". See Message Error Processing for the appropriate response.

4.4.1.4 Content Indicator Code (CIC) Field. - The four character CIC field contains information related to the type of message being processed. The CIC is also referred to as the Communication Action Identifier (CAI). Certain CICs such as ZOVW, ZZGW, IJJY, JGGC, NGGC, etc. predetermine further format line validation and internal processing, thus requiring the information be saved.

4.4.1.4.1 Check 2.4.a. - The CIC is validated for four alphabetic characters, or three alphabetic and one numeric character.

Error Condition - Not a valid CIC, one listed in LDMX table, or not enough characters in the CIC.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID CIC FORMAT". See Message Error Processing for the appropriate response.

4. .1.4.2 Check 2.4.b. - The CIC indicates an ADMS/ASC generated pilot, the original CIC from Format Line 2 is also validated (dual header only).

Error Condition - No valid CIC in piloted Format Line 2, or no Format Line 2 Extension present.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID FORMAT LINE 2". See Message Error Processing for the appropriate response.

4.4.1.4.3 Check 2.4.c. - The CIC "ZYVW" is detected, indicating a service message.

Error Condition - None - Checks are made during RI validation for non local RIs, and if present no further format validation is done.

Error Resolution - N/A

4.4.1.5 <u>Separator</u>. - The character following the CIC must be a space.

4.4.1.5.1 <u>Check 2.5.a</u>. - Check the character following the CIC field.

<u>Error Condition</u> - Any character other than a space.

<u>Error Resolution</u> - The message is rejected to a service position with the error annotation "INVALID CHARACTER AFTER CIC". See Message Error Processing for the appropriate response.

4.4.1.6 <u>Originating Station Routing Indicator (OSRI) Field</u>. - Following the separator is the seven character OSRI field. This may be a six or seven character Routing Indicator (RI) spaced filled to seven characters. A valid OSRI is saved for a later comparison to determine if the message is a duplicate. This is discussed in detail later in the document.

4.4.1.6.1 <u>Check 2.6.a</u>. - The OSRI is validated for seven alphabetic characters beginning with an "R".

<u>Error condition</u> - The OSRI begins with a character other than "R" or contains non-alphabetic characters.

<u>Error Resolution</u> - The message is rejected to a service position with the error annotation "INVALID OSRI". See Message Error Processing for the appropriate response.

4.4.1.7 <u>Originating Station Serial Number (SSN) Field</u>. - Immediately following the OSRI is the SSN field. The SSN field is validated for four numeric characters. A valid SSN is saved for later comparison with the Trailer Station Serial Number (TSSN) to ensure that a "straggler" condition does not exist. Straggler checking is discussed under End-of-Message validation. A valid SSN is used along with the OSRI during duplicate message validation. A valid SSN for FT, LA, KA, and NT messages is saved, but not used for straggler validation. All others are used for straggler checks.

4.4.1.7.1 <u>Check 2.7.a</u>. - The SSN field is validated for four numeric characters.

<u>Error Condition</u> - The SSN is not numeric or four characters in length.

<u>Error Resolution</u> - The message is rejected to a service position with the error annotation "INVALID SSN". See Message Error Processing for the appropriate response.

4.4.1.7.2 Check 2.7.b. - The SSN is compared to the TSSN.

Error Condition - The SSN does not match the TSSN (Format Line 15).

Error Resolution - The message is rejected to a service position with the error annotation "STRAGGLER SSN MISMATCH". See Message Error Processing for the appropriate response.

4.4.1.8 Separator. - The character following the SSN must be a space.

4.4.1.8.1 Check 2.8.a. - Check the character following the SSN field.

Error Condition - Any character other than a space.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID CHARACTER AFTER SSN". See Message Error Processing for the appropriate response.

4.4.1.9 Time-of-File (TOF) Field. - The TOF field is validated for seven numeric characters. Procedurally, the TOF field is composed of a three digit Julian date (001-365/366) and four digit time (0000-2359) and range checks are made. The TOF is used along with the OSRI and SSN in duplicate message validation, which will be discussed later in the document.

4. .1.9.1 Check 2.9.a. - Check the TOF field for seven numeric characters in the appropriate ranges.

Error Condition - The TOF is not numeric or seven characters in length.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID TOF". See Message Error Processing for the appropriate response.

4. .1.10 Security Redundancy Field Separator. - Following the TOF field, the character must be a dash or hyphen (ITA2 uppercase "A") signalling the start of the Security Redundancy field. If the Security Redundancy separator is misplaced, the message could be a pilot or a data pattern message (TC/AC). In either case the proper fields are validated.

4.4.1.10.1 Check 2.10.a. - The character following the IOF is not a dash or a blank character.

Error Condition - Any character other than a dash or a blank.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID SEPARATOR CHARACTER". See Message Error Processing for the appropriate response.

4.4.1.11 Piloted Message Field. - When the separator is a blank character this field is checked to determine if the message contains a pilot header or is possibly a data pattern message. Should the message contain a pilot FL2 and the CIC equal "ZZGW" or "IJJY", the pilot FL2 is stripped and a search done for the original FL2.

4.4.1.11.1 Check 2.11.a. - Check for "PLTS" (terminally prepared) or "Rxxx" (switch prepared) pilot indicators.

Error Condition - Pilot field contains data other than pilot headers and the message is not a data pattern (IAZZ) message.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID PILOT/CARD COUNT". See Message Error Processing for the appropriate response.

4.4.1.12 Record Count Field. - When the separator is a blank character and does not contain a pilot header, this field is checked for valid record count indicators.

4.4.1.12.1 Check 2.12.a. - Check for "MTMS" or for four valid numerics.

Error Condition - Record Count field contains data other than "MTMS" or four numeric characters.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID PILOT/CARD COUNT". See Message Error Processing for the appropriate response.

4.4.1.13 Security Redundancy (SR) Fields. - In the JANAP format, the four character Security Redundancy field is validated in different ways. All four characters of the Security Redundancy field must be identical to the single security character previously validated (fourth data character of the header) provided the message is not addressed to an Allied destination. If the message is addressed to an Allied destination, the last two characters of the Security Redundancy field must then be valid transmission release codes (TRCs). There may be two different TRC destinations within the message and both RIs must be in Format Line 2. When more than one TRC is indicated they have to be arranged in alphabetical order. Note that Format Line 4 must be present whenever a TRC indication is present in Format Line 2.

4.4.1.13.1 Check 2.13.a. - Check the first two security characters against the single security character field.

Error Condition - The first two characters are not identical to the single security character field.

Error Resolution - The message is rejected to a service position with the error annotation "SECURITY REDUNDACY ERROR - F/L 2". See Message Error Processing for the appropriate response.

4. .1.13.2 Check 2.13.b. - The last two characters of the Security Redundancy field are checked to see if they are valid TRCs, or security characters.

Error Condition - The two characters fail the validation check (not TRC characters, or security characters).

Error Resolution - The message is rejected to a service position with the error annotation "SECURITY REDUNDANCY ERROR - F/L 2". See Message Error Processing for the appropriate response.

4. .1.14 Start of Routing (SOR) Field. - After the Security Redundancy checks are complete, the SOR field is then validated. This field is a two character field containing dash dash (--).

4.4.1.14.1 Check 2.14.a. - The SOR field is validated for dash dash (--).

Error Condition - The SOR field contains characters other than a double dash (--).

Error Resolution - The message is rejected to a service position with the error annotation "INVALID START OF ROUTING". See Message Error Processing for the appropriate response.

4.4.2 JANAP Validation of the Routing Indicator (RI) Field.

4.4.2.1 Routing Indicator (RI) Field. - The RI is the "address" of a message. An RI may not be split by either spaces or by an End of Line (EOL) sequence in any instance. The RI is examined for the proper form, which begins with an "R" and ranges from four to seven alphabetic characters. A separator is provided between each RI unit. Format Line 2 may contain up to four seven character RIs, seven four character RIs, or any combination thereof, not to exceed the 69 character line length, with up to eight RIs on Format Line 2 continuation lines. The RIs are terminated when the End of Routing sentinel which is a period (.) is encountered. During RI validation the RIs are examined for Broadcast (BCST), Over-the-Counter (OTC), or Other to determine the RI type. It is the RI characteristics (i.e., OTC, Other) found here that influence to what extent TARE, FL7, 8, or 9 lines will be examined and validated.

Since the I-S/A AMPE will not receive RIs for local broadcast to the fleet, broadcast processing/validation will not be addressed further.

4.4.2.1.1 Check 3.1.a. - The first character of the RI must begin with an "R".

Error Condtion - First character of the RI is not an "R".

Error Resolution - The message is rejected to a service position with the error annotation "INVALID RI". See Message Error Processing for the appropriate response.

4.4.2.1.2 Check 3.1.b. - The RI must contain four to seven characters.

Error Condition - The RI contains more than seven characters, or the RI contains invalid characters.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID RI". See Message Error Processing for the appropriate response.

4.4.2.1.3 Check 3.1.c. - Is the intended RI destined for AUTODIN.

Error Condition - Either a CARP or non-local RI received from AUTODIN, or the message contains an invalid RI.

Error Resolution - The message is rejected to a service position with the error annotation "ILLEGAL ROUTING INDICATORS: XXXXXXX". See Message Error Processing for the appropriate response.

4.4.2.1.4 Check 3.1.d. - An Allied Routing Indicator must be accompained by a valid TRC.

Error Condition - A valid Allied RI is found and there is no associated TRC.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID TRANSMISSION RELEASE CODE FOR -". See Message Error Processing for the appropriate response.

4.4.2.1.5 Check 3.1.e. - The seventh character of a RIXT RI is "Y or Z" or not alphabetic.

Error Condition - The seventh character of the RIXT RI is a "Y or Z".

Error Resolution - The message is rejected to a service position with the error annotation "INVALID 7th CHAR IN RIXT RI". See Message Error Processing for the appropriate response.

4.4.2.1.6 Check 3.1.f. - Format Line 2 contains a Modified ACP 126 "SUU" RI and at least one other valid RI has been identified.

Error Condition - Either Format Line 2 is incorrectly formatted or this message contains a Modified ACP 126 "SUU" RI and it should not.

Error Resolution - The message is rejected to a service position with the error annotation "MOD ACP 126 MSG IDENTIFIED AS JANAP 128". See Message Error Processing for the appropriate response.

4.4.2.1.7 Check 3.1.g. - End of Routing sentinel detected without identifying a Routing Indicator.

Error Condition - No Routing Indicator or one which exists is illegal.

Error Resolution - The message is rejected to a service position with the error annotation "NO VALID RI OR ILLEGAL RI". See Message Error Processing for the appropriate response.

4.4.2.1.8 Check 3.1.h. - The RI has no primary delivery responsibility, and is valid.

Error Condition - The Format Line 2 RI is identified as a "SVC" RI.

Error Resolution - The message is rejected to a service position with the error annotation "PROTECT FOR ADDRESSEE OF -". See Message Error Processing for the appropriate response.

4.4.2.2 End-of-Routing Field. - The JANAP format End-of-Routing (EOR) consists of a period (.).

4. .2.2.1 Check 3.2.a. - Validate that there is a valid EOR.

Error Condtion - The last field in Format Line 2 contains an invalid EOR sentinel.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID RI". See Message Error Processing for the appropriate response.

4.4.3 JANAP Validation of "DE" Line. -

4. .3.1 Format Line 3 (FL3) Validation. - This format line is being discussed because of the ability of ACP 127 originated messages to enter an ASC, be converted to a JANAP 128 message, and thereby passed on to other AUTODIN subscribers. These messages will be identified by their Language Media Formats (LMFs). Format Line 3 (FL3) is positioned between FL2 and FL4, and contains the prosign "DE", the ACP 127 OSRI, SSN, and Time of File (TOF). Information found to be valid on this line is stored for subsequent duplicate message and recall processing.

Valid FL3 structures are:

DE	RxxxAAA	NNNN	JJJHHMM
1	... 2	3	4

1. Prosign.
2. Originating Station Routing Indicator (OSRI), starts with an "R" and is 4 to 7 alphabetic characters long.
3. Originating Station Serial Number (SSN), may exist in the following forms (N=numeric, A=alphabetic).

   A. #NNNN
   B. NNNN
   C. NNNA
   D. NNN

4. This field, the Time of File (TOF), is

optional. It [illegible] several formats.
(JJJ = Julian Day - values 001-366,
HH = Hours - values 00-23,
MM = Minutes - values 00-59, DD = Day - values
00-31, Z = Zulu Time Indicator).

A. JJJHHMM
B. DD/HHMMZ

Validation of the SSN and TOF fields are not exacting and will not cause errors if not in the proper format.

4.4.3.1.1 Check 4.1.a. - Ensure that more information exists on FL3 besides the prosign "DE ".

Error Condition - Prosign "DE " found but no other information exists.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID FL3". See Message Error Processing for the appropriate response.

4.4.3.1.2 Check 4.1.b. - Check for a valid OSRI.

Error Condition - The OSRI found does not begin with an "R", or is not 4 to 7 alphabetic characters long.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID OSRI FL3". See Message Error Processing for the appropriate response.

4.4.4 JANAP Validation of the Security Line. -

4.4.4.1 Security Line (FL4). - Following the EOR, original FL2, or FL3 processing the next field to be validated is the security line, format line four. If a pilot header is present, FL4 must follow the original FL2 or FL3. For all messages requiring FL4, the first four characters following the EOR must be the operating signal "ZNR" or "ZNY" followed by a space. When it is determined that FL4 is present, the remaining security fields are processed. The first of these is five characters in length and may consist of five redundant security characters, or three redundant security characters and two transmission release code (TRC) characters. Following this five character field and separated by a slash (/), may be from one to four optional special handling designator (SHD) fields (separated by a slash) or a SPECAT Release Code (SRC); each of which consists of a five character repetition of an SHD character. There may be only one set of SRC an may not be mixed with messages containing TRCs or other SHDs. Following the security field, separated by a space, may be operating signals, which may be followed by a space and misroute information if the Z-signal is one of "ZOV", (Z-signal processing other than "ZOV" is discussed later in the document for passing instructions.

4.4.4.1.1 Check 5.1.a. - The first four characters of FL4 are checked to see if they contain "ZNR" or "ZNY" and a space.

Error Condition - The first three characters are not "ZNR" or "ZNY" and followed by a space; "ZNY" and a space is used, but the FL2 security redundancy field is "UUUU"; or "ZNR" and a space is used, but the FL2 security redundancy field is other than "UUUU".

Error Resolution - The message is rejected to a service position with the error annotation "INVALID FORMAT LINE 4". See Message Error Processing for the appropriate response.

4.4.4.1.2 Check 5.1.b. - The first three characters of the security field are validated to be redundant and must match the security redundancy field.

Error Condition - The characters are not redundant or do not match those in FL2.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID SECURITY ON FORMAT LINE FOUR". See Message Error Processing for the appropriate response.

4.4.4.1.3 Check 5.1.c. - The next two characters are checked for security redundancy or valid TRCs.

Error Condition - The FL2 security redundancy field does not indicate TRCs required, and the characters in these two positions are other than security redundant characters.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID SECURITY ON FORMAT LINE FOUR". See Message Error Processing for the appropriate response.

4.4.4.1.4 Check 5.1.d. - The two characters are invalid, not redundant if only one TRC is required, not in alphabetical order if more than one TRC is required, or do not match those in FL2.

Error Condition - The TRC characters are invalid, not redundant if only one TRC is required, or not in alphabetical order if more than one TRC is required.

Error Resolution - The message is rejected to a service position with the error annotation "F/L4 TRC NOT EQUAL TO F/L2 TRC". See Message Error Processing for the appropriate response.

4.4.4.1.5 Check 5.1.e. - After validation of the security redundancy/TRC field, a check is made for the Special Handling Designator (SHD) sentinel, a slash (/), or a space.

Error Condition - Any character other than a slash (/), a space or a valid end-of-line sequence following the previous field.

Error Resolution - The message is rejected to a service position with the error annotation "ILLEGAL CHARACTERS ON FORMAT LINE FOUR". See Message Error Processing for the appropriate response.

4.4.4.1.6 Check 5.1.f. - The SHD sentinel is found, check the next five characters for redundancy and they must be valid SHD category characters as specified in ACP 117.

Error Condition - The five characters are not redundant, not a valid SHD category, SHDs found number more than four, or the classification of the message is below CONFIDENTIAL.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID OR DUPLICATE SHD ON F/L 4". See Message Error Processing for the appropriate response.

4.4.4.1.7 Check 5.1.g. - If the SHD sentinel is found, the input channel/position is checked to see if it is authorized to enter SHDs.

Error Condition - Special handling is required for the message and the input channel/position is not authorized to enter the SHD.

Error Resolution - The message is rejected to a service position with the error annotation "SPECIAL HANDLING REQUIRED". See Message Error Processing for the appropriate response.

4.4.4.1.8 Check 5.1.h. - If another SHD sentinel (/) is found, the next field is validated in the same manner as the first. If a valid SRC is detected a check is made to ensure there are no transmission release code(s) or SHDs in the message.

Error Condition - The message contains TRC(s) and a SRC in FL4, or the message contains an invalid SRC or the SRC does not agree with the message classification, or SRC is present with other SHDs.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID SRC ON FORMAT LINE FOUR" or "ILLEGAL CLASS WITH SRC OR SHD". See Message Error Processing for the appropriate response.

4.4.4.1.9 Check 5.1.i. - If the message TIC equals "ZOV" and no SHD sentinel is detected, FL4 is expected to contain a space following the security redundancy field and then the Z-signal "ZOV" followed by the misroute information.

Error Condition - FL2 processing indentified the message as a "ZOV" and FL4 does not contain the Z-signal.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID ZOV - F/L 4". See Message Error Processing for the appropriate response.

4.4.4.1.10 Check 5.1.j. - If FL4 contains the Z-signal "ZOV" followed by a space, the next position is validated to be the RI of the originator.

Error Condition - The RI does not begin with an "R", or does not match the OSRI found in FL2.

Error Resolution - The message is rejected to a service position with the error annotation "ZOV OSRI DOES NOT MATCH F/L 2 OSRI". See Message Error Processing for the appropriate response.

4.4.4.1.11 Check 5.1.k. - If the Reroute OSRI is valid, then the next four characters are validated for four numeric characters and that they are followed by "R/R" or "Reroute OF".

Error Condition - Non-numeric characters found in the SSN field, or the Reroute caveat does not follow the SSN.

Error Resolution - The message is rejected to a service position with the error annotation "SEQUENCE SERIAL NUMBER IS NOT NUMERIC ON F/L 4". See Message Error Processing for the appropriate response.

4.4.4.1.12 Check 5.1.l. - Check the OSRI/SSN fields following the Reroute information.

Error Condition - The RI does not begin with an "R" or contain the correct number of characters.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID RI ON FORMAT LINE FOUR". See Message Error Processing for the appropriate response.

4.4.4.1.13 Check 5.1 [illegible] - If a group is found after the security redundancy field or valid SHD/SHC fields, additional operating or passing instructions may be present.

Error Condition - None of the characters remaining on FL4 resemble any operating signals or TARE instructions.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID TARE LINE". See Message Error Processing for the appropriate response.

4.4.5 JANAP Validation of FL4 Continuations (FL4/E). - FL4/E may contain TARE instructions or operating signals. Each will be discussed in the following paragraphs.

4.4.5.1 Tare Instruction Search (FL4/E). - A test is made at the start of tare processing to see how many RIs are in format line 2. If only one RI was found, the following items are allowed:

T (Alone)
T Short Title or T-Short Title
T ZWL Short Title

When T (Alone) is found, the presence of any other format is illogical and constitutes an error.

T (Alone). T (Alone) indicates full routing responsibility.

T Short Title or T-Short Title. Based on short title delivery characteristics, if the delivery is not local, then the tare format is valid. For local addees (i.e., OTC), however, an RI is retrieved for that short title from the data base and compared against RIs existing in FL2. If a match occurs, delivery will be made to that specific short title, otherwise no delivery is made and TARE line is valid.

T ZWL Short Title. For these cases, the short title is validated and saved for later processing during format line seven and eight validation.

If the message has multiple RIs, the following are groupings of tare instructions allowed:

RXXXxxx T Short Title
RXXXxxx T-Short Title
T ZWL Short Title

If a side-routed tare does not have the local communication stations RI, it is simply validated.

If a message is misrouted (indicated by the presence of "ZOV") and contains "T SHORT TITLE" (or any variation); then message routing will be handled IAW the tare instructions only.

In the case of a "T" only single addressee message, or on messages which do not contain tare instructions and FL2 has only one RI, the message routing will be based on format line seven or eight processing.

In all cases, as was mentioned earlier, PLA or short title validation will only be done if FL2 contained a Local RI, and it should be kept in mind when reading about PLA or short title verification.

4.4.5.1.1 Check 6.1.a. - The format line four extension is validated for proper format, FL2 addees, and illegal short title combinations.

Error Condition - If the line cannot be identified as a valid tare line; the short title is a collective;. or a T-ZWL format is included in a misrouted message.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID TARE LINE". See Message Error Processing for the appropriate response.

4.4.5.1.2 Check 6.1.b. - The short title to be searched for contains valid characters.

Error Condition - The short title contains an unrecognizable combination of characters.

Error Resolution - The message is rejected to a service position with the error annotation "SHORT TITLE NOT IN DATA BASE". See Message Error Processing for the appropriate response.

4.4.5.1.3 Check 6.1.c. - A TARE instruction appears in the following format or variation thereof whereby the RI sideroute is present: Rxxxxxx T SHORT TITLE/SHORT TITLE

Error Condition - A valid Local short title is found, an RI retrieved from the LDMX to use as a search argument against FL2 RIs, no match was found and the sideroute does not match the LDMX retrieved RI either.

Error Resolution - The message is rejected to a service position with the error annotation "INCORRECT SIDEROUTE FOR XXXX...XXX". See Message Error Processing for the appropriate response.

Error Condition - Two or more short titles on the same TARE line which are not separated by a slash (/).

Error Resolution - The message is rejected to a service position with the error annotation "SHORT TITLE NOT IN DATA BASE". See Message Error Processing for the appropriate response.

4.4.5.1.4 Check 6.1.d. - A check is made on the number of local deliveries.

Error Condition - The message contains more than 500 Protect (local RIs) addees.

Error Resolution - The message is rejected to a service position with the error annotation "TOO MANY OTC ADDEES TO PROCESS". See Message Error Processing for the appropriate response.

4.4.5.1.5 Check 6.1.e. - Ensure all Local "T ZWL" short titles are processed.

Error Condition - The maximum number of "T ZWL" short title identifiers is reached.

Error Resolution - The message is rejected to a service position with the error annotation "CANNOT PROCESS ALL 'T ZWL'. MAX PER MSG: XX" where XX represents the numerical maximum.

4.4.5.2 Operating Signals (Z-Signal) Processing. - Operating signals or Z-signals as they are called may be found on format line 4, format line 4 extensions or format line 5. Whenever a potential Z-signal is detected, control is passed to the appropriate processing module for validation. Z-signal processing is discussed in three parts: Initial "Z" Signal Validation; ZPW Validation; and Other "Z" Signal Validation.

All operating signal validations are passive, to the extent that just because a word/trigraph/etc. may start with a "Z" it does not mean that it must be a "Z" signal and no errors are given based solely on a "Z" being present.

Initial "Z" Signal Validation. When a potential Z-signal is identified, the first three characters of the Z-signal are verified for alphabetics and the fourth character is verified to be either numeric or blank.

ZPW Validation. Whenever the Z-signal "ZPW" is identified the remaining data is verified to be a six digit numeric Date-Time-Group followed by the letter "Z".

Other "Z" Signal Validation. Z-signals "ZXY" and "ZNM" are invalid. For Z-signals other than "ZPW" a table is scanned for the corresponding Z-signal and if found the appropriate flag is set. Whenever the Z-signals: ZDK, ZDG, ZEL, ZFG, ZFF4, ZFF5, ZFF6, ZFH1, ZFH2, ZFH3, ZUI, or ZDS are identified the message is directed to a service position as well as the primary delivery indicated in FL2 routing.

4.4.5.2.1 Check 6.2.a - The [illegible] Z-signal is validated for proper format.

Error Condition - None - The Z-signal does not contain alphabetic characters in the first three positions, or the fourth character is not numeric or a space.

Error Resolution - N/A

4.4.5.2.2 Check 6.2.b. - The Z-signal is one of "ZPW".

Error Condition - The "ZPW" Z-signal is identified and the Date-Time-Group field contains invalid characters, or the line does not end with a "Z".

Error Resolution - The message is rejected to a service position with the error annotation "BAD ZPW TIME". See Message Error Processing for the appropriate response.

4.4.5.2.3 Check 6.2.c. - The Z-signal field contains the characters "ZNM".

Error Condition - The "ZNM" Z-signal is not permitted in the message.

Error Resolution - The message is rejected to a service position with the error annotation "ZNM ILLEGAL". See Message Error Processing for the appropriate response.

4.4.5.2.4 Check 6.2.d. - The Z-signal field contains the characters "ZXY".

Error Condition - The "ZXY" Z-signal is detected and requires delivery be made to the addresse indicated by the fourth character of the Z-signal.

Error Resolution - The message is rejected to a service position with the error annotation "ZXY SIGNAL FOUND". See Message Error Processing for the appropriate response.

4.4.5.2.5 Check 6.2.e. - A Z-signal is detected without format errors, but does not match a specific Z-signal requiring addition action.

Error Condition - None - The Z-signal is validated for proper format and stored as apart of the message.

Error Resolution - N/A

4.4.6 JANAP Validation of Date-Time-Group (DTG) Line. -

4.4.6.1 Date-Time-Group (FL5). - Following validation of fromat line four extensions' (tare instructions and operating signals), the next line validated is the Date-Time-Group. The Date-Time-Group consist of the Precedence field(s), the actual day, hour, and minutes of the message, a terminator, the month field, and a year field. Format line 5 may also contain operating signal(s) if the message warrants them. Operating signal processing has been previously discussed in this document.

VALID FORMAT LINE 5 STRUCTURE:

P DDHHMMZ MON YR
PI DDHHMMZ MON YR
P I DDHHMMZ MON YR

LEGEND:

P = ACTION PRECEDENCE
I = INFO PRECEDENCE
DD = VALID DAY - RANGE 01 THRU 31
HH = VALID HOUR - RANGE 00 THRU 23
MM = VALID MINUTE - RANGE 00 THRU 59
Z = ZULU TIME DESIGNATOR
MON = VALID MONTH
YR = NUMERICAL YEAR

Each of the aforementioned structures may contain operating signals and does not require "YR" if the message was input from AUTODIN.

4.4.6.1.1 Check 7.1.a. - Check the first character of the DTG for a valid precedence.

Error Condition - There is only one precedence in format line 5 and it does not equal the FL2 precedence.

Error Resolution - The message is rejected to a service position with the error annotation "PRECEDENCE ERROR ON F/L 5". See Message Error Processing for the appropriate response.

4.4.6.1.2 Check 7.1.b. - Validate the second position of the DTG for a space or valid INFO precedence.

Error Condition - An illegal INFO precedence character follows the action precedence character; or a character other than a space follows the second precedence character of the DTG field.

Error Resolution - The message is rejected to a service position with the error annotation "NO BLANK AFTER PRECEDENCE FIELD ON F/L 5". See Message Error Processing for the appropriate response.

4.4.6.1.3 Check 7.1.c. - The third position in the DTG is validated for a dual precedence or the beginning of the Date-Time-Group field.

Error Condition - If the third character is not an alphabetic precedence character less than the first precedence in FL5, a numeric character indicating the first character of the Date-Time-Group, or a space and the FL5 structure is "PI ".

Error Resolution - The message is rejected to a service position with the error annotation "INVALID DTG ON F/L 5". See Message Error Processing for the appropriate response.

4.4.6.1.4 Check 7.1.d. - Range checks are performed on the DTG field.

Error Condition - The six characters following the precedence field and that start in the correct position are not numeric; the day portion is zero or greater than 31; the hour portion is greater than 23; or the minute portion is greater than 59.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID DTG". See Message Error Processing for the appropriate response.

4.4.6.1.5 Check 7.1.e. - The DTG digits are valid numerics with the specified range and ends with a "Z".

Error Condition - The Date-Time-Group field ends with a character other than a "Z".

Error Resolution - The message is rejected to a service position with the error annotation "NO Z FOR ZULU ON F/L 5". See Message Error Processing for the appropriate response.

4.4.6.1.6 Check 7.1.f. - A valid separator must follow the Date-Time-Group.

Error Condtion - The character following the "Z" field of the DTG is not a space.

Error Resolution - The message is rejected to a service position with the error annotation "NO BLANK AFTER DTG FIELD ON F/L 5". See Message Error Processing for the appropriate response.

4.4.6.1.7 Check 7.1.g. - The month field following the separator is validated for the appropriate content.

Error Condition - The characters identified in the month field of FL5 do not match any of the valid twelve months.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID MONTH ON F/L 5". See Message Error Processing for the appropriate response.

4.4.6.1.8 Check 7.1.h. - If the month field is valid it must be followed by a valid separator.

Error Condition - The character following the month field is not a space.

Error Resolution - The message is rejected to a service position with the error annotation "NO BLANK AFTER MONTH ON F/L 5". See Message Error Processing for the appropriate response.

4.4.6.1.9 Check 7.1.i. - Messages not entered from AUTODIN require the year field to be present in FL5.

Error Condition - The message did not enter the system from AUTODIN and does not contain a year in FL5.

Error Resolution - The message is rejected to a service position with the error annotation "YEAR MISSING ON THIS F/L 5". See Message Error Processing for the appropriate response.

4.4.6.1.10 Check 7.1.j. - If the year field contains data it is checked for a valid year.

Error Condition - The year field contains data and it is not numeric data.

Error Resolution - The message is rejected to a service position with the error annotation "YEAR IS NOT NUMERIC ON F/L 5". See Message Error Processing for the appropriate response.

4.4.7 JANAP Validation of Originator (FL6) Lines. -

4.4.7.1 From Line (FL6). - The Originator's Short Title referred to as FL6, is verified to ensure it is within the correct character limits; and if it exist in the Data Base. For local LDMX processing there are two types of short titles: a Protect Short Title and a Guard Command Short Title. In either case, the LDMX performs special message distribution and backrouting dependent upon whether or not a Protect or Guard Short Title is found.

4.4.7.1.1 Check 8.1.a. - A search is made to find the short title in the database.

Error Condition - The short title is not contained within the Data Base.

Error Resolution - The message is rejected to a service position with the error annotation "SHORT TITLE NOT ON DATA BASE". See Message Error Processing for the appropriate response.

4.4.8 JANAP Validation of Action/Information Lines. -

4.4.8.1 Format Line 7 8 (FL7/8) Processing. - The processing of FL7/8 requires that the short title first be isolated. To do this, it is determined if the short title is siderouted and whether it is processing a format line containing the prosign "TO" or "INFO". When the prosign is present, it is skipped and validation starts with the sideroute search. Sideroutes consist of RIs, ZEN, ZEN1, or ZEN2 followed by a slash (/). Should the line contain "ZEN" in any of the aforementioned formats, no Short Title validation is done.

Format Line seven or eight may contain a single sideroute or dual sideroutes. In order to be classified as a RI sideroute, it must begin with the character "R", be between four and seven alphabetic characters in length, and end with a slash (/). Once the RI(s) have been identified they are saved for later processing and the short title has now been isolated for processing.

Once the short title is isolated, delivery requirements for the short title are pursued. Delivery to local (OTC) short titles is based upon a FL2-FL7 or FL2-FL8 RI correlation. This condition would only occur for RIs identified as OTC RxxxSCC. The exceptions will be discussed later.

When short title processing is required, the delivery characteristics (i.e., OTC, etc.) are determined. If the short title is OTC, the short title's RI retrieved from the data base is based upon the message classification, and that RI is used for the FL2-FL7 or FL2-FL8 RI correlation. Should the result of the FL2-FL7/8 RI correlation be positive the short title is delivered to. If negative, and the short title was siderouted, then the sideroute is compared against the retrieved data base RI. Should these not match, it is possible that the short title was incorrectly siderouted or the sideroute garbled. In either case, service action is required. If sideroute matches or the short title was not siderouted, then no delivery is made to that specific short title.

Again, FL2 RI characteristics are used to key short title processing. If FL2 contains a collective RI, RxxxSCC, or an OTC RI then short title processing is desired. Figure 4.4.8-1 is a delivery decision table based on a one to one comparison.

LDMX RI/SHORT TITLE VALIDATION
DELIVERY DECISION TABLE

If FL2 contains an RI which is:

Sideroute/Short Title	Non-Local	OTC	RxxxSCC
a. = SIDEROUTE b. = SHORT TITLE			
a. GARBLED	DR		
b. GARBLED		V	V
a. GARBLED	DR		
b. NON-LOCAL (AUTODIN)		V	V
a. GARBLED	DR		
b. OTC		D	V
a. NON-LOCAL (AUTODIN)	DR		
b. GARBLED		V	V
a. NON-LOCAL (AUTODIN)	DR		
b. NON-LOCAL (AUTODIN)		N	N
a. NON-LOCAL (AUTODIN)	DR		
b. OTC		D	N
a. RxxxSCC	DR		
b. ANY		N	D
a. ZEN	DR		
b. ANYTHING		N	N
a. OTC	DR		
b. GARBLED		V	V
a. OTC	DR		
b. NON-LOCAL (AUTODIN)		S	N
a. OTC	DR		
b. OTC		D	N

C = CONTINUE (no delivery responsibility)
DR = DELIVER TO FL2 RI LRN WITHOUT PLA LOOKUP
N = NO DELIVERY TO THAT SPECIFIC SHORT TITLE BASED UPON FL7/8-FL2 RI CORRELATION
D = DELIVER TO SHORT TITLE LRN IF RI IN FL2 MATCHES DATA BASE RI. IF NO MATCH, SIDEROUTE IS COMPARED TO DATA BASE RI, AND IF THESE DO NOT MATCH, DELIVERY IS TO SVC. (RxxxSCC exception to DATA BASE RI matching FL2 RI)
S = SVC DELIVERY BASED ON SIDEROUTE MATCH TO FL2 RI AND SHORT TITLE RI NOT = TO FL2 RI
V = VDT DISPLAY

FIGURE 4.4.8-1. Delivery Decision Table.

4.4.8.2 Delivery of Various Short Title Types. -

4.4.8.3 Non-Collectives. -

Over-the-Counter (OTC). If the delivery is one of OTC, the short title is either a "Protect" or "Guard" short title. Protect short titles are identified by a "P", "Q", or "R" in the data base, and Guard Command short titles are identified by a command number ranging from 01-30.

If FL7/8 contains FAS office codes, a FAS line is built for Guard Commands, but not for Protects. FAS office codes, if present are located between double slashs (//). The LDMX will save this information in the form: the short title identifier followed by the office codes (those longer than three characters are truncated to three characters), each of which is preceded by a slash; (i.e., ACPPTR/OP1/OP2/OP3). This information is used in distribution processing.

4.4.8.4 Collectives. - The processing of these short titles falls into four categories: RUCR Processing, Task Processing, Type Processing, and All Others.

RUCR Processing. When FL2 contains the collective RI, "RUCRxxx", and the short title is a collective short title, the FL2-FL7/FL2-FL8 correlation is suppressed. Every member of the collective will get delivery except for those which require AUTODIN delivery. Full period and dedicated deliveries which normally are set during FL2 processing will now be set.

TASK Processing. Those short titles with a naming convention (i.e., TF10, TG10.1) are TASK organizations, and those without a naming convention (i.e., Subron) are TYPE organizations. A distinction is made between the two during the checksum algorithm processing.

TYPE Processing. These kinds of collectives are processed like the category "All Others" except where their processing would have stopped, TYPE processing continues with a delivery to the organization's Commander. The Commander is processed as a single non-siderouted addee.

All Others. This processing entails delivery to all guarded and protect commands whose RIs appear in FL2.

When determining "ACTION" or "INFO" delivery requirements, the collective's location in the message is used. If a collective appears on FL7, the collective composition, which also contains ACTION/INFO indicators, is the sole source for the assignment. Should the collective appear on FL8, all members receive the message as info addees.

4.4.8.5 RxxxSCC Processing. - Any message received with an "RxxxSCC" RI in FL2 for which the LDMX is required to protect, and contains a siderouted short title in FL7 or FL8 with the same, will be delivered to all local addees (i.e., OTC) without a ZOV pilotted message being generated. Non-local RxxxSCC addees will be ZOV'd to the proper station automatically. A copy of the ZOV'd message will be delivered to a service position. (See Automated Misroute Section).

4.4.8.6 ZOV Message Processing. - Once a FL7 or FL8 has been identified, the message, if a ZOV, is delivered to all of the addees which were contained in any tare lines. Should no tare lines exist, and the number of RIs in FL2 is equal to one, then the ZOV message will be delivered to the addees in FL7 and/or FL8 which have matching RIs in FL2. If the message contains more than one RI, then the message is rejected to a service position. All addees whose RI does not appear in FL2 are rejected to a service position.

4.4.8.7 Readdressed Message Processing. - Upon finding a subsequent FL5, a readdressal format is presumed and no further action is taken on format lines 7, 8, 9, or 10.

4.4.8.8 T-ZWL Processing. - During FL7/8 processing, the "T ZWL" short title identifiers previously saved during FL4/FL4E validation are resolved. The "T ZWL" is used to "ZEN" members of a collective in which case delivery by electronic means is exempted.

4.4.8.8.1 Check 9.1.a. - After validation of the From Line the heading is searched for FL7 and/or FL8.

Error Condition - The prosign "TO" or "INFO" is not contained in the heading.

Error Resolution - The message is rejected to a service position with the error annotation "NO F/L7 or F/L8 FOUND". See Message Error Processing for the appropriate response.

4.4.8.8.2 Check 9.1.b. - A search is made to find the short title in the data base.

Error Condition - The short title is not contained within the Data Base.

Error Resolution - The message is rejected to a service position with the error annotation "SHORT TITLE NOT IN DATA BASE". See Message Error Processing for the appropriate response.

4.4.8.8.3 Check 9.1.c. - Format Line 7 or Format Line contains an RI followed by a slash (/), five spaces and a short title.

Error Condition - The short title line contains an RI but the short title is preceeded with five spaces.

Error Resolution - The message is rejected to a service position with the error annotation "RI/5 BLANKS + SHORT TITLE FOUND". See Message Error Processing for the appropriate response.

4.4.8.8.4 Check 9.1.d. - The short title RI retreived is based upon the message classification for local (OTC) deliveries.

Error Condition - The short title RI found in the data base is not cleared to receive this message.

Error Resolution - The message is rejected to a service position with the error annotation "NO CLEARED RI/RI'S FOR THIS SHORT TITLE". See Message Error Processing for the appropriate response.

4.4.8.8.5 Check 9.1.e. - The sideroute/short title combination contained in the message is checked for proper association.

Error Condition - The data base RI does not agree with the siderouted RI; or sideroute characteristics (i.e., OTC, FP, etc.) do not match short title characteristics.

Error Resolution - The message is rejected to a service position with the error annotation "INCORRECT-SIDE ROUTE FOR XXXX...XXX". See Message Error Processing for the appropriate response.

4.4.8.8.6 Check 9.1.f. - The RI indicates a local delivery is required.

Error Condition - The RI is a local RI found in the Data Base, but the destination is invalid.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID LRN IN DATA BASE FOR XXXXXXX". See Message Error Processing for the appropriate response.

4.4.8.8.7 <u>Check 9.1.g</u>. - Once a format line seven or eight is identified, and the message is a MISROUTE (ZOV).

<u>Error Condition</u> - The message contains multiple RIs in FL2, and no tare instructions exist.

<u>Error Resolution</u> - The message is rejected to a service position with the error annotation "INVALID USE OF ZOV SIGNAL - MSG SHOULD CONTAIN TARES". See Message Error Processing for the appropriate response.

4.4.8.8.8 <u>Check 9.1.h</u>. - The short title is a guard command and the Data Base entry is incorrect.

<u>Error Condition</u> - The guard command number for the short title is greater than the maximum, or during processing of a TASK short title the Data Base contained an invalid type.

<u>Error Resolution</u> - The message is rejected to a service position with the error annotation "DATA BASE INCORRECT FOR XXXX...XXX". See Message Error Processing for the appropriate response.

4. .8.8.9 <u>Check 9.1.i</u>. - The Total number of local addees exceed maximum allowed for processing.

<u>Error Condition</u> - The total number of local (OTC) addees exceeds 500.

<u>Error Resolution</u> - The message is rejected to a service position with the error annotation "TOO MANY OTC ADDEES TO PROCESS". See Message Error Processing for the appropriate response.

4.4.9 <u>JANAP Exempt Address Lines</u>. -

4.4.9.1 <u>Format Line 9 (FL9) Processing</u>. - The first step in FL9, or "XMT" processing as it is referred to is to determine if the prosign "XMT" exists and then validate the short title to be exempted. This is accomplished through a checksum algorithm of the short title and then determing if it is an entry in the Data Base.

If the characteristics of the addee being exempt indicate it is an OTC addressee, then the addressee may be either a guarded or a protect command. In either case, delivery to the command is inhibited and processing is finished.

4.4.9.1.1 Check 10.1.a. - After the prosign "XMT" has been identified, the short title following the prosign and all subsequent short titles are validated for the correct number of characters.

Error Condtion - The short title is not contained within the data base.

Error Resolution - The message is rejected to a service position with the error annotation "SHORT TITLE NOT ON DATA BASE". See Message Error Processing for the appropriate response.

4.4.9.1.2 Check 10.1.b. - The short title to be exempted is not a single addee addressee.

Error Condition - A collective short title has been detected on the exempt line.

Error Resolution - The message is rejected to a service position with the error annotation "COLLECTIVE SPECIFIED IN XMT LINE". See Message Error Processing for the appropriate response.

4.4.9.1.3 Check 10.1.c. - The subsequent FL9 has been found but the short title does not follow in the correct position.

Error Condition - The short title is indented 5 or more spaces.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID FORMAT LINE CONTINUATION". See Message Error Processing for the appropriate response.

4.4.9.1.4 Check 10.1.d. - The short title to be exempted is an OTC addressee.

Error Condition - The guard command number for the short title is greater than the maximum allowed.

Error Resolution - The message is rejected to a service position with the error annotation "DATA BASE INCORRECT FOR XXXX...XXX". See Message Error Processing for the appropriate response.

4.4.10 JANAP Accounting Line. -

4. .10.1 Format Line 10 (FL10) Processing. - FL10 is identified by the prosign "ACCT" or by a "GR" followed by either "NC" or a number. Once into FL10 processing, the accounting symbol is validated.

Error Condition - None.

Error Resolution - N/A

4.4.11 JANAP End of Header Line. -

4.4.11.1 Format Line 11 (FL11) Processing. - Header and heading validation is concluded when the first "BT" is identified. The first "BT" or FL11 separates the heading from the classification and text of the message. If a valid "BT" is found, message validation continues with FL12 processing. If an invalid or no "BT" condition exist, the message is rejected to a service position for the appropriate action.

4.4.11.1.1 Check 12.1.a. - Check for the prosign "BT", indicating FL11.

Error Condition - A "BT" has been found, but the message has no FL7/8; is not an abbreviated plaindress message (CIC contains "ZYVW"); or is not an offline encrypted message.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID BT". See Message Error Processing for the appropriate response.

4.4.11.1.2 Check 12.1.b. - Ensure that all Local (OTC) RIs contained on FL2 are accounted for.

Error Condition - FL2 contained OTC RIs which did not match any short title in the message.

Error Resolution - the message is rejected to a service position with the error annotation "NO MATCH FOUND IN FL4/7/8 FOR FL2 RI - Rxxxxxx". See Message Error Processing for the appropriate response.

4.4.12 JANAP Message Classification Line. -

4.4.12.1 Format Line 12 (FL12) Processing. - When the first "BT" or FL11 has been identified and processed without error, format line 12 (FL12) is the next line searched for. FL12, or the classification line as it is known, contains the message classification and it must correlate with the security of the message identified in FL2, FL4, and any special handling caveats. If the message is "SPECAT", FL12's security must be CONFIDENTIAL or above. During processing, the security narrative in FL12 is checked against a classification table for a match. Any discrepency results in the message being rejected to a service position.

When "SPECAT" is found in FL12, the message itself must have the appropriate SPECAT Release Code (SRC) in FL4. If it does not, either FL4 or FL12 is in error and the message is rejected to a service position. When the SRC in FL4 contains the letter "A", then the caveat following "SPECAT" in FL12 must be "SIOP-ESI". All other SPECAT caveats are valid when the SRC "B" is contained in FL4. An error in one of these conditions will result in the message being rejected to a service position.

When "SVC" is found in FL12, message delivery is set for the Service Center.

When "NOFORN" is found in FL12, it indicates that the message is not eligible for foreign delivery. If a foreign RI has already been identified in FL2 processing, then the message is rejected to a service position.

During FL12 processing a search is made for a Navy Standard Subject Identification Code (SSIC). If a SSIC if found (i.e., //N00000//) and further validation determines that a message SSIC is indeed in the line, then the message SSIC is saved for subsequent message distribution processing.

A unique feature of the LDMX is that it allows each site to handle Special Handling Instructions individually. If special handling is identified in FL12, the message will be processed IAW the special instructions.

After the security narrative and special indicators in FL12 have been processed, a search of FL12 is made for sectional information. If found, the current section number and total number of sections information associated to the message is updated. The following are examples of valid section information formats:

(1) Section 1 of 2

(2) Section 01 of 02

(3) Final Section of 2

(4) Final Section of 02

Following the search for additional information, a search is made for the word "SUBJ". "SUBJ" is used as to delimit the end of security and special handling information, and to identify the subject line of the message. "SUBJ" is required to be used as a delimiter whether or not a subject is given. FL12 analysis shall persist for 7 lines, or until recognition of other lines that indicate the subject line has been omitted. A reference line (left-justified "A. ") or a paragraph line (left-justified "1. ") found within 7 lines, before finding "SUBJ", shall be considered as evidence that the "SUBJ" line does not exist. In such cases the first physical line shall constitute the bounds of security and special handling information.

For DSSCS/GENSER LDMX sites, a phrase search is performed within the confines of the "SUBJ" line or the first 7 lines, starting with FL12. If a Phrase is detected which is associated to the DSSCS community only, then an error condition exists and the message is rejected to a service position.

4.4.12.1.1 Check 13.1.a. - The security narrative is checked against the message security classification.

Error Condition - The FL12 classification does not match FL2; an illegal condition exist (i.e., special handling instructions in a SPECAT message); or SPECAT was indicated in FL4 and not found in FL12.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID SECURITY CLASSIFICATION". See Message Error Processing for the appropriate response.

4.4.12.1.2 Check 13.1.b. - A check is made to see if the message is eligible for foreign delivery.

Error Condition - "NOFORN" was found in FL12, and TRCs are present in FL4.

Error Resolution - The message is rejected to a service position with the error annotation "NOFORN MSG ROUTED TO NON-US RI". See Message Error Processing for the appropriate response.

4.4.12.1.3 Check 13.1.c. - If a DSSCS/GENSER LDMX, a check is made for possible security violations between communities.

Error Condition - A DSSCS phrase has been detected in a GENSER message during FL12 processing.

Error Resolution - The message is rejected to a service position with the error annotation "SI-ONLY PHRASE FOUND IN GENSER MSG". See Message Error Processing for the appropriate response.

4.4.13 JANAP End of Message (EOM) Lines. -

4.4.13.1 Format Lines 13/15/16 (FL13/15/16) Processing. - When FL12 processing is complete, the remaining message body is treated as message text until the second "BT" or FL13 is found. When "BT" is found, EOM validation occurs. A check is made to determine the number of lines remaining in the message. If more than 2 lines remain, then an error is assumed and the message is rejected to a service position. If the "BT" appears to be in the proper location, then FL15 is validated. FL15 begins with the "#" sign, and if it is not present an error is assumed and the message is rejected to a service position. If the "#" sign is present, then the SSN in FL15 is validated to be numeric and match the FL2 SSN. Special processing is invoked for FL15 if the message is a Switch Converted ACP 127 to JANAP 128 message. After FL15 validation, the last line in the message is the 4 "N"s. Once again if the exact match is not found an error is assumed and the message is rejected to a service position.

After EOM validation the message is considered processed and placed in the appropriate transmission queues "FIFO" by precednece for delivery.

4.4.13.1.1 Check 14.1.a. - Check the message for a second "BT" (EOM indicator).

Error Condition - There are only 2 lines of data left in the message and the second "BT" has not been found.

Error Resolution - The message is rejected to a service position with the error annotation "NO BT F/L 13". See Message Error Processing for the appropriate response.

4.4.13.1.2 Check 14.1.b. - The second "BT" has been found and the next line must be FL15, provided the message LMF is not "FT", "NT", "KA", or "LA".

Error Condition - The "#" sign is missing or the 4 digits following the " " sign are not numeric.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID F/L 15". See Message Error Processing for the appropriate response.

4.4.13.1.3 Check 14.1.c. - FL15 is present and the last line must contain only the characters "NNNN".

Error Condition - The line following FL15 does not contain exactly "NNNN".

Error Resolution - The message is rejected to a service position with the error annotation "INVALID F/L 16". See Message Error Processing for the appropriate response.

4.5.0 LDMX DATA PATTERN MESSAGE PROCESSING REQUIREMENTS.

4.5.1 General Comments. -

4.5.1.1 This section will detail the existing LDMX Data Pattern format processing.

4.5.1.2 There are two categories of data pattern formats processed by the LDMX, Incoming Data and Outgoing Data Pattern. Within the two categories the LDMX processes multiple card and single card data pattern messages.

4.5.2 Validation/Verification Requirements. -

4.5.2.1 Format Line 1 - Transmission Identifier Line. - LDMX validation of the TI line is identical for both asynchronous (Mode II and V teletypewriter terminals whose use of a TI line is mandatory) and synchronous (Mode I users who employ line block framing and whose use of a TI line is optional, but must be specified at the time the LDMX sets the channel parameters) channels. All TI lines through the CD-CSN fields are processed as follows:

4.5.2.1.1 The first characters of the TI line block must be a Start of Header (SOH) and a select (SEL) character. If the channel is asynchronous, these have been inserted by the LDMX; if the channel is synchronous, the terminal has inserted them.

4.5.2.1.2 Check 1.1.a. - The first data character of the TI line must be the letter "C". (If the channel is asynchronous, the "ZCZC" portion of the Start of Message Sequence (SOMS) was previously validated and then discarded by the LDMX.)

Error Condition - None - nothing can be recognized prior to receipt of the SOH.

Error Resolution - N/A

4.5.2.1.3 Check 1.1.b. - The second, third and fourth characters of the TI line must be the Channel Designator (CD) and must match the CD stored at the LDMX for that channel.

Error Condition - A CD is considered to be in error if it does not match the CD stored in the LDMX for its associated channel.

Error Resolution - Except for messages of ECP or Flash precedence, messages having CD errors will be rejected to the service position. Precedence categories are explained later in this document.

45.2.1.4 Check 1.1.c. - The fifth character of the TI line can be either a figures shift or the first character of the CSN field; the figures shift must be present for "A" Select (ITA2) messages and may or may not be present for other selects. Note that for all processing purposes, "A" Select CSN's are always assumed to begin in the sixth position of the TI line. This is done so that the "CSN" to be quoted back to the terminal in a service message will be positionally correct even if the figure shift is garbled, leaving the CSN field in the lower case. If the CSN is correct, TI line processing is complete at this point.

Error Condition - A CSN is considered to be in error if it is either non-numeric or if it is not the next expected CSN (i.e., one greater than the last accepted from a Mode V channel or received from a Mode I or II channel.) For this purpose, a CSN of 000 is considered to be one greater than 999.

Error Resolution - Messages of ECP or Flash precedence will be accepted regardless of CSN errors detected. Other messages having CSN errors will be processed as follows:

If the CSN is a duplicate of the last accepted (Mode V) or received (Mode I/II), the message will be rejected to the service position. This is the only instance of CSN error where a message will be rejected by the LDMX which will generate an "OUT OF SEQUENCE" message to the input channel and log the error condition on an error file for future compilations (possibly similar to the existing Communications Improvement Memorandum (CIM) program.

If the CSN is incorrect for any other reason including being non-numeric, the message will be accepted. However, these errors shall cause the LDMX to generate a service message to the input channel citing the CD and CSN as well as other pertinent message identification data. This service message will indicate "POSSIBLE DUPLICATE", "OUT OF SEQUENCE" and whether the message needs to be protected for. Missing CSNs will cause generation of an open number (ZFX) service message to the input channel.

4.52.1.5 Further LDMX TI Line Processing. - In order to maintain CSN continuity between the LDMX and the terminal, the LDMX tables are updated based on the results of CSN and message processing. When a CSN is rejected (i.e., duplicate condition), no CSN updating is performed. When a CSN is accepted, even if it is out of sequence, the accepted CSN (or the expected CSN, if the received CSN is non-numeric) is made the last accepted CSN for processing of future messages. When the channel is Mode I or Mode II this update is done immediately on receipt of the TI line whether the associated message is accepted or not, since the Mode I or Mode II terminal is assumed to update the CSN at the beginning of each message transmission. This is also consistent with a terminal transmitting a tape in which there are pre-cut CSN's preceding each message. Since Mode V procedures require that CSN's be updated on acceptance of the message, Mode V terminal equipment does not update its TI generator until the associated message has been acknowledged by the LDMX. Consequently, the LDMX also does not update the last accepted CSN on a Mode V channel until the message has been validated and accepted.

4.53 Data Pattern Message Format. - For LDMX Data Pattern validation/verification purposes, the format is divided into five parts: Header data up to and including the Start-of-Routing Sequence (Format Line 2); the Routing Indicator Field (still a part of Format Line 2); the Security Line (Format Line 4); Text Data (Format Lines 5-12); and the End of Message (Format Line 16).

4.5.3.1 Format Line 2 Processing Through the Start-of-Routing.

4.53.1.1 Precedence Field. - The first header field to be validated is the precedence field. The precedence field is processed first. Once validated, the precedence is saved for later correlation with FL16 precedence(s).

4.53.1.1.1 Check 2.1.a. - Precedence is a single character, the first character of the header and is validated to be one of five characters:

"Y" - Emergency Command Precedence (ECP) which may be input only on authorized channels.
"Z" - Flash
"O" - Immediate
"P" - Priority
"R" - Routine

Error Condition - If the field is not one of the five precedence characters specified above.

Error Resolution - An error in the precedence field of either an invalid or an unauthorized character results in the message being rejected to a service position with the error annotation "INVALID PRECEDENCE". See Message Error Processing for the appropriate response.

4.53.1.2 Language Media Format (LMF). - The next field to be validated in a Data Pattern message is the Language and Media Format (LMF) field. This is a two character field in which the first character (LMF1) indicates the medium in which the input message was originally prepared. It is sometimes also called the Input LMF. The second character (LMF2) indicates the medium in which the originator prefers the message to be delivered to the addressee. It is sometimes also referred to as the Output LMF. Input header processing merely validates the Input Media/LMF combination. Further use of the LMF in input processing and in output message delivery will be discussed later.

4.53.1.2.1 Check 2.2.a. - LMF validation is always combined with the validation of the Input Media. If the message is from a TI user, the SEL is obtained from the second framing character of the TI line block. Otherwise, it is the second framing character of the header line block. Once the SEL-LMF combination passes validation, the LMF pair information is saved for RI processing, which must determine whether a message of the specified LMF can be delivered to a given RI. The LMF is also compared to the FL16 LMF during EOM processing.

Error Condition - If the Input Media/LMF combination does not match an LDMX table entry, the Input Media is validated separately.

Error Resolution - If the Input Media is invalid, an error condition is logged and the message is rejected to a service position with the error annotation "INVALID MESSAGE TYPE CODE". See Message Error Processing for the appropriate response.

4.53.1.2.2 Check 2.2.b. - The message is identified as data pattern, and the Input LMF or Output LMF must specify cards.

Error Condition - The LMF does not conform to a valid data pattern LMF.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID LMF". See Message Error Processing for the appropriate response.

4.53.1.3 Single Security Character Field. - The next field to be validated is the single character security field. Once validated, the security character is saved for further security checks in format line 2, 4, and 16 processing. The single character which indicates the security, must be one of the following characters:

"T" - Top Secret
"S" - Secret
"C" - Confidential
"R" - Restricted
"E" - Unclas E F T O (encrypted for transmission only)
"U" - Unclassified

4.53.1.3.1 Check 2.3.a. - The single character is compared to valid security characters above.

Error Condition - Detection of an invalid security character.

Error Resolution - The message is rejected to a service position, with the error annotation "INVALID CLASSIFICATION". See Message Error Processing for the appropriate response.

4.53.1.4 Content Indicator Code (CIC) Field. - The four character CIC field contains information related to the type of message being processed. The CIC is also referred to as the Communication Action Identifier (CAI).

4.3.1.4.1 Check 2.4.a. - The CIC is validated for four alphabetic characters, or three alphabetic and one numeric character.

Error Condition - Not a valid CIC or not enough characters in the CIC.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID CIC". See Message Error Processing for the appropriate response.

4.53.1.5 Separator. - The character following the CIC must be a space.

4.53.1.5.1 Check 2.5.a. - Check the character following the CIC field.

Error Condition - Any character other than a space.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID SEPARATORS IN F/L 2". See Message Error Processing for the appropriate response.

4.53.1.6 Originating Station Routing Indicator (OSRI) Field. - Following the separator is the seven character OSRI field. This may be a four or seven character Routing Indicator (RI) spaced filled to seven characters. A valid OSRI is saved for a later comparison to the FL16 OSRI.

4.53.1.6.1 Check 2.6.a. - The OSRI is validated for seven alphabetic characters or at least four alphabetic characters with the remaining positions space filled.

Error condition - The OSRI is less than four or greater than seven characters, or contains non-alphabetic characters.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID OSRI". See Message Error Processing for the appropriate response.

4.53.1.7 Originating Station Serial Number (SSN) Field. - Immediately following the OSRI is the SSN field. The SSN is is validated for four numeric characters. A valid SSN is saved for later comparison with the Trailer Station Serial Number (TSSN) to ensure that a "straggler" condition does not exist. Straggler checking is discussed under End-of-Message validation.

4.53.1.7.1 Check 2.7.a. - The SSN field is validated for four numeric characters.

Error Condition - The SSN is not numeric or four characters in length.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID SSN". See Message Error Processing for the appropriate response.

4.53.1.8 Separator. - The character following the SSN must be a space.

4.53.1.8.1 Check 2.8.a. - Check the character following the SSN field.

Error Condition - Any character other than a space.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID SEPARATORS IN F/L 2". See Message Error Processing for the appropriate response.

4.53.1.9 Time-of-File (TOF) Field. - The TOF field is validated for seven numeric characters. Procedurally, the TOF field is composed of a three digit Julian date (001-365/366) and four digit time (0000-2359) and range checks are made.

4.53.1.9.1 Check 2.9.a. - Check the TOF field for seven numeric characters in the appropriate ranges.

Error Condition - The TOF is not numeric or seven characters in length.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID TOF". See Message Error Processing for the appropriate response.

4.5.3.1.10 Separator. - The character following the TOF must be a space.

4.5.3.1.10.1 Check 2.10.a. - Check the character following the TOF field.

Error Condition - Any character other than a space.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID SEPARATORS IN F/L 2". See Message Error Processing for the appropriate response.

4.5.3.1.11 Record Count Field. - When the separator is a blank character this field is checked to determine if the message contains a pilot (i.e., "PLTS" or an ASC NARC "Rxxx"), or a valid card count (i.e., "MTMS" or 4 numeric digits).

4.5.3.1.11.1 Check 2.11.a. - Check for "PLTS" (terminally prepared) or "Rxxx" (switch prepared) pilot indicators, four numerics or "MTMS".

Error Condition - Record count field contains data other than pilot indicators, or a valid record count.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID RECORD COUNT FIELD FL/2". See Message Error Processing for the appropriate response.

4.5.3.1.12 Separator. - The security redundancy sentinel must follow the Record Count.

4.5.3.1.12.1 Check 2.12.a. - Check the character following the record count for a single dash (-).

Error Condition - The character following the record count is not a single dash (-).

Error Resolution - The message is rejected to a service position with the error annotation "INVALID SEPARATORS IN F/L 2". See Message Error Processing for the appropriate response.

4.5.3.1.13 Security Redundancy-TRC Fields. - In the Data Pattern format, the four character Security Redundancy field is validated in different ways. All four characters of the Security Redundancy field must be identical to the single security character previously validated (fourth data character of the header) provided the message is not addressed to an Allied destination. If the message is addressed to an Allied destination, the last two characters of the Security Redundancy field must then be valid transmission release codes (TRCs). There may be two different TRC destinations within the message and both RIs must be in Format Line 2. When more than one TRC is indicated they have to be arranged in alphabetical order. Note that Format Line 4 must be present whenever a TRC indication is present in Format Line 2. The classification redundancy field is saved to compare against the FL16 classification redundancy.

4.5 3.1.13.1 Check 2.13.a. - Check the first two security characters against the single security character field.

Error Condition - The first two characters are not identical to the single security character field.

Error Resolution - The message is rejected to a service position with the error annotation "CLASSIFICATION REDUNDANCY OR TRC ERROR". See Message Error Processing for the appropriate response.

4.5 3.1.13.2 Check 2.13.b. - The last two characters of the Security Redundancy field are checked to see if they are valid TRCs, or security characters.

Error Condition - The two characters fail the validation check (not TRC characters, or security characters).

Error Resolution - The message is rejected to a service position with the error annotation "CLASSIFICATION REDUNDANCY OR TRC ERROR". See Message Error Processing for the appropriate response.

4.5 3.1.14 Start of Routing (SOR) Field. - After the Security Redundancy checks are complete, the SOR field is then validated. This field is a two character field containing dash dash (--).

4.5 3.1.14.1 Check 2.14.a. - The SOR field is validated for dash dash (--).

Error Condition - The SOR field contains characters other than a double dash (--).

Error Resolution - The message is rejected to a service position with the error annotation "INVALID START-OF-ROUTING SIGNAL". See Message Error Processing for the appropriate response.

4,53.2 Validation of the Routing Indicator (RI) Field.

.3.2.1 Routing Indicator (RI) Field. - The RI is the "address" of a message. An RI may not be split by either spaces or by an End of Line (EOL) sequence in any instance. The RI is examined for the proper form, which ranges from four to seven alphabetic characters. A separator is provided between each RI unit. Format Line 2 may contain up to five seven character RIs, eight four character RIs, or any combination thereof, not to exceed the 80 character line length, with up to ten RIs on Format Line 2 continuation lines. The RIs are terminated when the End of Routing sentinel which is a period (.) is encountered. During RI validation the RIs are examined for US and Non-US RIs. It is the RI characteristics found that influence to what extent TRC and SHD processing is performed.

4.5.3.2.1.1 Check 3.1.a. - The RI must contain four to seven alphabetic characters.

Error Condition - The RI contains more than seven characters, or the RI contains invalid characters.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID ROUTING INDICATOR". See Message Error Processing for the appropriate response.

4,53.2.1.2 Check 3.1.b. - Is the intended RI destined for AUTODIN.

Error Condition - Either a CARP or non-local data pattern RI received from AUTODIN, the message contains an invalid RI, or the message contain no RIs.

Error Resolution - The message is rejected to a service position with the error annotation "NO VALID RI OR ILLEGAL RI". See Message Error Processing for the appropriate response.

4,5.3.2.1.3 Check 3.1.c. - An Allied Routing Indicator must be accompained by a valid TRC.

Error Condition - A valid Allied RI is found and there is no associated TRC.

Error Resolution - The message is rejected to a service position with the error annotation "NO TRC FOR XXXXXXX (XXXXXXX=RI)". See Message Error Processing for the appropriate response.

4.5.3.2.1.4 Check 3.1.d. - Check the routing for a Non-US destination.

Error Condition - The message is single card and addressed to an Allied RI.

Error Resolution - The message is rejected to a service position with the error annotation "SINGLE CARD AND NON-US RI NOT ALLOWED". See Message Error Processing for the appropriate response.

4.53.2.1.5 Check 3.1.e. - End of Routing sentinel has not been detected and the RI maximum (500) has not been reached.

Error Condition - The End of Routing sentinel has not been found and there are more than 500 RIs in the message.

Error Resolution - The message is rejected to a service position with the error annotation "MORE THAN 500 RI'S". See Message Error Processing for the appropriate response.

4.53.2.2 End-of-Routing Field. - The Data Pattern format End-of-Routing (EOR) consists of a period (.).

4.5.3.2.2.1 Check 3.2.a. - Validate that there is a valid EOR.

Error Condtion - The last field in Format Line 2 contains an invalid EOR sentinel.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID END-OF-ROUTING SIGNAL". See Message Error Processing for the appropriate response.

4.53.3 Validation of the Security Line. -

4.5.3.3.1 Security Line (FL4). - Following the EOR processing the next field to be validated is the security line, format line four. If a pilot header is present, FL4 must follow the original FL2. For all messages requiring FL4, the first four characters following the EOR must be the operating signal "ZNR" or "ZNY" followed by a space. When it is determined that FL4 is present, the remaining security fields are processed. The first of these is five characters in length and may consist of five redundant security characters, or three redundant security characters and two transmission release code (TRC) characters. Following this five character field and separated by a slash (/), may be from one to four optional special handling designator (SHD) fields (separated by a slash) or a SPECAT Release Code (SRC); each of which consists of a five character repetition of an SHD character. There may be only one set of SRC and may not be mixed with messages containing TRCs or other SHDs. Following the security field, separated by a space, may be operating signals, which are not validated.

4.53.3.1.1 Check 4.1.a. - The first four characters of FL4 are checked to see if they contain "ZNR" or "ZNY" and a space.

Error Condition - The first three characters are not "ZNR" or "ZNY" and followed by a space; "ZNY" and a space is used, but the FL2 security redundancy field is "UUUU"; or "ZNR" and a space is used, but the FL2 security redundancy field is other than "UUUU".

Error Resolution - The message is rejected to a service position with the error annotation "CLASSIFICATION REDUNDANCY OR TRC ERROR". See Message Error Processing for the appropriate response.

4.53.3.1.2 Check 4.1.b. - The first three characters of the security field are validated to be redundant and must match the security redundancy field.

Error Condition - The characters are not redundant or do not match those in FL2.

Error Resolution - The message is rejected to a service position with the error annotation "CLASSIFICATION REDUNDANCY OR TRC ERROR". See Message Error Processing for the appropriate response.

4.53.3.1.3 Check 4.1.c. - The next two characters are checked for security redundancy or valid TRCs.

Error Condition - The FL2 security redundancy field does not indicate TRCs required, and the characters in these two positions are other than security redundant characters.

Error Resolution - The message is rejected to a service position with the error annotation "CLASSIFICATION REDUNDANCY OR TRC ERROR". See Message Error Processing for the appropriate response.

4.53.3.1.4 Check 4.1.d. - After validation of the security redundancy/TRC field, a check is made for the Special Handling Designator (SHD) sentinel, a slash (/), or a space.

Error Condition - Any character other than a slash (/), a space or a valid end-of-line sequence following the previous field.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID SEPARATOR CHARACTER FL 4". See Message Error Processing for the appropriate response.

4.53.3.1.5 Check 4.1.e. - The SHD/SRC sentinel is found, check the classification of the message for an allowable range.

Error Condition - The classification of the message is below CONFIDENTIAL.

Error Resolution - The message is rejected to a service position with the error annotation "SRC NOT ALLOWED". See Message Error Processing for the appropriate response.

4.53.3.1.6 Check 4.1.f. - The message classification is acceptable, check for a valid SHD/SRC as specified in ACP 117.

Error Condition - The SHD/SRC character is not a valid special handling category; there are more than four SHDs in the message; the SHD is repeated more than once in the message, or there is more than one SRC in the message.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID OR DUPLICATE SHD-FL4". See Message Error Processing for the appropriate response.

4.53.3.1.7 Check 4.1.g. - The message classification is acceptable and a valid SHD/SRC exists, check the five SHD/SRC characters to ensure they are redundant.

Error Condition - A valid SHD/SRC is present but the 5 character group are not redundant.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID SRC". See Message Error Processing for the appropriate response.

4.53.3.1.8 Check 4.1.h. - If the SHD/SRC sentinel is found, the input channel/position is checked to see if it is authorized to enter SHD/SRCs.

Error Condition - Special handling is required for the message and the input channel/position is not authorized to enter the SHD/SRC.

Error Resolution - The message is rejected to a service position with the error annotation "SPECIAL HANDLING REQUIRED". See Message Error Processing for the appropriate response.

4,53.3.1.9 Check 4.1.i. - If another SHD/SRC sentinel (/) is found, the next field is validated in the same manner as the first. If a valid SRC is detected a check is made to ensure there are no transmission release code(s) in the message.

<u>Error Condition</u> - The message contains TRC(s) and a SRC in FL4.

<u>Error Resolution</u> - The message is rejected to a service position with the error annotation "SRC NOT ALLOWED". See Message Error Processing for the appropriate response.

4,53.3.1.10 <u>Check 4.1.j</u>. - The FL2 security redundnacy field indicates TRCs required, therefore the message must contain a FL4.

<u>Error Condition</u> - TRCs indicated in the FL2 security redundancy field and the message contains no FL4.

<u>Error Resolution</u> - The message is rejected to a service position with the error annotation "MSG WITH TRC BUT NO FL 4". See Message Error Processing for the appropriate response.

4,53.4 <u>Validation of TEXT Data Lines</u>. -

4,53.4.1 <u>TEXT Lines (FL5-12)</u>. Following validation of FL4, if applicable, all remaining lines of data (80 character record images) are treated as text lines. If and when format lines (i.e., FL5, FL6, etc.) are present in a data pattern message no validation is performed on them. At this point all message lines will be recorded as text until the Trailer card (FL16) is found. The following exceptions apply during text data processing.

4,53.4.1.1 <u>Check 5.1.a</u>. - Check the data immediately following the header card (FL2).

<u>Error Condition</u> - The Trailer card immediately follows the header card.

<u>Error Resolution</u> - The message is rejected to a service position with the error annotation "MESSAGE HAS NOT TEXT". See Message Error Processing for the appropriate response.

4.53.4.1.2 Check 5.1.b. - Tally the total number of message lines.

Error Condition - The total number of message lines including the Header and Trailer exceeds 500 lines.

Error Resolution - The message is rejected to a service position with the error annotation "MORE THAN 500 MESSAGE LINES". See Message Error Processing for the appropriate response.

4.53.5 End of Message (EOM) Line. -

.3.5.1 Format Line (FL16) Processing. - The message lines will continue to be processed as text lines until the maximum record count is exceeded, the message data lines are depleted or the Trailer card is identified. Once the Trailer card (FL16) is found EOM validation will be performed.

The Header and Trailer card is compared against each other to ensure the first 38 positions of each record match. Any deviation is considered to constitue an error.

After successful validation of FL16 the data pattern message is queued for delivery to the card punch or in some cases it resides in a Data Pattern Queue until the message is retreived and punched, written to magnetic tape, or printed. Any error in FL16 will cause the message to be rejected to the Service Center or an interactive service position.

4.53.5.1.1 Check 6.1.a. - Check the Header precedence, LMF, and security redundancy field against the Trailer card.

Error Condition - The message is input from AUTODIN or TERM TAPE (LDMX only) and the precedence, LMF, and security redundancy fields in the Header and Trailer do not match.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID MESSAGE TRAILER". See Message Error Processing for the appropriate response.

Error Condition - The message is an outgoing data pattern message and the precedence, LMF, and security redundancy fields in the Header and Traileer do not match.

Error Resolution - The message is rejected to a service position with the error annotation "NO MESSAGE TRAILER OR ILLEGAL OUTGOING TR". See Message Error Processing for the appropriate response.

4,5.3.5.1.2 Check 6.1.b. - Determine if the OSRI/SSN and separator fields in the Header card match the Trailer card.

Error Condition - The precedence, LMF, and security redundancy fields match but the OSRI/SSN fields do not match, and the message does not have a pilot header.

Error Resolution - The message is rejected to a service position with the error annotation "HEADER-TRAILER OSRI/SSN MISMATCH". See Message Error Processing for the appropriate response.

Error Condition - The precedence, LMF, and security redundancy field match but the OSRI/SSN fields do not match, and the message has a pilot header.

Error Resolution - The message is rejected to a service position with the error annotation "PILOT TRAILER OSRI/SSN MISMATCH". See Message Error Processing for the appropriate response.

4,53.5.1.3 Check 6.1.c. - The record count is checked to ensure proper format and correct line count.

Error Condition - The FL2 record count field is not "MTMS", all numeric data, or does not equal the record count in FL16.

Error Resolution - The message is rejected to a service position with the error annotation "RECORD COUNT MISMATCH". See Message Error Processing for the appropriate response.

4,53.5.1.4 Check 6.1.d. - The last four positions of the Trailer card (77-80) is checked for the EOM indicator.

Error Condition - Positions 77-80 in the Trailer card contains data other than "NNNN", and the message was received from AUTODIN or TERM TAPE.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID MESSAGE TRAILER". See Message Error Processing for the appropriate response.

Error Condition - Positions 77-80 in the Trailer card contains data other than "NNNN", and the message was an outgoing data pattern message.

Error Resolution - The message is rejected to a service position with the error annotation "NO MESSAGE TRAILER OR ILLEGAL OUTGOING TR". See Message Error Processing for the appropriate response.

5.0. ACP 127 Format Message Processing Requirements.

5.1. General Comments.

5.1.1. This section details the existing processing as it applies to ACP 127 message formats utilized by some of the GENSER community subscribers. As with the JANAP 128 message processing requirements, these checks and validations shall be performed by the I-S/A AMPE in such a manner that subscribers are provided the same service on an interface and interaction basis that they currently derive from existing ASCs and Service/Agency AMPEs.

5.2. Validation/Verification Requirements

5.2.1. Format Line 1 - Transmission Identifier (TI) Line. I-S/A AMPE validation of the TI line shall be identical for both asynchronous (Mode II and V teletypewriter terminals whose use of a TI line is mandatory) and synchronous (Mode I users who employ line block framing and whose use of a TI line is mandatory if utilizing ACP 127 format and must be specified at the time the I-S/A AMPE sets the port/channel parameters) channels. All TI lines through the CD-CSN fields shall be processed as follows:

5.2.1.1. The first characters of the TI line block must be a Start of Header (SOH) and a select (SEL) character. If the channel is asynchronous, these shall have been inserted by the I-S/A AMPE; if the channel is synchronous, the terminal has inserted them.

5.2.1.2. Check 1.1.a. The first data characters of the TI line must be a valid Start of Message Sequence (SOMS)

Error Condition - None - nothing can be recognized prior to receipt of the SOH.

Error Resolution - N/A

5.2.1.3. Check 1.1.b. The next three characters of the TI line must be the Channel Designator (CD) and must match the CD stored at the I-S/A AMPE for that port or channel.

Error Condition - A CD shall be considered to be in error if it does not match the CD stored in the I-S/A AMPE for its' associated channel.

Error Resolution - Except for messages of ECP or Flash precedence, messages having CD errors shall be rejected to the input port or channel.

5.2.1.4. Check 1.1.c. The next character of the TI line can be either a figures shift or the first character of the CSN field; the figures shift must be present for "A" Select (ITA 2) messages and may or may not be present for other selects. If the CSN is correct, TI line validation is complete at this point.

Error Condition - A CSN shall be considered to be in error if it is either non-numeric or if it is not the next expected CSN;i.e., one greater than the last "accepted" from a Mode V port/channel or "received" from a Mode I or II port/channel. For this purpose, a CSN of 000 shall be considered to be one greater than 999.

Error Resolution - Messages of ECP or Flash precedence shall be accepted regardless of CSN errors detected. Other messages having CSN errors shall be processed as follows:

If the CSN is a duplicate of the last "accepted" (Mode V) or received (Mode I/II), the message shall be rejected to the input port/channel. This is the only instance of CSN error where a message will be rejected by the I-S/A AMPE which shall generate an "INVALID CSN" message to the input port or channel and reecord the error condition for future compilations such as the existing Communications Improvement Memorandum (CIM) program. If the CSN is incorrect for any other reason including being non-numeric, the message shall be accepted. However, these errors shall cause the I-S/A AMPE to generate a service message to the input port/channel citing the CD and CSN as well as other pertinent message identification data. This service message shall indicate "INVALID CD", "INVALID CSN" and whether the message was accepted or rejected. A duplicate CSN shall cause generation of an additional service message, "DUPE CSN". When a CSN is received out of sequence, an open number (ZFX) service message shall be generated to the input port or channel detailing the missing CSNs.

5.2.1.5. Further I-S/A AMPE TI Line processing. To maintain CSN continuity between the I-S/A AMPE and the terminal, the I-S/A AMPE tables shall be updated based on the results of CSN and message processing. When a CSN is rejected (i.e., duplicate condition), no CSN updating shall be performed. When a CSN is accepted, even if it is out of sequence, the accepted CSN (or the expected CSN, if the received CSN is non-numeric) shall be made the last accepted CSN for processing of future messages. When the channel is Mode I or Mode II, this update shall be done immediately on receipt of the TI line whether the associated message is accepted or not, since the Mode I or Mode II terminal is assumed to update the CSN at the beginning of each message transmission. This is also consistent with a terminal transmitting a tape in which there are pre-cut CSN's preceding each message. Since Mode V procedures require that CSN's be updated on acceptance of the message, Mode V terminal equipment does not update its TI generator until the associated message has been acknowledged by the I-S/A AMPE. Consequently, the I-S/A AMPE also shall not update the last accepted CSN on a Mode V channel until the message has been validated and accepted, and the ACK for the message has been sent to the terminal.

5.3. Format Line 2 - Message Header. For I-S/A AMPE validation purposes, the ACP header shall be divided into four parts: The precedence field including the start-of-routing (SOR) and the optional high-precedence bell signal (FL2); the RI field (FL2); the originating subscriber line (FL3); and the security line (FL4).

5.3.1. Precedence/Start-of-Routing Field. The first step in processing an ACP format header shall be to perform a search for the SOR. In ACP format, this is a single space, normally in the third data position following the repeated precedence prosign.

5.3.1.1. Check 2.1.a. If the SOR is in the third position, the repeated precedence prosign shall be validated. The five valid prosigns are:

"YY" - Emergency Command Precedence (ECP)
"ZZ" - Flash
"OO" - Immediate
"PP" - Priority
"RR" - Routine

Error Conditions:

A non-alphabetic character or a lower case ASCII character in either position.

Error Resolution - The message shall be rejected without exception and an "INVALID HEADER - REJ" service message is automatically generated to the input port or channel.

Both characters are alphabetic, but not valid precedence characters.

Error Resolution - The message shall be accepted and processed as an immediate precedence ("OO") message.

Only one character is a valid precedence character.

Error Resolution - The message shall be accepted and processed at the precedence specified by the one valid precedence character.

Both precedence characters are valid, but unequal.

Error Resolution - The message shall be accepted and processed at the higher precedence.

Presence of a "Y" in either position of a message from a port or channel not authorized ECP input.

Error Resolution - The message shall be rejected and an "INVALID USE OF ECP" service message automatically generated to the input port or channel.

Note: In the above cases when the message is processed as one or another precedence, the precedence prosign shall be not corrected but shall be transmitted to an ACP format subscriber as received. A JANAP subscriber shall receive a header containing the precedence at which the message was processed.

5.3.1.2. Check 2.2.a. If the SOR is not properly positioned, a search shall be made to determine if either a valid or garbled bell signal (SO/FIGS, five apostrophe symbols, five bell signals, and a SI/LTRS) is present. The determination of a garbled bell signal shall be based on a search for two of any of the characters "apostrophe", "bell", "J", or "S". Presence of either a valid or garbled bell signal shall cause the message to be handled as Flash unless a "Y" is found in either precedence character and the port or channel is classmarked as being authorized ECP input.

Error Condition - Improperly positioned SOR.

Error Resolution - If a valid or garbled bell signal is not detected, the message shall be rejected and an "INVALID HEADER - REJ" service message automatically generated to the input port/channel.

5.3.2. Header Validation of the Routing Indicator Field. The processing of an ACP format RI field shall be essentially the same as that described previously for the JANAP teletypewriter format message with the exception of the EOR. In the JANAP format, this sentinel is a period. In the ACP format, it may be one of two letter perfect sequences: Carriage return, carriage return, line feed "D"; or carriage return, carriage return, line feed "Z". The "D" indicates the start of FL3 whereas the "Z" indicates the presence of an ACP format pilot.

5.3.2.1. Check 2.3.a. If the RI field contains only one RI, a check shall be made for a valid EOR sequence. If the RI field contains several RIs and consists of more than one line, a check shall be made for valid, letter perfect end-of-line sequences (CR,CR,LF) terminating each line and a valid EOR.

Error Condition - Any invalid EOL or EOR sequence.

Error Resolution - The message shall be rejected and an "INVALID RI FIELD" service message is automatically generated to the input port or channel.

5.3.3. Header Validation of the Originating Station Line (DE Line/FL3). When the EOR is found as CR,CR,LF"D", the program assumes that FL3 is present. See Navy JANAP variations, para 4.3.3.1 for FL3 validation requirements. When the EOR is found as CR,CR,LF"Z", the I-S/A AMPE program shall assume that an ACP format pilot precedes the original header and the "Z" shall be assumed to be the first character of the security line (FL4) and this line shall undergo processing prior to FL3. A separate search shall be then made for a LF"D" sequence indicating FL3 which then shall undergo FL3 validation.

5.3.3.1. Check 3.1.a. Once an EOR is validated and FL3 validation is complete, a search shall be made for the next line feed which indicates termination of FL3. This line feed character need not be part of a perfect EOLS, but the character immediately following it must be the beginning of FL4 which is indicated by the letter "Z".

Error Condition - Any character other than a "Z" immediately following the LF.

Error Resolution - The message shall be rejected and an "INVALID SECURITY FIELD" service message automatically generated to the input port or channel even though FL4 may be internally correct.

5.3.3.2. Check 3.1.b. If the channel is not classmarked as being exempt from straggler detection (as are some Allied channels), the FL3 originating station serial number shall be located and stored for later comparison with the serial number preceding the EOM function. The OSSN field immediately follows the straggler sentinel (#) and, unless a Cat 1 (ECP or Flash) message, must consist of four numeric characters.

Error Condition - The message is not a Category 1 and contains a non-numeric character in the OSSN field.

Error Resolution - The message shall be rejected and an "INVALID HEADER" service message automatically generated to the input port or channel.

5.3.4. Header Validation of the Security Line (FL4). FL4, whether part of a pilot or a normal header, shall be validated exactly in the same manner as described for teletypewriter JANAP format. The only significant difference in processing shall be that an ACP format message received from an Allied channel must not contain a TRC and all five security characters must be valid and identical.

5.3.4.1. Check 4.1.a. ACP format message received on a channel classmarked as Allied must contain five redundant valid security characters.

Error Condition - Use of a TRC, security character invalid or not repeated five times on an ACP formatted message received on an Allied channel.

Error Resolution - The message is rejected and an "INVALID SECURITY FIELD" service message is automatically generated to the input port or channel.

5.4. Routing Indicator Processing. RI processing for ACP format shall be nearly identical to that for JANAP format. RIs in an ACP format message from an Allied channel shall not undergo validation against the TRC since Allied ACP messages cannot use a TRC. Also, since there is no LMF field to specify message medium exchange limitations, an ACP format message shall be considered deliverable to any destination that is compatible on the basis of community and security. Message exchange, both header format and medium, shall be performed as necessary on output. RIs found invalid for any reason shall be included in a service message sent to the input port or channel. All system generated service messages concerning ACP format messages shall be routed to a predetermined RI (service message RI - SMRI) associated with the channel of receipt.

5.5. End-of Message (EOM) Processing. Upon completion of SOMS validation, a continual scan of each message for the end of message sequence (EOMS) shall be performed. The ACP format EOM procedurally consists of two carriage returns, eight line feeds, and the letters "NNNN" but the minimum required for recognition by the I-S/A AMPE shall be one line feed and four N's. This scan and others that shall be performed for the detection of significant character sequences are described in this section.

5.5.1. Straggler Protection. A "straggler" is caused by a message without a valid start of message sequence (SOMS) following a message without a valid end of message sequence (EOMS) on an asynchronous channel, or two messages entered as one on a synchronous channel and framed SOH-ETX as a single message. To protect against straggler messages, the I-S/A AMPE shall validate the Originating Station Serial Number (OSSN) in the message header (FL3) against the Trailer Station Serial Number (TSSN) found in the message trailer. All ACP format messages are not subject to the straggler validation check. If the straggler sentinel appears in either FL3 or FL15, straggler validation shall be performed unless the port or channel is specifically classmarked by the I-S/A AMPE as being exempt from straggler protection checking.

5.5.1.1. With ACP formatted messages, the OSSN is not positioned absolute (length of the OSRI is variable) and a straggler sentinel (#) is employed in FL3 prior to the four or more digit OSSN. The TSSN must also be preceded by a straggler sentinel (#) which must be within 23 characters of the End of Message Sequence (EOMS). Fields of over four characters shall be acceptable in an ACP FL3 and in the trailer but only the four characters immediately following the sentinel shall be used by the I-S/A AMPE for straggler validation. Failure of straggler validation shall result in message rejection unless the message is Flash precedence, and the automatic generation of a "SUSPECTED STRAGGLER" service message to the input port or channel. Flash messages shall be accepted and the service message generated shall advise the input port or channel "HIGH PRECEDENCE MESSAGE ACCEPTED, REPROTECT SUSPECTED STRAGGLER".

5.5.2. Cancel Transmission Sequence (CANTRANS). The I-S/A AMPE shall also scan for the presence of a CANTRANS which procedurally consists of 8 E's each separated by a space, the letters "AR", and an EOMS of two carriage returns, eight line feeds, and four N's. The minimum recognizable by the I-S/A AMPE shall be two E's separated and followed by a space, "AR", one linefeed, and four

N's. When a CANTRANS is recognized, the message shall be discarded by the I-S/A AMPE with notification to the operator that the message has been discarded.

5.5.3. Excessive Message Length. An additional check that shall be performed during receipt of message text is a count of total line blocks or characters being received. Should this count exceed 556 line blocks (44,480 characters), the message shall be rejected and an "EXCESSIVE MESSAGE LENGTH" service message generated to the input port or channel.

5.5.4. Excessive Input Hiatus. Incoming messages shall also be monitored for any delay (hiatus) in receipt by the I-S/A AMPE. When no additional data is received for a non-CRITIC message in progress for a period of approximately three minutes, the message shall be rejected and a "NO EOM RECEIVED" service message generated to the input port or channel.

5.5.5. Framing Character (FC) Processing. Framing characters shall be validated for all input messages. On asynchronous channels, these have been inserted and the message blocked and framed by the I-S/A AMPE itself so that FC validation shall be essentially a self-checking process by the I-S/A AMPE. On synchronous channels, FC validation shall insure proper framing by the terminal device. Any framing character error shall result in message rejection with a "REPROTECT TO ALL ADDEES" service message generated to the input port or channel. In addition, notification of the FC error shall be provided to the I-S/A AMPE operator so that any FC errors caused within the I-S/A AMPE itself may be detected and corrective action taken.

6.0 MODIFIED ACP 126 MESSAGE PROCESSING REQUIREMENTS.

6.1 General Comments. -

6.1.1 This section will detail the existing MODIFIED ACP 126 format processing.

6.1.1.1 - The NAVY originally introduced Modified ACP 126 message format into the telecommunications network basically to assist the Fleet. However, because of its effectiveness, the majority of Naval message originators and their communications centers prefer this format as it provides/performs:

1. All sectioning and paging.

2. All routing based upon message classification, short titles addressed, and existing siderouting.

3. TRC assignment and multiple transmissions where required.

4. TARE line generation based upon the requirements of each member of a collective.

5. Siderouting where applicable.

By automating these functions, the LDMX has reduced its manpower requirements and requires stringent checks be made on all short titles addressed. Short titles are the key to routing assignment and therefore must be recognizable.

6.2 Validation/Verification Requirements. -

6.2.1 Format Line 1 - Transmission Identifier Line. - LDMX validation of the TI line is identical for both asynchronous (Mode II and V teletypewriter terminals whose use of a TI line is mandatory) and synchronous (Mode I users who employ line block framing and whose use of a TI line is optional, but must be specified at the time the LDMX sets the channel parameters) channels. All TI lines through the CD-CSN fields are processed as follows:

6.2.1.1 The first characters of the TI line block must be a Start of Header (SOH) and a select (SEL) character. If the channel is asynchronous, these have been inserted by the LDMX; if the channel is synchronous, the terminal has inserted them.

6.2.1.2 Check 1.1.a. - The first data character of the TI line must be the letter "C". (If the channel is asynch the "ZCZC" portion of the Start of Message Sequence (SOMS) wa previously validated and then discarded by the LDMX.)

Error Condition - None - nothing can be recognized prior to receipt of the SOH.

Error Resolution - N/A

6.2.1.3 Check 1.1.b. - The second, third and fourth characters of the TI line must be the Channel Designator (CD) and must match the CD stored at the LDMX for that channel.

Error Condition - A CD is considered to be in error if it does not match the CD stored in the LDMX for its associated channel.

Error Resolution - Except for messages of ECP or Flash precedence, messages having CD errors will be rejected to the service position. Precedence categories are explained later in this document.

6.2.1.4 Check 1.1.c. - The fifth character of the TI line can be either a figures shift or the first character of the CSN field; the figures shift must be present for "A" Select (ITA2) messages and may or may not be present for other selects. Note that for all processing purposes, "A" Select CSN's are always assumed to begin in the sixth position of the TI line. This is done so that the "CSN" to be quoted back to the terminal in a service message will be positionally correct even if the figure shift is garbled, leaving the CSN field in the lower case. If the CSN is correct, TI line processing is complete at this point.

Error Condition - A CSN is considered to be in error if it is either non-numeric or if it is not the next expected CSN (i.e., one greater than the last accepted from a Mode V channel or received from a Mode I or II channel.) For this purpose, a CSN of 000 is considered to be one greater than 999.

Error Resolution - Messages of ECP or Flash precedence will be accepted regardless of CSN errors detected. Other messages having CSN errors will be processed as follows:

If the CSN is a duplicate of the last accepted (Mode V) or received (Mode I/II), the message will be rejected to the service position. This is the only instance of CSN error where a message will be rejected by the LDMX which will generate an "OUT OF SEQUENCE" message to the input channel and log the error condition on an error file for future compilations (possibly similar to the existing Communications Improvement Memorandum (CIM) program.

If the CSN is incorrect for any other reason including being non-numeric, the message will be accepted. However, these errors shall cause the LDMX to generate a service message to the input channel citing the CD and CSN as well as other pertinent message identification data. This service message will indicate "POSSIBLE DUPLICATE", "OUT OF SEQUENCE" and whether the message needs to be protected for. Missing CSNs will cause generation of an open number (ZFX) service message to the input channel.

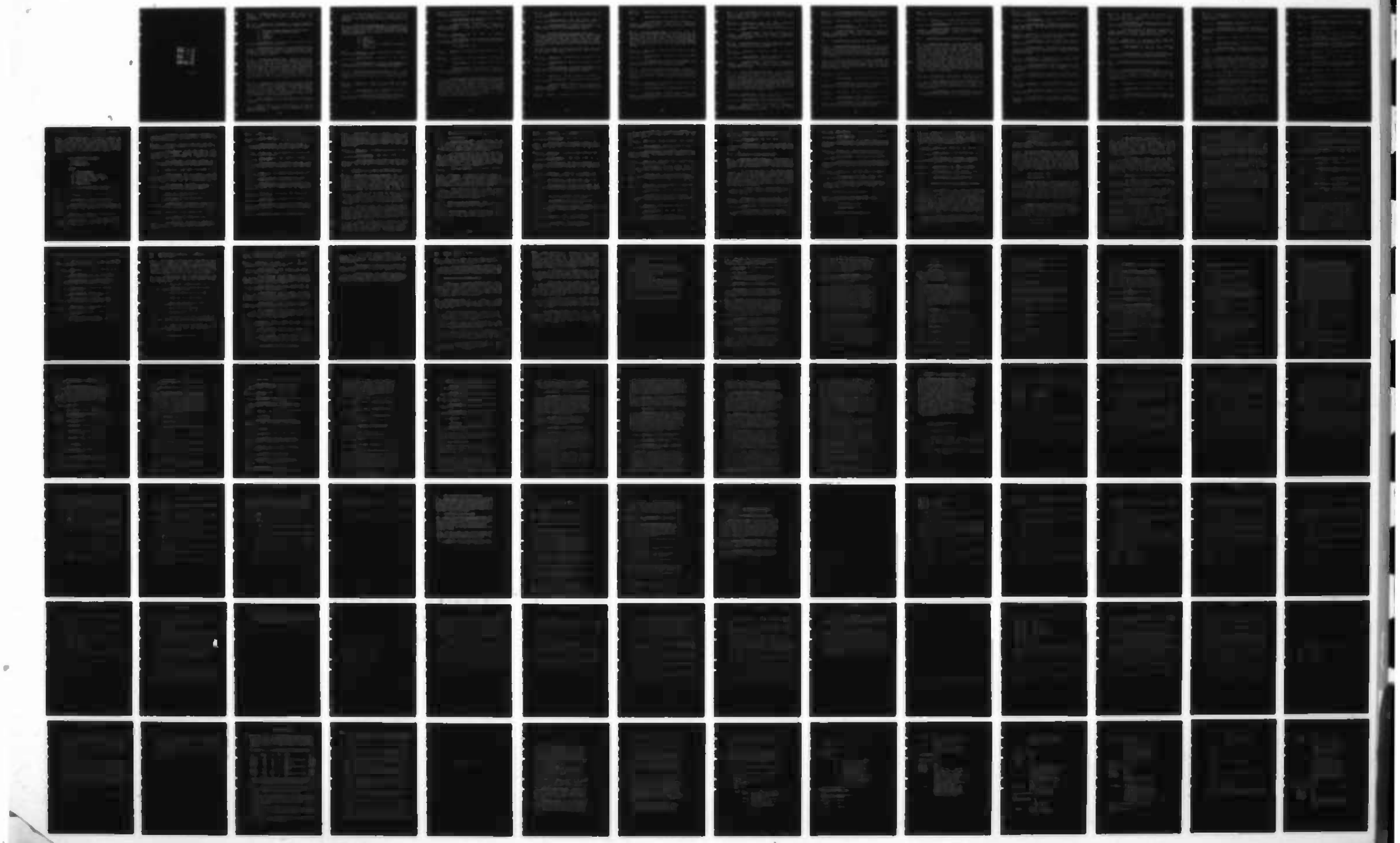
6.2.1.5 <u>Further LDMX TI Line Processing</u>. - In order to maintain CSN continuity between the LDMX and the terminal, the LDMX tables are updated based on the results of CSN and message processing. When a CSN is rejected (i.e., duplicate condition), no CSN updating is performed. When a CSN is accepted, even if it is out of sequence, the accepted CSN (or the expected CSN, if the received CSN is non-numeric) is made the last accepted CSN for processing of future messages. When the channel is Mode I or Mode II this update is done immediately on receipt of the TI line whether the associated message is accepted or not, since the Mode I or Mode II terminal is assumed to update the CSN at the beginning of each message transmission. This is also consistent with a terminal transmitting a tape in which there are pre-cut CSN's preceding each message. Since Mode V procedures require that CSN's be updated on acceptance of the message, Mode V terminal equipment does not update its TI generator until the associated message has been acknowledged by the LDMX. Consequently, the LDMX also does not update the last accepted CSN on a Mode V channel until the message has been validated and accepted.

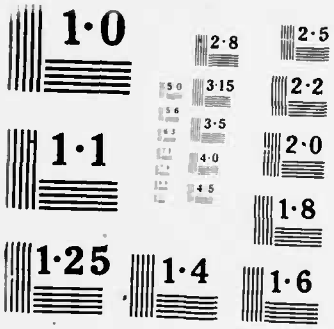
6.3 <u>Message Format</u>. - For NAVY LDMX validation/verification purposes, the MODIFIED ACP 126 format is divided into thirteen parts: Header data up to and including the Start-of-Routing Sequence (Format Line 2); the Routing Indicator Field (still a part of Format Line 2); the Security Line (Format Line 4); Passing Instructions (Format Line 4 Extensions); Operating Signals; the Date Time Group (Format Line 5); the Message Originator (Format Line 6); the Action/Information Addressees (Format Line7/8); the Exempt Addressee (Format Line 9); the Accounting Symbol (Format Line 10); the End of Header (Format Line 11); FL2, FL4, and TARE Line generation; the Message Classification (Format Line 12); and the End of Message (Format Lines 13 throught 16).

6.3.1 <u>Format Line 2 Processing Through the Start-of-Routing</u>. -

AD-A134 884 INTER-SERVICE/AGENCY AUTOMATED MESSAGE PROCESSING EXCHANGE PROGRAM FUNCTI..(U) DEFENSE COMMUNICATIONS AGENCY ARLINGTON VA 01 NOV 83 4/7

UNCLASSIFIED F/G 17/2 NL





NATIONAL BURFAU

MICROCOPY RESOLUT

6.3.1.1 Precedence Field. - The first header field to be validated is the precedence field. Once validatea, the precedence is saved for later correlation with FL5 precedence(s).

6.3.1.1.1 Check 2.1.a. - Precedence is a single character, the first character of the header and is validated to be one of five characters:

"Y" - Emergency Command Precedence (ECP) which may be input only on authorized channels.
"Z" - Flash
"O" - Immediate
"P" - Priority
"R" - Routine

Error Condition - If the field is not one of the five precedence characters specified above.

Error Resolution - An error in the precedence field of either an invalid or an unauthorized character results in the message being rejected to a service position with the error annotation "INVALID PRECEDENCE". See Message Error Processing for the appropriate response.

6.3.1.2 Language Media Format (LMF). - The next field to be validated in a MODIFIED ACP 126 format message is the Language and Media Format (LMF) field. This is a two character field in which the first character (LMF1) indicates the medium in which the input message was originally prepared. It is sometimes also called the Input LMF. The second character (LMF2) indicates the medium in which the originator prefers the message to be delivered to the addressee. It is sometimes also referred to as the Output LMF. Input header processing merely validates the Input Media/LMF combination. Further use of the LMF in input processing and in output message delivery will be discussed later.

6.3.1.2.1 Check 2.2.a. - LMF validation is always combined with the validation of the Input Media. If the message is from a TI user, the SEL is obtained from the second framing character of the TI line block. Otherwise, it is the second framing character of the header line block. Once the SEL-LMF combination passes validation, the LMF pair information is saved for RI processing, which must determine whether a message of the specified LMF can be delivered to a given RI.

Error Condition - If the Input Media/LMF combination does not match an LDMX table entry, the Input Media is validated separately.

Error Resolution - If the Input Media is invalid, an error condition is logged and the message is rejected with no exceptions. A "REPROTECT TO ALL ADDRESSEES" service message is generated.

When the Input Media is valid, but one of the LMF characters is invalid, specifically, not "TT" or "TC", it is rejected to a service position with an "INVALID LMF" error annotation. See Message Error Processing for the appropriate response.

6.3.1.3 Single Security Character Field. - The next field to be validated is the single character security field. Once validated, the security character is saved for further security checks in format line 2, 4, and 12 processing. The single character which indicates the security, must be one of the following characters:

"T"	- Top Secret
"S"	- Secret
"C"	- Confidential
"R"	- Restricted
"E"	- Unclas E F T O (encrypted for transmission only)
"U"	- Unclassified

6.3.1.3.1 Check 2.3.a. - The single character is compared to valid security characters above.

Error Condition - Detection of an invalid security character.

Error Resolution - The message is rejected to a service position, with the error annotation "*INVALID SECURITY*". See Message Error Processing for the appropriate response.

6.3.1.4 Content Indicator Code (CIC) Field. - The four character CIC field contains information related to the type of message being processed. The CIC is also referred to as the Communication Action Identifier (CAI). All valid CIC values are stored.

6.3.1.4.1 Check 2.4.a. - The CIC is validated for four alphabetic characters, or three alphabetic and one numeric character.

Error Condition - Not a valid CIC, one listed in LDMX table, or not enough characters in the CIC.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID CIC FORMAT". See Message Error Processing for the appropriate response.

6.3.1.4.2 Check 2.4.b. - The CIC indicates an ADMS/ASC generated pilot, the original CIC from Format Line 2 is also validated (dual header only).

Error Condition - No valid CIC in piloted Format Line 2, or no Format Line 2 Extension present.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID FORMAT LINE 2". See Message Error Processing for the appropriate response.

6.3.1.4.3 Check 2.4.c. - The CIC "ZYVW" is detected, indicating a service message.

Error Condition - None - Checks are made during RI validation for non local ris, and if present no further format validation is done.

Error Resolution - N/A

6.3.1.5 Separator. - The character following the CIC must be a space.

6.3.1.5.1 Check 2.5.a. - Check the character following the CIC field.

Error Condition - Any character other than a space.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID CHARACTER AFTER CIC". See Message Error Processing for the appropriate response.

6.3.1.6 Originating Station Routing Indicator (OSRI) Field. - Following the separator is the seven character OSRI field. This may be a six or seven character Routing Indicator (RI) spaced filled to seven characters. In the case of OCR input, the OSRI field may be blanks, and the LDMX supplies its service service center RI as the OSRI. In any case, a new OSRI is generated by the LDMX for Modified ACP 126 formatted messages so that subsequent servicing action will be assumed by the LDMX. Both the original and generated OSRI are saved for a later comparison to determine if the message is a duplicate. This is discussed in detail later in the document.

6.3.1.6.1 Check 2.6.a. - The OSRI does not begin with an "R", or is not alphabetic in all six to seven positions, and not input from an OCR.

Error condition - The OSRI begins with a character other than "R" or contains non-alphabetic characters.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID OSRI". See Message Error Processing for the appropriate response.

6.3.1.7 Originating Station Serial Number (SSN) Field. - Immediately following the OSRI is the SSN field. The SSN field is validated for four numeric characters. A valid SSN is saved for later comparison with the Trailer Station Serial Number (TSSN) to ensure that a "straggler" condition does not exist. Straggler checking is discussed under End-of-Message validation. A valid SSN is used along with the OSRI during duplicate message validation.

Here again, the LDMX will generate an SSN based upon the original message OSRI which is categorized as; Service Center, Message Center, or Data Center.

6.3.1.7.1 Check 2.7.a. - The SSN field is validated to be four numeric characters.

Error Condition - The SSN is not numeric or four characters in length.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID SSN". See Message Error Processing for the appropriate response.

6.3.1.7.2 Check 2.7.b. - The SSN is compared to the TSSN.

Error Condition - The SSN does not match the TSSN (Format Line 15).

Error Resolution - The message is rejected to a service position with the error annotation "STRAGGLER SSN MISMATCH". See Message Error Processing for the appropriate response.

6.3.1.8 Separator. The character following the SSN must be a space.

6.3.1.8.1 Check 2.8.a. - Check the character following the SSN field.

Error Condition - Any character other than a space.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID CHARACTER AFTER SSN". See Message Error Processing for the appropriate response.

6.3.1.9 Time-of-File (TOF) Field. - The TOF field is validated for seven numeric characters. Procedurally, the TOF field is composed of a three digit Julian date (001-365/366) and four digit time (0000-2359). Range checks are made provided the message was not input from an OCR. In this case the TOF may be all zeroes and the LDMX will assign a TOF using the computer clock. The TOF is used along with the OSRI and SSN in duplicate message validation, which will be discussed later in the document.

6.3.1.9.1 Check 2.9.a. - Check the TOF field for seven numeric characters.

Error Condition - The TOF is not numeric or seven characters in length.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID TOF". See Message Error Processing for the appropriate response.

6.3.1.10 Security Redundancy Field Separator. - Following the TOF field, the character must be a dash or hyphen (ITA2 uppercase "A") signalling the start of the Security Redundancy field. If the Security Redundancy separator is misplaced, the message could be a pilot. In either case the proper fields are validated.

6.3.1.10.1 Check 2.10.a. - The character following the TOF is not a dash or a blank character.

Error Condition - Any character other than a dash or a blank.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID SEPARATOR CHARACTER". See Message Error Processing for the appropriate response.

6.3.1.11 Piloted Message Field - When the separator is a blank character this field is checked to determine if the message contains a pilot header. All pilot lines are stripped and the original FL2 is used.

6.3.1.11.1 Check 2.11.a. - Check for "PLTS" (terminally prepared) or "Rxxx" (switch prepared) pilot indicators.

Error Condition - Pilot field contains data other than pilot headers.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID PILOT/CARD COUNT". See Message Error Processing for the appropriate response.

6.3.1.12 Record Count Field. - When the separator is a blank character and does not contain a pilot header, this field is checked for valid record count indicators.

6.3.1.12.1 Check 2.12.a. - Check for "MTMS" or for four valid numerics.

Error Condition - Record Count field contains data other than "MTMS" or four numeric characters.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID PILOT/CARD COUNT". See Message Error Processing for the appropriate response.

6.3.1.13 Security Redundancy/TRC Fields. - In the MODIFIED ACP 126 format, the four character Security Redundancy field is validated in different ways. All four characters of the Security Redundancy field must be identical to the single security character previously validated (fourth data character of FL2). If the message is addressed to an Allied destination, the last two characters of the Security Redundancy field will be changed to reflect valid transmission release codes once all PLA lookup and RI generation has been completed. At this point however, the original FL2 must contain four identical values which match the fourth data character of FL2.

6.3.1.13.1 Check 2.13.a. - Check the four security characters against the single security character field.

Error Condition - The four security characters are not identical to the single security character field.

Error Resolution - The message is rejected to a service position with the error annotation "SECURITY REDUNDACY ERROR - F/L 2". See Message Error Processing for the appropriate response.

6.3.1.14 Start of Routing (SOR) Field. - After the Security Redundancy checks are complete, the SOR field is then validated. This field is a two character field containing dash dash (--).

6.3.1.14.1 Check 2.14.a. - The SOR field is validated for dash dash (--).

Error Condition - The SOR field contains characters other than a double dash (--).

Error Resolution - The message is rejected to a service position with the error annotation "INVALID START OF ROUTING". See Message Error Processing for the appropriate response.

6.3.2 MODIFIED ACP 126 Validation of the RI Field. -

6.3.2.1 Routing Indicator (RI) Field. - The RI is the "address" of a message. An RI may not be split by either spaces or by an End of Line (EOL) sequence in any instance. The RI is examined for the proper form, which begins with an "R", is seven alphabetic characters, and has "SUU" as a suffix. Format Line 2 must contain only the one RI and be terminated with the End of Routing delimiter.

This RI field is what determines whether the message is JANAP 128 or Modified ACP 126. To be classified as a Modified ACP 126 formatted message, there must be only one RI whose suffix is "SUU", and whose NARC equals that of the processing LDMX or one which the processing LDMX has accepted delivery responsibility for.

6.3.2.1.1 Check 3.1.a. - The first character of the RI must begin with a "R".

Error Condtion - First character of the RI is not a "R".

Error Resolution - The message is rejected to a service position with the error annotation "INVALID RI". See Message Error Processing for the appropriate response.

6.3.2.1.2 Check 3.1.b. - The RI must contain four to seven characters.

Error Condition - The RI contains more than seven characters, or the RI contains invalid characters.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID RI". See Message Error Processing for the appropriate response.

6.3.2.2 End-of-Routing Field. - The MODIFIED ACP 126 format End-of-Routing (EOR) consists of a period (.).

6.3.2.2.1 Check 3.2.a. - Validate that there is a valid EOR.

Error Condtion - The last field in Format Line 2 contains an invalid EOR sentinel.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID END-OF-ROUTING SIGNAL". See Message Error Processing for the appropriate response.

6.3.3 MODIFIED ACP 126 Validation of the Security Line. -

6.3.3.1 Security Line (FL4). - Following the EOR or original FL2 processing the next field to be validated is the security line, format line four. In all cases, FL4 must follow the original FL2. The first four characters following the EOR must be the operating signal "ZNR" or "ZNY" followed by a space. When it is determined that FL4 is present, the remaining security fields are processed. The first of these is five characters in length and must consist of five redundant security characters. Following this, separated by a slash (/), may be from one to four optional special handling designator (SHD) fields (separated by a slash), each of which consists of a five redundant SHD characters. SPECAT Release Codes (SRC) are the exception, there may be only one set of SRCs. SRCs and SHDs may not both be contained within a message. Following the security field or SHD characters, separated by a space, may be operating signals (Operating signal processing is discussed later in the document) or passing instructions.

6.3.3.1.1 Check 5.1.a. - The first four characters of FL4 are checked to see if they contain "ZNR" or "ZNY" and a space.

Error Condition - The first three characters are not "ZNR" or "ZNY" and followed by a space; "ZNY" and a space is used, but the FL2 security redundancy field is "UUUU"; or "ZNR" and a space is used, but the FL2 security redundancy field is other than "UUUU".

Error Resolution - The message is rejected to a service position with the error annotation "INVALID FORMAT LINE 4". See Message Error Processing for the appropriate response.

6.3.3.1.2 Check 5.1.b. - The first five characters of the security field are validated to be redundant and must match the security redundancy field.

Error Condition - The characters are not redundant or do not match those in FL2.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID SECURITY ON FORMAT LINE FOUR". See Message Error Processing for the appropriate response.

6.3.3.1.3 Check 5.1.c. - After validation of the security redundancy field, a check is made for the Special Handling Designator (SHD) sentinel, a slash (/), or a space.

Error Condition - Any character other than a slash (/), a space or a valid end-of-line sequence following the previous field.

Error Resolution - The message is rejected to a service position with the error annotation "ILLEGAL CHARACTERS ON FORMAT LINE FOUR". See Message Error Processing for the appropriate response.

6.3.3.1.4 Check 5.1.d. - The SHD sentinel is found, check the next five characters for redundancy and they must be valid SHD category characters as specified in ACP 117.

Error Condition - The five characters are not redundant, not a valid SHD category, SHDs found number more than four, or the classification of the message is below CONFIDENTIAL.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID OR DUPLICATE SHD ON F/L 4". See Message Error Processing for the appropriate response.

6.3.3.1.5 Check 5.1.e. - If the SHD sentinel is found, the input channel/position is checked to see if it is authorized to enter SHDs.

Error Condition - Special handling is required for the message and the input channel/position is not authorized to enter the SHD.

Error Resolution - The message is rejected to a service position with the error annotation "SPECIAL HANDLING REQUIRED". See Message Error Processing for the appropriate response.

6.3.3.1.6 Check 5.1.f If another SHD sentinel (/) is found, the next field is validated in the same manner as the first. If a valid SRC is detected, a check is made to ensure there are no SHDs in the message.

Error Condition - The message contains an invalid SRC, or the SRC does not agree with the message classification, or SRC is present with other SHDs.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID SRC ON FORMAT LINE FOUR" or "ILLEGAL CLASS WITH SRC OR SHD". See Message Error Processing for the appropriate response.

6.3.3.1.7 Check 5.1.g. - If a space is found after the security redundancy field or valid SHD/SRC fields, additional operating or passing instructions may be present.

Error Condition - None of the characters remaining on FL4 resemble any operating signals or TARE instructions.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID TARE LINE". See Message Error Processing for the appropriate response.

6.3.4 MODIFIED ACP 126 Validation of FL4 Continuations. - This format line may contain only operating signals or "T ZWL" tares.

6.3.4.1 Tare Instruction Search (FL4/E). - Tare instructions, other than "T ZWL", are not allowed since Modified ACP 126 formatted messages require the LDMX to supply any required TARE instructions. Operating signals and "T ZWL" instructions carry through onto the fully formatted LDMX generated message.

6.3.4.1.1 Check 6.1.a. - Check for valid operating signal or "T ZWL".

Error Condition - The message contains "T ZWL" without a short title.

15;Error Resolution - The message is rejected to a service position with the error annotation "INVALID TARE LINE". See Message Error Processing for the appropriate response.

6.3.4.1.2 Check 6.1.b. - If a "T ZWL" is found, it should be followed by a recognizable short title. The short title identifier will be saved in order to properly process format lines 7 and 8.

Error Condition - The short title contained on FL4/E was not contained in the LDMX data base.

Error Resolution - The message is rejected to a service position with the error annotation "SHORT TITLE NO IN DATA BASE". See Message Error Processing for the appropriate response.

6.3.4.1.3 Check 6.1.c. - Ensure all "T ZWL" short titles are processed.

Error Condition - The maximum number of "T ZWL" short title identifiers is reached.

Error Resolution - The message is rejected to a service position with the error annotation "CANNOT PROCESS ALL 'T ZWL'. MAX PER MSG: XX" where XX represents the numerical maximum.

6.3.4.2 Operating Signals (Z-Signal) Processing. - Operating signals or Z-signals as they are called may be found on format line 4, format line 4 extensions or format line 5. Whenever a potential Z-signal is detected, control is passed to the appropriate processing module for validation. Z-signal processing is discussed in three parts: Initial "Z" Signal Validation; ZPW Validation; and Other "Z" Signal Validation.

All operating signal validations are passive, to the extent that just because a word/trigraph/etc. may start with a "Z" it does not mean that it must be a "Z" signal and no errors are given based solely on a "Z" being present.

Initial "Z" Signal Validation. When a potential Z-signal is identified, the first three characters of the Z-signal are verified for alphabetics and the fourth character is verified to be either numeric or blank.

ZPW Validation. Whenever the Z-signal "ZPW" is identified the remaining data is verified to be a six digit numeric Date-Time-Group followed by the letter "Z".

Other "Z" Signal Validation. Z-signals "ZXY" and "ZNM" are invalid. For Z-signals other than "ZPW" a table is scanned for the corresponding Z-signal and if found the appropriate flag is set. Whenever the Z-signals: ZDK, ZDG, ZEL, ZFG, ZFF4, ZFF5, ZFF6, ZFH1, ZFH2, ZFH3, ZUI, or ZDS are identified the message is directed to a service position as well as the primary delivery indicated in FL2 routing.

6.3.4.2.1 Check 6.2.a - The potential Z-signal is validated for proper format.

Error Condition - None - The letter "Z" is found in a line however it does not match an "Z" signal in the LDMX table.

Error Resolution - N/A

6.3.4.2.2 Check 6.2.b. - The Z-signal is one of "ZPW".

Error Condition - The "ZPW" Z-signal is identified and the Date-Time-Group field contains invalid characters, or the line does not end with a "Z".

Error Resolution - The message is rejected to a service position with the error annotation "BAD ZPW TIME". See Message Error Processing for the appropriate response.

6.3.4.2.3 Check 6.2.c. - The Z-signal field contains the characters "ZNM".

Error Condition - The "ZNM" Z-signal is not permitted in the message.

Error Resolution - The message is rejected to a service position with the error annotation "ZNM ILLEGAL". See Message Error Processing for the appropriate response.

6.3.4.2.4 Check 6.2.d. - The Z-signal field contains the characters "ZXY".

Error Condition - The "ZXY" Z-signal is detected and requires delivery be made to the addresse indicated by the fourth character of the Z-signal.

Error Resolution - The message is rejected to a service position with the error annotation "ZXY SIGNAL FOUND". See Message Error Processing for the appropriate response.

6.3.4.2.5 Check 6.2.e. - A Z-signal is detected without format errors, but does not match a specific Z-signal requiring addition action.

Error Condition - None - The Z-signal is validated for proper format and stored as a part of the message.

Error Resolution - N/A

6.3.5 MODIFIED ACP 126 Validation of Date-Time-Group Line.

6.3.5.1 Date-Time-Group (FL5). - Following validation of format line four extensions' (tare instructions and operating signals), the next line validated is the Date-Time-Group. The Date-Time-Group consists of the Precedence field(s), the actual day, hour, and minutes of the message, a terminator, the month field, and a year field. Format line 5 may also contain operating signal(s) if the message warrants them. Operating signal processing has been previously discussed in this document.

VALID FORMAT LINE 5 STRUCTURE:

```
P DDHHMMZ MON YR
PI DDHHMMZ MON YR
P I DDHHMMZ MON YR
```

LEGEND:

P = ACTION PRECEDENCE
I = INFO PRECEDENCE
DD = VALID DAY - RANGE 01 THRU 31
HH = VALID HOUR - RANGE 00 THRU 23
MM = VALID MINUTE - RANGE 00 THRU 59
Z = ZULU TIME DESIGNATOR
MON = VALID MONTH
YR = NUMERICAL YEAR

Each of the aforementioned structures may contain operating signals and the "YR" must always be present.

6.3.5.1.1 Check 7.1.a. - Check the first character of the DTG for a valid precedence.

Error Condition - There is only one precedence in format line 5 and it does not equal the FL2 precedence.

Error Resolution - The message is rejected to a service position with the error annotation "PRECEDENCE ERROR ON F/L 5". See Message Error Processing for the appropriate response.

6.3.5.1.2 Check 7.1.b. - Validate the second position of the DTG for a space or valid INFO precedence.

Error Condition - An illegal INFO precedence character follows the action precedence character; or a character other than a space follows the second precedence character of the DTG field.

Error Resolution - The message is rejected to a service position with the error annotation "NO BLANK AFTER PRECEDENCE FIELD ON F/L 5". See Message Error Processing for the appropriate response.

6.3.5.1.3 Check 7.1.c. - The third position in the DTG is validated for a dual precedence or the beginning of the Date-Time-Group field.

Error Condition - If the third character is not an alphabetic precedence character less than the first precedence in FL5, a numeric character indicating the first character of the Date-Time-Group, or a space and the FL5 structure is "PI ".

Error Resolution - The message is rejected to a service position with the error annotation "INVALID DTG ON F/L 5". See Message Error Processing for the appropriate response.

6.3.5.1.4 Check 7.1.d. - Range checks are performed on the DTG field.

Error Condition - The six characters following the precedence field and that start in the correct position are not numeric; the day portion is zero or greater than 31; the hour portion is greater than 23; or the minute portion is greater than 59.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID DTG". See Message Error Processing for the appropriate response.

6.3.5.1.5 Check 7.1.e. - The DTG digits are valid numerics with the specified range and ends with a "Z".

Error Condition - The Date-Time-Group field ends with a character other than a "Z".

Error Resolution - The message is rejected to a service position with the error annotation "NO Z FOR ZULU ON F/L 5". See Message Error Processing for the appropriate response.

6.3.5.1.6 Check 7.1.f. - A valid separator must follow the Date-Time-Group.

Error Condtion - The character following the "Z" field of the DTG is not a space.

Error Resolution - The message is rejected to a service position with the error annotation "NO BLANK AFTER DTG FIELD ON F/L 5". See Message Error Processing for the appropriate response.

6.3.5.1.7 Check 7.1.g. - The month field following the separator is validated for the appropriate content.

Error Condition - The characters identified in the month field of FL5 do not match any of the valid twelve months.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID MONTH ON F/L 5". See Message Error Processing for the appropriate response.

6.3.5.1.8 Check 7.1.h. - If the month field is valid it must be followed by a valid separator.

Error Condition - The character following the month field is not a space.

Error Resolution - The message is rejected to a service position with the error annotation "NO BLANK AFTER MONTH ON F/L 5". See Message Error Processing for the appropriate response.

6.3.5.1.9 Check 7.1.i. - All messages require the year field to be present in FL5.

Error Condition - The message did not enter the system from AUTODIN and does not contain a year in FL5.

Error Resolution - The message is rejected to a service position with the error annotation "YEAR MISSING ON THIS F/L 5". See Message Error Processing for the appropriate response.

6.3.5.1.10 Check 7.1.j. - If the year field contains data it is checked for a valid year.

Error Condition - The year field contains data and it is not numeric data.

Error Resolution - The message is rejected to a service position with the error annotation "YEAR IS NOT NUMERIC ON F/L 5". See Message Error Processing for the appropriate response.

6.3.6 MODIFIED ACP 126 Validation of Originator (FL6) Lines.

6.3.6.1 · From Line (FL6). - The Originator's Short title referred to as FL6, is verified to ensure it is within the correct character limits; and that it exists in the Data Base. For local LDMX processing there are two types of short titles: a Protect Short Title and a Guard Command Short Title. In either case, the LDMX performs special message distribution and backrouting dependent upon whether a Protect or Guard Short Title is found.

6.3.6.1.1 Check 8.1.a. - A search is made to find the short title in the data base.

Error Condition - The short title is not contained within the Data Base.

Error Resolution - The message is rejected to a service position with the error annotation "SHORT TITLE NOT IN DATA BASE". See Message Error Processing for the appropriate response.

6.3.7 MODIFIED ACP 126 Validation of ACTION/INFO Lines. -

6.3.7.1 Format Line 7 8 (FL7/8) Processing. - The processing of FL7/8 requires that the short title first be isolated. To do this, it is determined if the short title is siderouted and whether it is processing a format line containing the prosign "TO" or "INFO". When the prosign is present, it is skipped and validation starts with the sideroute search. Sideroutes consist of ris, ZEN, ZEN1, or ZEN2 followed by a slash (/). Should the line contain "ZEN" in any of the aforementioned formats, no Short Title validation is done.

Format Line seven or eight may contain a single sideroute or dual sideroutes. In order to be classified as a RI sideroute, it must begin with the character "R", be between four and seven alphabetic characters in length, and end with a slash (/). Once the RI(s) have been identified they are saved for later processing and the short title has now been isolated for processing.

The isolated short title can now be used to access the data base. From the data base and the message classification, it can be determined if the short title will be "cleared". It also provides FL7/8 processing with the proper RI assignment and TARE line requirements. This RI is used to sideroute the short title, if it is not already siderouted, and saved for building a "new" FL2. The creating of a "new" FL2 is discussed later in this document.

In addition, short titles identified as being "alternate spellings", (derivatives of a "preferred" spelling) will be replaced by their "preferred spelling". "Alternate spellings" were created in order to reduce manual intervention rates (MIRs) by allowing abbreviations, and frequent misspelling of a short title to be recognizable to the automated systems.

6.3.7.2 Delivery of Various Short Title Types.

6.3.7.3 Non-Collectives. -

Over-the-Counter (OTC). If the delivery is one of OTC, the short title is either a "Protect" or "Guard" short title. Protect short titles are identified by a "P", "Q", or "R" in the data base, and Guard Command short titles are identified by a command number ranging from 01-30. All pertinent data is saved for distribution processing.

If FL7/8 contains FAS office codes, a FAS line is built for Guard Commands, but not for Protects. FAS office codes, if present are located between double slashs (//). The LDMX will save this information in the form: the short title identifier followed by the office codes (those longer than three characters are truncated to three characters), each of which is preceded by a slash; (i.e., ACPPTR/OP1/OP2/OP3). This information is used in distribution processing.

Non-Local (NON-OTC). No special processing required.

6.3.7.4 Collectives. - Collectives are totally expanded to identify all members. Each member is looked at separately to determine RI assignment, proper clearances, and TARE line generation requirements. Each RI, in turn, is saved for the creation of a new FL2. Collective processing is basically not much different from non-collectives except processing requires the involvement of multiple member short titles vice one.

When determining "ACTION" or "INFO" delivery requirements, the collective's location in the message is used. If a collective appears on FL7, the collective composition, which also contains ACTION/INFO indicators, is the sole source for the assignment. Should the collective appear on FL8, all members receive the message as info addees.

6.3.7.5 Readdressed Message Processing. - Upon finding a subsequent FL5, a readdressal format is presumed and no further action is taken on format lines 7, 8, 9, or 10.

6.3.7.6 T-ZWL Processing. - During FL7/8 processing the "T ZWL" short title identifiers previously saved during FL4/FL4E validation, are resolved. The "T ZWL" is used to "ZEN" members of a collective in which case delivery by electronic means, is exempted.

6.3.7.6.1 Check 9.1.a. - After validation of the From Line the heading is searched for FL7 and/or FL8.

Error Condition - The prosign "TO" or "INFO" is not contained in the heading.

Error Resolution - The message is rejected to a service position with the error annotation "NO F/L7 or F/L8 FOUND". See Message Error Processing for the appropriate response.

6.3.7.6.2 Check 9.1.b. - A search is made to find the short title in the data base.

Error Condition - The short title is not contained in the Data Base.

Error Resolution - The message is rejected to a service position with the error annotation "SHORT TITLE NOT IN DATA BASE". See Message Error Processing for the appropriate response.

6.3.7.6.3 Check 9.1.c. - Format Line 7 or Format Line 8 contains an RI followed by a slash (/), five spaces and a short title.

Error Condition - The short title line contains an RI but the short title is preceeded with five spaces.

Error Resolution - The message is rejected to a service position with the error annotation "RI/5 BLANKS + SHORT TITLE FOUND". See Message Error Processing for the appropriate response.

6.3.7.6.4 Check 9.1.d. - The short title RI retreived is based upon the message classification for all addees.

Error Condition - The short title RI found in the data base is not cleared to receive this message.

Error Resolution - The message is rejected to a service position with the error annotation "NO CLEARED RI/RI'S FOR THIS SHORT TITLE". See Message Error Processing for the appropriate response.

6.3.7.6.5 Check 9.1.e. - The sideroute/short title combination contained in the message is checked for proper association.

Error Condition - The data base RI does not agree with the siderouted RI; or sideroute characteristics (i.e., OTC, FP, etc.) do not match short title characteristics.

Error Resolution - The message is rejected to a service position with the error annotation "INCORRECT-SIDE ROUTE FOR XXXX...XXX". See Message Error Processing for the appropriate response.

6.3.7.6.6 Check 9.1.f. - The RI indicates a local delivery is required.

Error Condition - The RI is a local RI found in the Data Base, but the destination is invalid.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID LRN IN DATA BASE FOR XXXXXXX". See Message Error Processing for the appropriate response.

6.3.7.6.7 Check 9.1.g. - The short title is a guard command and the Data Base entry is incorrect.

Error Condition - The guard command number for the short title is greater than the maximum, or during processing of a TASK short title the Data Base contained an invalid type.

Error Resolution - The message is rejected to a service position with the error annotation "ROUTFL INCORRECT FOR XXXX...XXX". See Message Error Processing for the appropriate response.

6.3.7.6.8 Check 9.1.h. - The Total number of local addees exceed maximum allowed for processing.

Error Condition - The total number of local (OTC) addees exceeds 500.

Error Resolution - The message is rejected to a service position with the error annotation "TOO MANY OTC ADDEES TO PROCESS". See Message Error Processing for the appropriate response.

6.3.7.6.9 Check 9.1.i. - Total number of RIs generated must remain within the maximum.

Error Condition - The total number of RIs generated exceeded 500.

Error Resolution - The message is rejected to a service position with the error annotation "MORE THAN 500 RIs". See Message Error Processing for the appropriate response.

6.3.7.6.10 Check 9.1.1. - When siderouting a short title, the combined length of the sideroute, short title, and FAS or office codes must not exceed maximum line length.

Error Condition - The line length is exceeded during sideroute insertion.

Error Resolution - The message is rejected to a service position with the error annotation "LINE TOO LONG, ENTER P. OR X.". See Message Error Processing for the appropriate response.

6.3.8 MODIFIED ACP 126 Exempt Address Lines. -

6.3.8.1 Format Line 9 (FL9) Processing. - The first step in FL9, or "XMT" processing as it is referred to is to determine if the prosign "XMT" exists and then validate the short title to be exempted. This is accomplished through a checksum algorithm of the short title and then determing if it is an entry in the Data Base.

If the characteristics of the addee being exempt indicate it is an OTC addressee, then the addressee may be either a guarded or a protect command. In either case, delivery to the command is inhibited and regardless of the short titles's characteristics (i.e., OTC, Non- Local, etc.), RI(s) generated during FL7/8 processing, are eliminated. The short title's RI(s) must be removed so that they will not be present in the "new" FL2 that is to be built. The creation of the "new" FL2 is discussed later in this document.

A special search is done through the FL7/8 generated RIs to detect whether a accounting symbol (FL10) is required in the message. This is done by scanning for a commercial refile RI.

6.3.8.1.1 Check 10.1.a. - After the prosign "XMT" has been identified, the short title following the prosign and that all subsequent short titles are contained within the data base.

Error Condtion - The short title is not contained within the data base.

Error Resolution - The message is rejected to a service position with the error annotation "SHORT TITLE NOT IN DATA BASE". See Message Error Processing for the appropriate response.

6.3.8.1.2 <u>Check 10.1.b</u>. - The short title to be exempted is not a single addee addressee.

<u>Error Condition</u> - A collective short title has been detected on the exempt line.

<u>Error Resolution</u> - The message is rejected to a service position with the error annotation "COLLECTIVE SPECIFIED IN XMT LINE". See Message Error Processing for the appropriate response.

6.3.8.1.3 <u>Check 10.1.c</u>. - The subsequent FL9 has been found but the short title does not follow in the correct position.

<u>Error Condition</u> - The short title is indented 5 or more spaces.

<u>Error Resolution</u> - The message is rejected to a service position with the error annotation "INVALID FORMAT LINE CONTINUATION". See Message Error Processing for the appropriate response.

6.3.8.1.4 <u>Check 10.1.d</u>. - The short title to be exempted is an OTC addressee.

<u>Error Condition</u> - The guard command number for the short title is greater than the maximum allowed.

<u>Error Resolution</u> - The message is rejected to a service position with the error annotation "DATA BASE INCORRECT FOR XXXX...XXX". See Message Error Processing for the appropriate response.

6.3.9 <u>MODIFIED ACP 126 Accounting Lines</u>. -

6.3.9.1 <u>Format Line 10 (FL10) Processing</u>. - FL10 is the identified by the prosign "ACCT" or by a "GR" followed by either "NC" or a number.

<u>Error Condition</u> - None.

<u>Error Resolution</u> - N/A

6.3.10 <u>MODIFIED ACP 126 End of Header Line</u>. -

6 3.10.1 Format Line 11 (FL11) Processing. - Header and heading validation is concluded when the first "BT" is identified. The first "BT" or FL11 separates the heading from the classification and text of the message. If a valid "BT" is found, message validation continues with FL12 processing. If an invalid or no "BT" condition exist, the message is rejected to a service position for the appropriate action.

6.3.10.1.1 Check 12.1.a. - Check for the prosign "BT", indicating FL11.

Error Condition - A "BT" has been found, but the message has no FL7/8.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID BT". See Message Error Processing for the appropriate response.

6.3.10.1.2 Check 12.1.b. - All NAVY originated traffic destined for Commercial Refile must contain a valid FL10.

Error Condition - The message contains a Commercial Refile RI but a valid FL10 was not found.

Error Resolution - Build a FL10 in the form "ACCT NA-CNRF" and insert it into the message prior to FL11.

6.3.11 Modified ACP 126 FL2, FL4, and TARE Line Generation.

6.3.11.1 Build a "NEW" FL2. - FL11 triggers this processing because at this point all addressee processing ceases. The necessary RI(s) have been saved, or eliminated by FL9 and "T ZWL" processing so that all remains that are required RI(s) (up to a maximum of 500). The saved RI(s) are sorted and duplicates removed. Each RI is then interrogated for TRC requirements, and a count kept of the total TRCs so that the number of transmissions may be calculated. The TRC(s) is/are then moved into the proper position in the FL2 security redundancy field. Upon completion of examination, the RI(s) is/are moved into FL2 following the SOR sentinel while keeping track of line maximums. Once the last RI has been processed, an EOR delimiter is moved in place. At this point the RxxxSUU, Modified ACP 126 identifier, is erased.

Additionally, the generated OSRI and SSN which were mentioned under FL2 processing, overlay the original FL2 information. The original message identity is not lost however since all pertinent data has been stored, along with the newly generated data, in a history file.

5.3.11.1.1 Check 12.2.a. - RIXT RIs are not allowed to possess a "Y" or "Z" device character.

Error Condition - A RIXT RI contains the letter "Y" or "Z" as its seventh character.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID 7TH CHARACTER IN RIXT RI". See Message Error Processing for the appropriate response.

5.3.11.2 Format Line 4 Generation. - Using the information stored in the message history file concerning TRCs, SHDs, and message classification, FL4 is rebuilt. Based upon message classification, it is determined whether the prosign "ZNR" or "ZNY" is to be used, then inserted after the EOR delimiter. Depending on the presence or absence of a TRC, a space and three or five classification characters are added. The TRC(s) are moved into place using the last two characters or the FL2 security redundancy field as a guide. Next, any existing SHDs are pulled from the message history file and appended to the newly built FL4, five redundant characters at a time separated by slashs.

Error Condition - None.

Error Resolution - N/A

5.3.11.3 TARE Line Generation. - TARE lines are built using the sorted RI/Short Title identifier table created by the FL2 generator. The short title identifier, saved during FL7 and 8 processing, not only indicates whether a TARE line should be built for this particular entry but also where to find the fully qualified PLA or short title spelling. TARE lines are generated in the forms; Rxxxx T SHORT TITLE or Rxxxxx T SHORT TITLE/SHORT TITLE/... Since a sorted table is used to glean the TARE information, short title identifiers with the same RI will be appended to the same line as long as line length remains within limits.

5.3.11.4 Summary of FL2, FL4, and TARE Line Generation. - The original message at this point has been modified to contain a new OSRI, SSN, FL4, and TARE lines. As mentioned earlier, the RI which identified the message as Modified ACP 126 has been replaced by the proper Routing Indicators. The old FL4, which could not contain TRCs in FL4 processing, may now possess them. All the original "T ZWL" and operating signal lines are retained, and are not overwritten by any generated line.

Error Condition - None.

Error Resolution - N/A

8.3.12 MODIFIED ACP 126 Message Classification Line

6.3.12.1 Format Line 12 (FL12) Processing. - When the first "BT" or FL11 has been identified and processed without error, format line 12 (FL12) is the next line searched for. FL12, or the classification line as it is known, contains the message classification and it must correlate with the security of the message identified in FL2, FL4, and any special handling caveats. If the message is "SPECAT", FL12's security must be CONFIDENTIAL or above. During processing, the security narrative in FL12 is checked against a classification table for a match. Any discrepency results in the message being rejected to a service position.

When "SPECAT" is found in FL12, the message itself must have the appropriate SPECAT Release Code (SRC) in FL4. If it does not, either FL4 or FL12 is in error and the message is rejected to a service postion. When the SRC in FL4 contains the letter "A", then the caveat following "SPECAT" in FL12 must be "SIOP-ESI". All other SPECAT caveats are valid when the SRC "B" is contained in FL4. An error in one of these conditions will result in the message being rejected to a service position.

When "SVC" is found in FL12, message delivery is set for the Service Center.

When "NOFORN" is found in FL12, it indicates that the message is not eligible for foreign delivery. If a foreign RI has already been identified in FL2 processing, then the message is rejected to a service position.

During FL12 processing a search is made for a Navy Standard Subject Identification Code (SSIC). If a SSIC if found (i.e., //N00000//) and further validation determines that a message SSIC is indeed in the line, then the message SSIC is saved for subsequent message distribution processing.

A unique feature of the LDMX is that it allows each site to handle Special Handling Instructions individually. If special handling is identified in FL12, the message will be processed IAW the special instructions.

Following the search for sectional information, a search is made for the word "SUBJ". "SUBJ" is used as to delimit the end of security and special handling information, and to identify the subject line of the message. "SUBJ" is required to be used as a delimiter whether or not a subject is given. FL12 analysis shall persist for 7 lines, or until recognition of other lines that indicate the subject line has been omitted. A reference line (left-justified "A. ") or a paragraph line (left-justified "1. ") found within 7 lines, before finding "SUBJ", shall be considered as evidence that the "SUBJ" line does not exist. In such cases the first physical line shall constitute the bounds of security and special handling information.

For DSSCS/GENSER LDMX sites a phrase search is performed within the confines of the "SUBJ" line or the first 7 lines, starting with FL12. If a Phrase is detected which is associated to the DSSCS community only, then an error condition exists and the message is rejected to a service position.

Sectioning requirements are calculated at this point. Upon initial receipt of the message data and prior to actual validation, the LDMX counted the total number of lines received. It is this count, in combination with the number lines processed from FL5 to FL12; and the number lines which were validated as FL2, FL2 continuations, FL4 and FL4E, that enables sectioning requirements to be calculated. The LDMX also takes into account "mixed" pages, those pages containing heading and text data.

Once the total number of sections has been determined, the number is saved in the message history file, and is used to indicate when sectioning is required and finished. A section line will be inserted following the message classification in the form: SECTION XX OF YY, where XX equals current section and YY always represents total sections.

Now that sectioning requirements have been established, the counts mentioned will key when the first and subsequent sections are complete. When the counts indicate that a section is complete, a check is made to ensure that the EOM sequence of the original message is not going to be the only data in the remaining section. If that is not the case, an EOM sequence is generated at that point, and the subsequent section heading built. The new heading is basically copied from the modified original message, starting with FL2 and ending with the "SUBJ" delimiter, if one existed. The new FL2 will be changed to include a new SSN.

All line counts will now reflect total lines processed thus far in the new heading, and line validation resumes where it had left off in TEXT processing.

There are five full textual pages in a section. The mixed page is not used to compute pages/section. A new section starts after the mixed page and 5 pages of text.

Paging requirements and validations will be discussed here under FL12 processing only for convenience, since page lines may also exist in the heading of a message.

The LDMX must also keep track of the number of lines processed from FL5 to the end of the message since paging is required every 20 lines, begining with FL5. A page line is built every 20th line and will contain all of the appropriate information as set down in the JANAP 128 publication.

In addition to building page lines, existing page lines are also identified and stripped from the original message

6.3.12.1.1 Check 13.1.a. - The security narrative is checked against the message security classification.

Error Condition - The FL12 classification does not match FL2; an illegal condition exists (i.e., special handling instructions in a SPECAT message); or SPECAT was indicated in FL4 and not found in FL12.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID SECURITY CLASSIFICATION". See Message Error Processing for the appropriate response.

6.3.12.1.2 Check 13.1.b. - A check is made to see if the message is eligible for foreign delivery.

Error Condition - "NOFORN" was found in FL12, and TRCs are present in FL4.

Error Resolution - The message is rejected to a service position with the error annotation "NOFORN MSG ROUTED TO NON-US RI". See Message Error Processing for the appropriate response.

6.3.12.1.3 Check 13.1.c. - If a DSSCS/GENSER LDMX, a check is made for possible security violations between communities.

Error Condition - A DSSCS phrase has been detected in a GENSER message during FL12 processing.

Error Resolution - The message is rejected to a service position with the error annotation "SI-ONLY PHRASE FOUND IN GENSER MSG". See Message Error Processing for the appropriate response.

6.3.13 MODIFIED ACP 126 End of Message (EOM) Lines. -

6.3.13.1 Format Lines 13/15/16 (FL13/15/16) Processing. - When FL12 processing is complete, the remaining message body is treated as message text until the second "BT" or FL13 is found. When "BT" is found, EOM validation occurs. A check is made to determine the number of lines remaining in the message. If more than 2 lines remain, then an error is assumed and the message is rejected to a service position. If the "BT" appears to be in the proper location, then FL15 is validated. FL15 begins with the "#" sign, and if it is not present an error is assumed and the message is rejected to a service position. If the "#" sign is present, then the SSN in FL15 is validated to be numeric and match the FL2 SSN of the original message. Straggler validation checks must be done using the original message data and not the data generated by Modified ACP 126 processing. In the case of a valid FL15, the SSN generated during FL2 processing or section processing replaces the original SSN. Now the Modified FL2 SSN matches the EOM SSN. After,FL15 validation, the last line in the message is the 4 "N"s. Once again if the exact match is not found an error is assumed and the message is rejected to a service position.

After EOM validation the message is considered processed and placed in the appropriate transmission queues "FIFO" by precednece for delivery.

6.3.13.1.1 Check 14.1.a. - Check the message for a second "BT" (EOM indicator).

Error Condition - There are only 2 lines of data left in the message and the second "BT" has not been found.

Error Resolution - The message is rejected to a service position with the error annotation "NO BT F/L 13". See Message Error Processing for the appropriate response.

6.3.13.1.2 Check 14.1.b. - The second "BT" has been found, and the next line must be FL15.

Error Condition - The "#" sign is missing or the 4 digits following the "#" sign are not numeric.

Error Resolution - The message is rejected to a service position with the error annotation "INVALID F/L 15". See Message Error Processing for the appropriate response.

6.3.13.1.3 Check 14.1.c. - FL15 is present and the last line must contain only the characters "NNNN".

Error Condition - The line following FL15 does not contain exactly "NNNN".

Error Resolution - The message is rejected to a service position with the error annotation "INVALID F/L 16". See Message Error Processing for the appropriate response.

6.4.0 AUTOMATIC SERVICE COMPOSITION "SCC" PROCESSING.

6.41 General Comments. -

6.4.1.1 (Fleet Router Processing?) "SCC" processing is invoked when the RI, "RxxxSCC" is contained in FL2 and should be considered as a continuation of JANAP 128 message processing. "RxxxSCC" is defined as an RI that the LDMX recognizes as one for which it has accepted delivery responsibility. As already mentioned, FL4/7/8 saved each short title identifier that required rerouting. OTC short titles did not qualify as requiring retransmission since they may be delivered locally.

Upon validating FL16 of a JANAP 128 message, the ZOV pilot generation begins. This involves making an entirely new message by copying and modifying the original message. "SCC" processing will:

1. Change LMF1 to LDMX input LMF of "T".

2. Change the CIC to "ZOVW" if the original CIC was "ZYUW" otherwise no change is made.

3. Change the OSRI to reflect the LDMX service center RI.

4. Change the TOF to reflect time of ZOV pilot generation.

5. Replace the existing FL2 RIs with the RIs of the short titles that are being Rerouted.

6. Assign TRCs where applicable.

7. Strip off any existing FL3 through FL4/E since these lines are to be rebuilt.

8. Add to FL4 the "ZOV" opsig followed by the LDMX service center RI and generated SSN, the words "Reroute OF" and the OSRI, SSN, and TOF that appeared in the original message FL2 or FL3.

9. TARE instructions identifying the short titles requiring Reroute are added. The RIs for these short titles are retrieved from the data base using the message classification as the criterion.

6.4.2 Validation/Verification Requirements. -

6.42.1 Most errors encountered while creating the ZOV message will only terminate the ZOV message and never the original message. Detected errors are annotated with the appropriate error notice and forwarded to the Service Center.

6 4,2.1.1 Check 1.1.a. - In order to persue ZOV pilot generation, the original message history file must contain valid format lines 2, 3 (when required), 5, and 16.

Error Condition - When scanning the original message's history file for a valid FL2, an invalid pilot FL2 was found or a valid FL2 was not found.

Error Resolution - The ZOV message is not built and a copy of the original message is dropped to a service position with the annotation "AUTOMATIC ZOV WILL NOT BE PERFORMED - NO FL2 FOUND IN THE ORIGINAL MESSAGE". The message requiring the ZOV must be manually Rerouted.

Error Condition - The original FL2 was found and the LMF indicated that the message should contain a FL3. The search for a valid FL3 was unsuccessful.

Error Resolution - The ZOV message is not built and a copy of the original message is dropped to a service position with the annotation "AUTOMATIC ZOV WILL NOT BE PERFORMED - NO FL3 FOUND IN THE ORIGINAL MESSAGE". The message requiring the ZOV must be manually Rerouted.

Error Condition - In the process of trying to append the rest of the original message to the newly created ZOV pilot lines, a valid FL5 could not be found.

Error Resolution - The ZOV message is not built and a copy of the original message is dropped to a service position with the annotation "AUTOMATIC ZOV WILL NOT BE PERFORMED - NO FL5 FOUND IN THE ORIGINAL MESSAGE". The message requring the ZOV must be manually Rerouted.

6 42.1.2 Check 1.1.b. - Before a proper ZOV pilot can be built, "SCC" processing must produce all the correct routing assignments and TARE lines.

Error Condition - During the retrieval of "cleared" RI(s) for a short title requiring Reroute, no "cleared" RI(s) could be found.

Error Resolution - Processing continues however an error notice is appended to the ZOV message. The error notice is: "NO CLEARED RIs FOR XXX...XXX". The error will be displayed at a service position upon the completion of "SCC" processing.

Error Condition - During the creation of the ZOV pilot, it is discovered that there were no RIs generated.

Error Resolution - The ZOV message is not built and a copy of the original message is dropped to a service position with the annotation "AUTOMATIC ZOV WILL NOT BE PERFORMED - NO VALID RIs COULD BE FOUND FOR ANY OF THOSE SHORT TITLES REQUIRING Reroute". The message requring the ZOV must be manually Reroute.

Error Condition - While trying to retrieve the proper routing assignments, an alternate spelling of a short title was encountered and there was no "preferred" spelling (merchant ships).

Error Resolution - "SCC" processing continues to completion however the generated ZOV message is delivered to a service position only, with the annotation "SUPPLY CORRECT SPELLING FOR MERCHANT SHIPS". Again, the original message is delivered to its assigned routing and will not be impacted.

6.5.0 REMOTE ENTRY RECALL/RETRANSMISSION.

6.5 1 General Comments. -

6.5 1.1 This section deals with the LDMXs capability to process preformatted automatic recall or retransmission request, hereafter referred to as "SRR" processing.

"SRR" processing allows remote subscribers, such as the Remote Information Exchange Terminals (RIXT) to retrieve messages from the LDMX online storage files which were addressed to the terminal or a subscriber served by that terminal. "SRR" request may also be entered from an interactive VDT at the LDMX.

6.5. 2 Validation/Verification Requirements. -

6.5 2.1 Format Line 1 - Transmission Identifier Line. - Since the interface between the RIXT terminals employ their own protocol, called the "LDMX IXS/RIXT Protocol", no formal validation of TI information is performed. If the RIXT control block contains a CD-CSN, it will be used to update the LDMX local tables, otherwise, the LDMX CSN will be updated with the next message sequence expected. In either case, no error conditions are noted for TI line processing.

6.5 3 "SRR" Message Format. - For NAVY LDMX validation/verification purposes, the "SRR" format is divided into three parts: Header data including the Routing Indicator (RI) field (Format Line 2); Recall parameters; and the End of Message (EOM) line.

6.5 3.1 "SRR" Format Line 2 Processing. - Format line 2 (FL2) of a recall request is formatted identically to that of a JANAP 128 message. The RI is unique to the LDMX, in that it contains the local LDMX NARC (i.e., Rxxx) and the derivative "SRR", thus the only RI contained in FL2 is "RxxxSRR".

Since the same basic FL2 checks made on a JANAP message are made for a "SRR" message they will not be discussed here in detail. The exceptions will be discussed, but not at the level of ERROR CONDITION/ERROR RESOLUTION.

When an error in FL2 is encountered, an abbreviated plaindress service message is generated back to the originator (i.e., RIXT input device) identifying the message in error and the reason for rejection. A copy of the "SRR" request and the reason for rejection is also delivered to the Service Center.

If no FL2 errors are detected prior to the RI field, and the RI field contains the RI "RxxxSRR" followed by the End of Routing (EOR) character, the remainder of the message is processed·as a recall/retransmission request.

6.5.3.2. Recall/Retransmission Parameter(s). - After the ECR has been identified the next line to be validated is the recall parameters. Various parameters range from: PSNA. XXXXXX (XXXXXX = 6 DIGIT PSN), ODTG. SHORT TITLE//010001Z JAN 83, OSRI. Rxxxxxx0001 0010001, etc. The recall parameter and arguments are checked against an allowable recall table and if the recall parameter is valid, the request is processed and the message that was requested is retransmitted with a "ZDK" header. The header includes the "ZUI" information necessary for the originator to reference the recall request.

If the parameter or it arguments(s) is in error the message is rejected to the Service Center with the appropriate annotation and an Automatic service message is sent to the originator with the reason for rejection. The originator at this point, would correct the recall request and resubmit to the LDMX.

RIXT terminals have the capability to retrieve data base information for their particular command. This is also accomplished through "SRR" processing. For example, if a RIXT terminal wished to obtain LDMX guide file information for guard command one, the recall parameter would be "GUID. SHORT TITLE//CMD NR". The LDMX would validate the request and that ensure the RIXT terminal is associated to the guard command which requested the information.

For readdressal processing, the RIXT terminal passes a new header, which after all validation is complete, will precede the header(s) on the original message. In all cases, if errors occur during parameter validation, the originator is informed of the error and the message is rejected to the Service Center.

6.5.3.3 End-of-Message (EOM) Line. - After the recall parameter line has been validated the last line in the recall request is the EOM. The EOM line will contain 4 "N"s, and no other data. Unlike JANAP processing, a FL13 and FL15 are not required. If the 4 "N"s are not found or data other than the 4 "N"s is detected, the recall request is in error and the originator is so informed.

7.0

DOI 103 Format Message Processing Requirements.

7.1. General Comments.

7.1.1. This section will detail the existing AUTODIN processing as it applies to DOI 103 message formats utilized by most of the DSSCS community subscribers. As with the JANAP 128 and ACP 127 message formats processing requirements, these checks and validations must be carried forward in the I-S/A AMPE program to ensure that the message integrity currently provided is maintained.

7.2. Validation Requirements

7.2.1. Format Line 1 - Transmission Identifier (TI) Line. I-S/A AMPE validation of the TI line is identical for both asynchronous (Mode II and V teletypewriter terminals whose use of a TI line is mandatory) and synchronous (Mode I users who employ line block framing and whose use of a TI line is optional but must be specified at the time the I-S/A AMPE sets the port/channel parameters) channels. All TI lines through the CD-CSN fields are processed as follows:

7.2.1.1. The first characters of the TI line block must be a Start of Header (SOH) and a select (SEL) character. If the channel is asynchronous, these have been inserted by the I-S/A AMPE; if the channel is synchronous, the terminal has inserted them.

7.2.1.2. Check 1.1.a. The first data character of the TI line must be the letter "C". (If the channel is asynchronous, the "ZCZ" portion of the Start of Message Sequence (SOMS) was previously validated and then discarded by the I-S/A AMPE.)

Error Condition - None - nothing can be recognized prior to receipt of the SOH.

Error Resolution - N/A

7.2.1.3. Check 1.1.b. The second, third and fourth characters of the TI line must be the Channel Designator (CD) and must match the CD stored at the I-S/A AMPE for that port/channel.

Error Condition - A CD is considered to be in error if it does not match the CD stored in the I-S/A AMPE for its' associated channel.

Error Resolution - All DOI 103 formatted messages having CD errors will be rejected and an "INVALID CD" service message automatically generated to the input port/channel. (CRITIC format is unique and not considered DOI 103 format for the purpose of these checks.)

7.2.1.4. Check 1.1.c. The fifth character of the TI line can be either a figures shift or the first character of the CSN field; the figures shift must be present for "A" Select (ITA 2) messages and may or may not be present for other selects. Note that for all processing purposes, "A" Select CSN's are always assumed to begin in the sixth position of the TI line. This is done so that the "CSN" to be quoted back to the terminal in a service message will be positionally correct even if the figure shift is garbled, leaving the CSN field in the lower case. If the CSN is correct, TI line processing is complete at this point.

Error Condition - A CSN is considered to be in error if it is either non-numeric or if it is not the next expected CSN (i.e., one greater than the last accepted from a Mode V port/channel or received from a Mode I or II port/channel. For this purpose, a CSN of 000 is considered to be one greater than 999.

Error Resolution - Messages of CRITIC precedence will be accepted regardless of CSN errors detected. Other messages having CSN errors will be processed as follows:

If the CSN is a duplicate of the last accepted (Mode V) or received (Mode I/II), the message will be rejected to the input port/channel. This is the only instance of CSN error where a message will be rejected by the I-S/A AMPE which will automatically generate an "INVALID CSN" message to the input port/channel and log the error condition on an error file for future compilations (possibly similar to the existing Communications Improvement Memorandum (CIM) program.

If the CSN is incorrect for any other reason including being non-numeric, the message will be accepted. However, these errors shall cause the I-S/A AMPE to automatically generate a service message to the input port/channel citing the CD and CSN as well as other pertinent message identification data. This service message will indicate "INVALID CD", "INVALID CSN" and whether the message was accepted or rejected. A duplicate CSN will cause generation of an additional service message, "DUPE CSN". Missing CSNs will cause automatic generation of an open number (ZFX) service to the input port/channel.

7.2.1.5. Further I-S/A AMPE TI Line processing. In order to maintain CSN continuity between the I-S/A AMPE and the terminal, the I-S/A AMPE's tables are updated based on the results of CSN and message processing. When a CSN is rejected (i.e., duplicate condition), no CSN updating is performed.

When a CSN is accepted, even if it is out of sequence, the accepted CSN (or the expected CSN, if the received CSN is non-numeric) is made the last accepted CSN for processing of future messages. When the channel is Mode I or Mode II this update is done immediately on receipt of the TI line whether the associated message is accepted or not, since the Mode I or Mode II terminal is assumed to update the CSN at the beginning of each message transmission. This is also consistent with a terminal transmitting a tape in which there are pre-cut CSN's preceding each message. Since Mode V procedures require that CSN's be updated on acceptance of the message, Mode V terminal equipment does not update its TI generator until the associated message has been acknowledged by the I-S/A AMPE. Consequently, the I-S/A AMPE also does not update the last accepted CSN on a Mode V channel until the message has been validated and accepted, and the ACK for the message has been sent to the terminal.

7.3. Format Line 2 - Message Header. For I-S/A AMPE validation purposes, the DOI formatted header is divided into three parts: Header data up to and including the Start-of-Routing Sequence (Format Line 2); the Routing Indicator Field (still a part of Format Line 2); and the Security Line (Format Line 4).

7.3.1. Header Validation/Verification Through the Start-of-Routing.

7.3.1.1. Precedence Field. The first header field to be validated is the precedence field. It should be noted that even though the TI line is the first data received from the port/channel, it is not the first message area to be processed. The precedence field is processed first since the precedence of the message affects the decision on whether to accept a TI line with errored fields.

7.3.1.1.1. Check 2.1.a. Precedence is a single character, the first character of the header and is validated to be one of four characters:

"Z" - Flash
"O" - Immediate

"P" - Priority
"R" - Routine

Error Condition - If the field is not one of the four precedence characters specified above.

Error Resolution - An error in the precedence field of either an invalid or an unauthorized character results in message rejection on all except Mode II channels where the invalid precedence character is replaced by an "O" (immediate) and the message processed at that precedence level. Errors in the precedence field which cause rejection result in the automatic generation of an "INVALID HEADER" error condition to the input port/channel.

7.3.1.2. Language Media Format (LMF). The next field to be validated in a DOI formatted message is the Language and Media Format (LMF) field. This is a two character field in which the first character (LMF1) indicates the medium in which the input message was originally prepared. It is sometimes also called the Input LMF or ILMF. The ILMF must be consistent with the select character (SEL). The second character (LMF2) indicates the medium in which the originator prefers the message to be delivered to the addressee. It is sometimes also referred to as the Output LMF (OLMF) or Preferred Output LMF (POLMF). Input header processing merely validates the SEL/LMF combination. Further use of the LMF in input processing and in output message delivery will be discussed later.

7.3.1.2.1. Check 2.2.a. In the I-S/A AMPE, the LMF pair will never be validated separately. LMF Validation is always combined with validation of the SEL, and the three characters are validated together. If the message is from a TI user, the SEL is obtained from the second framing character of the TI line block. Otherwise, it is the second framing character of the header line block. Once the SEL-LMF combination passes validation, the LMF pair information is saved for RI processing, which must determine whether a message of the specified LMF can be delivered to a given RI.

Error Condition - If the SEL/LMF combination does not match any I-S/A AMPE table entry, the SEL is validated separately.

Error Resolution - If the SEL is invalid, the message is rejected and a "REPROTECT TO ALL ADDRESSEES" service message is automatically generated to the input port/channel.

If the message is high-precedence (Cat I) and not magnetic tape, the LMF field is corrected to make the invalid LMF(s) the most common ones for that SEL ("T" for "A" Select, "A" for "H" Select, "C" for "D" Select). If LMF1 is valid and is "H", "E", or "R", an invalid LMF2 is made "C", "A", or "T" respectively.

When the SEL is valid, but one of the LMF characters is invalid, a test is made of the message precedence and of the SEL. If the message has a SEL of "B" or "C" (magnetic tape), or is of low precedence, it is rejected, with an "INVALID HEADER" service message being automatically generated.

7.3.1.3. Single Security Character Field. The next field to be validated is the single character security field which must be the character "M" for DOI formatted messages.

7.3.1.3.1. Check 2.3.a. The single character is checked to be an "M".

Error Condition - Dectection of a character other than "M".

Error Resolution - The message is rejected and an "INVALID SECURITY FIELD - SEC" serivce message is automatically generated to the input port/channel.

7.3.1.4. Content Indicator Code (CIC) Field. The four character CIC field (also called the Communications Action Identifier field when it contains communications instructions) contains information related to the type of message being processed. See Appendix 19A for specific additional codes and required action.

7.3.1.4.1. Check 2.4.a. If the message has a SEL of "A", indicating preparation in ITA2 paper tape, and the CIC contains a numeric character in the fourth character position, the appropriate shift characters must precede (SO/FIGS) and immediately follow (SI/LTRS) that character.

Error Condition - Absence of the necessary shifts indicates that the message preparation medium does not conform to the select character

Error Resolution - The message is rejected and an "INVALID HEADER" service message is automatically generated to the input port/channel.

7.3.1.4.2. Check 2.4.b. The CIC is validated to be four alphabetic characters or three alphabetic and one numeric character.

Error Condition - Any non-alphabetic character in any of the first three character positions.

Error Resolution - The message is rejected and an "INVALID HEADER" service message is automatically generated to the input port/channel.

7.3.1.5. Separator. The character following the CIC field must be a space (teletypewriter space, card no punch).

7.3.1.5.1. Check 2.5.a. Check the character following the CIC field.

Error Condition - Any character other than a space character.

Error Resolution - The message is rejected and an "INVALID HEADER" service message is automatically generated to the input port/channel.

7.3.1.6. Originating Station Routing Indicator (OSRI) Field. Following the separator is the seven character OSRI field. This may be a seven character RI or a six character RI and a space.

7.3.1.6.1. Check 2.6.a. The OSRI must be a valid RI and generally is validated in the same manner as a destination RI, i.e., all characters must be alphabetic; the relay portion of the RI (first four characters) must be valid; if the relay portion is the local I-S/A AMPE, the next two characters are checked for validity and the seventh character is verified to be either an alphabetic character, a space, or a shift out (figures) character.

Error Condition - The OSRI is invalid or, if a six letter OSRI is used, a space character or shift out (figures) is not used in the seventh position.

Error Resolution - Any error in the OSRI field results in message rejection and an "INVALID HEADER" service message being automatically generated to the input port/channel.

7.3.1.7. Originating Station Serial Number (OSSN) Field. Following the OSRI is the four-character OSSN field. After the alphabetic OSRI, an upshift (SO/FIGS) is required on "A" select messages No upshift is allowed with other selects. The OSSN is validated to be four numeric characters, and messages which fail this check are rejected for "INVALID HEADER". A valid OSSN is saved for later comparison with the Trailer Station Serial Number (TSSN) at the end of the message to ensure that a "straggler" condition does not exist. Straggler checking is described in detail under End of Message validation.

7.3.1.7.1. Check 2.7.a. Check "A" SEL messages for an upshift (SO/FIGS) after the alphabetic OSRI or space character. If a six letter OSRI is used, the next two characters are interchangeable - either a space and a shift out character, or a shift out character and a space.

Error Conditions - If an upshift (SO/FIGS) is not present on "A" select messages or if an upshift is present on any other type of message.

Error Resolution - The message is rejected and an "INVALID HEADER" service message is generated to the input port/channel.

7.3.1.7.2. Check 2.7.b. The OSSN shall be validated to be four numeric characters.

Error Condition - The OSSN is not four numeric characters.

Error Resolution - The message is rejected and an "INVALID HEADER" service message automatically generated to the input port/channel.

7.3.1.8. Separator. A space character separator (teletypewriter space, card no punch) must be present following the OSSN.

7.3.1.8.1. Check 2.8.a. Check for space character.

Error Condition - No space character following the OSSN.

Error Resolution - An error in the separator field results in message rejection and an "INVALID HEADER" service message being automatically generated to the input port/channel.

7.3.1.9. Time-of-File (TOF) Field. Validation of the TOF field is the same as that for the OSSN field except that a seven-character field is involved rather than a four. Procedurally, the TOF field is composed of a three character Julian date (001-365/366) and time (0000-2359) but no range tests need be made (e.g., 4567890 is acceptable as a TOF field).

7.3.1.9.1. Check 2.9.a. Check for seven numeric characters.

Error Condition - Any non-numeric character in any of the seven character positions of this field.

Error Resolution - The message will be rejected and an "INVALID HEADER" service message automatically generated to the input port/channel.

NOTE: The next two fields, 7.3.1.10, and 7.3.1.11 pertain to data pattern messages.

7.3.1.10. Separator. If the message is data pattern this paragraph applies and a space character (no punch) separator must be present following the TOF field. Use of a space separator in this field on non-data pattern messages will result in the message being rejected and an "INVALID HEADER" service message being automatically generated to the input port/channel.

7.3.1.10.1. Check 2.10.a. Check for space character.

Error Condition - Any character other than a space following the TOF field.

Error Resolution - The message is rejected and an "INVALID HEADER" service message is automatically generated to the input port/channel.

7.3.1.11. Record Count Field. If the message is data pattern, this paragraph applies. This field must be a four character Record

Count Field. There are no exceptions. The record count is intended as a further safeguard against lost data. The Record Count field may consist of the letters MTMS, the letters PLTS, or a four digit number in the range 0003-0500. No other characters are permitted in a message received from a terminal. If the field is numeric, it must be a count of the actual number of records (cards or line blocks) in the message, including the header and trailer. Since this field does not appear in a single card (LMF of SC) message (not valid in the DSSCS community), and a record count of two would indicate only a header and trailer, the minimum acceptable record count is 0003. The maximum record count which may be specified in this field is 0500. A Record Count field of MTMS indicates either that the message originator wishes to forego a record count check (MTMS also in trailer) or that the true record count will appear in the trailer card. Messages with a Record Count Field containing MTMS in both header and trailer or containing PLTS in the header may exceed the 500 line block limit, up to a maximum of 556 line blocks (see End-of-Message Processing, Data Pattern). The record count field is saved for later comparison with the record count field in the trailer card to ensure that the record count is correct. This is also described in detail under End-of-Message processing. Use of the Record Count field on non-data pattern messages will result in the message being rejected and an "INVALID HEADER" service message being generated to the input port/channel.

7.3.1.11.1. Check 2.11.a. If the field is numeric, the value of the field is checked.

Error Condition - A Record Count Field value which is less than 0003 or higher than 0500.

Error Resolution - The message is rejected and an "INVALID RECORD COUNT" service message automatically generated to the input port/channel.

7.3.1.11.2. Check 2.11.b. A Record Count field containing the letters PLTS or MTMS.

Error Condition - Any alphabetic characters other than PLTS or MTMS in this field.

Error Resolution - The message is rejected and an "INVALID RECORD COUNT" service is generated to the input port/channel.

7.3.1.12. Security Redundancy Field Sentinel. Following the record count field if the message is data pattern or following the TOF field if it is teletypewriter, must be the dash or hyphen (ITA2 uppercase "A", card "11" punch) signalling the start of the Security Redundancy field.

7.3.1.12.1. Check 2.12.a. Check for security sentinel.

Error Condition - Any character other than the dash.

Error Resolution - The message is rejected and an "INVALID HEADER" service message is automatically generated to the input port/channel.

7.3.1.13. Security Redundancy Field. When the message is "A" SEL teletypewriter, the character following the dash must be a downshift (SI/LTRS). Since there is no record count field in this format, the upper case of the TOF field is continued through the dash, then the lower case is required for the security field. This field must begin with the letter "M" and be followed by a valid transmission control code which consists of three alphabetic characters. The last three characters will be used later to check against each routing indicator and also against the equivalent field in Format Line Four.

7.3.1.13.1. Check 2.13.a. For "A" select message, check for downshift character.

Error Condition - Absence of the downshift.

Error Resolution - The message is rejected, without exception, and an "INVALID HEADER" service message is automatically generated to the input port/channel.

7.3.1.13.2. Check 2.13.b. Validate that the first character in this field is the letter "M".

Error Condition - Any character other than the letter "M".

Error Resolution - The message is rejected and an "INVALID SECURITY FIELD - SEC" service message automatically generated to the input port/channel.

7.3.1.13.3. Check 2.13.c. The last three characters of the Security Redundancy field are checked to see if they constitute a valid TCC.

Error Condition - The three characters fail the validation check (not a valid TCC).

Error Resolution - The message is rejected and an "INVALID SECURITY FIELD - TCC" service message automatically generated to the input port/channel.

7.3.1.14. Start of Routing (SOR) Field. Header validation then proceeds to the SOR field. If the message is "A" select this is a four character field, upshift (SO/FIGS), dash, dash, downshift (SI/LTRS). If other than "A" select, the field is the two-character field, dash dash.

Error Condition - Any error in this field, or detection of this field beyond the fifty-fifth character position of the header.

Error Resolution - The message is rejected and an "INVALID HEADER" service message automatically generated to the input port/channel.

7 .3.2. Header Validation/Verification of the Routing Indicator (RI) Field.

.3.2.1. Routing Indicator (RI) Field. The RI is the "address" of a message. In teletypewriter messages this first character must immediately follow the SOR field. In teletypewriter messages ("A" or "H" SEL) with more than one RI, each successive RI must be separated by either one space or by a valid End-of-Line (EOL) sequence consisting of two carriage return (CR) functions and one line feed (LF) function. An RI may not be split by either spaces or by an EOL sequence in any instance (teletypewriter, card, or data pattern messge). For multiple card and data pattern messages, spaces (no card punch) are allowed between the SOR and the first character of the first RI, between RIs, between the last RI in a line block (card) and the end-of-line block, and between the last RI and the End of Routing (EOR) sentinnel.

7.3.2.1.1. Check 3.1.a. If "A" or "H" select, first character must immediately follows the SOR field.

Error Condition - First character not found immediately following the start-of-routing field.

Error Resolution - The message is rejected and an "INVALID ROUTING FIELD" service message automatically generated to the input port/channel.

7.3.2.1.2. Check 3.1.b. No RI may exceed seven characters.

Error Condition - A routing indicator contains eight or more characters.

Error Resolution - The message is rejected and an "INVALID ROUTING FIELD" service message automatically generated to the input port/channel. No deliveries are made and there are no exceptions.

7.3.2.1.3. Check 3.1.c. No presence of shift characters or "lettering out" (except for the single upshift necessary before the EOR in an "A" select message).

Error Condition - Shift-in/shift-out function separating routing indicators.

Error Resolution - The message is rejected and an "INVALID ROUTING FIELD" service message automatically generated to the input port/channel. No deliveries are made and there are no exceptions.

7.3.2.1.4. Check 3.1.d. Presence of non-alphabetic or non-separator characters in this field.

Error Condition - Detection on a numeric character in this field.

Error Resolution - The message is rejected and an "INVALID ROUTING FIELD" service message automatically generated to the input port/channel. No deliveries are made and there are no exceptions.

7.3.2.1.5. Check 3.1.e. Mixture of GENSER and DSSCS community RIs on a Y or R/Y channel.

Error Condition - Any mixed "R" and "Y" routing indicators in this field on a Y or R/Y channel.

Error Resolution - The message is rejected and an "INVALID ROUTING FIELD" service message automatically generated to the input port/channel. No deliveries are made and there are no exceptions.

7.3.2.1.6. Check 3.1.f. Check for more than 500 RIs in this ıield.

Error Condition - 501 or more RIs in this field.

Error Resolution - The message is rejected and an "EXCESSIVE ROUTING FIELD" service message automatically generated to the input port/channel. No deliveries are made and there are no exceptions.

7.3.2.1.7. Check 3.1.g. An RI may not be split by an end-of-line (EOL) sequence.

Error Condition - A routing indicator is split by a valid EOL (2 CR, 1 LF).

Error Resolution - The message is rejected and an "INVALID ROUTING FIELD" service message automatically generated to the input port/channel. No deliveries are made and there are no exceptions.

7.3.2.1.8. Check 3.1.h. For "A" or "H" SEL, each successive RI must be separated by one (and only one) space or by a valid EOL (2 CR, 1LF) sequence.

Error Condition - Any character other than a single space character or a valid EOL (2CR, 1LF) sequence.

Error Resolution - The message is rejected and a "INVALID ROUTING FIELD" service message automatically generated to the input port/channel. No deliveries are made and there are no exceptions.

7.3.2.2. End-of-Routing Field. The DOI format end-of-routing (EOR) consists of either the three character field upshift (SO/FIGS), period (.), downshift (SI/LTRS) for "A" select messages or the one character field of period (.) for other selects. For "A" and "H" select, the period must be immediately followed by a valid end-of-line (EOL) sequence (2 CR, 1 LF). For card format messages ("D" select), the remainder of the card following the EOR must be blank. Any characters between a card EOR and the end of the card will cause message rejection. For magnetic tape messages ("B" or "C" select) an end-of-medium (EM) character may be used immediately following the EOR. The EM character in any other position will cause message rejection.

7.3.2.2.1. Check 3.2.a. Validate that there is a valid EOR.

Error Condition - Field contains other than the three valid characters for an "A" select, or contains an invalid EOR sentinnel.

Error Resolution - The message is rejected and an "INVALID HEADER" service message automatically generated to the input port/channel.

7.3.2.2.2. Check 3.2.b. "D" select multiple card message must not have extraneous characters between EOR and end of the card.

Error Condition - Any punch falling between the EOR and the end of the card (Col 80).

Error Resolution - The message is rejected and an "INVALID HEADER" service message automatically generated to the input port/channel.

7.3.2.2.3. Check 3.2.c. Insure EM character, if used in a "B" or "C" select, is immediately following the EOR. If not used, the remainder of the line block must be spaced filled.

Error Condition - EM character does not immediately follow the EOR sentinnel.

Error Resolution - The message is rejected and an "INVALID HEADER" service message automatically generated service to the input port/channel.

7.3.3. Header Validation/Verification of the Security Line.

7.3.3.1. Security Line (FL4). Following the EOR, the next field to be validated/verified on all teletypewriter ("A" or "H" SEL) messages is the security line, format line four. For all messages, the first four characters following the EOR (original header on piloted card messages) must be the operating signal "ZNY" followed by a space. When it has been determined that FL4 has been properly employed and the first four characters are valid, the next check to to find the characters "MM" followed by a valid TCC. No characters beyond the TCC are examined by the I-S/A AMPE for validation purposes.

7.3.3.1.1. Check 4.3.a. All messages are checked for the operating signal "ZNY", a space character, and the double "M" followed immediately by a three character transmission control code.

Error Condition - Any extraneuous character other than "ZNY" followed immediately by the space character in the first four character positions of the security line.

Error Resolution - The message is rejected and an "INVALID SECURITY FIELD - REJ" service message is automatically generated to the input port/channel.

7.3.3.1.2. Check 4.3.b. All messages are checked for the double "M" in positions five and six of the security line.

Error Condition - Any extraneous character other than "MM" in the double "M" field (character positions six and seven of the security line).

Error Resolution - The message will be rejected and an "INVALID SECURITY FIELD - SEC" service message automatically generated to the input port/channel.

7.3.3.1.3. Check 4.3.b. The next three characters are checked to be a valid TCC.

Error Condition - The TCC characters are not valid.

Error Resolution - The message will be rejected and an "INVALID SECURITY FIELD - TCC" service message automatically generated to the input port/channel.

Note: ALPS processing in DOI formatted messages indicated by the first letter of the TCC being a "Z". When this is the case and the TCC is valid, special processing is entered so that no message data will be written to the I-S/A AMPE history record past the TCC.

7.3.4. Routing Indicator Processing.

73.4.1. General. After processing of FL4 has concluded satisfactorily, Routing Indicator (RI) processing begins. If a message contains only one RI, and that RI is invalid, the message will be rejected. If a message is input on a Y or an R/Y channel and contains a mixture of R and Y RIs, the message will be rejected regardless of RI validity.

7.3.4.2. Check 5.1.a. The initial RI validation is to determine whether the RI is in the I-S/A AMPE's RI tables. All AUTODIN RIs are not included in every I-S/A AMPE's RI tables. Each I-S/A AMPE's RI tables contain all directly connected tributaries' RIs, all other I-S/A AMPEs' RIs, and all Non Automatic Relay Centers' (NARCs) RIs. A DSSCS RI may be from 4 to 7 characters but must contain 6 or 7 characters if addressed to an I-S/A AMPE tributary. If the RI is a local I-S/A AMPE tributary, the first six characters are checked for validity and determination of delivery destination, the seventh ignored. If the RI is a distant I-S/A AMPE tributary or a NARC, local or remote, only the first four characters are scanned for validity and determination of delivery destination. If, during the transition period, the first four characters indicate a collective RI (YHCR), the last two characters determine the actual collective list for delivery destinations.

Error Condition - A routing indicator is not found in the RI tables.

Error Resolution - If the message contains only one RI or no valid RIs, it will be rejected and an "INVALID ROUTING REPROTECT TO" service message will be automatically generated to the originating station. If received from another I-S/A AMPE, the message is "dumped and acked" (no message rejection instituted) but the service message is still generated to advise the originating station of the required reprotection. If the message contains at least one valid RI, it will be accepted and processed for delivery to the valid RI. An "INVALID ROUTING REPROTECT TO" service message will be automatically generated to the originating station advising of the invalid RI(s) requiring reprotection.

7.3.4.2.1. Check 5.1.b. Once the RI is found in the RI tables, the message TCC is checked against those authorized for the destination RI. In no case does the ability to accept one TCC imply acceptance of others; each TCC must be specifically authorized or delivery cannot be made.

Error Condition - TCC of the message is greater than the TCC authorized to be received by the destination RI.

Error Resolution - If message contained only one RI, or if all RIs failed the security check, the message is rejected and an "INVALID ROUTING - TCC" service message is automatically generated to the originating station. Messages received from remote I-S/A AMPEs will not be rejected, but "dumped and acked" and the same service message generated to the originator. If the message contained at least one RI which passed the TCC check, the message will not be rejected but will be processed for delivery to the RI passing the check. The service message will be automatically generated to the originating station advising the remaining RIs requiring reprotection.

7.3.4.2.2. Check 5.1.c. Each DSSCS community RI is checked against the LMF of the message. Three LMFs indicate magnetic tape traffic (BB, DD, and II) and these messages cannot be delivered to a non-compatible destination. In addition, three LMFs (HC-Cards, EA-eight level paper tape, and RT-five level paper tape) indicate the originator's desire that medium exchange be prohibited, and these also cannot be delivered to a non-compatible terminal.

Error Condition - Any incompatibility detected as a result of the above check.

Error Resolution - If the message is addressed to only one RI or if all RIs fail the LMF check, the message will be rejected and an "INVALID ROUTING REPROTECT - LMF" service message will be automatically generated to the originating station. Messages received from remote I-S/A AMPEs will not be rejected, but "dumped and acked" and the same service message generated to the originator. If the message contained at least one valid RI which passed the LMF check, the message will not be rejected but will be processed for delivery to the RI passing the check. The service message will be automatically generated to the originating station advising the remaining RIs requiring reprotection.

7.3.4.2.3. Check 5.1.d. If the message contains a collective RI (may be received from a directly connected ASC during the transition period), the initial check is to determine if the CRI is contained in the I-S/A AMPE's tables. DSSCS CRIs must contain six characters - the first four being the collective designator YHCR, the last two indicating the specific collective routing indicator.

Error Condition - Use of an invalid CRI.

Error Resolution - If the CRI is not found in the I-S/A AMPE's CRI tables and the message was only addressed to that RI or did not contain any valid RIs, the message is rejected and an "INVALID ROUTING REPROTECT TO" service message is automatically generated to the originating station. Messages received from remote I-S/A AMPEs will not be rejected, but "dumped and acked" and the same service message generated to the originator. If the message contained at least one valid RI which passed this check, the message will not be rejected but will be processed for delivery to the RI passing the check. The service message will be automatically generated to the originating station advising the remaining RIs requiring reprotection.

7.3.4.2.4. Check 5.1.e. A check is made to determine if the input station is authorized to introduce a CRI/CAD.

Error Condition - Attempted input of a CRI/CAD by a port/channel not classmarked for CRI/CAD input.

Error Resolution - The message is rejected and an "UNAUTHORIZED USE OF CRI/CAD" service message is automatically generated to the input port/channel.

RI Processing Note: When an RI is found to be the subject of some CARP action, it is first determined whether the message being processed is of a category meeting the requirements of the CARP action. If it is, the destination RI specified by the CARP action is used instead of the destination RI associated with the message and the message is routed accordingly. For TCC, LMF, and message type checking, the destination RI associated with the message is always used since the originator should not be serviced when the normal destination RI can accept the message. When the normal destination RI is unable to accept the message being processed, the RI is rejected as in normal single RI processing with appropriate service action. If the message could be delivered to the normal destination RI but delivery is to be diverted to a CARP destination

RI which is unable to accept a message of the type or TCC being processed, the message is accepted by input processing; output processing will divert the message to temporary storage until the CARP action is negated and the message can be delivered normally. Collective RIs are not subject to CARP action although CADs will be.

7.5. End-of Message (EOM) Processing. Although header processing terminates in the I-S/A AMPE with the end of FL4, the I-S/A AMPE cannot anticipate the point at which the end of message will occur. Therefore, a continual scan of the message for the end of message sequence (EOMS) is performed. The DOI narrative format EOM procedurally consists of two carriage returns, eight line feeds, and the letters "NNNN" but the minimum required for recognition by the I-S/A AMPE is one line feed and four N's. In a multiple block data pattern message it consists of the letters "NNNN" in columns 77 through 80 of the last line block/card. This scan and others necessary for the detection of significant character sequences are described in this section.

7.5.1. Straggler Protection. A "straggler" is caused by a message without a start of message sequence (SOMS) following a message without an end of message sequence (EOMS) on an asynchronous channel, or two messages entered as one on a synchronous channel and framed SOH-ETX as a single message. To protect against straggler messages, the I-S/A AMPE validates the Originating Station Serial Number (OSSN) in the message header against the Trailer Station Serial Number (TSSN) found in the message trailer. (See Section 7 for CRITIC exceptions.)

7.5.1.1. Data Pattern Messages. The EOMS must be the "NNNN" sequence in columns 77 through 80. The EOM line block must contain the ETX character in the third framing character (FC3) and it is incumbent on the terminal to ensure that the EOM is properly recognized and the block properly framed. Receipt of an ETC framing character without a correct EOM results in message rejection and generation of an "INVALID EOM" service message to the input port/channel. Receipt of a valid EOM without the ETX results in non-recognition of the EOMS and an input message hiatus rejection of a following SOH lineblock, and the ultimate rejection of the errored message. (See Section 7 for CRITIC exceptions.)

7.5.1.1.1. An offshoot of EOM processing is the check for a valid record count field in a multiple line block card or magnetic tape message. There is a relationship between this field and the record count field of the header. The trailer record count field must be either "MTMS", signifying a message from a magnetic tape terminal which does not count line blocks, or a four digit numeric field. The use of "PLTS" in the trailer is prohibited and will result in message rejection and an "INVALID RECORD COUNT" service message being automatically generated to the input port/channel. If "MTMS" appears in the record count field of both the header and trailer, no further checking of the actual line block/card count is performed. If a number appeared in the header and "MTMS" or a number in the trailer, the actual line block/card count received is checked against the header number, and the trailer record count field is effectively ignored. If "MTMS" appears in the header record count field and the trailer field contains a number, that number is compared to the actual count of the line blocks/cards received. Any disparity in the above two instances results in the message being rejected and an "INVALID RECORD COUNT" service message being automatically generated to the input port/channel. When the message header record count field contains the pilot indicator "PLTS", there is no check of either the header or trailer record counts against the actual number of blocks received.

7.5.1.2. Teletypewriter (Narrative) Messages. The minimum EOMS recognizable is one linefeed character and four N's in an uninterrupted sequence. More than eight line feeds, extraneous characters in the linefeed field, or extraneous characters between the TSSN and the required EOMS are acceptable provided that the straggler sentinel (#) falls within 23 characters of the required line feed and the required EOMS is not interrupted. If the EOMS does not fall within 23 characters of the TSSN, the message will be rejected and a "SUSPECTED STRAGGLER" service message automatically generated to the input port/channel. (See Section 8 for CRITIC exceptions.)

7.5.1.2.1. On asynchronous channels, there is no such thing as an invalid EOMS. If not correct, the result will be either an input message hiatus or a two consecutive SOM condition. Either results in message rejection. On synchronous channels, detection of the ETX framing character without prior detection of a valid EOMS results in message rejection and an "INVALID EOM" service message automatically generated to the input port/channel.

.5.2. Cancel Transmission Sequence (CANTRANS). The I-S/A AMPE also scans for the presence of a CANTRANS which procedurally consists of 8 E's each separated by a space, the letters "AR", and an EOMS of two carriage returns, eight line feeds, and four N's. The minimum recognizable by the I-S/A AMPE is two E's separated and followed by a space, "AR", one linefeed, and four N's. A CANTRANS is not recognized if it occurs prior to the line feed character that terminates message header processing or following the straggler sentinel preceding a valid TSSN. When recognized, the message is discarded by the I-S/A AMPE with printout notification to the system console operator that the message has been discarded.

7.5.3. Excessive Message Length. An additional check that is performed during receipt of message text is a count of total line blocks/characters being received. Should this count exceed 556 line blocks (44,480 characters), the message is rejected and an "EXCESSIVE MESSAGE LENGTH" service message automatically generated to the input port/channel. Mode II (non-Query/Response) channels are limited to 125 line blocks (10,000 characters). (See Section 8 for CRITIC exceptions.)

7.5.4. Excessive Input Hiatus. Incoming messages are also monitored for any delay (hiatus) in receipt by the I-S/A AMPE. When no additional data is received for a message in progress for a period of approximately three minutes, the message is rejected and a "NO EOM RECEIVED" service message automatically generated to the input port/channel. (See Section 8 for CRITIC exceptions.)

7.5.5. Framing Character (FC) Processing. Framing characters are validated for all input messages. On asynchronous channels, these have been inserted and the message blocked and framed by the I-S/A AMPE itself so that FC validation is essentially a self-checking process by the I-S/A AMPE. On synchronous channels, FC validation serves to ensure proper framing by the terminal device. In addition to the channel control functions between the Mode I terminal or I-S/A AMPE and the distant Mode I terminal or I-S/A AMPE, certain framing characters are used internally by the I-S/A AMPE to insure that there is no inadvertent loss, duplication or security mismatch of message data within the I-S/A AMPE. This is particularly true of FC4, which is the Block Parity Character in transmission over a channel but becomes a block sequence number within the I-S/A AMPE, and FC2 on all but the SOH lineblock, which is an ASCII delete in transmission to/from a terminal, but which is used within AUTODIN as a security or ETR sequence character. Any framing character error results in message rejection with a "REPROTECT TO ALL ADDEES" service message being automatically generated to the input port/channel. In addition, a printout of the FC error is provided to the system console operator so that any FC errors caused within the I-S/A AMPE itself may be detected and corrective action taken.

7.6.0 LDMX DOI 103 MESSAGE PROCESSING

7.6.1 General Comments.

7.6.1.1 This section will discuss the requirements for NAVY LDMX DOI 103 message processing.

7.6.1.2 The NAVY LDMX requirement to process DOI 103 message formats evolved with the upgrade of the NAVCOMMUNIT LONDON Communications Center. Since the NSA Streamliner system provided the necessary functions needed by the LDMX it was used as a basis for the NAVYs validation and verification processing within the LDMX.

Since NSA is currently developing an appendix for DSSCS validation/verification for the I-S/A AMPE, the NAVY elects to review NSAs document and recommend those changes necessary to incorporate LDMX functions not covered.

7.7.0. DOI-103 - DSSCS MESSAGE FORMAT

7.7, 1. Following is an EXAMPLE of a DOI-103 formatted message which shall be built from a DD-173 Form or an AMF. The I-S/A AMPE shall validate format lines 2 thru 15 when received from a terminal

FORMAT LINE 2	PTTMIYUW YYOSRI 1234 1231234-MNSH--YYDEST YYDEST.<<=
FORMAT LINE 4	ZNY MMNSH<<=
FORMAT LINE 4A	ZKZKZ PP SOA DE<<=
FORMAT LINE 5	P 011234Z JAN 83<<=
FORMAT LINE 6	FM ORIGINATOR<<=
FORMAT LINE 7	TO STATION ONE<<=
FORMAT LINE 8	INFO STATION TWO<<=
FORMAT LINE 11	ZEM<<=
FORMAT LINE 12	C L A S S I F I C A T I O N<<=
FORMAT LINE 12	QQQQ<<=
FORMAT LINE 12	SUBJ<<=
FORMAT LINE 12	TEXT<<=
FORMAT LINE 15	#1234
FORMAT LINE 16	<<=========NNNN

7,7 2. FORMAT LINE 2 contains the following:

7,7 2 1 • FIELD ONE is the precedence. Only FLASH, IMMEDIATE, PRIORITY and ROUTINE are authorized. Any invalid character will require the I-S/A AMPE to process the message at IMMEDIATE precedence, but leave the character as received

7,7 2 2 FIELD TWO AND THREE are the Language Media Format (LMF). The following LMF's are authorized in DSSCS; A, B, C, D, E, G, H.

7,7 2 2 1 The first LMF character is the input station media of transmission The second LMF character is the preferred output LMF

7,7 2 2 2 The LMF's of E, H, and F can only be paired with A, C, and T respectively, and the LMF's of B, D, and I can only be paired with themselves Any unauthorized pairing will result in the message being rejected

7.7 .2.2.3. The LMF's of "G" and "Y" are generated by the I-S/A AMPE. The LMF's of "GT" and "YT" indicates that the I-S/A AMPE preformed format conversion on the message.

7.7 2.3. FIELD FOUR - is the DSSCS security sentinel "M".

7.7 .2.4. FIELDS FIVE THRU EIGHT - is the Content Indicator Code (CIC). The four character CIC field (also called the communications action identifier field when it contains communications instructions) contains information related to the type of message being processed. The CIC is validated to be either four alphabetic or three alphabetic and one numeric characters.

7.7 2.5. FIELD 9 - is a space. If not present, the message must be rejected.

7.7 .2.6 FIELDS 10 THRU 16 is the Originating Station Routing Indicator (OSRI). On DSSCS messages, the OSRI must start with the latter "Y" and are six characters long. However, a seventh character may be added to indicate certain communication center functions. All characters must be alphabetic, or the message is rejected. If a six character OSRI is used, then the seventh position must be a space, or the message will be rejected.

7.7 2.7 FIELDS 17 THRU 20 is the Station Serial Number (SSN). If the station is operating in the ITA-2 code, then the SSN must be preceded by a figure (upper case) function. The SSN must be all numbers or the message is rejected. The SSN also is used as the End of Message (EOM) validation number in format line 15.

7.7 2.8. FIELD 21 - is a space, or the message is rejected.

7.7 2.9. FIELDS 22 THRU 28 - is the Time-of-File (TOF). This field must be all numbers. More then or less then seven numbers or alphabetic characters will result in the message being rejected.

7,7 .2.10. FIELD 29 - is a dash (-) which indicates the start of the security field. If not present, the message will be rejected.

7,7 7.2.11. FIELDS 30 THRU 33 - is the security field. Position 30 must be the DSSCS security sentinel of "M", or the message is rejected. Position 31 through 33 is the Transmission Control Code (TCC). The TCC is derived from information contained in message format line 12, that is the classification, codeword, caveats, and other data appearing in message Format Line 12. Messages are rejected if the TCC is not in accordance with data in Format Line 12 or if it is an invalid TCC.

7,7 2.11.1. The I-S/A AMPE must validate that the TCC in message format lines 2 and 4 are valid according to information contained in message format line 12. Any error will result in the message being rejected.

7.7 2.12. FIELDS 34 AND 35 - are 2 dashes (--), which indicates the start of routing. Any invalid character or less than two dashes will result in the message being rejected.

7.7 2.13. FIELD 36 - is the start of routing. All DSSCS RI's must start with the letter "Y", or the message is rejected. DSSCS RI's are six letters, but there can be a seventh letter. Each RI is separated by a space, or the message is rejected. A miximum of 4 RIs will appear on the first line of Format Line 2, with a maximum of 9 routing indicators on each successive line. A maximum of 500 RI's are authorized on a DSSCS message. If a message exceeds 500 RI's, the message is rejected. The message will be rejected if RI's are split across a line, such as the first 3 character on one line then end of line functions followed by the remainder of the RI. If any routing indicator begins with any character other then a Y, the entire message must be rejected and none of the remaining or valid routing indicators are processed. A period (.) will be inserted following the last addressee's RI to indicate end-of-routing. The RI's shall be checked agains the TCC level to ensure that the recipients are authorized to receive the message.

77.3. FORMAT LINE 4, SECURITY LINE

77.3.1. The first three characters are the security warning operating signal. On DSSCS messages this will always be "ZNY", including unclassified and unclassified EFTO messages. Following the security warning operationg signal, there must be a space character, or the message is rejected. Following the space is the DSSCS security sentinel "MM", any other characters or only one "M" will result in the message being rejected. Following the "MM" is the DSCCS Transmission Control Code (TCC). The TCCs in Format Line 2 and 4 must match, or the message is rejected. Additionaly, the I-S/A AMPE shall verify that the TCC is a valid TCC authorized for the input line. The I-S/A AMPE shall also verify the consistency of Format Lines 2 and 4 security paramters against the security data contained in Format Line 12. Any error or mismatch of TCC's will cause the message to be rejected.

77.4. FORMAT LINE 4A, DIRECTOR LINE

77. 17.4.1. The start of format line 4a is the processing indicator "ZKZK". A space function must follow the start of line processing indicator. The next two characters are the repeated precedence of the message. On dual precedence messages, this will be the action precedence If any two alphabetic characters appear in this field, the message will be processed. Following the precedence is a space function. The next field is the Delivery Distribution Indicators (DDI's). Each DDI is 3 alphabetic characters. There can be up to 14 DDI's per message, each separated by a space function. Following the last DDI, preceeded by a space, is the end of line indicator of "DE" Errors in Format Line 4A will not result in the message being rejected, but deverted to a local position at the delivery I-S/A AMPE for proper identification for delivery

7.7.4.2. If a message does not contain a Format Line 4A, the I-S/A AMPE must generate a Format Line 4A, using the DDI of "SDA".

7.7.5 FORMAT LINE 5 - Date-Time-Group (DTG).

7.7. 5.1. The first character is the precedence of the message (See paragraph 1.1. for valid precedence characters in the DSSCS community and DOI-103 Format). In case of dual precedences, the action precedence is first, followed by a space function and the information precedence, followed by a space function. (see paragraph 3.6.1. for trannissions when the action precedence is FLASH and the information precedence is IMMEDIATE or lower). Following the space is the DTG, which consist of 6 numbers and the Greenwich Zone suffix (Z).

7.7.5.2 Following the DTG, and preceded by a space function, is the abbreviated month, followed by a space function and the last two digits of the year.

7.7.5.3. Following the year, preceded by a space function, can be special operating signals (Z or Q Signals IAW DOI-103 or ACP-131). 131) On all DSSCS messages of IMMEDIATE precedence or higher, the operating signal of "ZYH" must appear on the message. If more then one operating signal is required for a message, each is separated by a space function.

7.7. 5.3.1. Certain phrases in message format line 12 will require the placing of a "Q" or "Z" signal in format line 5.

.6. FORMAT LINE 6 - MESSAGE ORIGINATOR

7.7.6.1. The first two characters is the prosign "FM". Following the prosign is a space, and the PLA of the activity which originated the message. The PLA must be valid in accordance with DSSCS Addressing documents.

7.7 7. FORMAT LINE 7 - ACTION ADDRESSEE(S) OF THE MESSAGE.

7.7 7.1. The first two characters are the prosign "TO" Following the prosign is a space, and the PLA, DAG, Product Distribution (PD). The PLA must be valid in accordance with the DSSCS addressing doucments.

7.7.8. Format Line 8 - INFORMATION ADDRESSEE(S) OF THE MESSAGE.

7.7.8.1. The first 4 characters are the prosign "INFO". Following the prosign is a space, and the PLA(s), DAG's, or PD. The address must be valid in accordance with DSSCS addressing documents.

7.7.9. FORMAT LINE 9 is not used in DSSCS.

7.7.10. FORMAT LINE 10 - is not normally used on DSSCS messages, unless the message is a five letter/number coded message. If used, format line 10 is not required to be validated by the I-S/A AMPE.

7.7.11. Format Line 11 - START OF TEXT INDICATOR.

7.7.11.1. The start of text indicator in the DSSCS community is "ZEM", and must appear on all messages, or the message is rejected.

7.7.12. Format Line 12, Text of the message.

7.7.12.1. Format line 12 consist of several specific items which must be in the proper sequence for correct validation.

7.7.12.2. CLASSIFICATION.

7.7.12.2.1. Unclassified is abbreviated as "UNCLAS" without spacing between the letters.

7.7.12.2.2. Unclassified Encrypted For Transmission Only is abbreviated as "UNCLAS E F T O". UNCLAS without spacing, followed by a space and E F T O with each letter separated by a space.

7.7.12.2.3. Other classifications, each letter of the classification must be separated by a space, e.g., C O N F I D E N T I A L.

7.7.12.2.4 Any special handling instructions, codewords, or caveats that follow the classification shall be separated from the classification by two spaces and also separated from each other by two spaces. In the classification line, words shall not be hyphenated and continued into the next line Each line shall end with a completed word. Caveats will be broken at a space but not hyphenated at the end of the line or with a slant. The TCC in format lines 2 and 4 are derived from information on this line.

7,7 12.2.5. On a separate line following the classification, special handling instruction, etc., is the DSSCS delimeter of 4 Q's.

7,7.12.2.6. On a separate line following the 4 Q's is the transmission sectional data.

7,7 12.2.7. On a separate line following the sectional data (if applicable) is the message reference number (if used)

7,7 12.2.8. On a separate line is the internal handling or command passing instructions, if used. (Exercise name or project name, if used).

7,7 12.2.9 Subject line. This line will always start with the letters "SUBJ". If a subject is not supplied by the originator the I-S/A AMPE must insert this line, which will contain the letters "SUBJ".

7,7 12.2.10 Validation of format line 12 by the I-S/A AMPE stops at this point of format line 12

7,7 12.2.11 Thought or idea as expressed by the originator.

7,7 13. FORMAT Line 13 and 14 are not used in DSSCS.

7,7 14 Format line 15 - has two separate functions. Each function must be on a line by itself. The first line(s) is the correction line (If used, it must contain the prosign "C" followed by necessary corrections)

On the last line is the End Of Message (EOM) validation. It contains a number symbol (#) immediately followed by the four digit station serial number which appeared in format line 2, positions 17 thru 20. If the is missing; there is less then four numbers, or the EOM validation numbers do not match the SSN in message format line 2, the message is rejected.

7,7 15. Format line 16 End of Message (EOM)

7,7 15.1 The EOM functions are "2 carriage returns (CR), 8 line feeds (LF) and 4 N's, e.g., "<<========NNNN". To allow for errors in the number of line feeds, the I-S/A AMPE shall accept as a minimum 2 line feeds and 4 N'

8.0. CRITIC Format Message Processing Requirements.

8.1. General Comments. CRITIC messages are unique to the DSSCS community and are to be afforded special processing throughout the system to ensure the most expeditious handling possible. They are recognized by detection of a CRITIC prosign which consists of a nine-character field "WW YEKAAH" in the header position. The I-S/A AMPEs must recognize this field and allow its use on any DSSCS (Y) port/channel or DSSCS/GENSER (R/Y) port/channel regardless of the normal format used by that port/channel.

8.2. Validation/Verification Requirements

8.2.1. Format Line 1 - Transmission Identifier (TI) Line. I-S/A AMPE validation of the TI line is identical for both asynchronous (Mode II and V teletypewriter terminals whose use of a TI line is mandatory) and synchronous (Mode I users who employ line block framing and whose use of a TI line is optional but must be specified at the time the I-S/A AMPE sets the port/channel parameters) channels. All TI lines through the CD-CSN fields are processed as follows:

8.2.1.1. The first characters of the TI line block must be a Start of Header (SOH) and a select (SEL) character. If the channel is asynchronous, these have been inserted by the I-S/A AMPE; if the channel is synchronous, the terminal has inserted them.

8.2.1.2. Check 1.1.a. The first data character of the TI line must be the letter "C". (If the channel is asynchronous, the "ZCZ" portion of the Start of Message Sequence (SOMS) was previously validated and then discarded by the I-S/A AMPE.)

Error Condition - None - nothing can be recognized prior to receipt of the SOH.

Error Resolution - N/A

8.2.1.3. Check 1.1.b. The second, third and fourth characters of the TI line must be the Channel Designator (CD) and must match the CD stored at the I-S/A AMPE for that port/channel.

Error Condition - A CD is considered to be in error if it does not match the CD stored in the I-S/A AMPE for its' associated channel.

Error Resolution - CRITIC messages will be accepted and a service message automatically generated to the input port/channel advising of the error and of message acceptance.

8.2.1.4. Check 1.1.c. The fifth character of the TI line can be either a figures shift or the first character of the CSN field; the figures shift must be present for "A" Select (ITA 2) messages and may or may not be present for other selects. Note that for all processing purposes, "A" Select CSN's are always assumed to begin in the sixth position of the TI line. This is done so that the "CSN" to be quoted back to the terminal in a service message will be positionally correct even if the figure shift is garbled, leaving the CSN field in the lower case. If the CSN is correct, TI line processing is complete at this point.

Error Condition - A CSN is considered to be in error if it is either non-numeric or if it is not the next expected CSN (i.e., one greater than the last accepted from a Mode V port/channel or received from a Mode I or II port/channel. For this purpose, a CSN of 000 is considered to be one greater than 999.

Error Resolution - CRITIC messages will be accepted and a service message automatically generated to the input port/channel advising of the error and of message acceptance.

8.2.1.5. Further I-S/A AMPE TI Line processing. In order to maintain CSN continuity between the I-S/A AMPE and the terminal, the I-S/A AMPE tables are updated based on the results of CSN and message processing. When a CSN is rejected (i.e., duplicate condition), no CSN updating is performed.

When a CSN is accepted, even if it is out of sequence, the accepted CSN (or the expected CSN, if the received CSN is non-numeric) is made the last accepted CSN for processing of future messages. When the channel is Mode I or Mode II this update is done immediately on receipt of the TI line whether the associated message is accepted or not, since the Mode I or Mode II terminal is assumed to update the CSN at the beginning of each message transmission. This is also consistent with a terminal transmitting a tape in which there are pre-cut CSN's preceding each message. Since Mode V procedures require that CSN's be updated on acceptance of the message, Mode V terminal equipment does not update its TI generator until the associated message has been acknowledged by the I-S/A AMPE. Consequently, the I-S/A AMPE also does not update the last accepted CSN on a Mode V channel until the message has been validated and accepted, and the ACK for the message has been sent to the terminal.

8.3. Format Line 2 - Message Header. For I-S/A AMPE validation purposes, the CRITIC header consists of one nine-character field - the CRITIC prosign field.

.3.1. CRITIC Prosign Field Validation/Verification. The CRITIC prosign field is the CRITIC precedence prosign repeated twice (WW), one space character, and the CRITIC routing indicator YEKAAH. It is validated as a single entity and no other header or RI validation is performed after detection of the CRITIC prosign. If either one of the precedence prosigns is in error, but the remainder of the field is correct, the non-"W" will be corrected and the message forwarded as a CRITIC.

8.3.1.1. Check 2.1.a. The CRITIC prosign field is validated to be "WW YEKAAH".

Error Conditions:

Use of the CRITIC precedence prosign "W" in a JANAP format header on either a DSSCS or GENSER port/channel.

Error Resolution - The message will be rejected and an immediate precedence "INVALID HEADER - REJECT" service message automatically generated to the input port/channel.

No space character separating the CRITIC precedence prosigns from the CRITIC RI.

Error Resolution - Regardless if entered on a DSSCS or GENSER port/channel, the message will be rejected and an "INVALID HEADER - REJECT" service message automatically generated to the input port/channel. If the input port/channel is classmarked as a "Y" or an "R/Y" circuit, the service message is at the flash precedence. If the input port/channel is classmarked as a "R" circuit, the service message is given immediate precedence.

CRITIC prosign received as "ZW YEKAAH" on a "Y" or "R/Y" port/channel.

Error Resolution - The message is accepted, the "Z" changed to a "W", and the message forwarded as a CRITIC.

Message recieved from a "Y" or "R/Y" port/channel as "WW YEKAAH RUEOCSA RUWTCSA."

Error Resolution - Since only the first nine characters constitute the CRITIC prosign, this message would be accepted and processed as a CRITIC.

8.3.2. Header Validation/Verification of the RI Field. There is no header validation of any kind performed on a CRITIC message by the I-S/A AMPE beyond the nine character CRITIC prosign.

.3.3. Header Validation/Verification of the Security Line. There are no checks of any kind for TCC presence or validity.

8.4. End-of-Message Processing. CRITIC messages undergo normal EOM processing but are not subject to straggler checks. Absence of an End-of-Message Sequence (EOMS) in a CRITIC being received on an asynchronous channel results in truncation for either input hiatus or for two consecutive Start-of-Message Sequences (SOMS), depending on whether a message with a valid SOMS follows. Absense of an EOMS in a Mode I channel CRITIC having a proper ETX framing character results in the ETX framing character being changed to an ETB and a truncation sequence with a valid EOMS being appended to the message. The message is accepted for delivery but is acknowledged as a partial CRITIC message.

8.4.1. Cancel Transmission Sequence (CANTRANS). There is a check made for a CANTRANS, and a CRITIC message may be cancelled by the input terminal using the CANTRANS procedure. If CANTRANS is present, the I-S/A AMPE will discard the message. It will not be truncated and forwarded.

8.4.2. Framing Character Validation. CRITIC messages are subject to normal framing character validation and any error will result in message rejection and a "REPROTECT TO ALL ADDEES" service message automatically generated to the input port/channel at flash precedence.

8,5 [illegible] MESSAGE

8,5 The following is an example of a fully formatted [illegible] generated by the [illegible] AMPS from a DD-173 Form or an AMF

```
FORMAT LINE 2     [illegible]
FORMAT LINE 3     [illegible]
FORMAT LINE 4     [illegible]
FORMAT LINE 4A    [illegible]
FORMAT LINE 5     W 012345Z JAN 83 ZYH<<=
FORMAT LINE 6     FM ORIGINATOR<<=
FORMAT LINE 7     TO DIRNSA<<=
FORMAT LINE 11    ZEM<<=
FORMAT LINE 12    C L A S S I F I C A T I O N AND TEXT<<=
FORMAT LINE 15    #9999
FORMAT LINE 16    <<========NNNN
```

8,5 2. The following paragraphs will show what is required to be in a CRITIC message formatted by the I-S/A AMPE.

8,5 3. Format Line 2

8,5 3.1. The routing line consists of the repeated CRITIC precedence prosign "WW" and the DSSCS Routing Indicator of "YEKAAH". The I-S/A AMPE will process a message as a CRITIC if only one of the two precedence characters is a "W" and the other character is an alpha/numeric in character position one or two, as long as the remainder (character positions 3 thru 9) of format line 2 meets the criteria of space and DIRNSA routing indicator YEKAAH. The I-S/A AMPE will change the non CRITIC precedence character to a "W" prior to tranmisssion.

8,5 3.2. If any other routing indicator on a CRITIC message follows YEKAAH, the routing indicator is not validated, and is allowed to stay on the message during transmission.

8,5 4. Format Line 3.

8,5 4.1. This format line contains the prosign "DE", space, the Originating Station Routing Indicator (OSRI), the Station Serial Number (SSN) preceded by the hatch mark (#), followed by a space character and the Time Of File (TOF) of the message. All CRITIC messages will have the SSN of "9999".

8,5 5. Format Line 4

8,5 5.1. The security line consist of "ZNY MMGAD". This line will always start with the security warning operating signal "ZNY", followed by a space and the DSSCS

Community sentinel "MM". Following the "MM" is the Tranmission Control Code (TCC). For all CRITIC messages, regardless of the classification, codeword, etc., in Format Line 12 the TCC will always be "GAD".

8,5 6. Format line 4A

8,5 6 1. Format Line 4A on all CRITIC messages is "ZKZK WW ZZZ DE". See paragraph 2.16.5 for explanation of the different elements of this Format Line.

8,5 7. Format Line 5.

8,5 7.1. This line contains the CRITIC precedence prosign "W", followed by a space, and the Date Time Group (DTG) of the message, the abbreviated month and year and the high precedence operating signal "ZYH".

8,5 8. Format Line 6

8.5 8.1. Prosign "FM" followed by a space and the PLA of the originating station.

8.5 9. Format Line 7.

8,5 .9 1. Prosign "TO" and the addressee of the CRITIC message. CRITIC messages are always single addressed to DIRNSA.

8,5 10. Format Line 11

8,5 10 1. Start of Text (SOT) line containing the operating signal "ZEM".

8,5 11. Format Line 12

8.5 11 1. Text of the CRITIC message consist of the classification, codeword (when assigned) special or restrictive handing instructions, the designator "CRITIC", CRITIC number and thought or idea as expressed by the originator.

8,5 12. Format Line 15.

8,5 12.1. This line consists of the End Of Message validation, which is the repeat of the SSN in format line 3 of the message heading. It will always be "#9999" on CRITIC messages.

8.5 13. Format Line 16.

8.5 13.1. End of Message Function.

8.5 13.1.1. The EOM for a CRITIC message is the same as any other message, that is 2 carriage returns, 8 line feeds, and 4 N's. The I-S/A AMPE shall accept a minimum of 2 line feeds and 4 N's as an valid EOM.

8.6.0 CRITIC MESSAGE INPUT VIA CARDS.

8.6 1. CRITIC messages can be sent to an I-S/A AMPE using card format.

8,6 1.1. If a CRITIC message is sent in card format, the delivery I-S/A AMPE will convert the message from card format to applicable code prior to delivery, as required.

8,6 1.2. Any error in cards 3 thru next to last card or missing cards will not delay or stop the processing of a CRITIC message from a terminal.

8.6 2. Following is an example of a CRITIC message in card format from a terminal.

CARD 2	WW YEKAAH
CARD 3	DE YYDERI #9999
CARD 4	ZNY MMGAD
CARD 5	ZKZK WW ZZZ DE
CARD 6	ZYH
CARD 7	FM ORIGINATOR
CARD 8	TO DIRNSA
CARD 9	ZEM
TEXT CARDS	C L A S S I F I C A T I O N AND TEXT
NEXT TO LAST CARD	C FT 1231234 DTG 012345Z JAN 83

```
LAST CARD          #9999                                    NNNN
```

8.6 .2.1. The last card must contain only the EOM validation number (#9999) in columns 1 thru 5 and the EOM (NNNN) in columns 77 thru 80. No other data can be included in this card. Cards 2 thru 9 and the last card may be pre-punched and be available when needed.

8.6.3. The data of each format line is the same as in paragraphs 8.5 .3. through 8.5. 12.

8.7.0 CRITIC MESSAGE USING THE ABBREVIATED MESSAGE FORMAT (AMF).

8.7 .1. CRITIC messages can be sent to the I-S/A AMPE in the AMF. This requires the I-S/A AMPE to build the CRITIC message in accordance with paragraphs 8.5.3 through 8.5.13.

8.7 .2. The AMF contains fields which are required and fields that are optional. If the optional fields (Format Lines 4a and 5) are not present, the I-S/A AMPE shall build the required format lines.

8.7 .2.1. Any error in format lines 1 and 4 thru 12 will not delay or stop the processing of a CRITIC message being received from a terminal.

8.7 .3. Following is an example of a AMF CRITIC messages from a terminal which shall be converted to a CRITIC formatted message.

```
FORMAT LINE 1      ZCZCABC123::=
FORMAT LINE 2      GGGG ::=
FORMAT LINE 3      W CRITIC ::=
FORMAT LINE 4      CC ::=
FORMAT LINE 4A     ZKZK WW ZZZ DE ::=
FORMAT LINE 5      W 011250Z JAN 83 ZYH ::=
FORMAT LINE 6      FM ORIGINATOR ::=
FORMAT LINE 7      TO DIRNSA ::=
FORMAT LINE 12     TEXT
FORMAT LINE 16     ::========NNNN
```

8,7.4. Format line 1.

8,7.4.1. If used it will be as stated in paragraph 3.12.4.10.

8,7.5. FORMAT LINE 2.

8,7.5.1. QQQQ - This is a required field, indicating that this is an AMF message. The absence of this group will cause the I-S/A AMPE to expect a fully formatted message. If the four Q's are present, the I-S/A AMPE will search for the next line of "W CRITIC" prior to rejecting any message. The stutter group will not be transmitted electrically nor appear on the feedback copy.

8,7.6. FORMAT LINE 3

8,7.6.1. W CRITIC - This is a required field and is the precedence of the message and indication that this is a CRITIC message.

8,7.7. FORMAT LINE 4.

8,7.7.1. CC - This field contains a two character classification code (TT, SS, CC, UU, or EE). If this field is not present, the I-S/A AMPE will not reject or delay the processing of the CRITIC message.

8,7.8. FORMAT LINE 4A

8,7.8.1. ZKZK NN ZZZ DE - This is an optional field. It is the Delivery Distribution Indicator (DDI) line.

8,7.9. FORMAT LINE 5

8,7.9.1. W 011250Z JAN 83 ZYH - This is an optional field. If present it will contain the precedence, DTG, Month, Year and operating signal ZYH.

8,7.10. FORMAT LINE 6 and 7

8,7 .10.1. FM ORIGINATOR and TO DIRNSA - These are optional fields, indicating the originator and addressee of the message.

8,7 11. FORMAT LINE 12.

8,7 11.1. CLASSIFICATION - This is an optional field and contains the classification, codeword(s) and/or special handling instructions.

8,7 12. FORMAT LINE 12

8,7 12.1. QQQQ - The stutter group signifies the end of classification, and special handling structions.

8,7 13. FORMAT LINE 12.

8,7 13.1. TEXT - Lines of text should not exceed 69 characters including spaces.

8,7 14. FORMAT LINE 16.

8,7 14.1 END-OF-MESSAGE - A required field. At least two (2) line feeds and 4 N's functions must be received by I-S/A AMPE. If not received, the I-S/A AMPE will truncate the CRITIC message.

8,8.0 DD-173 FORM CRITIC MESSAGE INPUT

8,8 1. Following is a copy of the DD 173 Form filled out for a CRITIC message.

(COPY OF DD 173 COMPLETED FOR A CRITIC MESSAGE)

8.8 2. The following special instructions will apply when filling out the Joint message Form 173 for CRITIC messages.

8,8 2.1. The CRITIC precedence prosign "WW" will be placed in the ACTION Addressee precedence block.

8.8 2.2. The word "CRITIC" will be placed in the "Orig/Message Ident" block.

8.8.2.3. CRITIC DDI "ZZZ" will be used in the message handling instruction block. If the DDI does not appear in this block, the I-S/A AMPE will build the proper Format Line 4A, but will not reject the message.

8.8. 2.4. The station designator of the station originating the CRITIC message will be placed in the "FM" line.

8.8 2.5. The "TO" line will show "DIRNSA" as the only addressee.

8.8.2.6. Start the text of the CRITIC message with security classification assigned by the originator with each letter separated by a space, CODEWORD (when assigned), special or restrictive handling instructions, the designator "CRITIC", CRITIC number and throught or idea as expressed by the originator.

8.9.0 GENSER CRITIC

8.9. 1. The I-S/A AMPE must be able to recognize a GENSER CRITIC, in the JANAP 128 Format. For a JANAP 128 formatted message to be recognized as a CRITIC, the precedence must be "Z", the Routing Indicator must be "RUETIAA", and the word "CRITIC" must appear in Format Line 12 followed by a space, carriage return, or line feed. If the word CRITIC is preceded or followed by the words "FOLLOW-UP" or "LATERAL", the message shall not be handled as a CRITIC. If the GENSER CRITIC criteria is met and any Routing Indicator other than "RUETIAA" appears in Format Line 2, they will be ignored. Once a message is recognized as a CRITIC message, CRITIC processing is required until output to the terminal.

9.0 NAVY ABBREVIATED SI VALIDATION REQUIREMENTS.

9.1 The Navy Abbreviated SI format is the DSSCS equivalent of Modified ACP 126 format. It is, basically, DOI-103 format routed to an LDMX DSSCS NARC derivative "SMM" and is used only as a vehicle to pass the appropriate information from a DD173 Message Form from a remote terminal (RIXT) to the LDMX for formatting and routing purposes.

10.0 DOI-103 SPECIAL FORMAT

10.1 Following is an example of a DOI-103 SPECIAL FORMAT message

```
FORMAT LINE 2   PP YYDEST YYDEST<<=
FORMAT LINE 3   DE YYDSRI #1234 1231547<<=
FORMAT LINE 4   ZNY MMNSH<<=
FORMAT LINE 4A  ZKZK PP EOA DE<<=
FORMAT LINE 5   P 011234Z JAN 83<<=
FORMAT LINE 6   FM ORIGINATOR<<=
FORMAT LINE 7   TO STATION ONE<<=
FORMAT LINE 8   INFO STATION TWO<<=
FORMAT LINE 11  ZEM<<=
FORMAT LINE 12  C L A S S I F I C A T I O N<<=
FORMAT LINE 13  [illegible]<<=
FORMAT LINE 13  [illegible]<<=
FORMAT LINE 14  [illegible]<<=
FORMAT LINE 15  #1234
FORMAT LINE 16  <<=========NNNN
```

10.2 FORMAT LINE TWO

10.2.1 The first two characters in the precedence [illegible] repeated: FLASH, IMMEDIATE, PRIORITY and ROUTINE are authorized in the DOI-103 SPECIAL Format. Any invalid character will require the I-S/A AMPE to process the message at IMMEDIATE precedence, but leave the characters as received. Following the precedence is a space function. Following the space, are the Routing Indicators (RI's) of the addressees of the message. All RI's must start with the letter "Y", or the message is rejected. DSSCS RI's are six characters, however, seven letter routing indicators are authorized. Nine routing indicators are authorized on each line. RI's can not be split across a line, such as the first three characters on one line, the end of line functions and the last 3 or 4 characters on the next line, or the message is rejected. The mixing of both "R" and "Y" routing indicators in the same message are not authorized, or the message is rejected.

10.3 FORMAT LINE THREE.

10.3.1 The first two characters of this line must be the prosign "DE" Following the prosign, is a space, or the message is rejected After the space is the Originating Station Routing Indicator (OSRI) This will always start with the letter "Y", or the message is rejected Following the space after the OSRI, is the hatch mark (#) Immediately after the hatch mark (no space) is the four digit Station Serial Number (SSN) The SSN is also used as the end of message validation number in format line 15 Following a space function after the SSN, is the Time-Of-File (TOF). The TOF must be all numbers. If less than seven characters or non numeric characters appear in this field, the message is rejected

10.4 The remaining format lines of the DOI-103 Special Format are the same as that of a DOI-103 formatted message (See paragraphs 7.7.3 through 7.7.15.

11.0 DD FORM 173

11.1. This form has been designed for use with the Optical Character Readers (OCR) for automatic processing. Specific instructions on preparation of the form are considered essential in the interest of standardization and economy.

11.2. When preparing a DD Form 173, the following rules apply.

11.3. All lines on the DD Form 173 will be double spaced.

11.4. Each page of the message shall have no more then 20 double spaced lines of addressees and/or text, except for the last page which may have less then 20 lines.

11.5. Double spacing throughout the message from the horizontal guidemarks printed at the left and right margins to the end of the text area is mandatory, except information other than automatic distribution data typed in the DISTRIBUTION block.

11.6. For OCR preparation, pen and ink corrections, initials, annotations, stamps and other markings will not appear on the message form from the security classification at the top of the form down through any portion of the form reserved for message addressees and/or text.

11.7. Following is a Sample DD Form 173, and will be complete as indicated in the following paragraphs.

(BLANK COPY OF DD FORM 173)

11.7.1. PAGE NUMBER - A two-character field. Start at the left margin and the number must contain two digits. On numbers one through nine the leading digit will be zero.

11.7.2 MESSAGE PAGE COUNT - A two-character field. The number must contain two digits. On numbers one through nine the leading digit will be zero. The message page count is mandatory only on the last page of the message. However, if a page count is used on all pages it must be consistent.

11.7.3 DATE-TIME-GROUP (DTG)/RELEASER TIME - A 16 character field. This field is optional and can be left blank if the originator desires the I-S/A AMPE to assign the DTG.

11.7.4 PRECEDENCE - A four-character field. The precedence assigned to action and information addressees. Precedence prosign to be used are: WW for CRITIC, ZZ for FLASH, OO for Immediate, PP for Priority, and RR for Routine. Unless the message is dual precedence, the information precedence block will be left blank.

11.7.5 CLASSIFICATION: A four-character field. Enter the proper security classification designator repeated four times, e.g., UUUU for Unclassified, EEEE for Encrypted for Transmission Only (EFTO), CCCC for Confidential, SSSS for Secret and TTTT for Top Secret.

11.7.6. SPECAT/SPECIAL HANDLING DESIGNATOR: A four-character field. This block will not be used on DSSCS messages.

11.7.7 LANGUAGE MEDIA FORMAT (LMF) - A two-character field. Normally left blank. If the message is to be delivered to the addressees in any form other then narrative, insert the proper LMF. If the LMF block is left blank, the I-S/A AMPE will assign the proper characters, from the internal setting of the input terminal.

11.7.8. CONTENT INDICATOR CODE (CIC) - A four character field. A content indicator code is a four-character designator to identify the general subject of the message.

The OCR will read the characters typed in the content idicator block. If the block is blank, the I-S/A AMPE will automatically assign the approriate CIC. This field is optional.

11.7.9 ORIGINATOR/MESSAGE IDENTIFICATION: - A maximun of 12 characters field. A unique sequence of characters assigned by the message originator for positive originator/message identification. This sequence of characters will appear on each page of the message.

11.7.10. BOOK - A three-character field. For book messages enter "YES", for all other messages leave blank.

11.7.11. MESSAGE HANDLING INSTRUCTIONS - When required, this block will contain Delivery Distribution Indicators. (DDI's) and/or Operating Signals. DDI's and operating signals will be placed in the message handling block at the top of the DD Form 173 in the following order: SOL/ZZS. DDI's will be separated from the operating signals by a slant (/) sign. Multiple DDI's/Operating signals will be shown as: SOL RNI SOA/ZES ZZS.

11.7.12. FROM - (Leave 14 blank spaces from left margin). Identify the message originator using the proper plain language address (PLA) provided in the current DSSCS Addressing publications.

11.7 13. TO - (Leave 14 blank spaces from left margin). List action addressee(s) using the proper PLA, DAG, PD, etc., listed in the appropriate documents

11.7 14. INFO ADDRESSEE(S) - (Leave nine blank spaces from left margin). On the line with the first information addressee type "INFO". The PLA, DAG, PD, etc., for information addressee(s) will be placed directly below action addressee(s).

11.7.14 1. Plain Language Address (PLA). When the PLA's and office symbols, including slants, exceed 55 characters, the second and succeeding lines of the PLA will be indented five spaces past the first letter of the first line of the PLA

11.7.15. ZEN - Addressees that are to be taken care of by other than electrical means will be the responsibility of the originator and will have ZEN placed in front of such PLAs. ZEN will be placed in the first three positions normally containing the PLA (14 blank spaces from the left margin) followed by a space and the appropriate action or information PLA.

11.7.16. CLASSIFICATION LINE AND CAVEAT(S) - Double linefeed down from the last PLA and start the text at the left margin. Indentation of the first line of text is not permitted. The first word of the first line of text will contain the classification. Other information may be contained in the classification line, in accordance with paragraph 7.7.1.2.

11.7.16.1. SPECIAL ACTIVITY OFFICER (SAO)- All Special Activity Officer (SAO) messages addressed to U. S. Naval commands will contain the additional special handling instructions, "DO NO TRANSMIT VIA OPINTEL BROADCAST", immediatley following the classification line, and prior to the four Q's Also the "Z" signal "ZYS" will be placed in the message handling instruction block. If this phrase is in Format Line 12, then the operating signal "ZYS" must either appear in the message handling block or be added by the I-S/A AMPE.

12.0 ABBREVIATED MESSAGE FORMAT (AMF)

12.1 The purpose of the abbreviated message format is to provide a means of entering originated messages into the I-S/A AMPE from a teletype keyboard, tape reader, computer or equivalent device or circuit. Messages entered in the abbreviated message format will be formatted by the I-S/A AMPE in the appropriate format.

12.2. Following example is an AMF message with all optional fields included.

```
FORMAT LINE 1      ZCZCABC123<<=
FORMAT LINE 2      QQQQ<<=
FORMAT LINE 3      PTTMZYUN<<=
FORMAT LINE 4      TT<<=
FORMAT LINE 4A     ZKZK PP ABC GHA DE<<=
FORMAT LINE 5      P R 022056Z JAN 83<<=
FORMAT LINE 6      FM ORIGINATOR<<=
FORMAT LINE 7      TO STATION ONE<<=
FORMAT LINE 8      INFO STATION TWO<<=
FORMAT LINE 12     C L A S S I F I C A T I O N<<=
FORMAT LINE 12     QQQQ<<=
FORMAT LINE 12     SUBJ<<=
FORMAT LINE 12     TEXT
FORMAT LINE 12     <<========NNNN
```

12.3. The abbreviated message format will contain optional fields and essential fields The DTG is an example of an optional field When not provided on input of an abbreviated message, the I-S/A AMPE will assign the DTG. An electrical feedback copy of each message entered, both abbreviated and fully formatted, must be automatically provided to the sending terminal

12.4 Following is breakdown of each format line of an AMF message.

12.4.1 FORMAT LINE 1 - ZCZCABC123 - If used, it will contain the start of message sequence, channel designator, and sequence number Error conditions will be handle as stated in paragraph 3.7.4 10 2 3

12.4.2 QQQQ - FORMAT LINE 2 - Required field. Stutter groups indicating the abbreviated message format The absence of this group will cause the I-S/A AMPE to expect a fully formatted message, and reject the message. The stutter group will not be transmitted electrically nor appear on the feedback copy

12 4.3. FORMAT LINE 2 - PTTMZYUW - The precedence indicated by the "P" is a required field. The LMF (TT), DSSCS security sentinel (M) and CIC are optional and will be inserted by the I-S/ AMPE if omitted.

12.4.4. FORMAT LINE 4 - TT - A two-character classification code (TT, SS, CC, UU, EE, and RR.) This is an optional field.

12.4.5. FORMAT LINE 4A - ZKZK PP ABC GHA DE - An optional field. Delivery Distribution Indicator (DDI) line, if used, this field must be complete. The number of DDIs may vary with each message up to a maximum of 14. If a DDI is not assigned to the message, the I-S/A AMPE will build the format line using "ZKZK PP SOA DE", in accordance with DOI-103.

12 4.6. FORMAT LINE 5 - P R 022056Z JAN 83 - Optional field. Contains the precedence prosign(s), DTG and any OPSIGS which are required for denoting special handling or other communications functions. Both single and dual precedence may be indicated. If the message is dual precedence, then the precedences are required, and the DTG is optional.

12.4.7. FORMAT LINE 6 - FM ORIGINATOR - Required field, The PROSIGN "FM" and PLA denoting the originator of the message.

12 4.8. FORMAT LINE 7 - TO STATION ONE - Required field. The PROSIGN "TO" followed by the PLA(s), DAGs, AIG, ETC. (as appropriate) which denote the action addressee(s) of the message, in accordance with appropriate DSSCS addressing documents.

12 4.9. FORMAT LINE 8 - INFO STATION TWO - A required field if applicable for the particular message: the PROSIGN "INFO" followed by applicable addressee indicators (same as as paragraph 12.4.8. above)

12 4 10 FORMAT LINE 12

12.4.10.1 Unclassified is abbreviated as "UNCLAS" without spacing between the letters.

12.4.10.2. Unclassified Encrypted For Transmission Only is abbreviated as "UNCLAS E F T O". UNCLAS without spacing, followed by a space and E F T O with each letter separated by a space

12.4.10.3. Other classifications, each letter of the classification must be separated by a space, e. g., C O N F I D E N T I A L.

12.4.10.4. Any special handling instructions, codewords, or caveats that follow the classification shall be separated from it by two spaces and also separated from each other by two spaces. In the classification line, words shall not be hyphenated and continued into the next line. Each line shall end with a completed word. Caverts will be broken at a space but not hyphenated at the end of the line or with a slant

12.4.11. FORMAT LINE 12 - QQQQ - Required field. Stutter group which signifies the end of the classification line This stutter group will not be transmitted electrically or appear on the feedback copies.

12.4.11.1. Other information may be contained in format line 12, in accordance with paragraph 7.7.12.

12.4.12. FORMAT LINE 12 - SUBJ - Subject Line. This line will always start with the letters "SUBJ". If a subject is not supplied by the originator, the I-S/A AMPE will insert this line, which will contain the letters "SUBJ".

12.4.13 FORMAT LINE 12 - TEXT - Required field Lines of text should not exceed 69 characters, including spaces

12.4.14 FORMAT LINE 16 - (EOM) - Required field The normal EOM sequence OF 2 Carriage Returns, 8 Line Feeds and 4 N's The I-S/A AMPE shall accept as a mimimum 2 line feeds and 4 N's

13.0 DSSCS Card Message Format

13 1 EXAMPLE of an DSSCS card message

```
CARD 1        RCCMCC31 YYDERI 0000 1231234 0011-MNSH--YYDEST
CARD 2        ZNY MMNSH
CARD 3        ZKZK PP ONI DE
CARD 4        P 021800Z FEB 83
CARD 5        FM ORIGINATOR
CARD 6        TO STATION 85
CARD 7        ZEM
CARD 8        C L A S I F I C A T I O N
CARD 9        BUBJ
TEXT CARDS    THOUGHT, IDEA OF DATA  AS REQUIRED BY ORIGINATOR
LAST CARD     RCCMCCD1 YYDERI 0000 1231234 0011-MNSH               NNNN
(EOT CARD)
```

13 .2 For these DSSCS MODE I terminals that employ TI Lines, a TI line is required for CARD messages as well The abbreviated SCM of only "C" is used The rest of the TI Line is the same as paragraph [illegible]

13 .3 Data in Format line 5 is the same as paragraphs 7.7.2.1 thru 7.7.2.13 except for positions [illegible] through [illegible]

13.3.1. Positions 30 thru 33 is the card count. The card count is the total number of 80-character records in the card message, including header and EOT card. Left most positions are filled with zeros when they contain no other numerics. "MTMS" may be used in this field to facilitate the processing of messages in batches. However, the actual record count must be placed in the record count field of the EOT (last) card. The TI line is NOT included in the card count. If this field is less than four characters, the numbers do not match the card count field in the EOT card, or any characters other than MTMS appears in this field, the message will be rejected

13.4 Cards 1 through text cards are the same as paragraphs 7.7.3 thru 7.7.14.

13.5. LAST CARD - EOT CARD. The final record of a card message is used to identify the originating station, SSN, TOF, Card count, TCC, associated tranmission information to the addressee after the header (Format Line 2), is stripped from the message by the receiving I-S/A AMPE. The EOT is an 80-position record for card and magnetic tape. The EOT consist of a repeat of header (format line 2) information starting with the precedence, including all intervening elements, and ending with the character before the start-of-routing signal. When MTMS is used in the record count field of format line 2, the actual record count must be placed in the EOT card. The remaining positions are filled with separators (spaces) up to the position required for the end-of-tranmission signals (EOTS). Any errors in positions 1 thru position 30 is handled the same as paragraphs 7.7.2.1 through 7.7.2.10. Errors in the card count field shall be handled the same as paragraph 13.3.1 above.

14.0 MAGNETIC TAPE FORMAT

14.1. DSSCS stations having magnetic tape capability, the format is the same as that of a CARD message (paragraph 13.0)

14.2. The text material on magnetic tape may consist of a wide variety of information recorded in either structured or non- structured formats depending upon the type of associated computer system. Computer magnetic tapes may contain streams of binary signals in no common codes or language. Regardless of the type of information used in the text (coded or binary stream), the format (structured or non-structured), and the arrangement of bits as recorded on the source tape is preserved accurately. Bits may be added to the binary stream to create ASCII characters for transmission; however, this must be accomplished in a standard manner to allow the receiving station to strip these added bits and record on the receive magnetic tape a mirror image of the bits as recorded on the source tape.

15.0 CIC SHREDOUT REQUIREMENTS

15.1 The Air Force performs unique Data Pattern message processing at the Lowry TCC known as "CIC Shredout". Shredout differs from normal Data Pattern Processing in that received messages go straight to an Intermediate Access Storage (IAS). The messages are placed on IAS until a "pull" is requested by the customer. Messages are checked for specific RI, CIC, LMF and SEC combinations, and are placed in separate file groups on disc based on those combinations.

The current names of these file groups, along with their block size on output, security, LMF, CIC and Routing Indicators are listed in the table below.

FILE	BLK SZE	SEC	LMF	CIC(s)	RI
Z7110150	800	U,E	C	FFJJ	RUVEGAA
Z7110151	2200	U,E	C	FFEH DFEH IFEH FMEZ FMFZ	RUVEGAA
Z7110152	1500	U,E	D	FDDB	RUVEGAA
LOWRYACD	80	U,E	C	FDDB FDDZ	RUVEGAC
Z7110154	1500	U,E	D	FFEA	RUVEGAA
FITZUNCL	80	U,E	C	ADJA ADJC ADJT ANBL AHDT ANBC AD	RUVEGAD
Z7110156	1500	U,E	D	FFEB	RUVEGAA
Z7110157	800	U,E	C	FFCI	RUVEGAA
Z7110158	800	U,E	C	AFAG DFAG FFAG NFAG IFBB	RUVEGAA
FITZBINE	1500	U,E	B	ANCE	RUVEGAD

Messages arriving at the TCC having the above combinations of RI, CIC, LMF and Security Classification must be stored in such a manner that all messages associated with a given file group may be pulled from IAS upon request and written to a specified magnetic tape in the appropriate format.

15.2 A pull of a specified shredout file group will be activated by operator request from the system operator's console. Each shredout file group has predetermined output format requirements for writing to magnetic tape. These requirements and the files to which they are applicable are listed below:

15.2.1. Tape labels. The following files will be written to tape preceded by an IBM standard label: Z7110150, Z7110151, Z7110154, Z7110156, Z7110157 and Z7110158. The modules responsible for output to tape must insure that the tape being written to has a label on it. The label must be read, validated, updated appropriately and rewritten to the tape prior to delivery of any message data.

15.2.2. Sequence number. File Z7110151 has a requirement for the application of a sequence number to each record written to tape. The starting sequence number for the file will be supplied by the operator. Each message delivered to that tape will have a sequence number updated by one from the previous message.

15.2.3. Block size. Message records written to tape must be buffered by the block size indicated in the table listed above in I.A. The maximum block size is 2200 characters for file Z7110151.

15.2.4. Record size. The files which contain messages of BB or DD LMF will have variable length records. These records, however, should have a maximum size of 1200 characters. Provision is made for messages which have greater than 1200 character records. All "C" LMF files will have fixed length, 80 character records.

15.2.5. Tape Density. All files except for LOWRYACD will be written to magnetic tape at 1600 Bits Per Inch (BPI). The LOWRYACD file will be written to tape at 800 BPI.

15.2.6. Output Character Set. All files except FITZBINE will be written to tape in the EBCDIC character set. The FITZBINE file will have header and trailer written in EBCDIC and all data between will be written in Binary.

15.3 Additional requirements. The modules responsible for outputting shredout files shall accumulate for output to the printer, a list of the Autodin header, the text header, the text trailer and the Autodin trailer of each message delivered to magnetic tape. Only the Autodin header and trailer will be accumulated for the FITZBINE file.

15.4 Statistics must be maintained on the total number of IAS slots in use, both in terms of total numbers and percentage of IAS slots available. Statistics must be maintained as to the number of messages in each file group and these statistics should be output each time a shredout file pull is completed. These statistics should also be available by operator request at any time.

15.5 The I-S/A AMPE operator must receive a notification and be alerted by an audible alarm whenever the number of IAS slots in use for any file group reaches 85%. Once this condition exists, the operator is to be notified every five minutes until the condition subsides. If the number of slots in use reaches 95% the operator is to be notified every minute until the condition subsides.

15.6 The operators will have the capability of rebuilding a specified shredout file from history. Parameters for this procedure should include file name, file time and UMI parameters. This capability must include recovery of all messages in each current file in the event of a catastrophic loss of the shredout disc.

15.7 Software will have the capability of purging messages associated with the largest previous file group when IAS resources reach certain critical usage thresholds.

15.8 The integrity of the Shredout File should be maintained through system reload, restart, degradation or in the event of a system operating system crash.

15.9 In order to reduce requirements for history recovery of previous shred files (i.e., those which have already been delivered), messages associated with a pull will be maintained on IAS until a subsequent pull on that file is accomplished. Thus, once a file has been pulled, those messages become a part of the previous pull for that file name.

SECTION 21.0

SERVICE MESSAGE APPENDIX

SERVICE MESSAGES

A. Description and Use.

1. Format and Classification. Standard system generated service messages are generated in JANAP format for the R-Community (AT LMF). Service messages for the Y-Community are generated in DOI-103 Special (ACP) format (AT LMF). Format and/or media exchanges are performed, as necessary, on output. All system generated service messages include FL4 and are considered either Unclassified (R-Community) or requiring "No Special Handling" (Y-Community). A proper TRC is inserted when the routing indicator requires it. The word "UNCLAS" appears in the text of R-Community service messages, but not in the text of Y-Community service messages.

2. Service Message Header. The OSRI, OSSN and TOF of the service message itself indicate the transmitting AMPE, the sequence number of the service message, and the time the service was generated. In those conditions in which the validity of the information is ephemeral (e.g., a "ZID" message), the TOF should be noted if there is doubt that the information is current.

3. Precedence. Precedence of the service message is equal to the precedence of the message being serviced except as noted in the remarks on a specific message type. In cases where a se+vice is sent in reference to a recognized Critic, the service will be Flash or Immediate. No service message is ever sent at W precedence.

4. Disposition of Rejected Messages. A message which is unacceptable due to an error is rejected on Modes I and V and an RM (Mode I) or RT (Mode V) sequence is transmitted by the AMPE to the connected station. An unacceptable message from a Mode II cannot or will not be subject to electrical (RM/RT) rejection and is removed from the system on generation of the service message.

5. Cited Header Information. The OSRI, OSSN and TOF cited in the service message text are derived from the JANAP header. In those cases in which the data received from the terminal in the header position is garbled or is not a header, this garbled data will appear in the service message text in lieu of the header. Where the service message text cites an ACP message, the OSRI and OSSN are constructed from the CID and CSN. The

TOF is the SOH-IN time of the message. If the serevice message cites an R-Community high-precedence message accepted with errors in the OSSN and/or TOF fields(s), the errored field(s) will be made all 9's (i.e., 9999 and/or 9999999).

6. Omission of CD/CSN. Where the service message pertains to a JANAP format user employing TI lines and does not concern the TI line itself, the CD and CSN will be cited as received. This is not done for services pertaining to ACP format messages, since the OSRI and OSSN are derived from the CID-CSN and repetition of the CID-CSN is not necessary.

7. Terminal Action. It should be noted that message garbling and resultant rejection can be the result of malfunction in terminal equipment, signal path (especially Mode II and Mode V), or AMPE equipment. If, in any case in which a message is rejected, a careful check of the message itself shows no error, and re-entry is successful, equipment or path malfunction should be considered as a cause and appropriate action taken. Even if the message is accepted by the AMPE with no errors in those message portions which it validates, garbled message text will result in delay in delivery and probable service action.

The reader is also referred to the current editions of JANAP128, DOI103, ACP127 and NTP4 for additional information.

8. Routing of Service Messages. Service Messages are noted in the examples as being routed to "OSRI" or "SMRI". Only JANAP format Invalid Routing Indicator service messages are routed to the OSRI of the message. All other services are routed to the stored Service Message Routing Indicator which the terminal has designated for service action. In the case of a R/Y channel, the SMRI is that of the Y component for all except invalid RI services, so that all service messages on those channels except those citing invalid routings on JANAP format messages will be routed to the Y-community RI. If the R component of a combined R/Y channel uses ACP format, invalid RI services for R-Community messages are sent to the SMRI of the R component.

9. Terminal Action The "Action Required" section indicates the action which must be taken by the terminal on receipt of the service message. This is advisory only and is intended to expand on, not supersede, terminal station operating instructions, JANAP128, DOI103, ACP127 or NTP4.

10. Special Service Message Precedence Change Condition. When the R-Component of an R/Y channel is authorized to enter ECP messages, any Y-Community service pertinent to an R-Community ECP message which normally would be ECP precedence, is made Flash instead, since ECP is not valid for the Y-Community.

3. Service Message Examples.

The following service message samples cite only the actual text. The header format is shown in the first example as generated, but the header as well as the TSSN and EOMS or Trailer Card are modified on transmission as appropriate to the receiving terminal. The generating AMPE's Service Operator Position(SOP) is an addressee of the service message except as noted in the examples. Examples show texts of both communities, with and without the cited CID-CSN.

The headers of service messages generally conform to the examples below, one for each community. These are the headers as generated;as noted above, format and medium exchange will be performed as necessary.

R-Community Service Message Example. (Invalid Header text is used for illustration only).

```
         RTTUZYVW RUXXCSD4213 1231506-UUUU--RUXXABA RUXXCUA.
         ZNR UUUUU
(TEXT)   UNCLAS SVC ABA127 RUXXABA1296 1231504
(TEXT)   INVALID HEADER REJ
         #4213
         (2 CR, 8 LF)
         NNNN
```

REMARKS:
ZYVW - CIC indicating a service message
RUXXCSD - CSD indicates a system generated service message; for an AMS service message this is CSR.
RUXXCUA - SOP RI reserved for system generated messages.
ABA 127 - TI line of cited message. Not present if terminal does not use TI lines or if message refers to CD or CSN.

Y-Community Service Message Example (Invalid Header text is used for illustration only).

```
        OTTMZYVW YEXXSVD4214 1231507-MNSH--YEXXBA YEXXSZ
        ZNY MMNSH
        ZYH
        ZEM
(TEXT)  SVC AYA143 YEXXAYA1402 1231503
(TEXT)  INVALID HEADER REJ
        #4214
        (2 CR, 8 LF)
        NNNN
```

REMARKS: YEXXSVD - SVC indicates a system generated service message; for the AMS service message, this is SVR.

YEXXSZ - SOP RI reserved for system generated service messages.

ZYH - This operating signal appears only in service messages of Flash and Immediate precedence.

ZEM - This operating signal indicates that start of text follows.

AYA123 - TI line of cited message. Not present if terminal does not use TI lines or if message refers to CD or CSN. A 4-digit CSN is used on ETR channels.

Note that the word "UNCLAS" does not appear in Y-Community service messages.

1. REPROTECTION REQUIREMENT, GENERAL.

```
TEXT
UNCLAS SVC ABA123 RUXXABA1234 1231225
REPROTECT TO ALL ADDRESSEES
```

PRECEDENCE:	Message
COMMUNITY:	Both
ADDRESSEES:	SMRI, SOP

CIM CATEGORY: None

CONDITIONS: Framing character error; internal AMPE error; invalid character on ASCII TTY channel; cancel received in mid-message from Mode I TI-using terminal.

AMPE ACTION: Message rejected.

ACTION REQUIRED: Reprotect message; Mode I terminal monitor for equipment trouble if service was not result of operator action; ASCII TTY terminal check tape or equipment.

2. INVALID MESSAGE HEADER.

TEXT:
SVC ACA124 YEXXACA1235 1231226
INVALID HEADER REJ (or ACC)

PRECEDENCE: Message

COMMUNITY: Both

ADDRESSEES: SMRI, SOP

CIM CATEGORY: IHR (no CIM for an "ACC" condition)

CONDITIONS: Invalid header through start-of-routing except JANAP FL2 security fields; no straggler sentinel in Y-Comm FL3; no SOR (space) in ACP format message. Data found in a card/block following the EOR in a multi-card card/magnetic tape message. No second EOR found following a PLTS header in a card or magnetic tape message.

AMPE ACTION: Message rejected, except for high-precedence accept condition. An R-Community high-precedence JANAP message may be accepted with some errors; in this case the service text reads "ACC" in lieu of "REJ."

ACTION REQUIRED: If message was rejected, correct as necessary and reprotect. If accepted, message may be received by addressee(s) with erroneous fields (9's); correct and reprotect as suspected duplicate at discretion.

3. INVALID ROUTING FIELD.

TEXT:
UNCLAS SVC ABA125 RUQQABA1237 1231232
INVALID ROUTING FIELD REJ

PRECEDENCE:	Message
COMMUNITY:	Both
ADDRESSEES:	SMRI, SOP
CIM CATEGORY:	RFR
CONDITIONS:	Errors in routing indicator field, including any character that is not lower case five-level teletypewriter, ASCII upper case alphabetic (capital letters) or a valid separator (space); error in end-of-line sequence; erroneous or missing end-of-routing symbol or sequence: RI of over 7 characters; a Y-Community message has an RI not beginning with Y; mixed R and Y RI's in any message from an R/Y channel.
AMPE ACTION:	Message rejected.
ACTION REQUIRED:	Correct RI field as required and reprotect to all addressees. No delivery is made to any RI.

4. INVALID SECURITY FIELD or INPUT SECURITY MISMATCH.

TEXT:
UNCLAS SVC RUXXBCA1238 1231234
INVALID SECURITY FIELD - REJ
- SEC
- SRC (R-Comm Only)
- TRC (R-Comm Only)
- TCC (Y-Comm Only)

PRECEDENCE:	Message
COMMUNITY:	Both (note that not all codes are applicable to both communities)

AMPE ACTION: Message Rejected.

ACTION REQUIRED: Correct security field error and reprotect message to all addressees. If rejection is due to input security mismatch and the message security or ALPS usage should be authorized, contact the AMPE for assistance. If rejection is result of attempt to transmit an unauthorized message security, consult terminal operating procedures or reprotect message by other means if possible.

5. UNAUTHORIZED USE OF EMERGENCY COMMAND PRECEDENCE (Y).

TEXT:
UNCLAS SVC ABA127 RUXXABA1239 1231341
UNAUTHORIZED USE OF ECP REJ

PRECEDENCE: Immediate

COMMUNITY: R-Only

ADDRESSEES: SMRI, SOP

CIM CATEGORY: IHR

CONDITIONS: Terminal not authorized use of ECP has attempted to enter message of that precedence; a garbled entry contained the letter "Y" in the precedence field.

AMPE ACTION: Message Rejected

ACTION REQUIRED: If reject was caused by an error, correct message header and reprotect; if message is ECP and terminal should be authorized its use, contact the AMPE for assistance. Re-entry of an ECP message as a result of a later discontinued alternate route condition must be in accord with procedures outlined in JANAP128/ACP127.

6. UNAUTHORIZED USE OF A COLLECTIVE ROUTING INDICATOR (CRI).

TEXT:
UNCLAS SVC RUXXBCA1242 1231343
UNAUTHORIZED USE OF CRI REJ

ADDRESSEES: SMRI, SOP
CI4 CATEGORY: SFR
CONDITIONS: Terminal attempted to enter message for which the channel is not cleared (REJ); terminal not authorized ALPS use attempted to enter ALPS message (TRC/TCC). Errors in other security fields result in reject codes as indicated by the diagram below:

```
R-Comm, FL2

      RATCZYUW RUXXCSA0001 1232341-CCBB--RUXXCSA.

        SEC                          SEC TRC

Y-Comm, FL2

      RATMZYUW YEXXSVA0001 1232341-MNSH--YEXXSV.

        SEC                         SEC  TCC

R-Comm, FL4

   -ZNR(sp)       -ZNR(sp)          ZNR UUUBB/AAAAA/BBBB/CCCC/DDDD

REJ(JANAP128)   REJ(ACP127)          SEC TRC SRC (up to 4 SHD's)

Y-Comm, FL4

     -ZNY(sp)  -ZNY(sp)                ZNY MMNSH

REJ(DOI-103)    REJ(DOI-103 Special)  SEC TCC
```

Note that an error in R-Community TRC field is coded as -TRC whether or not a true TRC may have been intended. The same is true of an erroneous FL4 termination which appears as an SHD(SRC) error even though no SHD may actually be intended, as, for example, the presence of redundant characters which the program may interpret as an invalid Special Handling code.

PRECEDENCE: Message
COMMUNITY: Both
ADDRESSEES: SMRI, SOP
CIM CATEGORY: RFR
CONDITIONS: A Collective RI beginning with RCHR (R-Community) or YCHR (Y-Community) has been selected in a message from a terminal not authorized its use. Also generated when a Collective RI beginning with RUCH (R-Community) or YECR (Y-Community) has been detected in a message from any terminal.

AMPE ACTION: Message Rejected. Other, non-collective RI's are not protected.

ACTION REQUIRED: If reject caused by error, correct error and reprotect message to all addressees. If an attempt was being made to re-enter a collectively routed message received from the AMPE, consult local station procedures for correct message handling. If the use of a CRI is legitimate and should be authorized, contact the AMPE for assistance. If the use of a CRI is not authorized, reprotect message using the correct single RI for each of the collective addressees.

7. INVALID RECORD COUNT FIELD.

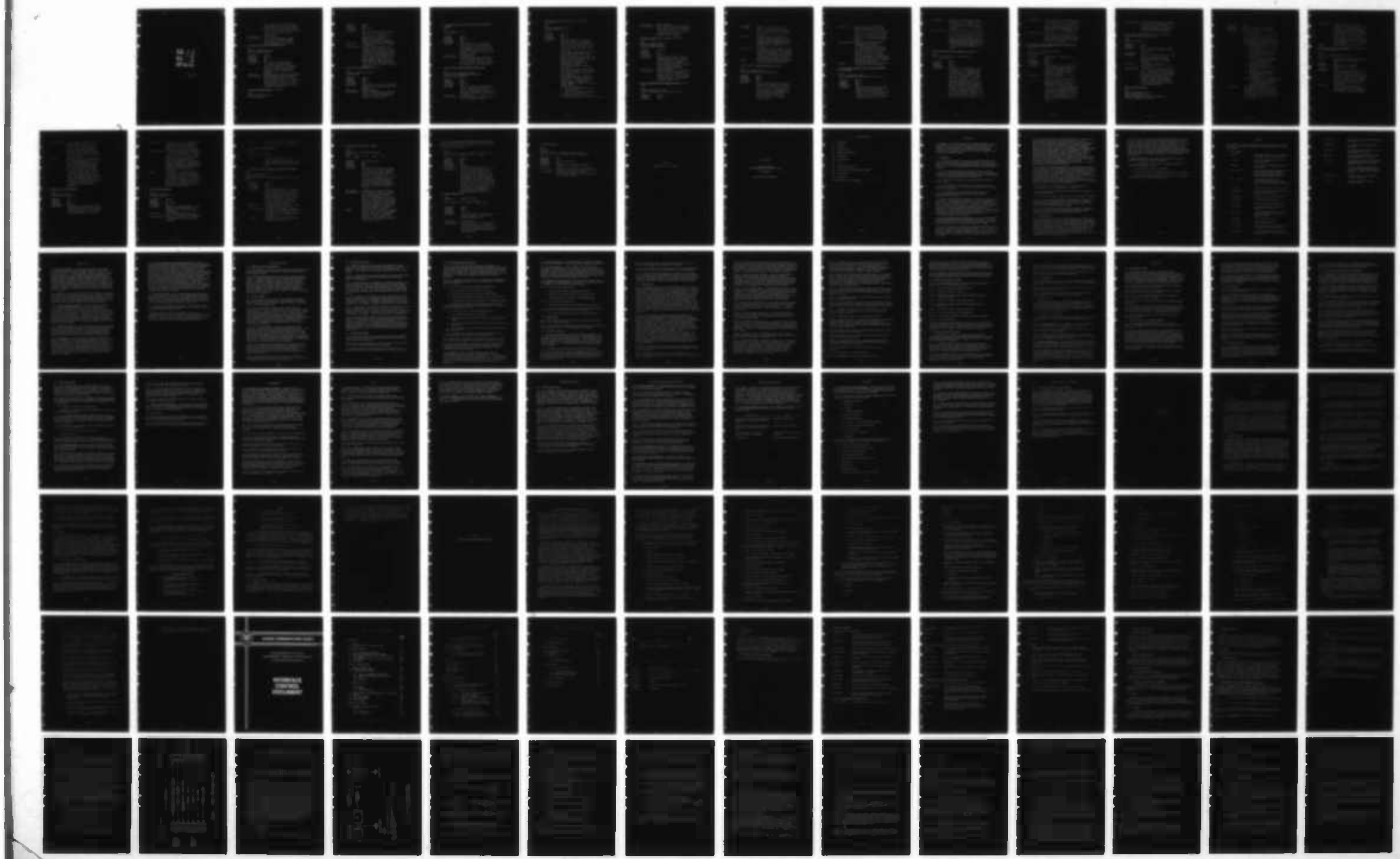
TEXT:
UNCLAS SVC RUXXBCA1244 1231345
INVALID RECORD COUNT REJ

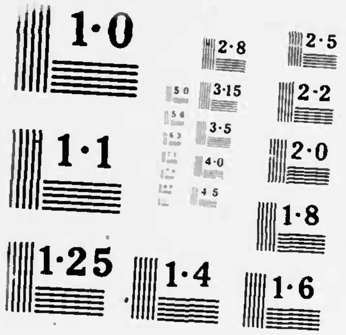
PRECEDENCE: Message
COMMUNITY: Both
ADDRESSEES: SMRI, SOP
CIM CATEGORY: RCR
CONDITIONS: Card or Magnetic Tape multi-card messages only. The header record count is not a numeric field between 0003 and 0500, MTMS or PLTS. If a count is in the header, the actual number of records (cards/

AD-A134 884 INTER-SERVICE/AGENCY AUTOMATED MESSAGE PROCESSING
EXCHANGE PROGRAM FUNCTI..(U) DEFENSE COMMUNICATIONS
AGENCY ARLINGTON VA 01 NOV 83

5/7

UNCLASSIFIED F/G 17/2 NL





NATIONAL BUREAU

MICROCOPY RESOLUT TEST

blocks) received does not match the header count; if MTMS was in the header and a count in the trailer, the actual number of records received does not match the trailer card count. The trailer card record field is not MTMS, or a numeric field.

AMPE ACTION: Message Rejected

ACTION REQUIRED: Insure card/record count is correct. The count must include both header and trailer cards as well as data cards. Reprotect to all addressees.

8. <u>EXCESSIVE LENGTH OF ROUTING INDICATOR FIELD</u>.

TEXT:
SVC ACA129 YEXXACA1243 1231353
EXCESSIVE ROUTING FIELD REJ

PRECEDENCE: Message

COMMUNITY: Both

ADDRESSEES: SMRI, SOP

CIM CATEGORY: ERR

CONDITIONS: More than 500 Routing Indicators in a message. No End-of-Routing found in 55 line blocks (56 including TI line if applicable) or 4400 data characters including header fields. Erroneous or missing EOR symbol or sequence.

AMPE ACTION: Message Rejected. No RI's are protected.

ACTION REQUIRED: Reprotect message to all addressees by making separate transmissions of no more than 500 RI's each. In exceptional cases, this service may result from an erroneous end-of-routing; correct and reprotect after insuring that actual RI count does not exceed 500.

9. <u>EXCESSIVE LENGTH OF MESSAGE</u> (non-Critic)

TEXT:
UNCLAS SVC RUXXBCA1246 1231357
EXCESS MSG LENGTH REJ

PRECEDENCE: Message
COMMUNITY: Both
ADDRESSEES: SMRI, SOP
CIM CATEGORY: ELR
CONDITIONS: Message exceeds 556 line blocks (556 cards or 44, 480 characters) from a Mode I or Mode V. Message exceeds 125 line blocks (10,000 characters) from a Mode II. Mode II channel is running out of crypto synchronization ("jumped set").
AMPE ACTION: Message rejected. No part of message is protected.
ACTION REQUIRED: If message exceeds maximum length, separate message into sections and reprotect to all addressees. For Mode II channels, if the cited message does not exceed the maximum length, insure proper restoral of the transmission path or crypto synchronization. Note that messages following the cited message may also require reprotection; if so, additional AMPE service action (ZFX) will indicate the CSN's requiring reprotection.

10. <u>INPUT HIATUS IN MID MESSAGE</u> (Non-Critic)

TEST:

```
SVC ACA132 YEXXACA1247 1231359
NO EOM RCVD REJ
```

PRECEDENCE: Message
COMMUNITY: Both
ADDRESSEES: SMRI, SOP
CIM CATEGORY: None
CONDITIONS: No data has been received by the AMPE for approximately a 3-minute period in mid-message.
AMPE ACTION: Message Rejected.
ACTION REQUIRED: Insure that EOM sequence is valid, and that there has been no equipment malfunction. Correct as necessary and reprotect to all addressees.

11. NO VALID EOM FOUND IN MESSAGE WITH AN ETX BLOCK FRAMING CHARACTER

TEXT:
UNCLAS RUXXBCA1248 1231402
INVALID EOM REJ

PRECEDENCE: Message
COMMUNITY: Both
ADDRESSEES: SMRI, SOP
CIM CATEGORY: EMR
CONDITIONS: An ETX framed block has been found without an EOM sequence appropriate to the message type. This condition can result only from terminal equipment or software malfunction on Mode I, or AMPE equipment or software error on Mode II and Mode V channels.
AMPE ACTION: Message Rejected.
ACTION REQUIRED: Reprotect message to all addressees. If condition is repeated, take steps to locate equipment problem. Mode II/V users should contact the AMPE to report the condition and request assistance.

12. INVALID CONTROL CHARACTER SEQUENCE (Mode V Only)

TEXT:
UNCLAS SVC AVA132 RUXXAVA1322 1231407
INVALID CONTROL CHARACTER SEQUENCE RECEIVED
REPROTECT TO ALL ADDRESSEES

PRECEDENCE: Message
COMMUNITY: Both
ADDRESSEES: SMRI, SOP
CIM CATEGORY: None
CONDITIONS: Mode V two-character control sequence in error. Possibility exists that a control character may be mistaken for data and text corrupted. Can only result from Mode V Control Unit malfunction.
AMPE ACTION: Reject Message
ACTION REQUIRED: Reprotect message. Take necessary steps to correct equipment problem.

13. SUSPECTED STRAGGLER (Y-Community or Low Precedence R-Community)

TEXT:
UNCLAS SVC RUXXBCA1327 1231412
SUSPECTED STRAGGLER REJ

PRECEDENCE: Immediate
COMMUNITY: Both
ADDRESSEES: SMRI, SOP
CIM CATEGORY: SSR
CONDITIONS: An actual straggler, i.e., a second message or portion of a message has been sent in the same transmission as the cited message. If this is not the case, other errors may depend on the format and medium of the cited message as follows:

- JANAP Format Teletypewriter Input-Trailer Station Serial Number (TSSN) is not present; TSSN sentinel (#) is not present; TSSN does not match Header SSN; TSSN and sentinel present but not within 23-character range of EOMS.
- JANAP Format Card/Magnetic Tape Input-Trailer card SSN missing, mispositioned, or does not match HSSN.
- ACP Format, R-Community - Sentinel (#) missing from FL3 or FL15; serial numbers do not match; TSSN not within proper range of EOMS.
- ACP Format, Y-Community - TSSN sentinel missing; TSSN and HSSN do not match; TSSN missing. (A missing HSSN (FL3) sentinel results in rejection for "INVALID HEADER"); TSSN not within proper range of EOMS.

Exceptions are made for -
(1) High Precedence R-Community (see Number 14 below)
(2) Critic (No validation is performed past the Critic sequence)

The CRITIC exception (2) is "silent"
The message is accepted and no service is sent.

AMPE ACTION: Message Rejected.

ACTION REQUIRED: Correct header and/or trailer station serial numbers as necessary and reprotect to all addresses. If a straggler is actually present, insure protection of both messages by corrections or service action as necessary.

14. SUSPECTED STRAGGLER (High precedence R-Community)

TEXT:
UNCLAS SVC RUXXBCA1328 1231417
HIGH PREC MESSAGE ACCEPTED
REPROTECT SUSPECTED STRAGGLER

PRECEDENCE: Immediate

COMMUNITY: R

ADDRESSEES: SMRI, SOP

CIM CATEGORY: None

CONDITIONS: A high-precedence (ECP or Flash) R-Community message has been accepted with straggler errors. There may or may not be an actual straggler, i.e., a second message or portion of a message sent in the same transmission as the cited high-precedence message.

AMPE ACTION: Message Accepted

ACTION REQUIRED: Insure reprotection as suspected duplicate of any actual straggler. No further action is required if service message is result of straggler number or sentinel error in the cited high-precedence message itself.

15. INVALID CHANNEL DESIGNATOR CHANNEL IDENTIFIER (TI Users Only)

TEXT:
UNCLAS SVC RUXXABA1322 1231419
INVALID CD EXPECTED ABA123 RCVD BBA123 REJ(or ACC)

PRECEDENCE: Message

COMMUNITY: Both

ADDRESSEES: SMRI, SOP

CIM CATEGORY: COR

CONDITIONS: Channel identifier in TI line was found in error. The expected CD and CSN are extracted from the ASC tables; the received CD and CSN are quoted as received.

AMPE ACTION: Y-Community messages are rejected. (Critic messages are accepted with CD error but no service message is sent.) R-Community ECP and Flash messages are accepted ("ACC") if there are no other error conditions; all others are rejected.

ACTION REQUIRED: If message was rejected ("REJ"), correct channel identifier and reprotect message; if message was accepted ("ACC"), message need not be reprotected. In either case, terminals using a Transmission Identifier Line generator should take action to correct a possible equipment malfunction.

REMARKS: Since this message concerns the CD-CSN, no CD-CSN is cited in the SVC line.

16. INVALID CHANNEL SEQUENCE NUMBER (TI Users Only)

TEXT:

```
UNCLAS SVC RUXXABA1323 1231419
INVALID CSN EXPECTED ABA127 RCVD ABA133 ACC
```

PRECEDENCE: Message

COMMUNITY: Both

ADDRESSEES: SMRI, SOP

CIM CATEGORY: None

CONDITIONS: Channel sequence number in TI line did not match that expected. The expected CD and CSN are extracted from the AMPE tables; the received CD and CSN are quoted as received. Not applicable to Critic messages. This message may also be sent if an AMPE program reload required resetting of input CSN's. If this is the case, the expected CSN will be 001.

AMPE ACTION: Message accepted with any CSN error other than a duplicate of the last accepted (see next example). If the CSN is non-numeric, it is accepted as if it were the one expected and the AMPE counter is incremented. If the CSN is numeric, it is accepted and the AMPE counter set to next expect one number higher.

ACTION REQUIRED: The message was accepted therefore reprotection is not required. If accepted CSN is numeric, it is suggested terminal continue in that range if possible and reprotect messages associated with any missing CSN's as indicated by CSN range message (ZFX) which will accompany this service message. Terminals using a Transmission Identifier Line Generator should take action to correct equipment malfunction if necessary.

REMARKS: Since this message concerns the CD-CSN, no CD-CSN is cited in the SVC line.

17. CHANNEL SEQUENCE NUMBER DUPLICATE OF LAST CSN ACCEPTED (TI Users Only)

TEXT
UNCLAS SVC RUXXABA1324 1231423
DUPE CSN EXPECTED ABA135 RCVD ABA134 REJ (or ACC)

PRECEDENCE: Message
COMMUNITY: Both
ADDRESSEES: SMRI, SOP
CIM CATEGORY: CNR

CONDITIONS: Channel Sequence Number in TI line is identical to that last accepted. The expected CD-CSN are from the ASC tables. The received CD-CSN are quoted as received; the received CSN will always be one less than that expected. Not applicable to Critic messages.

AMPE ACTION: R-Community high precedence (ECP and Flash) messages are accepted; Y-Community Critic messages are accepted with a duplicate CSN, but this service message is not sent. All other messages are rejected.

ACTION REQUIRED: If cited message was accepted, terminal may continue in this CSN range. No CSN range (ZFX) message is generated under the duplicate CSN condition. Terminals using a Transmission Identifier Line Generator should take action to correct equipment malfunction if necessary. If message was rejected, insure reprotection of the message to all addressees. The expected CSN cited remains the next expected.

18. CHANNEL SEQUENCE NUMBER(S) MISSING (TI Users Only)

TEXT:
UNCLAS SVC (this line not in Y-Comm message)
ZFX ABA128 THRU ABA132

PRECEDENCE: Immediate

COMMUNITY: Both

ADDRESSEES: SMRI, SOP

CIM CATEGORY: None

CONDITIONS: The AMPE has detected an "open number" condition, i.e., a transmission has been received with a CSN higher than the next expected. Because of CSN "rollover", a lower CSN will be interpreted as a higher one, e.g., CSN's received in the order 423, 424, 420, will cause generation of a service message citing 425 through 419 as ZFX. Where only one CSN, 148 for example, is missing, the message cites "ZFX ABA148 THRU ABA148". The cited range may include transmissions rejected for other reasons. This message may also be sent if a program reload at the AMPE required resetting CSN's to zero. If this is the case, the first number cited will be 001.

AMPE ACTION: The last CSN accepted becomes one higher than the second cited. The next expected is one more higher. In the examples above, terminal RUXXABA sent ABA127, then ABA133. The latter was accepted, and the terminal advised that ABA128-132 were open numbers. The next expected is 134.

ACTION REQUIRED: Reprocess as required duplicate any message transmission made under the CSN(s) cited. Terminals using a Transmission Identifier Line Generator (TIG) should take action to correct equipment malfunction if necessary.

19. TWO CONSECUTIVE SOM SEQUENCES RECEIVED WITHOUT AN INTERVENING EOM (Mode II/V Only)

TEXT:
UNCLAS SVC ABA133 RUXXABA1346 1231426
TWO CONSEC SOMS REJ

PRECEDENCE: (First) Message: Immediate if no message.

COMMUNITY: Both

ADDRESSEES: SMRI, SOP

CIM CATEGORY: TSR

CONDITIONS: The AMPE has received two consecutive start-of-message (ZCZC) sequences without an intervening end-of-message sequence. The message cited is incomplete. A second message may or may not be involved.

AMPE ACTION: The first transmission is rejected. An exception is made for a recognized Critic, but in that case, no service message is sent. If a second message is involved, it is accepted, barring other errors, on a Mode II channel; it is rejected on Mode I and V. If no first message is involved and there are merely two SOM's ahead of a message, the precedence of the service is Immediate, and the SVC line may contain irrelevant data, such as X's or spaces. The next expected CSN is one higher than that associated with the first SOM.

ACTION REQUIRED: Insure that no SOM sequence is actually present in cited message; reprotect cited message to all addressees. Terminals using a Transmission Identifier Line Generator should take action to correct any equipment malfunction.

20. CHANNEL CONTINUITY VERIFICATION (Mode II or Specially Classmarked Y-Community Channels Only)

TEXT:
UNCLAS SVC ZID ABA142

PRECEDENCE: Priority

COMMUNITY: Both

ADDRESSEE: SMRI (In the case of specially classmarked Y-Community channels, a special RI is used)

CIM CATEGORY: None

CONDITIONS: No traffic has been received by the AMPE for a period of 30 minutes. For specially designated Y-Community channels, the interval is reduced to 15 minutes.

AMPE ACTION: The message is repeated at 30 minute intervals so long as no traffic is received.

ACTION REQUIRED: If station records show that the cited CSN is the last transmitted,no further action is necessary. If station records not show that the cited CSN is the last transmitted, the terminal station must establish contact with the AMPE to determine traffic status and, when channel continuity has been restored, to reprotect the message(s) associated with any missing CSN(s).

21. INVALID ROUTING INDICATORS

TEXT:
UNCLAS SVC RUXXBCA1278 1231245
INVALID ROUTING REPROTECT TO:
RUXXBBA-INV RUXXALA-SEC RUXXFMA-LMF RUXXLLA-INV
RUXXJJA-INV RBFBCS-TRC RUXXJBA-SRC

PRECEDENCE: Message

COMMUNITY: Both

ADDRESSEES: SMRI; SOP of original (entry) AMPE.

CIM CATEGORY: RIR (each invalid RI is counted as a separate violation).

CONDITIONS: The cited message cannot be delivered to the listed RI(s) for the reason(s) given. The message is protected to other RI(s). The codes and the community to which they are applicable are as follows:

INV - The RI does not appear in the AMPE routing tables (R and Y)

SEC - Message basic security classification exceeds the level authorized for the addressee. (R)

LMF - The addressee terminal equipment cannot accept a message in this medium and message exchange is prohibited.

TRC - The RI listed is not validated by a proper Transmission Release Code or the addressee cannot accept ALPS traffic (R).

SRC - The addressee cannot accept a message of the Special Handling Designator of the cited message.(R)

TCC - The addressee cannot accept a message containing the Transmission Control Code of the cited message (Y).

MFE - The message is of data pattern and is either piloted or does not contain a security line (FL4). Delivery to the addressee teletypewriter station is prohibited.

AMPE ACTION: The message is protected to RI's other than those cited. Note that another AMPE may find other RI's to be invalid and there may be other services on the cited message. If all RI's are invalid, the message is rejected to Mode I and Mode V terminals.

ACTION REQUIRED: Determine the correct routing indicator(s) and reprotect only to those necessary. There is no separate or distinct message indicating that all RI's are invalid and it is incumbent on the terminal operator to insure proper reprotection of the message to all addressees whose RI's were found invalid. Because more than one service message may be received for invalid RI's on the same message, all such service messages must be honored.

REMARKS: This service lists 5 RI's per line.

22. HIGH-PRECEDENCE MESSAGE ACKNOWLEDGMENT (R-Community Mode II, all Y-Community channels)

TEXT:
UNCLAS SVC R Z ABA143 RUXXABA1438 1231527

PRECEDENCE: Immediate for acknowledgment of ECP and Flash; Flash for acknowledgment of Critic.

COMMUNITY: Both

ADDRESSEES: SMRI; Special RI's on CRITIC Acknowledgment, see Remarks.

CIM CATEGORY: None

CONDITIONS: Transmitted to the terminal from which the high-precedence message was received. Transmitted at EOM-IN time for ECP and Flash. Transmitted at ECM-ACK time for Critic, i.e., transmission of this message for a Critic indicates the original AMPE has transmitted the Critic, not merely accepted it for transmission.

AMPE ACTION: Flash or ECP message accepted; Critic message transmitted and electrical acknowledgment received. AMPE accepts full responsibility for the message.

ACTION REQUIRED: File for record purposes. If no acknowledgment is received on transmission of a high-precedence on a Y-Comm channel or a Mode II R-Comm channel, insure circuit continuity and contact the AMPE for assistance. Reprotect the high precedence message as suspected duplicate and/or by other means as necessary.

REMARKS: The letter "R" stands for "received"; the second letter is the precedence of the acknowledged message, W, Y or Z. For Critic acknowledgment only: The OSRI is the pre-stored prime channel RI. If the terminal uses TI lines, the OSSN is the CSN with a leading zero, if the terminal does not use TI lines, the OSSN is 9999. The TOF is the SOH-IN time, not the time the Critic was transmitted onward by the AMPE- the transmission time is the TOF of the service message itself. The CD-CSN, if any, are not separately cited. A copy of this message is also sent to NSA and to DCA at Immediate precedence.

23. PARTIAL CRITIC MESSAGE RECEIVED

TEXT:
SVC YEXXAYA0123 1231446
PARTIAL WW MESSAGE RECEIVED

PRECEDENCE: Flash
COMMUNITY: Y
ADDRESSEES: SMRI, SOP
CIM CATEGORY: None
CONDITIONS: Generated when a Critic message being received experiences an input hiatus of approximately 60 seconds, a two consecutive SOM condition, or is over 75 line-blocks (6000 characters) in length.

AMPE ACTION: This service, like the high-precedence acknowledgment for Critic ("RW"), is generated when the original AMPE has transmitted the partial Critic and received an electrical acknowledgment.

ACTION REQUIRED: If the Critic was transmitted incomplete, file for record purposes. If a complete message was transmitted, take action to insure circuit continuity and retransmit message or reprotect by any alternate means in accordance with station operating instructions. If the message is over 75 line blocks, reprotect entire message by separating into sections or reprotect the portion over 75 line blocks as directed by station operating instructions.

REMARKS: The CD-CSN are not separately cited in this message. The OSRI is the prime channel (pre-stored) RI for the channel. The OSSN is the CSN with a leading 0. If the channel does not use a TI line the OSSN is 9999. The TOF is SOH-IN time, not the time of transmission from the AMPE, which is indicated by the TOF of the service message itself.

24. CRITIC MESSAGE FORWARDED

TEXT:
SVC YEXXAYA 0122 1231442
WW MESSAGE FORWARDED

PRECEDENCE: Immediate

COMMUNITY: Y

ADDRESSEES: NSA, DCAOC

CIM CATEGORY: None

CONDITIONS: Generated by each AMPE handling a CRITIC message at the time the electrical acknowledgment is received for a transmitted Critic.

AMPE ACTION: Critic message transmitted to either destination terminal or another AMPE.

ACTION REQUIRED: File for record purposes; other handling in accordance with current operating procedures.

REMARKS: Allows "tracking" of a Critic message by NSA and DCAOC. Aids in recognizing and correcting any transmission delays.

25. PARTIAL CRITIC MESSAGE FORWARDED

TEXT:
SVC YEXXAYA0123 1231446
PARTIAL MM MESSAGE FORWARDED

REMARKS: This service message pertains to a partial (truncated) Critic. All other information shown above for Critic Message Forwarded applies to this message also.

26. AUTODIN LIMITED PRIVACY SERVICE (ALPS) REPROTECT MESSAGE

TEXT:
UNCLAS SVC RUXXBCA1332 1231450
AMS-REPROTECT MESSAGE TO:
RUXXABA RUXXBBA RUXXCBA RUXXCCA RUXXDDA RUXXEEA RUXXFFA RUXXGGA
RUXXHHA

PRECEDENCE: Message

COMMUNITY: Both

ADDRESSEES: SMRI; SOP

CIM CATEGORY: None

CONDITIONS: Since ALPS message text is not recorded on the AMPE history record, an ALPS message cannot be retransmitted by the AMPE at the request of an addressee or recovered after an AMPE failure. When retrieval/recovery is necessary, this service is generated to the message originator listing the RI's to which retransmission must be made.

AMPE ACTION: No further action is taken on the message after generation of this service.

ACTION REQUIRED: Retransmit cited message as suspected duplicate to all listed RI's. Note that more than one service message may be received for the cited message; all must be honored.

REMARKS: The OSRI of this service message reads "RUXXCSR" instead of "RUXXCSD". There are eight RI's to a line.

27. ALTERNATE ROUTING INVOCATION MESSAGE.

```
TEXT:
UNCLAS SVC
TRAFFIC IS BEING DIVERTED TO YOUR STATION,
PROTECT TO:
RUXXAB    RUXXBC    RUXXCD    RUXXDE    RUXXEF
RUXXFG    RUSSGH
```

PRECEDENCE: See conditions below

COMMUNITY: Both

ADDRESSEE: SMRI

CIM CATEGORY: None

CONDITIONS: The header of this message is exactly like that of a normal service message. Its precedence is normally Immediate, but may be Flash if high-precedence traffic will be subject to the diversion. For example, if all traffic is to be diverted, the notification message will be Flash precedence. The notification message is placed at the head of the queue by precedence, so that it will precede any diverted traffic.

AMPE ACTION: Implementation of alternate routing

ACTION REQUIRED: Protect diverted traffic in accordance with established altroute agreements and/or local procedures. Note that each invocation message lists only those RI's whose traffic is now being diverted. The terminal remains responsible for protection of traffic to RI's listed in any previous alternate route invocation message until a specific revocation message is received.

REMARKS: Only the first six characters of diverted RI's are given. These are all AUTODIN actually routes on. The seventh RI character, if present, of diverted traffic may be any alphabetic. In this message and the following one there are five RI's to a line.

28. Alternate Routing Revocation Message - The second message transmitted to a terminal as a result of AMPE alternate routing activity advises that traffic for certain RI's will no longer be diverted to the terminal.

TEXT:
UNCLAS SVC
TRAFFIC IS NO LONGER BEING DIVERTED TO YOUR STATION FOR:
RUXXBC RUXXCD RUXXDE RUXXEE RUXXFG

PRECEDENCE:	Immediate
COMMUNITY:	Both
ADDRESSEE:	SMRI
CIM CATEGORY:	None
CONDITIONS:	See above
AMPE ACTION:	Revocation of alternate routing
ACTION REQUIRED:	Continue to protect diverted traffic for any RI's previously listed in an invocation message but not listed in this message. In the examples, the terminal must still protect for RUXXAB and RUXXGH, whose altroutes have not been revoked. Any traffic subsequently received for RI's listed in this message (because traffic was on the AMPE output queue at time of revocation) may be protected either in accordance with WARP or by re-entry into AUTODIN, as prescribed by local procedures and applicable operating instructions.

29. INVALID FORMAT LINE 12

TEXT:
UNCLAS SVC: RUXXBCA1327 1231412

Inavlid Format Line 12 or Security Mismatch - REJ
ACC

PRECEDENCE:	Message
COMMUNITY:	Both
ADDRESSEES:	SMRI, SOP
CIM CATEGORY:	
CONDITION:	The security in format line 12 is not expanded properly or does not match security in format line 2.
AMPE ACTION:	Reject Message.
ACTION REQUIRED:	Correct the security field in error and reprotect message to all addressees. If the error occurred on a high precedence message indicating correct security and transmit message at the next lower precedence level.

30. AMPE Reload Message

TEXT:
2CR, 8LF
UNCLAS SVC
RUXX AMPE RELOADED. ANY MESSAGES PARTIALLY RECEIVED
IMMEDIATELY PRIOR TO THIS MESSAGE WILL BE RETRANSMITTED.

PRECEDENCE: Flash
COMMUNITY: Both
ADDRESSEES: All connected stations
CIM CATEGORY: None
CONDITION: Generated when an AMPE has performed a reload.
AMPE ACTION: This service message is the first message transmitted to each channel following a reload.
ACTION REQUIRED: Take note whether preceding message was incomplete, annotate logs and handle as cancelled message received.

SECTION 30

COMPUTER SECURITY REQUIREMENTS

SECTION 30.0

Inter-Service/Agency
Automated Message Processing Exchange

(I-S/A AMPE)

System Security Requirements

Table of Contents

INTRODUCTION

1.0 Purpose. This section specifies the multilevel security (MLS) requirements for the Inter-Service/Agency Automated Message Processing Exchange (I-S/A AMPE) Program. It contains the system security requirements and taskings to ensure certification and subsequent accreditation. Furthermore, it provides the basis for developing the Functional System Specification.

1.1 Background

1.1.1 The I-S/A AMPE Program is an element of the Integrated AUTODIN System Architecture (IASA). The overall objective of the IASA is the design of a common-user data communications system for the Department of Defense (DoD). The I-S/A AMPE Program contributes to that objective by providing:

a. The minimum essential functional capabilities and features necessary to functionally replace the existing Service and Agency base -level Automated Message Processing Exchanges and meet validated Service and Agency automated telecommunications requirements.

b. A functional replacement for the current AUTODIN Switching Centers (ASCs).

c. An interface for the AUTODIN community of terminals to the Defense Data Network (DDN) using Host-To-Host Protection (H^2P) devices (e.g., BLACKER Program).

d. A capability to consolidate Defense Special Security Communications System (DSSCS) and General Service (GENSER) telecommunications centers.

1.1.2 When initially deployed, separate I-S/A AMPEs will be employed for the GENSER or "R" community and the DSSCS or "Y" and "Y/R" community. (Note that "Y/R" terminals are in fact "Y" terminals allowed to pass "R" traffic in addition to their normal "Y" traffic.) Communications between I-S/A AMPEs will be via a multilevel secure backbone (i.e., the ASC network or the Defense Data Network with BLACKER Host-to-Host Protection). Each employment of the I-S/A AMPE shall be designed to be certifiable to support a multilevel secure accreditation. The I-S/A AMPE will be subjected to extensive design analyses, testing, and certification leading to accreditation.

1.2 General Multilevel Security Objectives. The following paragraphs provide an overview for the I-S/A AMPE security measures. The reader should consult Section 10.0 of the FRD as well as the "Trusted Computer System Evaluation Criteria" glossary for definition of terms.

1.2.1 The I-S/A AMPE is to be designed to support current DoD policies concerning the protection of classified information. The policies deal with authorizations to access information based on: security level clearances, security compartment (category) authorizations, need-to-know, and the combination of security classification and compartments of information.

These policies are contained in DoD Regulation 5200.1-R, "Information Security Program Regulation"; DoD Directive 5200.28, "Security Requirements for Automated Data Processing (ADP) Systems"; DoD Directive 5215.1, "Computer Security Evaluation Center", Defense Intelligence Agency Manual DIAM 50-4, "(C) Security of Compartmented Computer Operations (U)"; DoDD C-5030.58, "(C) Consolidation of Telecommunications Centers Involving Defense Special Security Communications Systems and General Services Communications (U)"; DoD C-5030.58M, "(C) Defense Special Security Communications Systems--Security Criteria and Telecommunications Guidance (U)"; USSID 702,"(C) Automatic Data Processing (ADP) Systems Security (U)"; SM 36-76, "(S) Safeguarding the SICP(U)"; DCID 1/16, "(C) Security of Foreign Intelligence in Automated Data Processing Systems and Networks(U)"; and in the DCA "Inter-Service/Agency Automated Message Processing Exchange (I-S/A AMPE) Selected Security Architecture" memorandum.

1.2.2 Messages and data processed by the I-S/A AMPE will be of varying security levels and security compartments encompassing the full range of DoD classifications, including unclassified. Furthermore, the I-S/A AMPE will support users (i.e., subscribers, subjects, and individuals) having various clearances and authorizations which span a range for which an I-S/A AMPE has been accredited. The I-S/A AMPE is to be certifiable and accreditable as a multilevel secure and compartmented mode telecommunications system. To meet these accreditation requirements, the I-S/A AMPE system must have computer security, reliability, and integrity features to ensure that the I-S/A AMPE prevents:

(a) Deliberate or inadvertant access to classified material by unauthorized users (i.e., subscribers and individuals),

(b) Unauthorized manipulation of the I-S/A AMPE and its associated peripheral devices, and

(c) Both loss of system integrity and loss of information integrity.

1.2.2.1 The I-S/A AMPE must provide reliable information that will aid in the discovery and investigation of: (a) Violations or attempted violations of DoD Security Policy; (b) Technical attacks against the I-S/A AMPE oriented towards denial of service.

1.2.2.2 The I-S/A AMPE must provide isolation mechanisms complementary to the secure operating system to provide the protection support necessary to meet the criteria specified in this document.

1.3 Design Criteria.

1.3.1 Trusted Computing Base (TCB) requirements are an integral part of the total I-S/A AMPE solution and are not to be developed independently from other requirements. The TCB is to be developed along with the other functional requirements of the I-S/A AMPE as specified in the I-S/A AMPE Functional Requirements Description (FRD). Correspondence shall be shown between each level of MIL-STD-490 A-, B-, and C-Specifications as the design is further refined. Complete correspondence from the security policies down to the Configuration Item (CI), Computer Program Configuration Item (CPCI), and Computer Program Component (CPC) levels of implementation shall be demonstrated.

1.3.2 The Class A1 of the Trusted Computer System Evaluation Criteria requires the use of formal methods to specify and verify the design of the TCB. Formal verification begins with the development of a mathematical model implementing the DoD security policies. A Formal Top Level Specification (FTLS) shall be developed and verified for all elements of the I-S/A AMPE system that implement the formal security model. The FTLS shall be written using a government approved verifiable formal specification language or equivalent. A mapping shall be provided between the High Order Language implementation of the TCB and the verified FTLS.

1.4 Section 30 Overview. This part of the FRD uses the following structure to divide the information presented.

a. An introduction and bibliography of referenced documents is presented in paragraphs 1 and 2.

b. Security policy is stated in paragraph 3.

c. The actual functional requirements are identified in paragraph 4.

d. Paragraphs 5 through 12 define the contractor taskings required to support the intensive design and analysis.

DOCUMENTS

2.1 General. Documents identified in this paragraph are binding on the contractor only to the extent specified in the requirements section of this document.

2.2 DoD Documents.

AFNAG-5B	"(C-NOFORN) Red and Black Engineering and Installation Criterions (U)" Mar 74
AFNAG-9A	"Using NACSEM Documents and TEMPEST Emanations Limits"
DIAM 50-4	"(C) Security of Compartmented Computer Operations (U)"
DoDD C-5030.58	"(C) Consolidation of Telecommunications Centers Involving Defense Special Security Communications Systems and General Service Communications (U)"
DoD C-5030.58M	"(C) Defense Special Security Communications Systems -- Security Criteria and Telecommunications Guidance (U)"
DoDR 5200.1-R	"Information Security Program Regulation"
DoDD 5200.28	"Security Requirements for Automated Data Processing (ADP) Systems"
DoDD 5215.1	"Computer Security Evaluation Center"
JCS SM 36-76	"(S) Safeguarding the SIOP(U)"
JCS Pub 22	"WWMCCS ADP System Security, Jan 80"
MIL-HDBK 232	"Red/Black Engineering Installation Guidelines", 14 Nov 72
MIL-STD-483	"Configuration Management Practices for Systems, Equipment, Munitions, and Computer Programs"
MIL-STD-490	"Specification Practices"
MIL-STD-881A	"Work Breakdown Structure"
MIL-STD-1521C	"Technical Reviews and Audit for Systems, Equipment, and Computer Programs"
NACSIM 5100A	"(C) Compromising Emanations Laboratory Test Requirements, Electromagnetics (U), Jul 81"

NACSEM 5112	"(S-NOFORN) Nonstop Evaluation Techniques (U)" Apr 75
NACSEM 5201	"(S) Compromising Emanations Design Handbook (U)"
NACSEM 5203	"(C) Guidelines for Facility Design and Red/Black Installation (U)"
USSID 702	"(C) Automatic Data Processing (ADP) Systems Security (U)", 24 Sep 80
DCID 1/16	"(C) Security of Foreign Intelligence in Automated Data Processing Systems and Networks", Jun 78
	"(C) Technical Development Plan for Inter-Host Multilevel Network Security Program (U)", Computer Security Center, 18 Nov 82
CSC-STD-001-83	"Trusted Computer System Evaluation Criteria", 15 Aug 83
OMB A71-TM1	"Security of Federal Automated Information System"

SECURITY POLICY

3.1 DoD Security Policy. The DoD security requirements are stated in DoD Information Security Program Regulation 5200.1-R. Additional guidance for security of Federal automated information systems is found in OMB Circular A-71. This Circular makes the head of each executive branch, department and agency responsible "for the establishment of physical, administrative and technical safeguards required to adequately protect personal, proprietary or other sensitive data not subject to national security regulations, as well as national security data." From these fundamental regulations and the objectives (e.g., protection from unauthorized disclosure (compromise), denial of service, or unauthorized alteration) specified in paragraph 1.2 of this section of the FRD are derived the following five basic security policy requirements which must be met by the TCB.

3.1.1 Marking. The I-S/A AMPE shall maintain the integrity of security classification and other sensitivity marking labels and their unambiguous association with all information processed by the I-S/A AMPE. The I-S/A AMPE shall ensure that classified or other sensitive information is accurately marked with the received classification and other sensitivity labels when stored and when included in output from the system.

3.1.2 Mandatory Security Control. The I-S/A AMPE shall enforce the formal system of information control inherent in the security classification designation and special handling restriction set(s) associated with the information and the clearance set(s) associated with the subscribers, subjects, or individuals who may directly or indirectly request access to the information. Specifically, no subscriber, subject, or individual shall have access to classified information or material unless that subscriber, subject, or individual has been determined to possess the requisite security clearance and such access is necessary for the performance of official duties. Community separation shall always be enforced by the I-S/A AMPE.

3.1.3 Discretionary Security. The I-S/A AMPE shall enforce need-to-know access restrictions placed on information as determined by the originator of a message, the owner of information, or the Security Administrator. Need-to-know restrictions are based on Routing Indicators and Plain Language Addresses and the associated delivery attributes explicitly stated in the Attribute Table(s) and in the Access Control Mechanism.

3.1.4 Accountability. The I-S/A AMPE shall identify, authenticate, and record the identity of subscribers, operating positions, operators, and system administrators and validate their authorization for access to services and information. The I-S/A AMPE shall provide the capability for recording the individual accountability of a person in question to which access was granted or denied, the security level at which the request was made, the type of access granted, and the date and time-stamp of the access request. Additionally, the I-S/A AMPE shall provide the capability for authorized agents to securely access and evaluate the above audit information.

3.1.5 Continuous Protection of the I-S/A AMPE System. Classified information and material in the I-S/A AMPE shall be safe-guarded by the continuous employment of protective features in the system's hardware and software design and configuration control and by other appropriate administrative, physical, personnel, and communications security controls. Since mechanisms within the I-S/A AMPE will be responsible for the protection of the classified information entrusted to the I-S/A AMPE for processing, the I-S/A AMPE system shall be protected by appropriate physical means, procedures, and configuration control. Software mechanisms shall be protected beginning with their initial design and continuing throughout the life of the program. Hardware mechanisms shall be protected beginning with government approval of the C-level specification (i.e., Critical Design Review) and continuing throughout the life of the program. The I-S/A AMPE protection shall be implemented so that the Government can maintain its administration. This rigorous and continuous protection shall include recording all changes and attempted changes to the I-S/A AMPE.

3.2 Evaluation Criteria. Trusted Computer System Evaluation Criteria are a vital part of the overall I-S/A AMPE system security evaluation process as specified in DoDD 5215.1. DoD Computer Security Evaluation Center will use the Functional Requirements Description and the Class A1 Trusted Computer System Evaluation Criteria as the basis for evaluation criteria for computer security aspects of the I-S/A AMPE.

3.3 Independent Verification and Validation. The Government reserves the right to have an independent contractor(s) attend all contractor or Government held meetings and reviews.

3.4 Denial of Service. During the development, testing, and implementation of I-S/A AMPE, the availibility, reliability, and recovery features of the I-S/A AMPE which impact on authorized access to information or service, will be demonstrated and certified as reducing the denial of service threats to an acceptable level of risk.

SECURITY REQUIREMENTS

4.1 Subject and Object Identification.

4.1.1 The software and data shall be modularized and identified in a way that makes effective use of the protection features provided by the Trusted Computing Base.

4.1.2 Subject and object creation, name association, and protection attribute assignment or modification shall always take place under TCB control. An object is defined as a passive entity that contains or receives information. Software created entities such as buffers, records, files, formal messages, programs and directories as well as hardware resources such as memory blocks, disk tracks, tapes, and peripheral devices that contain the data are considered objects. A subject is defined as an active entity, generally in the form of a person, process, or device that causes information to flow among objects or changes the system state.

4.2 Security Labeling

4.2.1 Every subject and object shall have an associated label that indicates security related attributes. These labels will provide the basis for the TCB to grant access to objects by subjects in accordance with the defined security policy.

4.2.2 At a minimum, label information shall include security classifications and security compartments, which collectively are termed security label. In addition, security labels for objects shall include discretionary access control attributes. The TCB shall provide for a minimum of sixteen hierarchically ordered security classifications. These sixteen ordered classifications shall include the ordered set of classifications: UNCLASSIFIED, CONFIDENTIAL, SECRET and TOP SECRET. The system shall also provide for a minimum of 255 non-hierarchial categories. The design shall not preclude expansion to at least 512 non-hierarchical categories.

4.2.3 The TCB shall establish, associate, and preserve against alteration, a security label for each subject and for each object. Label association shall apply to the display of information as well as to manipulation within the TCB established security perimeter. The TCB shall maintain the integrity of the security label(s). The TCB shall ensure that all displayed information is clearly labeled with respect to security classification, category, and other optionally indicated access restrictions. The TCB shall ensure display information is restricted to display devices authorized access to the information.

4.2.4 Object labeling shall be satisfied at the message level and support the requirements for telecommunications processing; statistics development; generation, editing and preparation of messages; and security audit actions. The TCB shall prevent unauthorized reclassification of information and the unauthorized association of a label with information.

4.2.5 The security label parameters of an access line shall be changeable only under the control of the TCB and only with the approval of the Security Administrator, and shall be audited.

4.3 Trusted Access Control.

4.3.1 Access of objects by subjects shall be mediated by an access control mechanism within the TCB that has been certified as enforcing the Mandatory and Discretionary Access Control requirements of this document. The TCB access control mechanism shall enforce the following rules:

4.3.1.1 A subject must have satisfied Mandatory and Discretionary Access Control requirements for an object or the access shall neither be authorized nor permitted.

4.3.1.2 The security level of subjects to be used during a session (the session security level) shall be determined by the TCB before access shall be authorized. The session security level of a subject shall be verified by the TCB to be within the accredited security authorizations for the subject. Changes to the session security level of each subject shall be mediated by the TCB and shall require the initiation of a new session.

4.3.1.3 A subject shall be allowed read access to an object only if the security classification of the subject is greater than or equal to the security classification of the object and the collection of the security compartments of the object is included in the collection of the security compartments of the subject. Community separation shall be maintained.

4.3.1.4 A subject shall be allowed write access to an object only if the security classification of the subject is less than or equal to the security classification of the object and the collection of the security compartments of the subject is included in the collection of the security compartments of the object. Community separation shall be maintained.

4.3.2 The physical media containing the TCB shall be protected against unauthorized modification and shall be placed under strict configuration control. The TCB shall include mechanisms that protect it from unauthorized modification. The TCB shall be self protecting to prevent unauthorized changes. Each attempted modification to the TCB shall be rejected, an audit record of the attempt shall be made, and the Security Administrator Position shall be immediately advised of any attempt to modify the TCB.

4.4 Security Label Change.

4.4.1 The TCB shall include a privileged trusted process that allows change of security labels of system resources under explicitly defined carefully controlled conditions.

4.4.2 Only the change process(es) shall have access to an object while that object's security attributes are being changed.

4.4.3 Resources whose security labels are being changed shall be inaccessible to all but the change process until the change is complete.

4.5 Secure Management Process Control.

4.5.1 The TCB shall mediate access to processes and objects. An individual address space shall be provided for each process (often called a "per process virtual space") and the TCB shall mediate access to these spaces. The requirement for individual address space shall not preclude the sharing of contents of such address space under TCB control. The TCB shall manage in a trusted way scheduling execution time among the processes.

4.5.2 An inter-process communication (IPC) feature shall be provided for authorized cooperating processes. The TCB shall enforce "confinement" upon the IPC feature.

4.5.3 The TCB shall provide a Create-Process feature which:

a. Assigns execution space for a specific process.

b. Associates subject identity with the created process,

c. Assigns subject protection attributes to the created process.

d. Assigns address space for data accessible by the created process.

e. Guarantees that the effects of the creation process are not visible below the security level of the created process. This should not preclude the capability in 4.3.1.4.

4.5.4 The TCB shall provide a Delete-Process feature which:

a. Purges execution space from the process,

b. Purges the subject identity associated with the process to be deleted,

c. Purges the protection attributes assigned to the process to be deleted, and

d. Purges the address space for the data that was accessible by the process to be deleted.

e. Guarantees that the effects of the deletion process are not visible below the security level of the deleted process.

4.5.5 If provided, an Await-Process shall be under the control of the TCB and shall have the capability to suspend and reschedule a process.

4.5.6 The TCB shall provide a Process-Session feature that establishes to a well defined state (e.g., all zero's), security attributes and precedence to be associated with the process, or session, prior to initiating that process or session.

4.6 Trusted Path. Each I-S/A AMPE TCB shall support trusted communications paths between itself and subscribers for use when a positive TCB-to-subscriber connection is required (e.g., by the Security Administrator at the Security Administration Position). Communications via this trusted path shall be activated by the TCB or the entity at the other end and shall be logically and unmistakably distinguished from other paths.

4.7 Control Information. The information that is passed to a process shall be confined by the TCB to that information necessary for execution.

4.8 TCB Span-of-Control. In the I-S/A AMPE the TCB shall either directly or indirectly control all processes. The TCB, to meet other requirements, must be relatively small to facilitate verification and be designed for minimum impact on system throughput; thus great care must be exercised in determining which functions are part of the TCB. Of special concern are processes which allow access such as input and output. All input and output shall be under the control of the TCB.

4.9 Management of Storage Objects. The term "storage object" refers to those objects that support read and write access. The TCB shall provide the capability to create and delete storage objects.

4.9.1 The Create-Object feature shall:

a. Uniquely identify each storage area as an object,

b. Assign the security label to each storage object, and

c. Allocate the domain and extent of each storage object

4.9.2 The Delete-Object feature shall;

a. Disassociate the identity of the storage area as an object,

b. Purge the security label and the content of the storage object by changing it to a well defined state (e.g., all zeros),

c. Deallocate the domain and extent of each storage object.

4.10 Storage Reuse.

4.10.1 The TCB shall provide for the purging of each area of storage before it is introduced for reuse.

4.10.2 Requirements for elimination of residual information shall be met as specified in JCS Pub. 22, DoD C-5200.28-M, and USSID 702.

4.11 IAS Network Security.

In order to obtain access to the packet switching backbone, an A1 certified and accredited H^2P element must be in place between the I-S/A AMPE and the Defense Data Network (DDN) node. The H^2P element will be government furnished from the BLACKER program. The I-S/A AMPE to H^2P element interface that is specified will also serve as the H^2P element to DDN interface. All applicable mandatory and discretionary security shall be enforced.

4.12 Identification, Authentication and Individual Acountability.

4.12.1 The I-S/A AMPE shall identify and authenticate each subscriber and identify each operating position collocated with the I-S/A AMPE. The identification shall include the unique identity of the subscriber and its authorized security attributes as well as the terminal and its accredited security level.

4.12.2 Authentication data shall be protected so that it cannot be acquired by an unauthorized subscriber or individual.

4.12.3 The I-S/A AMPE shall associate the subscriber's identity with all auditable actions taken by that subscriber (e.g., retrieval request).

The I-S/A AMPE shall have the capability to identify and authenticate (e.g., passwords) an individual and mediate the activity of individuals at the I-S/A AMPE operating positions. In these circumstances, the I-S/A AMPE shall include the individual's identification, in addition to the subscriber identification, with all actions taken by that individual.

4.13 Security Audit.

4.13.1 All subscribers accessing the I-S/A AMPE are required to provide positive subscriber identification and have available positive individual identification for an audit trail. This is necessary to ensure that an unbroken path of responsibility can be subsequently audited. This audit trail begins with the drafters, includes the releaser, the subscriber's operator, the subscriber terminal, the I-S/A AMPE, the exit and entry to/from IAS Network, the receiving I-S/A AMPE, receiving terminal, an operator and finally the recipient; in short, writer-to-reader. Each I-S/A AMPE shall maintain an audit trail of those auditable events which occur only while a message is being processed by that I-S/A AMPE. On a subscriber basis, each subscriber shall be classmarked in the Attribute Table(s) as either requiring subscriber identification only or requiring both subscriber and individual identifications. For I-S/A AMPE operating positions both positive position and individual identifications shall be required.

4.13.2 The I-S/A AMPE shall create, maintain, and protect from modification or unauthorized access or destruction an audit trail of access to the objects it protects. The audit data shall be protected by the TCB so that read access to it is limited to those who are authorized access to audit data. The I-S/A AMPE shall be able to record the following types of events: use of identification and authentication mechanisms, introduction of objects into the users address space (e.g., file open, program initiation), and the deletion of objects. For each recorded event, the audit record shall identify: date and time of the event, and the success or failure of the event. For identification/authentication events the origin of the request (e.g., terminal ID, subscriber ID, individual ID) shall be included in the audit record. In addition, the I-S/A AMPE shall be able to record actions taken by the I-S/A AMPE operators, System Administrators, and/or Security Administrators. The Security Administrator shall be able to selectively audit the actions of any one or more subscribers based on individual identity.

4.13.3 Time sensitive results of security monitoring features shall be provided to the Security Administration Position with precedence handling equivalent to FLASH.

4.13.4 Once recorded the TCB shall ensure the integrity of Audit Trail(s) and permit read only access from an operating position connected via a Trusted Path.

4.13.5 TCB controls shall be provided for monitoring the occurrence of auditable events and; notifying the Security Administration Position, and taking the least disruptive course of action when programmed thresholds are exceeded. If the event persists the TCB shall have the capability to protect the system by taking stronger action necessary to preserve system security. I-S/A AMPE auditable events shall include as a minimum:

4.13.5.1 Unauthorized Access Attempts. Correctly formatted access requests which contain errors shall be recorded for audit upon occurrence. The threshold for operator notification shall be adjustable in the range of 1 to 10 per hour by the security administrator for each subscriber, operator, and subsystem. When the threshold of 10 per hour is reached, the TCB shall cause the access path to be disabled with notification to the operator and an audit trail record created.

4.13.5.2 Illegal Access Attempts. Unrecognizable data during initiation of access shall be recorded in the audit trail, including content, upon occurrence. The threshold for operator notification shall be adjustable in the range of 1 to 5 per hour by the system operator for each subscriber, operator, and subsystem. When the threshold of 5 per hour is reached, the TCB shall cause the access path to be disabled with notification to the operator and an audit trail record created.

4.13.5.3 System and SubSystem Faults. System and subsystem faults which occur shall be recorded in the audit trail if possible. The operator shall be notified of all system and subsystem faults. The TCB shall execute security confidence tests prior to restart after a system or subsystem fault.

4.13.5.4 System and SubSystem Restarts. All system and subsystem restarts shall be recorded in the audit trail with the identification of the initiator of the restart. The operator shall be notified of all system and subsystem restarts.

4.13.5.5 Security Administration Actions. All actions of the Security Administrator shall be recorded with the identification of the individual initiating the action. All action of the Security Administrator shall be presented for review on the initiating device prior to implementation of the results. Security Administrator actions shall be treated as security label changes.

4.13.5.6 Operator Actions. All actions of the operators shall be recorded in the audit trail with the identification of the operator and a means of auditing the content of the action.

4.13.5.7 Inactivity timeouts. Inactivity timeouts shall be recorded in the audit trail with the identification of the subscriber. The timeout threshold shall be adjustable in the range of 1 to 99 minutes by the system operator for each subscriber. Subscribers with individual identification requirements shall be required to reestablish access subsequent to reaching the threshold and before access is again permitted. The operator shall be notified of Subscriber Access Terminations and reactivations due to timeouts.

4.13.5.8 Modifications to the accesses accorded to individual users shall be recorded in the audit trail with the identification of the initiator and the effected user. The TCB shall ensure that the modification does not cause the permissions established by the Security Administrator to be exceeded. Attempts to exceed security access attributes shall be treated as unauthorized access attempts.

4.13.5.9 Security related hardware and software failures. All security related hardware and software failures shall be recorded in the audit trail. Failure shall cause the TCB to execute security confidence tests which shall permit the security of the system to be reestablished. Processing shall be suspended until the system security is reestablished. Attempted execution of data received from a communication line is a security related failure.

4.13.5.10 Label changes shall be permitted only under the control of the TCB and only when initiated by the Security Administrator. Label Change Actions shall be recorded in the audit trail with the before and after image of the label.

4.13.5.11 Diagnostically detected errors shall be recorded in the audit trail and the operator notified.

4.13.5.12 The occurrence of a specified number of serial CANTRANs from a specified terminal without an intervening valid message shall be recorded in the audit trail and the I-S/A AMPE system operator shall be notified.

4.13.6 TCB features shall be invoked to record History and Journal File(s) information. In particular, the following shall always be recorded per DoD C-5030.58M:

4.13.6.1 Unauthorized internal and external access attempts

4.13.6.2 Message identifiers : security, Channel Designation and Channel Sequence Number (CD and CSN), Transmission Control Code (TCC), Originating Station Routing Indicator (OSRI), Destinations, Date Time Group (DTG), the classification level identified in Format Line 12, and the Unique Message Identifier

4.13.6.3 Retrieval data : message requested, when requested, disposition (allowed or denied), and destination

4.13.6.4 Security faults : identification of rejected message, reason, disposition, when, and action taken

4.13.6.5 Security attribute changes : changes to security labels, changes to routing tables including alternate routing tables, authority for change, discretionary access change

4.13.7 TCB Features shall be provided to support the following activities:

4.13.7.1 Accountability of classified data;

4.13.7.2 Investigations of suspected security violations.

4.13.8 Features shall be provided to audit system security related activities to provide a history of system security relevant information (Reference DoD 5200.28-M, JCS Pub 22, DIAM 50-4 and DoD C-5030.58M). For each activity the History File(s) shall include the user, resource, type of access attempted or obtained, day and time.

4.13.9 Features shall be provided for the capability to audit the use of the covert channels identified during the formal verification of the FTLS that have bandwidths that may exceed a rate of one bit in ten seconds.

4.14 Security Administration Support

4.14.1 The I-S/A AMPE shall provide the following trusted features to support the Security Administration Position:

4.14.1.1 Audit system security-related activities

4.14.1.2 Determine system configuration

4.14.1.3 Establish and change classification markings on objects other than messages

4.14.1.4 Establish and control access authorization

4.14.1.5 Enable and disable subscriber access authorizations and activities

4.14.1.6 Enable and disable subscriber connections

4.14.1.7 Selectively enable or disable diagnostics

4.14.1.8 Select security hardware and software monitoring intervals

4.14.1.9 Run confidence tests

4.14.2 The Security Administration function shall only be invoked from correctly classmarked I-S/A AMPE operating positions and through the use of authentication procedures. Individual and terminal identification and authentication shall be used to ensure continuity of operations.

4.15 System Generation and Loading.

At system start-up and for all subsequent reload and restart situations, the TCB for the I-S/A AMPE should be loaded first. After the TCB has been successfully loaded, the remainder of the I-S/A AMPE program shall be loaded under TCB control.

4.15.1 A validated automatic sequence of operations for loading and initializing the CIs, CPCIs, and CPCs of the I-S/A AMPE including establishment of the initial secure state for the TCB shall be provided. This sequence shall also validate the correct functioning of those hardware CIs of the system which are included within the TCB.

4.15.2 The loading operations shall not depend upon any untrusted system CIs, CPCIs, or CPCs for correct functioning. Any errors detected in the loading or initialization function shall result in operator error messages and cause the system to halt.

4.15.3 All subsequent loading operations shall be performed under the control of the TCB. Reloading operations shall ensure the integrity of the TCB and shall re-establish a secure state prior to return to service.

4.15.4 Diagnostics shall be performed to verify the integrity of the TCB during system startup and prior to system operation.

4.16 Trusted Restoral

4.16.1 Features shall be provided to ensure the trusted accomplishment of functions and to assure restoral of the I-S/A AMPE to a demonstratably secure state.

4.16.2 Check point or other environmental "snap-shots" features shall operate under the control of the TCB.

4.16.3 The restart features shall rebuild from the last completely consistent record for which a secure state was recorded.

4.17 Security Tests

Features shall be provided to periodically conduct comprehensive security tests of the entire system without degrading operational performance parameters identified in para 3.5 of the FRD. These tests shall be executable in real-time with the on-line system throughout the life of the I-S/A AMPE and shall provide the necessary information to support security related investigations.

4.18 Safe Storage of Information

Upon receipt, incoming messages shall be entered into the I-S/A AMPE storage by the TCB. Following this action, an acknowledgement will be sent.

4.19. Security Diagnostics. The I-S/A AMPE shall include features for diagnosing the operation of security-related CIs, CPCIs, CPCs.

4.19.1 Diagnostics shall not interfere with the correct functioning of the TCB or other I-S/A AMPE features.

4.19.2 The security policy enforced by the TCB shall not be relaxed while on-line diagnostic functions are executing or during any degraded conditions detected by the diagnostic functions.

4.20 Communications Security. All I-S/A AMPE transmission media shall be secured. A Protected Wireline Distribution System (PWDS), secured in accordance with NACSEM 5203; a Host-to-Host Protection; and/or link encryption Government approved cryptographic equipment will be employed.

4.21 Compromising Emanations Control (TEMPEST). All equipment shall be designed to reduce electromagnetic compromising emanations below the applicable radiation and conduction limits of NACSIM 5100A and NACSEM 5112 for hardened equipment and NACSIM 5100A for non-hardened equipment. All TEMPEST designs shall follow NACSEM 5201. Equipment installation shall conform to the applicable requirements of MIL-HDBK 232 or NACSEM 5203.

DEVELOPMENT

5.1 Formal Security Model.

5.1.1 The contractor shall develop a mathematical "model" implementing the DoD security policy which describes the intended security behavior of the TCB. The contractor shall provide an English language description which explains the meaning of the model. The model will be subject to review by the Government. (The Government will provide documentation describing mathematical models (e.g., Bell and Lapadula) developed for existing DoD programs upon request.)

5.1.2 The model shall specify and be consistent with the security policy cited in Section 3 of this document.

5.1.3 The model shall be in a form suitable for use in the formal verification of the TCB design specifications.

5.1.4 The model shall explicitly identify abstract classes of subjects and objects of the I-S/A AMPE.

5.1.5 The model shall define the rules governing subject and object interactions.

5.1.6 The model shall be shown to be consistent with and sufficient to allow satisfaction of the functional capabilities specified in the Functional System Specification. The model shall be sufficient as well as consistent with respect to the management of the security.

5.1.7 The confinement properties of the overall system shall be described by the model.

5.2 Verified Design - Top Level Specification.

5.2.1 A formal development methodology shall be used in the specification, design, analysis, and verification of security related CIs, CPCIs, and CPCs.

5.2.2 Formal Top Level Specifications shall be prepared for the TCB and included as part of the MIL-STD 490 B-5 specifications. The Formal Top Level Specifications shall be verified, using verification techniques, to conform to the security behavior of the mathematical security model. Verification evidence shall be consistent with that provided within the state-of-the-art of the selected, accepted, formal specification and verification techniques. These techniques shall be approved by the government before verification is initiated.

5.2.3 Formal Top Level Specification shall include definitions and functions characteristics of hardware and/or firmware mechanisms that are within the TCB.

5.2.4 The correspondence shall be shown between the elements of the Formal Top Level Specification and the elements of the system design as implemented. System software design shall express the protection required of the DoD security policy. The correspondence shall be shown between detailed design specifications of the protection elements and the elements of the Formal Top Level Specification.

5.2.5 Access control verification and information flow analyses shall be applied iteratively during the design and implementation processes (e.g., successive refinements of CI, CPCI, and CPC design). Errors detected by the formal analyses shall be corrected and formal analysis reiterated until complete.

5.3 Design Analysis.

5.3.1 The contractor shall demonstrate how the TCB implements the Formal Top Level Specification.

5.3.2 The contractor shall describe how the TCB implementation satisfies the security protection features for an implementation of a reference monitor (e.g., always invoked, tamperproof, and a correct implementation of policy model) and how the TCB shall be structured to facilitate testing and to enforce mandatory and discretionary DoD security policy.

5.3.3 The contractor shall provide documentation that presents the results for the confinement channel analyses and the tradeoffs involved in restricting the covert use of such channels.

5.3.4 The contractor shall use formal techniques that are mathematically based, to identify timing channels, within the TCB, to the Government. An estimate of the bandwidth and countermeasure recommendations shall also be provided by the contractor.

5.3.5 The contractor shall provide analyses of the primitive protection mechanisms used to implement the formal model, mechanisms, and features of the TCB.

5.3.6 The contractor shall provide comprehensive formal reviews as specified by MIL-STD-1521C.

5.3.7 The contractor shall provide documentation and analysis on the protection elements of the system which address detection or prevention of actions which could result in disruption or denial of service.

5.4 Development Environment.

5.4.1 The contractor shall provide a developmental environment which prohibits the exposure of all products, to include development tools, (whether deliverable or not) to unauthorized access. Access to all such products shall be controlled commensurate with the security levels of the products or other measures specified by the Government (e.g., DoD 5220.22M, "Industrial Security Manual for Safeguarding Classified Information").

5.4.2 All system documentation (e.g., developmental software tools) shall be protected in accordance with current regulations regarding the protection of information as specified by the Government.

5.5 Trusted Software Development and Documentation.

5.5.1 The contractor shall develop a separate section in the MIL-STD 490 Type A Specification which shall consolidate, in a comprehensive form, all the pertinent security related issues and solutions defined in the other parts of the specification with appropriate references to those other parts. The security section shall describe the security related hardware and software in terms of CIs, CPCIs, and CPCs respectively.

5.5.2 State-of-the-art software engineering techniques shall be applied in all phases of system development. Software production shall be consistent with modern engineering practice (e.g., top-down structured programming, information hiding, loop-free module hierarchy, stepwise refinements, stubs).

5.5.3 Protective measures shall be designed to detect attempts to tamper with evolving software and hardware.

5.5.4 Software will be developed in a SECRET environment. The software itself will be assigned any classification necessary based on information contained. Strict configuration control shall be employed to protect against unauthorized hardware and software changes.

5.5.5 Programming languages used in the implementation of the TCB software shall be selected with consideration to their suitability for the validation and verification of the design specifications and the High Order Language code. These programming languages proposed shall be submitted to the Government for approval.

5.5.6 Programming shall be performed using design methods that support rigorous implementation of the design (i.e., the correspondence between the design and its implementation can be verified). The contractor shall provide validation of all security related software and thus demonstrate the correspondence between specifications and CPCs).

5.5.7 All software considered for use within the I-S/A AMPE shall be evaluated for suitability and operation in conjunction with the system security policy. The contractor shall provide convincing evidence supporting the ability of the choosen CIs, CPCIs and CPCs to interoperate with the I-S/A AMPE TCB.

5.5.8 The contractor shall provide the following documentation:

a. Results of functional testing of the security features and the efectiveness of the confinement channel minimization.

b. The mappings for correspondence between the Formal Top Level Specification and all security protection related CIs, CPCIs, and CPCs.

5.6 System Security Plan.

5.6.1 The contractor shall submit a system security plan to the Government for approval which describes the strategy for the design, development, and implementation of the I-S/A AMPE. The System Security Plan shall include a description of the organizational structure, staffing, and functional activities which will be used by the contractor to support the security engineering effort.

5.6.2 The System Security Plan shall describe verification techniques to be followed during system design and development. The System Security Plan shall describe, in detail, the elements and relationships for the following tasks:

a. Development of mathematical security model.

b. Development of Formal Top Level Specifications for the design of the system security mechanisms.

c. Development of formal validation methods to verify that the Formal Top Level Specifications conform to the rules of the mathematical security model, that is, documentation shall be provided that describes the analysis techniques that produce theorems to be proven about the formal specifications.

d. Verification of the CIs, CPCIs, and CPCs developed to implement the Formal Top Level Specification.

e. Analysis efforts (e.g., trade-off analysis).

f. Security testing.

5.6.3 The contractor System Security Plan shall be updated, as necessary, during the course of the I-S/A AMPE development and shall be subject to Government approval prior to implementing proposed changes.

5.7 Trusted Computing Base. The CIs, CPCIs, and CPCs which perform security related functions shall be shown to be: segregated from the rest of the system, isolated to prevent tampering, and provide protection from unauthorized access.

5.7.1 The contractor shall provide verification evidence (i.e., formal proof, test plans and test results) that all CIs, CPCIs, and CPCs which perform security related functions are within the TCB. The Government will approve the selection of the TCB elements. The correct operation and integrity of the CIs, CPCIs, and CPCs within the TCB shall be shown to be independent of the actions of CIs, CPCIs, and CPCs outside the TCB.

5.7.2 The security of the TCB shall be demonstrated by the contractor and certified by the Government as providing the requisite protection from unauthorized disclosure (compromise), denial of service, and unauthorized alteration of data.

5.7.3 The contractor shall demonstrate the ability of the computer system to provide reliable and efficient service.

5.7.4 The contractor shall demonstrate how his design minimizes the extent of the TCB including all CIs, CPCIs, and CPCs. Hardware that provides mechanisms for isolating security features and controlling the flow of information between isolated contexts is encouraged (e.g., segmentation and protection domains).

5.7.5 The contractor shall provide capabilities to detect failures in TCB related CIs, CPCIs, and CPCs.

5.8 Trusted Process Identification. The contractor shall specify which CIs, CPCIs, and CPCs compose the TCB and the rationale for selection of each CI, CPCI, and CPC. The government will certify that the specified list is necessary and complete for the TCB.

5.9 Security Audit.

5.9.1 The contractor shall develop a detailed listing of information to be audited, including rationale for the selection of each audited item. The list shall be approved by the Government.

5.9.2 The contractor shall provide an assessment of the capabilities to detect failures in CIs, CPCIs, and CPCs, which are part of the TCB.

IMPLEMENTATION

6.1 Implementation and Trusted Distribution. Implementation shall employ a language for which there is a well understood, reliable language processor (e.g., compiler). There are some languages (e.g., GYPSY, EUCLID) that have been designed with the intention that programs written in them be formally verified. Other languages (e.g., PASCAL) have proposed designs to implement "verifiable subsets." Experience to date indicates that a reliable language processor and the disciplined use of a conventional language are preferable to a relatively untested language processor and a "to be verifiable" language. The contractor shall assure the following:

6.1.1 The FTLS of the TCB shall be written using a Verifiable Formal Logic (VFL) (e.g., Formal Specification Languages, Formal Graphics, Program Design Language (PDL)) that facilitates the automated verification of completeness and sufficiency of the implementation of the FTLS. This verification will encourage that the system be structured and use well defined primitives and a loop-free module hierarchy. Module hierarchy is referenced in an MIT doctorial dissertation titled "Using Type Extention to Organize Virtual Memory Mechanisms", MIT/LCS/TR-167, MIT, September 1976 by Janson, P.A.

6.1.2 The TCB shall be written using a High Order programming Language (HOL) and using structured and well defined primitives (e.g., "DO...WHILE", "IF...THEN...ELSE"), that permit a loop-free module hierarchy.

6.1.3 The source language statements of the TCB shall be well documented.

6.1.4 The language selected for software implementation shall be justified for suitability in terms of cost, schedule, quality of compiler and tools, and technical performance.

6.1.5 Use of control structures shall be justified to be a minimum implementation necessary to realize TCB features.

6.1.6 The Formal Top Level Specifications shall be baselined as the "certified design" for resolution of design issues.

6.1.7 The contractor shall develop a well defined and documented set of procedures for system generation and loading. These procedures shall ensure the integrity of the TCB during system generation and loading.

6.1.8 The contractor shall develop a procedure for ensuring that the system software, microcode, and hardware updates distributed are exactly as specified by the master copies. Such procedures shall include site security acceptance testing. The contractor shall provide audit procedures for an I-S/A AMPE to the Government for approval.

6.1.9 The procedure for implementing the requirements of Paragraph 6 shall be submitted to the Governmnet for approval.

TEST

7.1 Security Testing. Thorough testing continues to be a necessary requirement in the design and implementation of multilevel secure systems. When test plans are constructed, specific attention shall be given to testing the security provisions of the system.

7.1.1 The contractor shall arrange for penetration tests by the Government and estimate the bandwidth of confinement channels that cannot be eliminated.

7.1.2 The Government shall provide to the contractor a list of paragraphs of the Functional System Specification which are testable, and shall cross reference these paragraphs with the test(s) which are used to verify that compliance. The cross reference shall establish correspondence from the Functional System Specification through the CIs, CPCIs, and CPCs verified by the test(s). Additionally, each test procedure shall identify which paragraph(s) of the Functional System Specification are being verified.

7.1.3 The contractor shall input test combinations against the system security mechanism. The TCB shall be tested using valid and invalid input combinations under normal and stress scenarios to exercise each CI, CPCI, and CPC. Stress testing scenarios shall be developed by the contractor and approved by the Government. Each security feature (operational as well as configuration related) shall be tested.

7.1.4 The contractor shall select a test approach designed to exercise each CPC (referencing at least one relevant security test which executes that CPC). Strict configuration control shall be employed for any changes in the test procedure, data, or the system to be tested. The testing approach shall ensure that changes to CIs, CPCIs, or CPCs are adequately tested to detect any affects of the changes.

7.1.5 The maximal use of the formal specifications shall be used in the development of test sets.

7.1.6 Prior to Government Acceptance Testing, the contractor shall perform the system security test(s) identified in paragraph 7.1 above. These tests shall be performed to exercise the TCB in an environment that simulates actual operation. Test result documentation shall be provided to the Government that demonstrates that all TCB requirements have been met.

7.1.7 When test results indicate that the TCB does not meet the Functional System Specification requirements, the contractor shall be required to take the corrective action. Retesting shall be required.

7.1.8 Government Security Acceptance Test. The Government acceptance test will be conducted prior to a Production Buy Decision. The contractor shall provide support for this testing. The Government will conduct the testing and prepare the test report. Latent defects discovered during Government acceptance testing shall be corrected by the contractor within the scope of the contract.

7.1.9 The contractor shall provide a set of security confidence tests which exercise all security features and mechanisms in both real-time and on-line modes of operation. These tests must be available throughout the system life cycle, shall be executed periodically, and be capable of being executed on any I-S/A AMPE system configuration. These tests will include specific attributes which address detection or prevention of actions which could result in disruption or denial of service.

7.2 System Performance. The contractor shall conduct performance evaluations, analyze performance results, and document performance levels achieved. The contractor shall demonstrate that the required performance level has been achieved.

VULNERABILITY ANALYSIS

8.1 Vulnerability Analysis.

8.1.1 An independent contractor should perform a comprehensive system Clandestine Vulnerability Analysis (CVA) for the I-S/A AMPE. The CVA shall consist of the allocation of critical functions, and analyses of countermeasures for the I-S/A AMPE related to: hardware and software modifications, the effects of each external interface; security-related special functions (e.g., TCB); TEMPEST; and security design and development approach for each CI, CPCI, or CPC. The Government shall provide the contractor with the necessary threat information to perform his CVA.

8.1.2 An initial CVA report shall be produced for the System Design Review and shall be updated throughout development activities. This document shall be classified TOP SECRET until Government review and a final classification applied. The initial CVA report and updates shall fully document the contractor's continuing refinements and analyses. Each update shall form separate, clearly delineated portions (e.g., chapters) of the total report. The final classification level of the report will be determined by the Government. The chapters of the CVA report shall be reviewed by the Government as they are produced.

8.1.3 Each vulnerability, threat, and related countermeasure will be categorized into one or more of the following areas: unauthorized disclosure (compromise), denial of service, or unauthorized alteration. The contractor shall perform an analysis to determine and assess the effectiveness of the countermeasures designed, implemented, and employed by the I-S/A AMPE. The Government will rank the vulnerabilities identified by the CVA according to ease of exploitation and the potential benefits to the exploiter. All I-S/A AMPE test plans, security alternatives, and procedures shall incorporate CVA results.

8.1.4 As part of the CVA report, documentation of residual vulnerabilities in the system shall be prepared and countermeasures (e.g., procedures) recommended by the contractor.

8.1.5 The contractor shall provide information necessary for the Government to conduct an independent CVA.

CERTIFICATION AND ACCREDITATION SUPPORT

9.1 Certification Support. A security analysis (e.g., security testing and penetration testing) of the overall I-S/A AMPE system is an essential part of the certification process.

9.1.1 The contractor shall provide support for Government efforts related to the security certification of the I-S/A AMPE. The Government will coordinate security evaluation activities.

9.1.2 The Government will conduct a penetration test of the I-S/A AMPE. The contractor shall support this effort by providing full access to technical expertise (e.g., I-S/A AMPE designers and developers) in order to gather information for penetration test scenarios. The contractor shall provide support for operating the system during penetration testing.

9.1.3 The Government will perform analyses of the I-S/A AMPE design and implementation as part of the security certification effort. The contractor shall provide for use by the Government, automated design, implementation, and analysis aids used during the development of the I-S/A AMPE, which may assist the Government in its analysis efforts. The contractor shall provide reference material describing the use of any aids made available.

9.1.4 The contractor shall make available to the Government, on magnetic media: source language statements, machine object code, and the software support environment used to produce and maintain them.

9.1.5 The contractor shall develop a generic certification test plan to facilitate the certification of an I-S/A AMPE. This test plan shall be modular to support separate certification efforts (e.g., GENSER-only, DSSCS-only).

9.1.6 The contractor shall develop a certification test plan to facilitate the certification of the I-S/A AMPE Prototype and Test Facility and the follow-on Software Support Facility (SSF).

9.2 Facility Accreditation Test Plan. The contractor shall develop a generic Facility Accreditation Test Plan for Government approval. The Facility Accreditation Test Plan shall be a subset of the Certification Test Plan and shall verify the correct installation and operation of an I-S/A AMPE at each facility.

9.3 Facility Accreditation Support. The contractor shall provide technical support during facility accreditation testing when requested by the Government.

9.4 Prototype and Test Facility Accreditation Test Plan. The contractor shall develop a Prototype and Test Facility Accreditation Test Plan for Government approval. The Prototype and Test Facility Accreditation Test Plan shall be a subset of the Certification Test Plan and shall verify the correct installation and operation of the I-S/A AMPE Prototype and Test Facility and the follow-on SSF.

9.5 Prototype and Test Facility Accreditation Support. The contractor shall provide technical support during the Prototype and Test Facility accreditation testing and during accreditation testing of the follow-on SSF when requested by the Government.

ACCREDITATION AUTHORITIES

10.1 General. Completion of a system evaluation and certification does not constitute accreditation for the system to be used in an operational environment. Certification provides a technical evaluation, along with supporting data, which describes the system's security strengths and weaknesses. Evaluations which lead to the certification recommendations will be based on this document and the Trusted Computer System Evaluation Criteria for Class Al. The accreditation procedures found in DODD C-5030.58 or its successor document (IAS Network Telecommunications Security Certification Manual) and DOD C-5030.58M will be followed before the system can be approved for use in processing or handling classified information.

10.2 Designated Approving Authorities. The following organizations are the Designated Approving Authorities (DAA) for the specified classified processing areas.

Security Area	DAA
Defense Special Security Communications System/Critical Intelligence Communications	National Security Agency
Defense Special Security Communications System/Special Intelligence Communications	Defense Intelligence Agency
Single Integrated Operation Plan/ Extremely Sensitive Information	Organization of the Joint Chiefs of Staff
General Service	Defense Communications Agency

MAINTENANCE

11.1 Security Configuration Management. Strict configuration controls shall be applied to all TCB CIs, CPCIs, and CPCs throughout the design and development process, and shall continue throughout the operational life of the system in accordance with MIL-STD 483.

11.1.1 The security configuration controls developed for the TCB shall specifically address the following areas:

a. TCB Development System

(1) Hardware

(2) Software

(3) System documentation

b. TCB System Deliverables

(1) Hardware components

(2) All TCB and untrusted software components

(3) Design and analyses documentation

c. TCB Test Deliverables

(1) Test plans and procedures

(2) Test data

11.1.2 During development and maintenance of the TCB, a security configuration management system shall control the following:

a. Formal security model development

b. Formal logic representation (e.g., PDL)

c. Implementation documentation

d. Source language statements

e. Operational version of the object code

f. Test fixtures

g. Documentation

h. Hardware components

i. Software Support Environment (e.g. compiler)

11.1.3 The configuration management system shall ensure a consistent correspondence between all of the documentation and software and hardware associated with the current baseline version of the system. The selected configuration management system shall support audits of changes to the baseline.

11.1.4 Capabilities shall be provided for generating a new version of the system from source language statements. The configuration management system shall provide a complete audit including reference to the requirement, designer, coder, date and time of each revision of the source language.

11.1.5 Capabilities shall be available for comparing the newly generated version with the previous version of the system at the source language statment and object code levels. The results of the comparison shall be auditable.

11.1.6 A trusted facility for system control and distribution shall be provided for maintaining the integrity of the mapping between master library documentaton and the master copy of the source language statement for the current baselined version.

11.1.7 All material used to generate the TCB shall be protected against unauthorized modification.

11.1.8 The contractor shall provide to the Government recommended configuration management procedures for auditing "as installed" security parameters (e.g., terminal security level) for a site and all subsequent changes to that site baseline.

OPERATIONAL FACILITY SECURITY

12.1 Operational Site Security Documentation.

12.1.1 The contractor shall develop and submit to the Government for approval a site manual that describes the operator and security administrator functions related to security including changing security characteristics and examining and maintaining audit files. The manual shall provide guidelines for the consistent and effective use of the protection features of the system, how they interact, how to generate a secure system, and cautions regarding countermeasures for known flaws. The manual shall include cautions about functions and privileges that must be controlled in a secure facility.

12.1.1.1 A separate manual or section shall address guidelines for securely interacting with the system.

12.1.1.2 A separate manual or section shall provide instructions on how to identify and handle failed components that may contain classified information.

12.1.2 The contractor shall submit to the Government for approval procedures for packing, shipping, repair, storage, and handling of failed components that may contain classified information (e.g., disposal of memory boards).

12.1.3 The contractor shall develop a description of expected system reaction to security-related events (e.g., access violations, security-related failures, etc.). This information will be used by the Government to develop security procedure documentation for system support personnel and penetration tests.

SECTION 40

DESCRIPTION OF SNAPS

DESCRIPTION OF SNAPS

BASIC DATA

AUTODIN TRAFFIC

40.0 General

a. Each time a message is processed into, through, and out of the message switching unit of a DCS AUTODIN Switching Center (ASC), an entry is made on a disc and in Journal/History. This entry consists of routing indicators, time of file, time of entry into the ASC, time of start of message out, time of exit from the ASC, the precedence category, and other operational, statistical and managerial information about the message. Most of these items, or the numerical difference between two items are used in traffic engineering.

b. The numerical information associated with a single message has no engineering merit. Because of this fact, many messages have to be processed before sufficient information is available to determine average values for each item of interest, e.g., average message length. The time required to gather a sufficient number of individual values to get a true average is prohibitive. The field of mathematical statistics has developed practical concepts and procedures of sampling. These concepts use a small section of the total data available, and from this data sample, determine the average values. The DCA-developed Switch Networks Automatic Profile System (SNAPS) is based on a sampling concept and is the primary source of data used in traffic engineering.

40.1 Data Requirements

a. Traffic volume is the major determining factor in the design of a communications system. The traffic volume in line blocks (84 characters), for a specified time period, is determined approximately by multiplying the number of messages transmitted during this time period by the average message length expressed in line blocks. Traffic volume is not a constant. It varies from time period to time period. Busy periods are those time periods during which the most traffic is being processed. Generally, in traffic engineering applications, the busy period values are used in the calculations. Variations in traffic volume are caused by variations in the message lengths, as well as, the rate of message transmission. Average message lengths are determined by dividing the total number of line blocks by the total number of messages in a specified time period. The duration of the time period used is the total time of the sampling period.

b. Using precedence categories is a way of indicating the relative importance of messages. The precedence categories in the AUTODIN are: (1) ECP and CRITIC, (2) Flash, (3) Immediate, (4) Priority, and (5) Routine. The order of transmission is first-in, first-out (FIFO) for each precedence category, with all of the messages of higher precedence being transmitted before the next lower precedence on each ASC output channel. An ECP or CRITIC message will interrupt a message of lower precedence to allow the ECP or CRITIC message to be transmitted immediately. A Flash message will interrupt a message of lower precedence to allow the Flash message to be transmitted immediately. CRITIC will not interrupt an ECP nor will an ECP interrupt a CRITIC. An Immediate precedence message will not interrupt a message of lower precedence in the process of transmission: but, upon completion of the lower precedence message, the Immediate precedence messages will be the next to be transmitted.

c. The number and length of messages by precedence category, as well as, the total number of messages and the average length of the message, are needed to help determine the effective transmission rate required to ensure that speed of service objectives, as specified in ACP 121, and DCAC 310-130-2, and discussed in TEP, Volume XII, Section 3, are met.

d. The traffic engineer, in determining the homing assignment of subscribers, should know the community of interest of the subscriber. That is: does the subscriber primarily receive from and transmit to a certain set of stations? Are these stations homed on the same ASC?

e. Associated with community of interests are destination and collective routing. Destination routing requires that each addressee be separately listed in the message header; collective routing requires that a single routing indicator be used for a group of addressees. The ASC has tables of collective routing indicators (CRIs) which, in turn, list the actual addressees. The ASC will then send the message to each station indicated by the particular CRI.

f. By using a series of data from previously produced reports, the values of each of the above factors may be plotted against time. These plots will show the trend of the factor with time; e.g., increasing, no significant change, or decreasing. These trends may then be extended into the near future to give forecast values for each of the plotted factors.

g. The above numerical factors, when combined with the system facilities data (see Traffic Engineering Practices (TEP), Volume IX, Basic Data, Section 3, AUTODIN Facilities), describe the capabilities of the system as well as what the system was doing at the time the numerical information was collected. These descriptions make up the network/switch profiles.

h. Using the traffic volume to be processed and the speed of transmission of a circuit as entries, the ETR may be determined by referring to the trunk capacity curves in TEP, Volume XII, Estimating Facility Quantities, Section 5, Curves and Tables.

40.2 Data Sources

a. Traffic data is of two types: (1) measures and (2) calculated from measured data. Examples of each type of data are presented in the DCA Switch Networks Automatic Profile System (SNAPS), which was developed by DCA to present most of the traffic information needed by the traffic engineer. Measured data are items such as the Time of File (TOF), the number of line blocks, the time of Start of Message In (SOM IN), and the time of End of Message Out (EOM OUT). Calculated data are items such as average message length, processing time, and handling time.

b. SNAPS processes data which has been extracted from the discs, and Journal/History tapes at each switch. Instead of using the information for each day of the month, a sample period is used.

c. This sample period is the first Thursday of each month unless the preceding Tuesday or the following Friday is a holiday, in which case the sample period is the second Thursday. The same sample period is used at all switches.

40.3 Reports

a. SNAPS consists of five reports: (1) Switch Profile, (2) Network Profile, (3) ECP-SPECAT Subscriber Report, (4) Speed of Service Analysis, and (5) System Speed of Service by Time Intervals. Report 1 is subdivided into three sections. Section I consists of static facilities information which is explained in Basic Data, TEP, Volume IX, AUTODIN Facilities, Section 3, Paragraph 9-301.2a. Section II consists of traffic measurements for each ASC, which are divided by types of traffic: i.e., teletypewriter, data pattern, and magnetic tape. Under each type of traffic, the measurements are further subdivided by precedence, security, number of destinations, message length by precedence, and in-station processing time parameters. Section III provides traffic distribution information by time and destination. This same basic format is followed for report 2. System traffic processing information is presented in reports 3, 4, and 5.

b. Description of SNAPS Printouts.

(1) SNAPS, Report 1, Switch Profile, Section II, this section of the SNAPS printout describes the total traffic volume using the parameters of trunk traffic, terminal traffic, Language Media Formats, send/receive traffic, precedence, security, and number of destinations. The first subsection of the printout describes the terminal traffic in terms of message lengths, send and receive, and in-station processing time. Trunk traffic is described in the second subsection.

(2) SNAPS, Report 1, Switch Profile, Section III. Section III gives traffic distribution by 2-hour periods and the speed of service by switch.

(3) SNAPS, Report 2, DCS Network Profile, Section II. Section II of the DCS Network Profile presents the traffic volume distribution of the DCS AUTODIN. The total volume of traffic, in the number of messages and line blocks is described by language media format, terminals, precedence category, security level, number of destinations per message, message lengths, and average in-station processing time.

(4) SNAPS, Report 2, DCS Network Profile, Section III, Subsection A, Actual Inter-Switch Trunk Loading. This subsection presents the distribution of traffic in number of messages and line blocks transmitted between directly connected ASCs.

(5) SNAPS, Report 2, DCS Network Profile, Section III, Subsection B, Traffic Distribution Between ASCs. This subsection presents the distribution of traffic in number of messages and lineblock transmitted from an originating to a destination ASC.

(6) SNAPS, Report 2, DCS Network Profile, Section II, Subsection C, Speed of Service, Average Message Length by Areas and Precedence. This SNAPS printout presents the distribution of traffic by DCA area, average message length, and Speed of Service by Precedence. Time is presented in two categories:

1. Time of AUTODIN Entry to Time of AUTODIN Exit.

2. Time of AUTODIN Entry to Time of Receipt at Last ASC.

(7) SNAPS, Report 3, ECP - SPECAT Subscriber Report. This SNAPS printout presents a list of the ECP-SPECAT messages originated and delivered during the sample period. Speed of Service is presented in 3 periods:

Time 1 refers to elapsed time between Time-of-File and Start-of-Message In into AUTODIN.

Time 2 refers to elapsed time between Start-of-Message In into AUTODIN and End-of-Message Out at last ASC.

Time 3 refers to elapsed time between Time-of-File and End-of-Message Out at last ASC.

(8) SNAPS, Report 4, Speed of Service (SOS) Analysis. This SNAPS printout lists those high precedence messages (Flash Override, Flash and Immediate), which were not processed within established thresholds. Speed of Service is presented in 3 periods for each precedence.

Flash Override and Flash

SOS1: The elapsed minutes between Time of File and End-of-Message-Out Time.
Threshold set for this study: 10--MIN

SOS2: The elapsed minutes between System-In time and End-of-Message-Out Time.
Threshold set for this study: 5--MIN

SOS3: The elapsed minutes between System-In time and End-of-Message-In Time.
Threshold set for this study: 3--MIN

Immediate

SOS1: The elapsed minutes between Time of File and End-of-Message-Out Time.
Threshold set for this study: 30--MIN

SOS2: The elapsed minutes between System-In Time and End-of-Message-Out Time.
Threshold set for this study: 23--MIN

SOS3: The elapsed minutes between System-In Time and End-of-Message-In Time.
Threshold set for this study: 8--MIN

(9) SNAPS, Report 5, System Speed of Service by Time Intervals. This subsection presents the average speed of service in minutes by precedence category for all messages entered into the DCS AUTODIN. It also presents the distribution of messages by precedence category by speed of service ranges. The speed of service is determined in two ways: (1) The time elapsed from the time of the DCS AUTODIN entry to the time of the DCS AUTODIN exit, and (2) The time elapsed from the time of file (TOF) to the time of the DCS AUTODIN exit.

c. Other Sources of Traffic Engineering Data.

(1) DCA Circular 310-D70-30. This DCA Circular describes the type, format, and frequency of reports required to supply the information needed to direct and manage the DCS AUTODIN. Some of the information is directly applicable to traffic engineering. The following paragraphs will identify the reports that contain traffic engineering data and will give examples to show where in the report the data is located.

(a) General. Each ASC has the capability to process the history tapes in an off-line mode to generate statistical information.

(b) Monthly ASC Summary. This report is to be received at Headquarters, DCA not later than 5 working days after the end of the month in the format as shown in DCAC 310-D70-30, Chapter 6.

(c) Header Extract Report. This shows the distribution of traffic for each channel, send and receive, by ASC Routing Indicator. DCAC 310-D70-30, Chapter 6.

40.3 Collection Methods

a. General. Many of the real-time, on-line, automatically generated DCS AUTODIN reports have little or no impact on traffic engineering. Most of the reports are either operational or managerial. Most of the data needed for use in traffic engineering is presented in DCS SNAPS reports, but some useful data is available from other sources. The following paragraph outline how these data are obtained.

b. Header Extract Program. This is an off-line program that is used at each ASC to develop the data base for a 1-day monthly sampling period. This sample day is the first Thursday of the month, unless the preceeding Tuesday or the following Friday is a holiday, in which case the sample day is 1 week later. The Header Extract Program extracts data from the discs and Journal/History tapes and writes this data on magnetic tape. The magnetic tape generated by the Header Extract Program is used for input to the DCA SNAPS program. The magnetic tape for SNAPS is sent by airmail to Director, DCA, ATTN: Code B651(251), Washington, D.C. 20305.

SECTION 50

STATISTICS AND REPORT GENERATION CRITERIA

STATISTICS AND REPORT GENERATION CRITERIA

A. Generally stated, the philosophy upon which the AMPE Statistics and Report Generation function of this appendix is based is that if system performance indicators, both historical and real-time, can be easily accessed, displayed, printed and subjected to near real-time statistical analysis under AMPE operator control, then the need for periodic, voluminous AMPE historical and statistical reports for use at local, network, and intervening levels of management will be substantially reduced. To attain a system with these attributes requires that the AMPE system record the data elements specified in this appendix in an easily accessible manner and that a versatile Report Generator Program (RGP) be developed which can access these data elements and perform the many functions specified in section B of this appendix. Although the RGP is a complex program, the intent is to have a highly functional program available when needed, but invoke its use sparingly and limit the information and data processing requirements to the minimum essential elements necessary.

The three standard AMPE management and status reports, the DCS Message Quality Control Report, the Circuit and Equipment Outage Report and the Terminal Capacity Report supplemented by a Message traffic summary report should provide sufficient information as to the acceptability of AMPE performance. Should problems with system performance be encountered, the real time aspect of the RGP would be employed to request data and assist in the analysis of the data to support a quick identification and resolution of the problem area. The one-time cost of developing the RGP as specified herein, should result in staff-hour savings by permitting operator and management personnel to obtain specific items of information quickly to support timely decision-making without resorting to time consuming analysis of voluminous, comprehensive printouts and reports.

The AMPE system shall support the preparation of system status and statistical reports as required by Function I.16. These reports will be generated from a wide range of data elements which shall be recorded and maintained by the system. The requirement for the AMPE to record and maintain these data elements derives not only from Function I.16, Statistical and Statistical Report Generation, but also from other functions such as Function I.8, History Logs and Files. It is therefore, important that the recording of the data elements be accomplished in an efficient and well organized manner,i.e., a data base, to which the Report Generator Program (RGP) shall have ready access.

The RGP function shall be designed to support two broad categories of reports and displays. The first category is that of User Site/System Control reports and displays which are, in general, current system status information and short term system performance statistical reports. These User Site/System Control Reports will include both automatically generated displays and reports and operator requested displays and reports, and are used principally for new time site and system control functions.

The second category, Network Statistical Management reports, are generally less concerned with real-time equipment status, keyed more to average performance figures over specified periods of time and also to peak conditions at key network elements (e.g., peak traffic through an AMPE during the busiest hour of the month, largest backlog of messages on queue during the month). These reports tend to require much more computer processing power since they involve the application of statistical operations to a large number of data elements. The aspect of the RGP supporting the preparation of these reports would be a background or off-line type of operation, and must be extremely flexible to permit the network managers to obtain the analyses necessary to solve the wide range of management situations likely to occur in a network with the large number of AMPEs expected to be fielded.

B. To support the required statistics and report generations (both Site/System Control and Network Statistical Management reports) the following set of data elements must be recorded and maintained and available for retrieval, manipulation, and formatting by the RGP:

1. Each message transiting the system shall have the following data elements generated or extracted from the message and recorded:

   a. Community (R or Y)

   b. Precedence

   c. Language Media Format (for send and receive)

   d. Classification (to include TCC, TRC and SHD)

   e. Content Indicator Code (CIC)/Communications Action Identifier - (CAI)

   f. Originating Station Routing Indicator (OSRI)

   g. Originating Station Serial Number (OSSN)

   h. Time of File (TOF)

   i. Date Time Group (DTG) (if present)

   j. Time of Delivery (TOD) to each station

   k. Line number of any unsuccessful delivery attempt

   l. Channel Designator and sequence number under which the system received the message (from connected Mode II, Mode V, and Mode I TI line users)

   m. Number of characters and lineblocks in the message

   n. Incoming line number from which the system received the message (from the network)

o. Day and time message was originally received in the system (Time of Receipt [TOR])

p. History file Number

q. Delivery Channel Designator and Channel Sequence Number for Mode IIs, Mode Vs and Mode Is using TIs.

r. Destination Routing Indicator(s)

s. SSIC only in Format Line 12

t. System Generated Unique Message Identifier (UMI)

u. Message Format Type

v. Operator ID Number(s) if message was intervened

w. Time of Transition from Queue to Queue (input to output, etc.)

2. For each peripheral/terminal (channel), the system shall have the following data elements generated and recorded:

a. Time of each connection (log-on)

b. Identification (ID number), [channel and/or jack number]

c. Highest classification channel can accept (to include TCC's, TRC's and SHD's)

d. Language Media Format(s) (LMF) it can process

e. Restoration priority

f. Amount of traffic on queue at time of log-on

g. Time of each disconnection (log-off)

h. Amount of traffic on queue at time of disconnection

i. Disposition (Altroute) instructions in force

3. The following system performance data elements shall be generatedand maintained:

a. Number of system restarts and reloads

b. Number of successful and unsuccessful peripheral accesses, for the current RADAY.

c. Processor idle time

d. Listing of all message retrieval requests to include:

(1) Requesting terminal/station ID number

(2) Number of messages per request

(3) Date and time of request

e. Listing of each channel/line/trunk outage occurence to include:

(1) Channel/line/trunk ID number

(2) Time logged out

(3) Time logged back to service

(4) Reason for Outage (RFO) Code (to be assigned by the AMPE operator when determined)

f. Listing of occurences of message rejections to include:

(1) Source terminal/station ID number

(2) Date and time of occurence

(3) Terminal/position ID number to which the message was rejected for correction/service

(4) Whether message was rejected automatically to service or manually

(5) Reason for Rejection code (assigned automatically by AMPE when possible or by AMPE operator)

4. Any other data elements required to support generation of Site/System Control Reports and displays (Section C). Network Statistical Management Reports (Section D), and required preformatted reports (E).

C. The following data elements will be available on a real-time basis (without having to use background or off-line capabilities of the RGP) to support User Site/System control reports and displays:

1. The cumulative total of messages and lineblocks received and transmitted over each channel during the current RADAY by:

a. Community

b. Channel

c. Precedence

d. Media

2. The cummulative total of messages rejected during the current RADAY by:

   a. Community

   b. Channel

   c. Type of reject

3. Current message status:

   a. Total number of messages and lineblocks on each queue in the AMPE, expressed both in actual numbers and as percentage of the total capacity.

   b. Total number of messages and lineblocks on intercept and overflow storage, expressed both in actual numbers and as percentage of the total capacity.

   c. Numbers of messages and lineblocks on queue, intercept, and overflow by channel number, designation, media, and precedence.

   d. Any channel which has exceeded it predetermined message/lineblock threshold based upon bit rate, to be reported on a real time basis.

   e. The oldest message in the system, the oldest message on each queue, the oldest message on intercept, and the oldest message on overflow, identified by unique message identification and time/cycle of entry into the system; also to be available on a by-channel basis.

   f. The number of messages scrubbed during the current RADAY by channel.

   g. Number of message retrievals in progress by:

      (1) Requesting terminal/station number

      (2) Precedence

      (3) Average number of messages specified per request in progress

   h. Number of messages by router type and classification awaiting manual intervention.

   i. Average message length of all messages received.

4. The following system status information shall be generated and maintained and available on a real time basis.

   a. The configuration of the AMPE system equipment shall be maintained using the following categories of status:

(1) On-line

(2) Off-line

(3) Standby

b. The version of the AMPE system software, to include the operator invoked options in effect, shall be maintained

c. The network status shall be maintained with the following information provided:

(1) The status and configuration of each channel (to include all input, output and local lines)

(a) Classification including TCC, TRC and SHD

(b) Channel designator and sequence number (if applicable)

(c) Line type

(d) Line status

(2) Alternate routes in effect by routing indicator

(3) Intercepts in effect by routing indicator

(4) Table change notices

d. Service directory information

e. Cumulative number of blocks reruns/retransmissions (per channel - final RADAY count) (counter to be reset to zero at the start of each RADAY)

f. Cumulative number of security errors, e.g., mismatches by channel (counter to be reset to zero at the start of each RADAY)

g. Number of successful and unsuccessful peripheral accesses for the current RADAY

D. The following data elements, information, and functions will be available through the RGP (using the background or off-line capabilities of the RGP if required) to support Network statistical Management reports:

1. The following Message Input Statistical calculations shall be supported:

a. Number and average length of messages received per hour of each RADAY for periods not to exceed 31 days by:

(1) Community (R or Y)

(2) Channel

(3) Classification

(4) Content Indicator Code (CIC)/Communications Action Identifier (CAI)

(5) Language Media Format (LMF)

(6) Message Type

(7) Precedence

b. Number and percent of messages received above:

(1) Bearing AMPE's service RI

(2) Entered through VDT, OCR or in modified ACP 126 format

(3) Generated by the AMPE

(4) Which are suspected duplicates

(5) Of each LMF format (narrative, card, type)

c. Percent of RADAY utilized by each input channel using specified line speed of the particular channel

d. Number of messages and lineblocks from the DDN

e. Number of messages and average delay time

2. The following Message Processing Statistical calculations shall be supported for each RADAY:

a. Number of messages accepted

b. Number and average processing time of messages processed by precedence per hour of each RADAY

c. Number of messages rejected by type (k,j,...)

(1) Automatically to service

(2) Manually

d. Number of messages requiring manual intervention, includes both operator intervened and system rejected messages

e. Number of messages in error by correction line

f. Number of lines corrected by line type code

g. Number of messages journaled per unit time

3. The following Message Output Statistical calculation shall be supported:

a. Number and length of messages transmitted per hour for each RADAY by:

(1) Channel

(2) Classification

(3) Destination RI

(4) Language Media Format (LMF)

(5) Message type

(a) Narrative

(b) Data

(c) Service

(d) Magnetic tape

(6) Precedence

b. Percent of RADAY utilized by each output channel (based on line speed of each channel)

c. Amount of delay in making delivery for each message transmitted (i.e., time of transmission minus time of receipt)

4. The following Message Distribution Statistical calculation shall be supported for each RADAY:

a. Number of messages delivered Over-the-Counter (OTC)

b. Number of messages delivered OTC by receiving organization which received office code distribution:

(1) via manual assignment

(2) via subject code

(3) via flagword

(4) via reference

c. Number of messages delivered OTC which received Protect Distribution by receiving organization

d. Number or messages and copies of messages delivered OTC to each receiving organization by classification

e. Total number of copies delivered OTC for each classification

5. Message Status Statistics: Average number of messages by precedence and LMF queued in the AMPE per unit time (specified at SYSGEN, not to exceed 31 days) to:

a. Input queue

b. Processing queue

c. Output queue

d. Intercept queue

e. Overflow queue

E. In addition to the above requirement for data element generation and maintenance, Site/System Control reports, and Network Statistical Language reports, following specific reports must be preformatted, automatically generated (in real-time), and printed out, stored, displayed, and/or transmitted (in message format when applicable):

1. DCS Message Quality Control Report. Statistics on messages rejected for specified reason codes and other data necessary to implement the DCA Message Quality Program as prescribed by ACP 121 US SUPP-1.

2. Circuit and Equipment Outage Report. In its capacity as a DCS Reporting Station, the AMPE will report AMPE system, equipment, network ans subscriber channel outages to DCA IAW DCAC 310-55-1. To the maximum extent possible, 55-1 reporting must be automated. Outage data must be collected and accumulated and reports formatted, generated and transmitted in message format. Only the "S" (Station) "U" (User) line reports require automatic generation for transmission.

3. Termination Capacity Report. In order to maintain network configutation control, specifically as pertains to sizing, traffic engineering and user acess, the AMPE shall be capable of providing the status of termination/access capacity in terms of AMPE limiting factors, e.g., software, memory, hardware and throughput as determined by AMPE design. This report shall be forwarded via message to DCA as provided for under DCA Circular instructions.

F. The Statistical Analysis/Report Generation Program shall be compatible with the AMPE message processing software package. This program shall be designed to perform the on-line functions specified in this appendix and also to operate in a background mode as prescribed for the majority of the statistical analysis operations. The program shall be designed to use the recorded data elements specified in this appendix and shall be designed for utilization on a non-interference basis with the message processing function on the AMPE. It shall provide the following capability to the AMPE operator:

1. The AMPE operator shall be provided the capability to design and specify the contents (configuration) of a report to include any

set or subset of data elements listed in paragraph A through E above.

2. The array of data elements in a report shall be selectable and sequenced in any order specified by the AMPE operator.

3. The AMPE shall be capable of storing at least ten report formats as specified by the AMPE operator. Each report shall be capable of being specified to contain all data elements, each data element to be displayed/presented in every possible combination of its associated parameters (i.e., There shall be no limitation on the number of data elements that can be incorporated into a report except that there shall be no duplication of a data element assigned a repetitive set of parameters).

4. Stored-format reports or single data elements shall be capable of being requested through the AMPE operator and delivered to specified remote network control station(s).

5. The AMPE operator shall have the capability to design and command-generate a report from a designated operator's console.

6. The report generation module (software routine) shall permit the report programmer to insert up to fifty (50) lines of comments/remarks within the heading and body of the report.

7. The report generation module shall provide all operator prompts necessary to permit the operator to design the report.

8. The AMPE system shall support the loading of preformatted report specifications, up to the limits established for store-format reports in paragraph D.3 above, at System Generation time.

9. The report generator shall provide the capability to selectively compute, summarize and analyze the selected data elements. The report generator shall be capable of operating on any of the data elements listed in paragraphs A through E. For example, the report generator shall be able to compute, sort and display/print out the following typical analysis products:

   a. Compute the time in station for each message (time of arrival - time of delivery), summarize/sort by precedence, compute mean and standard deviation; also time for last ZDK retransmission.

   b. Compute the time in station for each message, summarize/sort by destination channel

   c. Summarize by precedence, classification and source channel, the number of messages transmitted and received

   d. Summarize by source and destination channel, the number of packets and lineblocks received and transmitted

e. The AMPE shall have the capability to generate reports similar to the present COMOPS, ASC Daily Summary, SRPA, SRTMA, etc, based upon formats set up either at SYSGEN time or later by operator input.

DEFENSE COMMUNICATIONS AGENCY

INTER-SERVICE/AGENCY
AUTOMATED MESSAGE PROCESSING
EXCHANGE PROGRAM

INTERFACE CONTROL DOCUMENT

TABLE OF CONTENTS

TABLE OF CONTENTS (Continued)

TABLE OF CONTENTS (Continued)

TABLE OF CONTENTS (Continued)

LIST OF FIGURES

LIST OF APPENDICES

1.0 INTRODUCTION

1.1 Scope

The I-S/A AMPE will be an element of the Integrated AUTODIN System, (IAS), to satisfy various Military Service and Defense Agency communications requirements at the base/camp/post/station level and also to serve as as a functional replacement for the AUTODIN Switching Centers (ASCs). These applications create a need for the I-S/A AMPE to interface with DCS facilities, tactical and allied switched and data terminal facilities. This Interface Control Document (ICD) includes environmental, mechanical, electrical, protocol/format and human interface criteria controlling or constraining the development of the I-S/A AMPE.

1.2 Standard Definitions and Terminology

Definitions for the technical terms used will be found in the I-S/A AMPE Functional Requirements Description (FRD) Section 10.0.

2.0 APPLICABLE DOCUMENTS

2.1 Military and Federal Standards

FED-STD-1003	Telecommunications, Synchronous Bit Oriented Data Link Control Procedures (Advanced Data Communications Control Procedures)
FED-STD-1031	Telecommunications, General Purpose 37 Position and 9 Position Interface Between Data Terminal Equipment and Data Circuit Terminal Equipment
MIL-STD-188C	Military Communication System Technical Standards.
MIL-STD-188-100	Common Long Haul and Tactical Communication System Technical Standards
MIL-STD-188-114	Electrical Characteristics of Digital Interface Circuits
MIL-STD-195	Marking of Connections for Electronic Assemblies
MIL-STD-454	Standard General Requirements for Electronic Equipment
MIL-STD-461	Electromagnetic Interference Characteristics Requirements for Equipment
MIL-STD-781C	Reliability Tests Exponential Distribution
MIL-STD-1472B	Human Engineering Design Criteria for Military Systems, Equipment and Facilities
MIL-P-7788	Panels, Information, Integrally Illuminated
MIL-H-232	(C) RED/BLACK Engineering - Installation Guidelines (U)
MIL-H-46855B	Human Engineering Design Criteria for Military Systems, Equipment and Facilities

2.2 Joint/Allied Communications Publications

ACP 121, US SUPP 1	(C) Communications Instructions - General (U)

ACP 127, US SUP 1 & NATO SUP 3	(C) Communications Instructions - Tape Relay Procedures (U)
JANAP 128( )	Automatic Digital Network (AUTODIN) Operating Procedures
DOI-103	(Confidential Compartmented Document) Defense Special Security Communications System Operating Instructions, System/Data Procedures (U)

3 Service/Agency Telecommunications Instructions and Procedures

AFNAG-9A	Using NACSEM Documents and TEMPEST Emanations Limits
DCAC 370-D175-1	DCS AUTODIN Interface and Control Criteria, Revised Draft Attached
DCAC 370-D195-1	Test and Evaluation, DCS AUTODIN Interface, Category I Testing
DCAC 370-D195-2	Test and Evaluations, DCS AUTODIN TEMPEST Category II Testing
DCAC 370-D195-3	DCS AUTODIN Category III, Operational Acceptance Test
DCAC 370-V175-6	AUTOVON System Interface Criteria
NTP-4( )	Naval Telecommunications Publication 4

4 Industry Specifications, Instructions and Manuals

ANS X3.28, 1976	Establishment and Termination Control Procedures
CCITT Recommendation X.25	Interface Between Data Terminal Equipment (DTE) and Data Circuit Terminating Equipment (DCE) for Terminals Operating in the Packet Mode on Public Data Networks, CCITT 1976, revised February 1980.
EIA-RS232C	Interface Between Data Terminal Equipment and Data Communications Equipment Employing Serial Binary Data Interchange
EIA-RS-449	General Purpose 37-Position and 9-Position Interface For Data Terminal Equipment and Data Circuit Terminating Equipment Employing Serial Binary Data Interchange

IBM BISYNC	IBM Corporation Order No. GA27-3004-2 10/70, Binary Synchronous Communication
NACSEM 5100	(C) Compromising Emanations Laboratory Test Standards Electromagnetics (U)
NACSEM 5200	(S) Compromising Emanations Design Handbook for Non-Cryptographic Equipment (U)

2.5 References

a. NARDAC, Document Number 85 C1002, FD-01, "Local Digital Message Exchange/Remote Interface Exchange Terminal Interface, (RIXT)" dated July 1979.

b. CCTC Technical Memo TM 173-78, "AUTODIN-WWMCCS Direct Access Communications Module" (DINDAC) TR-01 dated 30 June 1979.

c. NAVAL COMMAND SYSTEM SUPPORT ACTIVITY Technical Report "NAVCOMM Communication Line Protocol" NAVCOSSACT Document No. 85P012A TR-05 dated Feb 1975.

d. UNIVAC Publication UP-7532, "DCT 2000 Programmers Reference" revised May 6, 1969.

e. DARPA Report DoD Standard Internet Protocol, January 1980.

f. DARPA Report DoD Standard Transmission Control Protocol, September 1981.

g. DCA Code 532, "NICS TARE AUTODIN Interface Device", September 1979.

h. TRI-TAC Interface Control Document, ICD-015.

i. Defense Data Network Program Plan, January 1982 with changes.

j. Draft AUTODIN I System Function Specification, DCA B650, August 1982.

3.0 PHYSICAL CHARACTERISTICS

3.1 Operator System Layout

The I-S/A AMPE system, equipment, and facilities shall be designed and installed to provide work environments which foster effective procedures, work patterns, and personnel safety, and which minimize discomfort, distraction, and any other factors which degrade human performance or increase the probability of error. Layout of equipment shall also be directed toward minimizing personnel and training requirements within the limits of time, cost, and performance tradeoffs. Controls, displays, marking, coding, labeling, and arrangement schemes (equipment and panel layout) shall be uniform for common functions of all equipments. MIL-STD-1472B shall be used as a guide.

3.2 Health and Safety Criteria

During I-S/A AMPE design, health and safety factors should be given major consideration to achieve safe, reliable, and effective performance by operator, maintenance, and control personnel, and to optimize personnel skill requirements and training time. The I-S/A AMPE shall meet requirements of MIL-H-46855B and MIL-STD-1472B in applying health and safety design criteria.

3.3 Environmental Conditions

3.3.1 Operating Temperature and Humidity

The I-S/A AMPE shall be capable of operating without degradation within a temperature range of 15° to 30°C, 40% to 60% relative humidity, non-condensing, at altitudes from sea level to 10,000 feet.

3.3.2 Non-Operating Temperature and Humidity

The I-S/A AMPE shall be capable of being stored or transported within a temperature range of -10° to +55°C, at 10% to 90% humidity, non-condensing, at altitudes from sea level to 15,000 feet, without affecting operational performance.

3.3.3 Noise

Acoustical noise generated by the I-S/A AMPE shall be controlled in accordance with paragraph 5.8.3.3.2 of MIL-STD-1472B. Individual and collective equipment noise shall not exceed 65 db(A). Acoustical energy shall not be concentrated in narrow bandwidths approximating a pure tone (5 db above neighboring frequency bands).

3.3.4 Vibration

Vibration requirements shall be as specified in MIL-STD-781C, paragraph 50.1.3, which tests the equipment with the mild vibration normally experienced in the business office-type environment, and vibration that is normally experienced during maintenance. In addition, see MIL-STD-1472B, paragraph 5.8.4.2 which refers to Equipment Vibrations.

3.4 Physical Criteria

3.4.1 Size

Physical size of the I-S/A AMPE and its peripheral devices shall be designed and constructed to not exceed the size of comparable equipments developed for commercial applications. Due to the wide variety of existing facilities in which the I-S/A AMPE must be installed, the equipment size must be limited. Equipment components for shipping and installation must be smaller than 34"w X 80"l X 96"h. As installed, the equipment and its required cooling area above the equipment must be no higher than 84".

3.4.2 Weight

Weight requirements of the I-S/A AMPE shall not exceed a floor loading of 1000 pounds point load and 250 pounds per square foot distributed.

3.4.3 Maintenance Access

I-S/A AMPE design and construction shall provide readily accessible test points throughout the equipment to allow rapid evaluation of equipment performance. Hardware subsystems (e.g., power supplies, logic) shall be readily removable with the use of a minimum of effort; tools, if required, shall be common hand tools normally carried by maintainers; cables shall be plug and socket, quick disconnect, no terminal strips shall be used. Where required, maintenance adjustments shall be readily accessible and easily identified. The need for special tools or equipment must be justified. Maintenance access to the interior shall be from the front and/or rear with all components readily accessible. Trouble shooting shall be facilitated through the use of passive extender boards and cables.

3.5 Electromagnetic Interference/Compatibility (EMI/EMC)

The I-S/A AMPE equipment shall operate compatibly within its RF environment. Equipment for both secure and nonsecure applications shall meet the electromagnetic emission and susceptibility requirements included in table 4-1 of MIL-STD-461B and Test Methods described in MIL-STD-462. The "limited" requirements listed in table 4-1 shall be applied, including CS09. The following additional details of the requirements are provided:

(a) Signal and control leads shall be included in CE01 and CE03 tests.

(b) Air Force and Navy requirements shall be used for CS06 tests.

(c) Minimum sensitivity within the I-S/A AMPE equipment shall establish the testing sensitivity. If this cannot be determined, 1 millivolt shall be used.

(d) RS01 requirements shall be applied, use AF and Navy requirements for RS02, part 1.

(e) The limits for RS03 shall be as shown for "all other sites" in the table shown in paragraph 19.2 of MIL-STD-461B.

3.6 TEMPEST

The I-S/A AMPE shall be TEMPEST compliant in accordance with NACSEM 5100. Testing for compliance shall be in accordance with the current version of DCA Circular 370-D195-2.

3.7 Electrical Grounding

The I-S/A AMPE shall comply with MIL-STD-188-124, Grounding, Bonding and Shielding for Common Long Haul/Tactical Communications Systems and shall have provisions for bonding the units to the green wire ground in accordance with MIL-HDBK-232, RED/BLACK Engineering-Installation Guidelines.

3.8 Power Requirements

The I-S/A AMPE, to include the entire facility, shall operate on 120 or 208 VAC, 60 Hz. There shall be an option available for 220/380 volts or 240/415 volts, 50 Hz where required by the available power frequency. The internal power supplies shall provide filtering so transients of less than +10%, -20% in voltage or ±10% in frequency lasting less than 500 milliseconds shall not cause failures.

3.9 HEMP Protection

The I-S/A AMPE hardware shall have HEMP protection in the form of Electro-magnetic shielding and line isolation and surge protection.

4.0 PROTOCOLS AND FORMATS

4.1 Protocol Hierarchical Layers

For the purposes of this document, a protocol is defined to be a set of rules governing the formats and procedures used for communication between two cooperating modules. Protocols operate at many different levels of the communications process, ranging from physical connection and electrical signals on a simple link to the high-level interaction among users and processes across several networks.

The concept of protocol layering has been incorporated in the development of most current data network protocols. However, these efforts have tended to be based on different layering concepts and definitions. The International Standards Organization (ISO) and the American National Standards Institute (ANSI) have been collaborating to alleviate this problem by developing a standard reference model of a hierarchical layering of communications protocols. Subsequently Defense Advanced Research Projects Agency (DARPA) proposed an adaptation which has been adopted for the I-S/A AMPE.

The architecture proposed for this reference model (Figure 1) consists of seven independent layers, and is included here to put the I-S/A AMPE protocols in perspective. Each protocol layer accesses the services of the layer below, performs a well-defined function aided by those services, and, in turn, provides services to the layer above it. An important property of this hierarchical structure is that for any given protocol layer, the structure of the layers below it appears transparent, i.e., each layer is aware only of the services of the layer immediately below, regardless of which lower layer actually performs the service. The relationship between protocols in adjacent layers is called an interface. Thus, the interactions among protocols in different layers are defined by the interfaces between layers.

The seven layers in the reference model are defined as follows:

- Level 1 - Physical Control, concerns the mechanical construction of physical connections and the actual electrical means of bit transmission across a physical medium.
- Level 2 - Link Control, enables logical sequences of messages to be exchanged across a single physical data link.
- Level 3 - Network Control, provides logical channels capable of transferring information between two endpoints in a single communication network.
- Level 4 - Internet Control, provides the necessary protocol constructs so that, in conjunction with a gateway, intercommunications between disjoint packet networks using different protocols at Levels 1, 2 and 3, e.g., between the DDN and an X.25 commercial network, can be achieved.

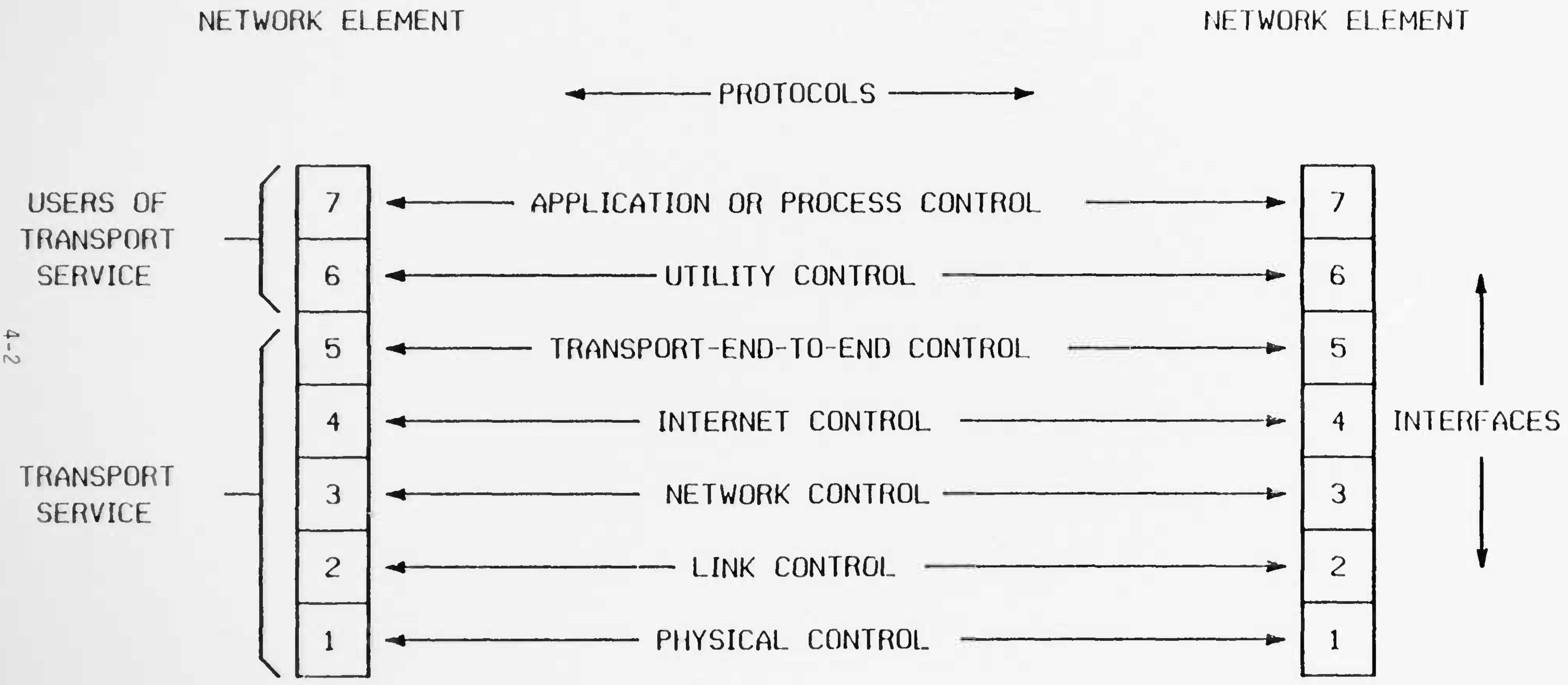


FIGURE 1. SEVEN LAYER PROTOCOL MODEL

- Level 5 - Transport End-to-End Control, provides reliable end-to-end transport of messages across an arbitrary topological configuration, possibly through several interconnected networks.

- Level 6 - Utility Control, provides interpretation of the information exchanged.

- Level 7 - Application, is the level of the subscriber or communicating process itself.

4.2 Protocols

The protocols that shall be implemented in the I-S/A AMPE are as specified herein. While the ISO model has been adapted by the IAS, the IAS protocols do NOT map directly to the ISO model, therefore do not read any significance into, e.g., TCP being labeled "Session Layer," as none is intended.

4.2.1 Physical Level

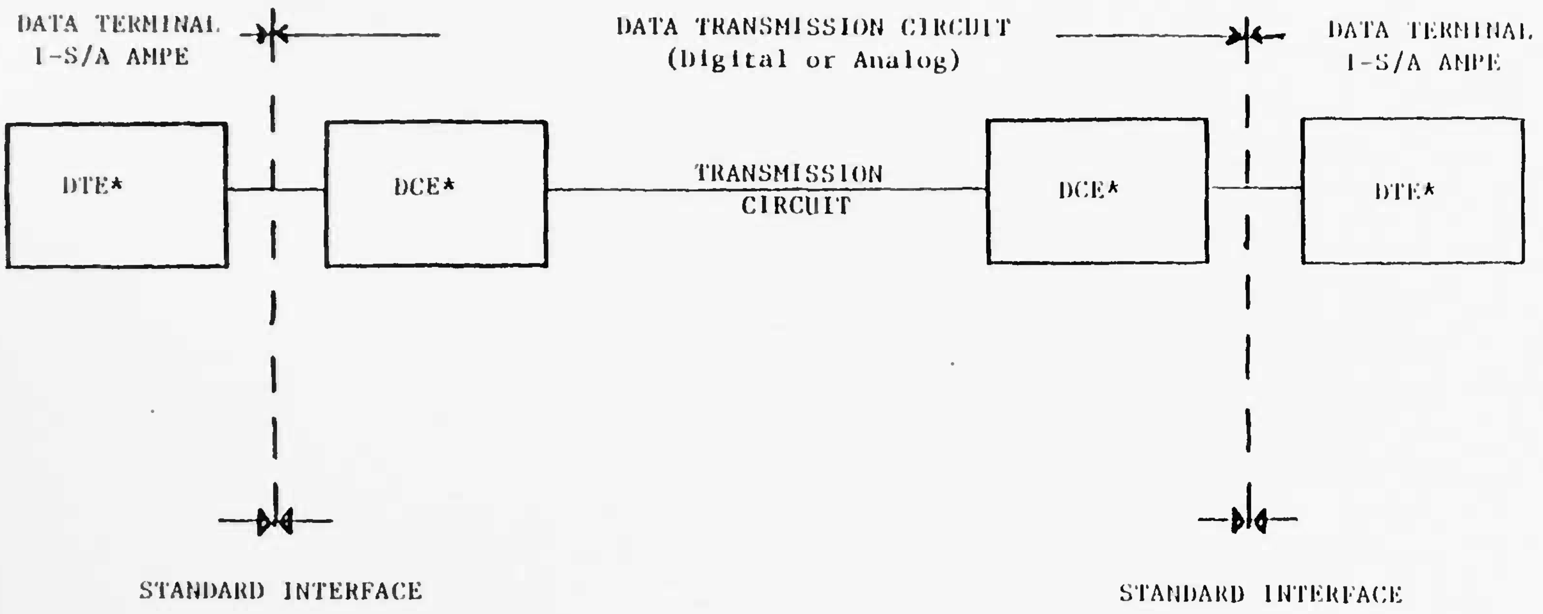
The physical level shall provide bit serial and character serial electrically coded outputs. Both asynchronous, synchronous, and isochronous interfaces shall be provided. As a minimum, each interface shall provide for data transfer, status, and control signalling necessary to meet the performance characteristics defined in this specification. The functional and mechanical characteristics of the digital interface circuits between the I-S/A AMPE and terminals or network elements shall conform to the requirements of Federal Standard 1031 (FED-STD-1031). The electrical characteristics shall conform to MIL-STD-188-114. FED-STD-1031 specifies the interface between Data Terminal Equipment (DTE) and Data Communications Equipment (DCE). Figure 2 shall be considered the schematic for defining the standard interface between DTE and DCE. Applicable DTE/DCE include teletypewriters, data terminals, the DC side of signal conversion (MODEM) equipment, both terminal and line side of cryptographic or cryptographic control equipment, digitized voice equipment, and remotely operated equipment where the interface is at the DC baseband. Interoperability shall be provided between I-S/A AMPE equipment designed to conform to FED-STD-1031 and MIL-STD-188-114 and older equipment designed to conform to the EIA Standard RS-232C and MIL-STD-188C. FED-STD-1031 and MIL-STD-188-114 do not specify other characteristics of the DTE/DCE interface, such as signal quality and clock/data phase relationship, essential for satisfactory operation of the interconnected equipments. These characteristics are described in MIL-STD-188-100 and the I-S/A AMPE electrical interfaces shall conform to the requirements of this document.

4.2.2 Link Layer

4.2.2.1 IAS Standard Link Protocols

a. DCS Mode I

DCS Mode I is a full duplex, character-oriented, synchronous operation with automatic error and channel controls allowing independent and



LEGEND

DTE - Data Terminal Equipment

DCE - Data Communication Equipment
*May include Modems, Error Control Devices, Control Units, and Other Equipment as required.

Figure 2. Standard Interface Between Data Terminal Equipment and Data Communication Equipment

simultaneous two-way operation. In addition, Mode I uses character parity and block parity checking along with retransmission of errored blocks to achieve an automatic error detection and correction capability. The terminal responds automatically to control characters by continuing or stopping transmission or displaying action information to a human operator. DCS Mode I shall be supported as described in DCA Circular 370-D175-1 and Reference 2.5.j. The mechanical and electrical interface for DCS Mode I shall conform to FED-STD-1031.

The allowable transmission speeds shall be:

75 X 2**n bits/sec
n=0,1,2,3,4,5,6,7

The AMPE shall be capable of supporting an effective transfer rate of at least 90% for each Mode I access line connected. As a minimum, the AMPE shall be capable of accepting an SOH prior to acknowledging receipt of an EOM without losing message accountability.

b. DCS Mode IB

DCA Mode IB shall be implemented as specified in Appendix A.
The speeds for DCS Mode IB shall be a. 75 X 2**n bits/sec
n=1,2,3,4,5,6,7

b. 110 bits/sec

c. DCS Mode II

Mode II is a full-duplex asynchronous operation allowing simultaneous two-way operation without automatic error and channel controls. It shall be supported as specified in DCA Circular DCAC 370-D175-1 and Reference 2.5.j.

d. DCS Mode V

DCS Mode V is a full duplex asynchronous operation allowing independent and simultaneous two-way transmission with limited channel and error controls. DCS Mode V shall be supported as described in DCA Circular DCAC 370-D175-1 and Reference 2.5.j.

e. ADCCP

Advanced Data Communications Control Procedures (ADCCP) is a bit-oriented, synchronous link control procedure and shall be supported as described in FED-STD-1003. The speeds for ADCCP shall be:

75 X 2**n bits/sec where n=3,4,5,6,7.

This is a post IOC item. The protocol will be defined in greater detail at time of implementation.

f. CCITT X.25

The I-S/A AMPE shall implement link access procedures (LAPB) as specified in International Telegraph and Telephone Consultative Committee (CCITT) Recommendation X.25 - Interface between Data Terminal Equipment (DTE) and Data Circuit Terminating Equipment (DCE) for Terminals operating in the Packet Mode on Public Data Networks, CCITT 1976, revised February 1980.

4.2.2.2 User Unique Link Protocols

The user unique link protocols described herein shall be implemented in the IOC I-S/A AMPE. These user unique protocols shall be implemented in a modular fashion so that they need not be implemented in every I-S/A AMPE and may be removed as appropriate in the future.

a. Army AMPE-MART Interface Requirements

The Army AMPE-MART interface, including the SIDPERS print expansion requirements, shall be implemented as specified in Appendix B.

b. Army IRT Interface Requirements

The Army IRT interface shall be implemented as specified in Appendix C.

c. Army DPI Interface Requirements

The Army DPI interface including the Preamble Format requirements shall be implemented as specified in Appendix D.

d. Navy DCT 2000 Data Communication Terminal Interface

The Navy DCT 2000 interface shall be implemented as specified in Reference 2.5d.

e. Shore Station Message Processing Set (SSMPS)

Requirement deleted by U. S. Navy.

f. Navy Remote Information Exchange Terminal (RIXT)

The Navy RIXT interface shall be implemented as specified in Reference 2.5a.

g. World Wide Military Command and Control System (WWMCCS) Computer Interfaces

All communications with the Honeywell H-6000 computer used by the WWMCCS must pass through a Datanet 335 (DN-355) GE Remote Terminal Supervisor

(GRTS). In order to pass AUTODIN traffic through this restrictive interface, three "generic" systems were developed which have evolved to the existing three WWMCCS interface requirements. Each consists of a procedure in a programmable device (in line between an ASC and a DN-355) cooperating with a procedure in the H-6000 to bridge the DN-355. Each system also accomplishes message formatting, and performs a number of special message management functions within the H-6000. Provision shall be made for variation within each generic interface on a site-by-site basis. The generic WWMCCS interfaces are:

(1) WWMCCS NATS - NACE Protocol

The NACE procedure within an H-6000 communicates (through the DN-355) with the NMCS AUTODIN Terminal Subsystem (NATS) procedure in a "Remote Computer" that is connected to AUTODIN. "Remote Computers" presently used for that function include the AMME, LDMX, AFAMPE, Honeywell H-716, DCT-9000, and the Univac 1108. It is intended that the I-S/A AMPE interface directly with the DN-355 as the "Remote Computer" specified in the protocol in Appendix F.

(2) AUTODIN-WWMCCS Direct Access Communications Module (DINDAC) Interface

The DINDAC procedure, implemented on the Army AMME and Navy LDMX, communicates through the DN-355 and the DAC to TPAS, a procedure implemented in the WWMCCS H-6000. The I-S/A AMPE shall interface directly to the DN-355, and communicate with the TPAS procedure in the H-6000 using the protocol specified in References 2.5 b and c.

(3) Remote Terminal Operating System (RTOS) Interface

RTOS is a variation of NATS implemented on the DCT-9000 and AFAMPE. The I-S/A AMPE interface shall be directly to the DN-355, and communicate with the RTOS procedure in the H-6000 using the protocol specified in Appendix G.

h. OPINTEL Fleet Broadcast

The OPINTEL Fleet Broadcast interface will be implemented Post IOC.

4.2.3 Network Layer - CCITT X.25

The I-S/A AMPE shall implement the datagram option of the packet level DTE/DCE interface as specified in CCITT X.25. This interfaces to the Internet Protocol in the internet layer (4.2.4) and to LAPB in the link layer (4.2.2.1f).

4.2.4 Internet Layer - Internet Protocol (IP)

The DoD Standard Internet Protocol provides two basic services: addressing and fragmentation. The protocol is distributed among hosts and gateways, and provides neither reliable communication nor flow control. The basic unit of data exchanged between protocol modules is the datagram, which may be fragmented for transmission through "small packet" networks. The IP header defines the standard format for the protocol. The IP shall be implemented in the I-S/A AMPE as specified in DARPA, DoD Standard Internet Protocol, January 1980.

4.2.5 Transport Layer - Transmission Control Protocol (TCP)

The DoD Standard Transmission Control Protocol provides connection management, reliable data transfer, error checking, sequencing, flow control, process-level addressing, and multiplexing. It is a connection-oriented end-to-end transport protocol, implemented in hosts. The TCP shall be implemented in the I-S/A AMPE as specified in DARPA, DoD Standard Transmission Control Protocol, January 1980.

4.2.6 Utility Layer

4.2.6.1 Terminal-to-Host Protocol (THP)

The Terminal-to-Host Protocol (THP) is a Post-IOC host-to-host level network protocol that is required in order that terminals whose circuits are terminated on IAS elements other than the I-S/A AMPE (e.g., a multilevel secure Terminal Access Controller) can obtain FMS from a designated I-S/A AMPE. The THP to be used in the I-S/A AMPE shall be the TELNET protocol. Post IOC THP will be used to allow (1) directly connected terminals to access other network elements including other local terminals, and (2) remote terminals to access the I-S/A AMPE through the network. It supports both terminal-to-terminal and terminal-to-process transactions. A primary function of THP is to present a standard appearance (called the Network Virtual Terminal) for all terminals to be accessed by a network element.

4.2.6.2 Formal Message Protocol (FMP)

The contractor shall design and implement the FMP in the I-S/A AMPE. FMP is a network protocol that shall perform control and coordination functions necessary to allow exchange of formal message traffic through the IAS network. The FMP shall be the means by which the I-S/A AMPE can reliably and efficiently transfer messages to other remote I-S/A AMPEs for eventual delivery to the appropriate addressees. Similarly, FMP shall accept messages routed to the I-S/A AMPE by these other facilities for delivery to the I-S/A AMPE subscribers. The functions performed by the FMP shall consist of at least the following:

a. Accept or reject delivery responsibility for each message received and notify the sender of the message of such acceptance or rejection.

b. Perform multiple addressed message routing in a manner which makes efficient use of the I-S/A AMPE and IAS backbone network resources.

c. Ensure network level message alternate routing is accomplished when required.

d. Indicate the format and code as received of each message transmitted (e.g., JANAP-128, DOI-103 or CRITIC).

e. Detect message looping and shuttling (that is, messages which have traversed this I-S/A AMPE previously). Any detected messages shall be rejected and the I-S/A AMPE operator shall be notified.

f. Interface with the set of routines/processes that constitute the FMS.

g. Interface with the TCP (ICD 4.2.5).

4.3 Formats

The I-S/A AMPE shall support the message formats specified herein.

4.3.1 DD Form 173

DD Form 173 is a message preparation form, with instructions contained in paragraphs 324 through 330 and Annex F to ACP-121 US Supplement 1, which is used to prepare messages to be entered into the I-S/A AMPE via an OCR device.

4.3.2 Modified ACP-126

ACP-126, Communications Instruction - Teletypewriter (Teleprinter) Procedures, as modified by Naval Telecommunications Publications (NTP 4( ), ICD 2.3), paragraph 03.08.0500, describes formats and procedures which shall be accommodated by the I-S/A AMPE.

4.3.3 ACP-127

ACP-127, Communications Instructions - Tape Relay Procedures, with U.S. Supplement 1 and NATO Supplement 3 describes message formats and procedures which shall be accommodated by the I-S/A AMPE. The overall document shall be used as a guide and in addition see FRD Table 3.2.1.2.1.2-2 ACP-127/DOI 103 Special, Message Processing Requirements for the specific paragraphs that shall be implemented and also Reference 2.5.j.

4.3.4 DOI-103

DOI-103, DSSCS Operating Instruction, System/Data Procedures, describes message formats and procedures which shall be accommodated by the I-S/A AMPE. The specific DSSCS formats that shall be supported as specified in DOI 103 and Reference 2.5.j are:

a. DOI-103

b. DOI-103 Special

c. Abbreviated

d. CRITIC

4.3.5 JANAP-128

JANAP-128, Automatic Digital Network (AUTODIN) Operating Procedures, describes message formats and procedures which shall be accommodated by the I-S/A AMPE, as specified by Reference 2.5.j.

4.3.6 Preamble Format

The I-S/A AMPE shall provide the capability to process data received over the communication line interface from the data processing installation using the message preamble in lieu of a JANAP 128 header. Upon receipt of a message with the message preamble, the I-S/A AMPE shall create a JANAP 128 formatted message containing text headers and/or text trailers and will sectionalize the message as required by communications procedures (See Appendix D ARMY DPI Interface Requirements).

4.3.7. Special Format/Format Conversion Criteria:

4.3.7.1. Straggler detection variations (input):

a. Allied/NATO Alliance classmarked channels: If received from Allied/NATO channels, these formats undergo no straggler detection processing. Format line 15, if present, is ignored.

b. General Services Administration (GSA) classmarked channels (JANAP 128 format): If format line 15 is present, normal straggler detection processing shall be performed. If format line 15 is not present, no straggler detection processing shall be performed. In either case, the message is marked on input by the AMPE as a GSA originated message. This marking is used only if the message undergoes JANAP-to-ACP format conversion for output delivery (see below).

4.3.7.2. Straggler detection variations (output):

a. Allied/NATO Alliance classmarked (ACP 127 format) channel methods of straggler detection. Format line 3 (DE line) processing requires:

(1) NATO channels: To give each message delivered the appearance of an ACP 127 NATO SUPP-3 formatted message, the format line 3 OSSN crosshatch (#) used for normal straggler detection processing, if present, is removed prior to output delivery.

(2) Other Allied channels: The format line 3 OSSN crosshatch, if present, is left intact for output delivery.

b. When GSA originated JANAP 128 formatted messages (marked on input) are to be delivered in ACP 127 format to U.S., Allied or NATO channels, the format line 3 (DE line) OSSN built by the AMPE will not include the straggler detection crosshatch (#).

4.3.7.3. Output Delivery Prohibitions:

a. Delivery of EFTO security level messages is prohibited on Allied/NATO Alliance channels.

b. Delivery of messages containing CRIs to Allied/NATO Alliance or Diplomatic Telecommunications Service (DTS) channels is prohibited.

4.3.7.4. Output transmission identification (TI) line (format line 1) variations:

a. In support of Allied/NATO Alliance requirements, the AMPE-provided output TI line for all paper tape TI line user channels (including U.S.) shall be modified to terminate with 5 spaces, 2CR, 1LF vice the original U.S. termination of 2CR, 1LF.

b. On specifically classmarked Allied/NATO Alliance channels, the output TI line shall be terminated in one of the following two ways depending on the security classification of the message being delivered.

(1) 5 spaces, "UU", 2CR, 1LF for unclassified messages.

(2) 5 spaces, "HH", 2CR, 1LF for messages of Restricted, Confidential, Secret or Top Secret security levels.

4.3.7.5. Output delivery exceptions for GSA classmarked channels:

a. AMPE system generated suspected duplicate pilot headers shall not be appended to messages delivered to GSA channels.

b. Messages originated in JANAP 128 format with input LMF codes of C (card) or A (8-level paper tape) undergo no format or media conversion on output to GSA channels, regardless of the output LMF code specified.

4.3.7.6. Line Code Variations: The NICS/TARE Network will use ITA-5, employing SI/SO characters. Consequently, if present on input, the AMPE shall processes ASCII SI/SO characters as unchanged to ASCII (ITA-5) output channels and as LTRS/FIGS to Baudot (ITA-2) output channels.

4.4 Line Character Sets

The I-S/A AMPE shall support standard and user unique line character sets. In the IAS system all standard line transmission is in the bit serial manner with two codes, ASCII (ITA5 - both odd and even parity) and Baudot (ITA2), being employed. The I-S/A AMPE shall also support unique line codes for existing terminals; these are: BCD and EBCDIC. The I-S/A AMPE shall, when necessary, perform code conversion; e.g., ASCII shall be converted to Baudot and vice versa as required by the characteristics of the sending and receiving terminal. The code chosen for line transmission on any given channel is totally dependent on the type of terminal equipment and mode of operation employed. The code conversion software shall be modular.

c. For traffic originating in card format or 8-level paper tape, no format or code conversion takes place on output.

d. 5-level Code on input is always converted to 8-level Code on output.

5.1.2.1.4 World Wide Military Command and Control System (WWMCCS) Interface

The I-S/A AMPE shall provide FMS support to the WWMCCS community, via subscriber interfaces, some of which require unique processing in accordance with references 2.5b and 2.5c and Appendices F and G.

5.1.2.2 Allied Subscriber Interfaces

5.1.2.2.1 NATO (NICS TARE) Interface

The contractor shall design the I-S/A AMPE to interface with the NATO (NICS TARE). The interface for the NATO (NICS TARE) shall be in accordance with MIL-STD-188C low level and in accordance with "Equipment Specification for NICS TARE AUTODIN Interface Device" DCA Code 532, September 1979. The speeds for the NATO (NICS TARE) shall be 150, 300, 600, 1200, 2400, and 4800 bps selectable. The data code for the NATO (NICS TARE) shall be ITA #5. When a NICS TARE interface point is moved from a closed ASC to an I-S/A AMPE, the AUTODIN Interface Device (AID) will also be moved to, and reside in, that I-S/A AMPE Facility. NICS TARE AID size, power requirements, electrical characteristics and maintenance details will be provided when available.

5.1.2.2.2 Allied Subscriber Formats

Allied subscribers normally will exchange traffic with the I-S/A AMPE via the ACP-127 format, however some Allied subscribers do use the JANAP-128 format. Those Allied subscribers that use JANAP 128 format shall use the Transmission Release Code (TRC) on all messages.

5.1.2.2.3 Australia/New Zealand Interface

In the transmission identifier (TI) line following the channel sequence number and 5 spaces the classification of the message shall be indicated by the character "UU" for unclassified or "HH" for all levels of classified messages.

5.1.3 Linked Channels

The I-S/A AMPE shall be capable of providing linked channels to subscribers. Where the volume of traffic between the I-S/A AMPE and a subscriber is so great that a single channel cannot provide adequate service without delays, additional channels are provided and "linked" to the first. This linking is a program convention whereby the two or more channels of the link are treated for routing purposes as a single channel. When there is message traffic for

5.0 COMMUNICATIONS INTERFACES

The IOC I-S/A AMPE shall implement a standard set of interfaces and protocols to communicate with standard subscriber terminals and the IAS network. There shall be variations required for certain specific subscribers as specified herein.

5.1 Subscriber Interfaces

5.1.1 General Subscriber Terminal Interfaces

The I-S/A AMPE shall be capable of interfacing to terminals which conform to the IAS physical and link level protocols specified in paragraphs 4.2.1 and 4.2.2. Terminal speeds up to and including 9.6 kilobits/sec shall be supported.

5.1.2 Specific Subscriber Interfaces

The interfaces of specific US and Allied subscribers are specified herein.

5.1.2.1 US Subscriber Interfaces

5.1.2.1.1 ASC Transitional/I-S/A AMPE Contingency Interface

The I-S/A AMPE shall be required to interface with the AUTODIN Switching Centers (ASCs) to exchange message traffic. The I-S/A AMPE shall interface with the ASC using AUTODIN MODE I protocols for terminals. During traffic interchange with ASCs, the I-S/A AMPE will be viewed by the ASCs as an AUTODIN terminal. In like fashion, under contingency conditions, two directly connected I-S/A AMPEs shall be able to interchange message traffic.

5.1.2.1.2 Tactical Interface

The I-S/A AMPE shall be designed to interface with the TRI-TAC equipment in accordance with TRI-TAC Interface Control Document, ICD-015, see 2.5h.

5.1.2.1.3 General Services Administration (GSA) Interface

The GSA Advanced Record System (ARS) users shall interface to the I-S/A AMPE via DCS Mode I, using the JANAP-128 format with the following exceptions (see Reference 2.5j.):

a. Straggler detection is not universally provided on messages received from GSA. Upon receipt of a GSA message without an EOM validation number (EOMVALNO), the I-S/A AMPE shall append the correct EOMVALNO to the message so that the message can then be processed through the AUTODIN network the same manner as other messages.

b. Suspected duplicate messages received for delivery to GSA shall have the pilot stripped by the destination I-S/A AMPE prior to transmission to GSA.

transmission to the subscriber, the primary channel (the "prime" is the first linked member) is used. If it is busy, the second channel is selected. If it is busy, the third, and so on. While there is no theoretical limit to the number of channels which can be linked, the practical limit so far as need is concerned is usually 4 or 5 members. These channels are designated for reference purposes as A, B, C, etc. When members of a link use Transmission Identifier (TI) lines, the Channel Identifier portion of the TI Line has the alphabetic designator as the third character so that if, for example, terminal RUXXKLA is connected to the I-S/A AMPE by three linked channels, the "Channel Identifier" will be KLA, KLB, and KLC. All link member channels shall be classmarked identical so far as communities, security, and Language Media Format (LMF) are concerned. Members can be of different speed and contain different cryptos and modems. This will be a controlled capability offered only to selected subscribers and shall be under close control by the I-S/A AMPE.

5.2 Network Interface

The I-S/A AMPE shall have a standard network interface with the IAS backbone. The IOC I-S/A AMPE standard interface to the backbone is supported by a layered protocol structure described in paragraph 4.1. The standard link protocol to the network shall be in accordance with paragraph 4.2.2.1.f. At higher levels the standard protocols to the network shall be in accordance with paragraphs 4.2.3, 4.2.4, 4.2.5 and 4.2.6.

Strict adherence to protocol layering is required so that (1) additional protocols can be added at the appropriate levels under the functional modularity growth feature, and (2) existing protocols can be modified and/or replaced without mutual interferences. The requirement for security shall not nullify the requirement for protocol layering. This constraint is necessary so that Red/Black separation can be placed at any desired level in the protocol hierarchy. If for security reasons a protocol is separated into secure and non-secure functions, these functions shall not be combined with functions of other protocols.

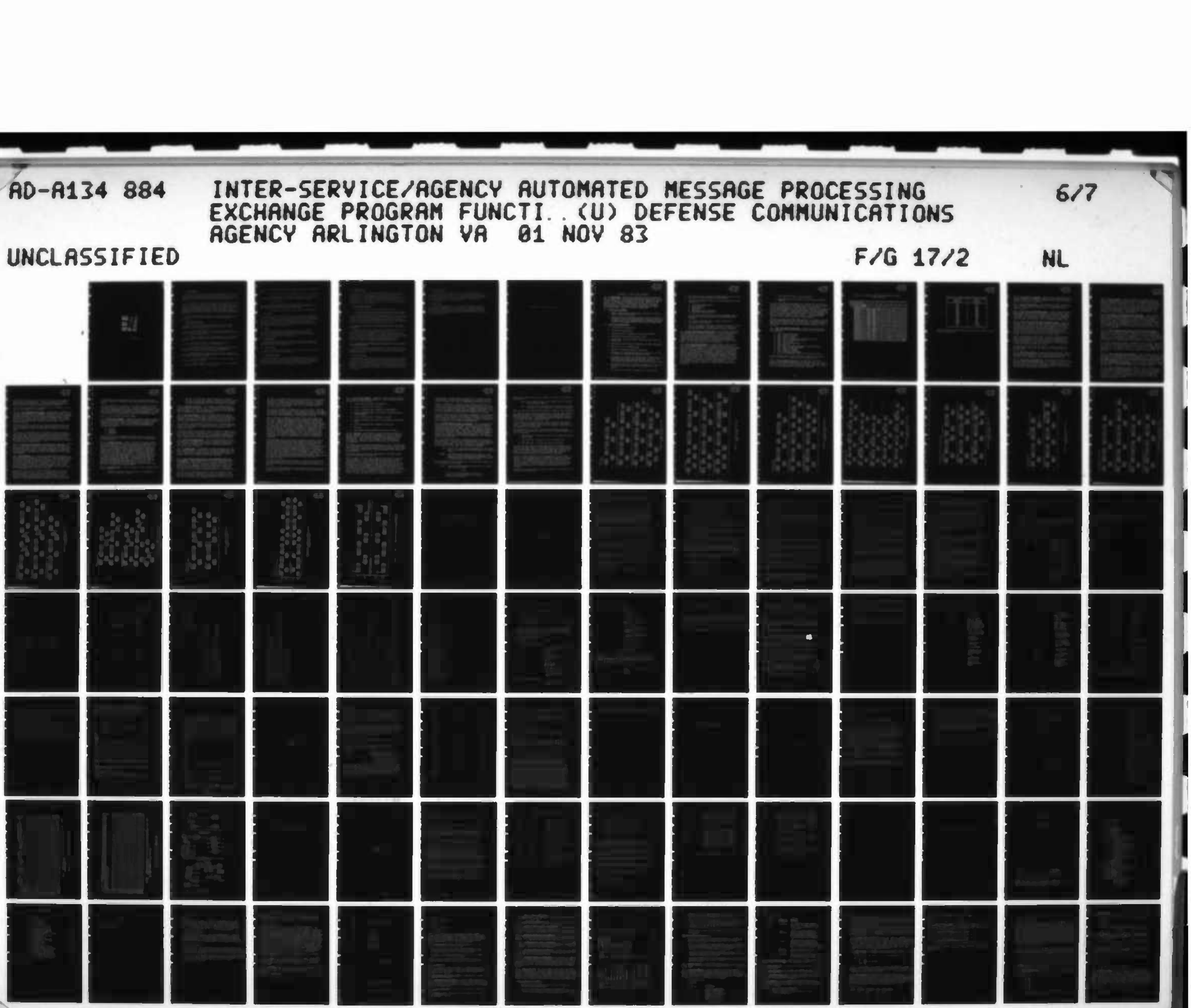
5.3 AUTOVON Interface

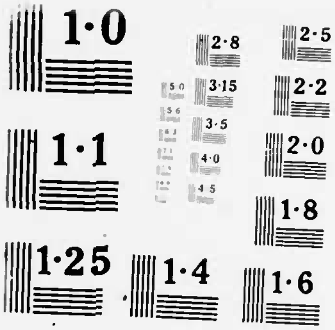
The contractor shall design the AUTOVON interface to be used for trunk and subscriber line restoral in degraded mode by dial-up and manual patch. The parameters for the interface shall be in accordance with DCAC 370-V175-6 "AUTOVON System Interface Criteria, Chapter XI, Interface with Other Systems." The contractor shall use available AUTOVON station arrangements to provide the terminal and modems and data auxiliary equipment. The speeds that shall be accommodated are:

75 X 2**n bits/sec
n=1,2,3,4,5,6,7

AD-A134 884 INTER-SERVICE/AGENCY AUTOMATED MESSAGE PROCESSING 6/7
EXCHANGE PROGRAM FUNCTI..(U) DEFENSE COMMUNICATIONS
AGENCY ARLINGTON VA 01 NOV 83

UNCLASSIFIED F/G 17/2 NL





NATIONAL BUREAU
MICROCOPY RESOLUTION TEST

6.0 HUMAN INTERFACES

The purpose of human engineering design principles and practices is to achieve mission success through integration of the human factors into the system, subsystem, equipment, facility and achieve effectiveness, simplicity, efficiency, reliability and safety of system operation, training and maintenance.

The I-S/A AMPE shall be designed to provide work environments which foster effective procedures, work patterns and personnel safety and health and which minimize discomfort, distraction and any other factors which degrade human performance or increase the probablity of error. A fail safe design shall be provided in those areas where failure can disable the system or cause catastrophe through damage to equipment. The I-S/A AMPE shall represent the simplest design consistent with functional requirements and expected service conditions.

The contractor shall use and comply with the criteria specified in MIL-STD-1472B, MIL-P-7788, MIL-STD-188-114, MIL-STD-195, MIL-STD-454 and MIL-H-46855.

6.1 Human Engineering Design

The design of the I-S/A AMPE shall include consideration of human engineering, life support, and biomedical factors that affect human performance including, when applicable:

a. Satisfactory atmospheric conditions including composition, pressure, temperature and humidity, including safeguards against uncontrolled variability beyond acceptable limits.

b. Range of acoustic noise, vibration, acceleration, shock, blast, and impact forces and safeguards against uncontrolled variability beyond acceptable limits.

c. Protection from thermal, toxicological, radiological, electromagnetic, pyrotechnic, visual, and other hazards.

d. Adequate space for personnel, their equipment, and free volume for the movements they are required to perform during operation and maintenance tasks under both normal and emergency conditions.

e. Adequate physical, visual, auditory, and other communication links between the personnel, and between personnel and their equipment, under both normal and emergency conditions.

f. Efficient arrangement of operation and maintenance workplaces, equipment, controls, and displays.

g. Adequate natural or artificial illumination for the performance of operation, control, training, and maintenance.

h. Provision of non-restrictive personal life support and protective equipment.

i. Provisions for minimizing psychophysiological stress, and fatigue.

j. Design features to assure rapidity, safety, ease and economy of maintenance in normal, adverse and emergency maintenance environments.

k. Satisfactory tools.

l. The clothing and personal equipment (C/PE) to be worn by personnel operating or maintaining the equipment shall be considered in the design location and layout of workspace and maintenance.

m. Information processing rates, decision-making effectiveness.

6.2 Interaction

The design of the I-S/A AMPE shall reflect the interaction requirements of crew served equipment. If more than one crew member must have simultaneous access to a particular group of controls or displays in order to insure proper functioning of a system/subsystem, the operator assigned to control and monitor a particular function shall have physical and visual access to all controls and displays necessary. The interaction shall be in accordance with the documents specified in paragraph 6.0.

6.3 Safety

The contractor shall give careful consideration to safety factors including minimization of potential human error in the operation and maintenance of the system. The contractor shall conform to the procedures within the documents specified in paragraph 6.0.

6.4 Maintainability

The contractor shall design the I-S/A AMPE to incorporate standard parts to the maximum extent possible and shall conform to the specifications within the documents specified in paragraph 6.0.

6.4.1 Special Tools

Special tools required for adjustment shall be securely mounted within the equipment in a readily accessible location.

6.4.2 Modular Replacement

The I-S/A AMPE shall be designed and constructed for replacement of small electronic assemblies by replacing modular packages. It shall be designed in a manner such that rapid and easy removal and replacement can be accomplished by one person where structural and functional limitations permit within the weight limitations contained in paragraph 5.9.11.3 of MIL-STD-1472B.

7.0 SECURITY CONTEXT

It must be carefully noted that the I-S/A AMPE has the requirement to simultaneously handle messages at varying levels of classification and compartmentation. This simultaneous multi-classification, multi-compartmentation usage dictates very close attention to the security aspects associated with the I-S/A AMPE (e.g., design, test, installation, etc.) Adequate security reliability (i.e., the required security protection level is maintainable) can be achieved provided there is strict compliance with the following security requirements.

7.1 Functional Requirements

The I-S/A AMPE design shall provide the following features:

7.1.1 Protection from Unauthorized Disclosure or Compromise of Information

This feature implements both the nondiscretionary (or mandatory) and the discretionary DoD Security Policies in that information will be disclosed only to users or subscribers who are cleared for the information's level of classification and also possess the required "need to know" certification. This feature requires that all authorized users or subscribers be "well known" to their servicing I-S/A AMPE and be positively identified.

7.1.2 Protection from Denial of Authorized Service to Authorized Users or Subscribers

This feature entails that information be accepted from, and delivered to, only authorized and specifically addressed users or subscribers. Additionally, for certain categories or classes of users or subscribers, authorized services are guaranteed to be available, assuming that the system is in fact operational. Other terminology often used for this feature is that the system will be "non blocking" to certain categories of users or subscribers. However, this feature obviously must comply with the restrictions imposed by the protection from compromise feature.

7.1.3 Protection from the Undetected Unauthorized Alteration of Information Entrusted to the System

This feature insures the integrity of both the system itself as well as the information (messages) transiting the system. Additionally, this feature complements and complies with the restrictions imposed by the two features previously discussed.

7.2 Network Connection

For DDN connectivity, the Fault Isolation and Correction (FI&C) Capability (see FRD para 3.3.7) shall ensure that the network connections(s) are via an End-to-End Encryption (E^3) device and if the network switching node is not collocated, that an appropriate link encryption device is also on the line and operational. The FI&C shall ensure that units associated with the network interconnection are properly synchronized. For AUTODIN connectivity, the FI&C shall ensure an appropriate link encryption device is online and operational where required.

7.3 I-S/A AMPE Design

The design of I-S/A AMPE shall take full advantage of the Trusted Computing Base Technology (see FRD 3.4). At IOC there shall be two general categories of I-S/A AMPE; GENSER - processing traffic to and from subscribers in the GENSER community only, and DSSCS - processing GENSER and DSSCS traffic to and from subscribers in the DSSCS community ONLY (DSSCS terminal are allowed to process traffic in both communities).

7.4 Terminal Data

All terminals requiring FMS will have a "home" I-S/A AMPE. Therefore, each terminals's characteristics will be well known. These characteristics shall be stored in the I-S/A AMPE and checked on a message by message basis. For terminals that are dual homed or have a pre-planned alternate servicing I-S/A AMPE, the terminal characteristics shall also be stored in the second or alternate I-S/A AMPE(s).

APPENDIX A: Mode IB Link Protocol

SECTION 25 - MODE IB LINK PROTOCOL

25.1 INTRODUCTION. Mode IB is a character-oriented synchronous type of link control which uses character parity and block parity checking along with retransmission of errored messages to achieve an error detection and correction capability. AUTODIN II will operate with subscribers conforming to the Two-Way Alternate Point-to-Point link control procedures described in documents referenced below. This mode is used by subscribers who employ Binary Synchronous Communications (BSC) procedures.

25.2 APPLICABLE DOCUMENTS

a. Binary Synchronous Communications, IBM Order No. GA27-3004-2, dated October 1970.

b. American National Standards Institute (ANSI) X3.28-1971 - Procedures for the use of Communication Control Characters of American National Standard Code for Information Interchange in Data Communications Links, dated 10 March 1971.

25.3 MODE IB CHARACTERISTICS

a. Block-by-block coordination

b. Synchronous transmission

c. Half-duplex data transmission (two-way alternate)

d. Character parity and block parity (BCC)

e. Transmission code 8-bit ASCII (seven data bits plus one parity bit)

f. Odd parity for all control characters and data characters

g. Each block is of variable length

h. Number of blocks per message is variable

i. Characters are transmitted serially bit-by-bit, with the low order bit first and the parity bit last

j. A message will consist of a header block preceded with SOH characters and ending with ETB and BCC. Also, the last block begins with STX and ends with ETX and BCC. Intervening blocks begin with STX and end with ETB and BCC

k. The character parity is checked and generated by the Line Termination Unit (LTU), both at the input and at the output

l. The status of the check is passed on to LCM software

1

m. The block parity is checked and generated by the LCM, and the status is made available to TAC software

n. The status information that will be made available to TAC software is:

   1. Loss of synchronization
   2. Character error
   3. Block error
   4. ETB, ETX
   5. Synchronization established
   6. Byte count equal to zero

o. LCM will not initiate recovery or acknowledgment procedures other than inform TAC with the above-mentioned statuses

p. All actions resulting from the above statuses are initiated by TAC software

q. LCM will recognize and remove all SYNC characters from the input data stream. Indication that LCM is receiving synchronization will be available for status reporting.

25.4 BINARY SYNCHRONOUS COMMUNICATIONS. Binary Synchronous Communications (BSC) procedure provides a set of rules for synchronous transmission of binary coded data. All data in BSC is transmitted as a serial stream of binary digits. Synchronous communications means that the active receiving station on a communications channel operates in step with the transmitting station through the recognition of a specific bit pattern (sync pattern) at the beginning of each transmission.

25.5 POINT-TO-POINT OPERATION. A point-to-point data link consists of a communications facility between only two stations. For point-to-point operation, a contention situation exists whereby both stations can attempt to use the communication line simultaneously. To minimize this possibility, a station bids for the line using the ENQ control character. Refer to the Mode IB formats in paragraph 25.12. The SYNC SYNC ENQ sequence (SYNC SYNC represents the synchronous idle characters) provides the means for controlling the line. If simultaneous bidding occurs, one station must persist in its bidding attempt to break the contention condition. A station receiving this sequence (and ready for message reception) replies with SYNC SYNC ACK0. If the station is not ready to receive, it replies with either of the following:

a. SYNC SYNC NAK (negative acknowledgment)

b. SYNC SYNC WACK (wait before transmit positive acknowledgment).

To avoid the problems associated with simultaneous transmission requests, each station is assigned a priority - primary or secondary. The higher priority (primary) station sends an ENQ to acquire the idle line. It will continue to do so until it receives an affirmative response or until the retry limits of the primary station are reached. If the primary station receives an ENQ and it has not initiated a request for the line, then it replies with ACK0 (if ready to receive), WACK, or NAK. Thus the secondary station can gain control of the line for a transmission only when the line is left free by the primary station.

Message transmission is ended and the line is returned to an idle state by the transmission of SYNC SYNC EOT. The station sending SYNC SYNC EOT will not send an initialization sequence before 3 seconds have elapsed, thus allowing the other station to bid for the line.

25.6 DATA LINK CONTROL CHARACTERS. Mode IB protocols control data links through the use of the following control characters and sequences:

a. SYNC - Synchronous idle
b. SOH - Start of heading
c. STX - Start of text
d. ITB - End of intermediate transmission block
e. ETB - End of transmission block
f. ETX - End of text
g. EOT - End of transmission
h. ENQ - Enquiry
i. ACK0/ACK1 - Alternate affirmative acknowledgment
j. NAK - Negative acknowledgment
h. DLE - Data link escape
l. RVI - Reverse interrupt
m. TTD - Temporary text delay
n. DLE EOT - Disconnect sequence for switched network.

The bit configuration of Mode IB control characters is shown in Tables B-IV and B-V. Refer to Mode IB formats in 25.12.

25.6.1 SYNC - Synchronous Idle. This character is used to establish and maintain synchronization and as a time fill in the absence of any data or other control character. Two contiguous SYNC's at the start of each transmission (SYNC SYNC) are referred to as the character-phase synchronization pattern.

Table B-IV. USASCII Character Assignments in Mode IB or BSC Protocols

b7 b6 b5 Bits					0 0 0	0 0 1	0 1 0	0 1 1	1 0 0	1 0 1	1 1 0	1 1 1
b4	b3	b2	b1	COLUMN / ROW	0	1	2	3	4	5	6	7
0	0	0	0	0	NUL	DLE	SP	0	@	P	`	p
0	0	0	1	1	SOH	DC1	!	1	A	Q	a	q
0	0	1	0	2	STX	DC2	"	2	B	R	b	r
0	0	1	1	3	ETX	DC3	#	3	C	S	c	s
0	1	0	0	4	EOT	DC4	$	4	D	T	d	t
0	1	0	1	5	ENQ	NAK	%	5	E	U	e	u
0	1	1	0	6	ACK	SYN	&	6	F	V	f	v
0	1	1	1	7	BEL	ETB	'	7	G	W	g	w
1	0	0	0	8	BS	CAN	(	8	H	X	h	x
1	0	0	1	9	HT	EM	)	9	I	Y	i	y
1	0	1	0	10	LF	SUB	*	:	J	Z	j	z
1	0	1	1	11	VT	ESC	+	;	K	[	k	{
1	1	0	0	12	FF	FS	,	<	L	\	l	¦
1	1	0	1	13	CR	GS	–	=	M	]	m	}
1	1	1	0	14	SO	RS	.	>	N	^	n	~
1	1	1	1	15	SI	US	/	?	O	_	o	DEL

Table B-V. Control Character Conversion Chart

Data Link Character	ASCII Character
SYN	SYN
SOH	SOH
STX	STX
ETB	ETB
ETX	ETX
EOT	EOT
ENQ	ENQ
ACK0	DLE0
ACK1	DLE1
NAK	NAK
DLE	DLE
ITB	US
WACK	DLE;
RVI	DLE<
TTD	STX ENQ

NOTE: Control Characters ACK0, ACK1, WACK, RVI, and TTD are two character sequences.

25.6.2 SOH - Start of Heading. This character precedes a block of heading characters. A heading consists of auxiliary information (such as routing and priority) necessary for the system to process the text portion of the message.

25.6.3 STX - Start of Text. This character precedes a block of text characters. Text is that portion of a message treated as an entity to be transmitted through to the ultimate destination without change.

25.6.4 ETB - End of Transmission Block. The ETB character indicates the end of a block of characters started with SOH or STX. The blocking structure is not necessarily related to the processing format. The block-check character (BCC) is sent immediately following ETB. ETB requires a reply indicating the receiving station's status (ACK0, ACK1, NAK, or, optionally, WACK or RVI).

25.6.5 ITB - End of Intermediate Transmission Block. The ITB character (US in USASCII) is used to divide a message (heading or text) for error checking purposes without causing a reversal of transmission direction. The block check character (BCC) immediately follows ITB and resets the block check count. After the first intermediate block, successive intermediate blocks of the same type (heading or text) need not be preceded by STX or SOH. If one intermediate block is heading and the next intermediate block is text, STX must begin the text block.

Normal line turnaround occurs after the last intermediate block, which is terminated by ETB or ETX. When one of these ending characters is received, the receiving station responds to the entire transmission. If a block check error is detected for any of the intermediate blocks, a negative reply is sent requiring transmission of all intermediate blocks.

All BSC stations must have the ability to receive ITB and its attendant BCC. The ability to transmit the ITB character is a station option.

25.6.6 ETX - End of Text. The ETX character terminates a block of characters started with STX or SOH and transmitted as an entity. The block check character is sent immediately following ETX. ETX requires a reply indicating the receiving station's status.

25.6.7 EOT - End of Transmission. This character indicates the end of a message transmission, which may contain one or more blocks, including text and associated heading. It causes a reset of a station on the line. EOT is also used as an abort signal to indicate a system malfunction or operational situation that precludes continuation of the message transmission.

6

25.6.8 ENQ - Enquiry. The ENQ character is used to obtain a repeat transmission of the response to a message block if the original response was garbled or was not received when expected. ENQ is also used to bid for the line when using a point-to-point line connection. If the sender wishes to abort a transmission, an ENQ may be inserted following text characters and the block is not terminated with ETB or ETX and BCC. The receiver will discard the transmission. NAK (Negative Acknowledgment) is the reply to the aborted transmission.

25.6.9 ACK0/ACK1 - Affirmative Acknowledgment. ACK0 and ACK1 are the two character sequences DLE0 and DLE1, respectively. Where required, these replies, in proper sequence, indicate that the previous block was accepted without error and that the receiver is ready to accept the next block of the transmission. ACK0 is the positive response to line bid in operation. Mode IB alternately uses ACK0 and ACK1 as affirmative replies. The use of ACK0 and ACK1 provides a sequential checking control for a series of replies.

25.6.10 WACK - Wait-Before-Transmit Positive Acknowledgment. WACK (DLE; in USASCII) allows a receiving station to indicate a temporarily not ready to receive condition to the transmitting station. It can be sent as a response to a text or heading block, line bid (point-to-point with contention), or an ID (identification number) line bid sequence (switched network). WACK is a positive acknowledgment to the received data block or to selection.

The normal transmitting station response to WACK is ENQ, but EOT and DLE EOT (switched network) are also valid responses. When ENQ is received, the receiving station will continue to respond with WACK until it is ready to continue. The ability to receive WACK is mandatory for all stations, but the capability to send WACK is optional.

25.6.11 NAK - Negative Acknowledgment. NAK indicates that the previous block was received in error and that the receiver is ready to accept a retransmission of the erroneous block. It is also the not-ready reply to line bid. Upon receipt of 3 NAKS for a single line block, the higher level protocol will be notified and attempts to deliver this line block will continue.

25.6.12 DLE - Data Link Escape. DLE is a control character used exclusively to provide supplementary line control characters, such as WACK (DLE;), ACK0 (DLE0), ACK1 (DLE1), and RVI (DLE<).

25.6.13 RVI - Reverse Interrupt. The RVI (DLE< in USASCII) control sequence is a positive response used in place of the ACK0 or ACK1 positive acknowledgment. RVI is transmitted by a receiving station to request termination of the current transmission because of a high priority message which it must transmit to the sending station. Successive RVI's cannot be transmitted, except in response to ENQ.

7

The sending station treats the RVI as a positive acknowledgment and responds by transmitting all data that prevents it from becoming a receiving station. More than one block transmission may be required to empty the sending station's buffers.

The ability to receive RVI is mandatory for all stations, but the ability to transmit RVI is optional.

25.6.14 TTD - Temporary Text Delay. The TTD control sequence is sent by a sending station in message transfer state when it wishes to retain the line, but is not ready to transmit. The TTD control sequence (STX ENQ) is normally sent after approximately 2 seconds if the sending station is not capable of transmitting the next text block or initial text block within that time. This 2-second timeout avoids the nominal 3-second receive timeout at the receiving station.

The receiving station responds NAK to the TTD sequence and waits for transmission to begin. If the sending station is still not ready to transmit, the TTD sequence can be repeated one or more times.

This delay in transmission can occur when the sending station's input device has not completely filled the buffer due to inherent machine timings. TTD is also transmitted by a sending station in message transfer mode to indicate to the receiver that it is aborting the current transmission. After receiving NAK to this TTD sequence, the sending station sends EOT resetting the stations to control mode (forward abort).

25.6.15 Disconnect Sequence for a Switched Line - DLE EOT. Transmission of DLE EOT on a switched line indicates to the receiver that the transmitter is going on-hook. Either the calling or the called station may transmit this disconnect sequence. DLE EOT is normally transmitted when all message exchanges are complete and may optionally be transmitted at any time instead of EOT to cause a disconnect.

25.7 ERROR CHECKING. All characters received from the terminal subscriber will be passed to TAC (except for SYNC characters) after they are checked for odd parity by the LCM. If a character parity is detected, the appropriate status information will be set, and the LCM will continue to accept characters until a valid terminating character is received. On detection of ETX, ETB, or ITB, the next succeeding character will be compared to the locally generated longitudinal redundancy check (LRC), and an error status will be generated if the two do not compare.

In general, LRC is a longitudinal redundancy check on the total data bits within a block. An LRC is accumulated at both the sending and receiving ends during the transmission of a block. This accumulation is called the block check character (BCC), and it is transmitted immediately following an ETB, ETX, or ITB character. The transmitted BCC is compared with the accumulated

BCC character at the receiving station for an equal condition. An equal comparison indicates a good transmission of the previous block.

The LRC accumulation is reset by the first STX or SOH character received after a line turnaround. In normal transmission, all characters received after the SOH or STX to the ETB or ETX including control characters are included in the BCC accumulation. Only SYNC characters are not included in the BCC accumulation. Following an ITB BCC, the accumulation resets the block check count.

Refer to 25.12 for Mode IB data formats.

25.8 TIMEOUT REQUIREMENTS. Timeouts are used to prevent indefinite data-link tie-ups due to false sequences or missed turnaround signals by providing a fixed time within which any particular operation must occur. Due to the different requirements for the various operations, four specific timeout functions are provided as follows:

a. Transmit
b. Receive
c. Disconnect
d. Continue

The various timeout requirements of this protocol will not be performed by the LCM. These requirements will be implemented in the TAC software.

25.8.1 Transmit Timeout. There is a nominal 1-second timeout that establishes the rate at which synchronizing idles are automatically inserted into transmitted heading and text data. In normal data, the data is being transmitted over the link in a normal, or nontransparent mode, (data link control characters are recognized as such without being preceded by a Data Link Escape (DLE) character). Two consecutive SYNC-idle characters (SYNC SYNC) are inserted every second. If business machine clocking is used, DLE SYNC insertion is required at least every 84 characters to ensure maintenance of bit synchronization in the event of transitionless data. There must be at least 54 characters between each DLE SYNC. If there are less than 54 characters between DLE SYNC sequences, the line will lose its link protocol synchronization and loss of data will occur. SYNC-idles are inserted in the message for timing purposes only, and have no effect on the message format.

25.8.2 Receive Timeout. This is a nominal 3-second timeout and is used as follows:

a. Limits the waiting time tolerated for a transmitting station to receive a reply.

b. Permits any receiving or monitoring station to check the line for SYNC-idle signals. These SYNC-idles indicate that the transmission is continuing; thus, this timeout is reset and restarted each time a SYNC-idle is detected.

25.8.3 Disconnect Timeout. This timeout is used optionally on switched network data links. It is a nominal 20-second timeout used to prevent a station holding a connection for prolonged periods of inactivity. After 20 seconds of inactivity, the station will disconnect from the switched network.

25.8.4 Continue Timeout. This is a nominal 2-second timeout associated with the transmission of TTD and WACK. The continue timeout is used by stations where the speed of input devices (for transmitting stations) or output devices (for receiving stations) affect buffer availability and may cause transmission delays.

TTD is sent by the transmitting station up to 2 seconds after receiving acknowledgment of the previous block, if the transmitting station is not capable of sending the next transmission block before that time.

A receiving station must transmit WACK to indicate a temporarily not-ready-to-receive condition if it is not able to receive within the 2-second timeout. The purpose of the timeout interval is to permit the receiving station to send an appropriate affirmative reply immediately if it becomes appropriate within the interval.

25.9 LOSS OF SYNCHRONIZATION. Loss of synchronization will be determined by the reception of one 8-bit character of all zeros or all ones after character framing has already been established. Under these two conditions the LCM will immediately return to a waiting-for-input condition.

25.10 STANDARD CODE. The AUTODIN II system design provides for Mode IB subscribers to use an 8-bit, odd parity ASCII code. The ASCII code is shown in Table IV and will have an added eighth bit to form odd parity on each character. Parity code conversion on output lines will be matched to the ANSI standard.

25.11 LINE CONTROL MODULE (LCM) - LINE TERMINATION UNIT (LTU) REQUIREMENTS. Mode IB communication lines will be terminated in a synchronous LTU which, in turn, will be connected to an LCM microprocessor. Mode IB LTU's will terminate and control the operation of full-duplex, synchronous communication lines using point-to-point procedures. Mode IB utilizes 8-bit ASCII with seven bits used for data plus one odd-parity bit. Odd parity is maintained for all data, control, and block framing characters.

The interface of these communication lines is through a time-division multiplexer (TDM) which, in turn, interfaces the TDMI LCM on a bit serial, character multiplexed data stream. A ninth bit with each character is exchanged between the TDMI LCM and the TDM for providing TDM control and line control over and above the Mode IB protocol. This bit, when set to a one, indicates TDM control is contained in the following eight bits. This bit, when set to a zero, indicates valid data or control information is buried within the protocol and is to be exchanged between the node and the terminals.

The LTU will interface with the LCM via a bit parallel interface and convert the data to a serial bit stream on output. The least significant bit of the data will be serialized first and the parity bit position serialized last. Incoming serial data will be packed into a byte or word format prior to transfer to the LCM.

Mode IB data are formatted into blocks of variable length text data, with leading and trailing control characters framing this text data. Refer to paragraph 25.12 for Mode IB Data Formats. The final character of a block is a BCC, which is used for error control. The first character of a block is a SOH or STX. Receipt and recognition of SOH or STX will trigger the BCC accumulation for the block. The LTU/LCM will recognize the leading and trailing control characters. On input, recognition of the SOH/STX will start the text data transmission to the TAC. Detection of ETX or ETB will cause the BCC check to occur. The LCM will notify the TAC of block message completion by causing the appropriate status and interrupt to be generated. On output, these control characters will cause the appropriate actions in the opposite directions.

The maintenance of data and control character integrity requires proper synchronization between the transmitting and receiving elements of the communication path between the terminals. The synchronous channel card (SCC) in the TDM will maintain this synchronization in conjunction with commands from the KMC-11B/DMS-11B. The transmitter will precede all blocks of data with a minimum of four consecutive ASCII SYNC characters. The receiver will recognize two consecutive SYNC characters to synchronize itself. SYNC characters will not be forwarded to the TAC; however, an indication that the SCC is receiving synchronization will be available to the LCM for status reporting purposes. Synchronization will also be transmitted during the idle link state in the absence of data.

All Mode IB characters have odd parity. Once synchronization has been established, the LTU will check and flag any character received with even parity as an error and forward this condition to the LCM.

At the end of each transfer and upon request, a status word will be returned to the TAC processor. The status word will indicate the status of the lines.

25.12 MODE IB DATA FORMATS. Figure B-4 shows the Mode IB data formats that will be used in AUTODIN II. The following items are illustrated in these figures:

a. Initialization and One Way Operation

b. Control Character ENQ - Enquiry

c. Control Character NAK - Negative Acknowledgment

d. Control Character WACK - Wait Before Transmit Positive Acknowledgment

e. Control Character RVI - Reverse Interrupt

f. Control Character ITB - End of Intermediate Transmission Block

g. Control Character TTD - Temporary Text Delay

h. Timeouts

i. Half-Duplex Data Transmission (Two Way Alternate)

25.12.1 Heading. The heading is a block of data starting with SOH and containing one or more characters that may be used for message control, eg, message identification, routing, priority and security). SOH initiates the block-check-character (BCC) accumulation. The SOH is not included in the accumulation. The heading is ended with ETB followed by BCC as illustrated in Figure B-4.

The heading can be terminated prematurely by use of the ENQ (indicating disregard the block) without the ETB and BCC. The receiver will reply with a NAK and the heading will be retransmitted. This is illustrated in Figure B-4C., Control Character NAK - Negative Acknowledgment.

The Mode IB heading data is in accordance with the THP command procedures described in Section 27.

25.12.2 Text. The text data is the most significant portion of the transmission. It is transmitted in complete units called messages, which are initiated by STX and concluded with ETX. Each message is a complete unit that can stand alone and is not necessarily directly related to other messages being transmitted. A message can be subdivided into smaller blocks for ease in processing and more efficient error control. Each block starts with STX and ends with ETB (except for the last block of a message, which ends with ETX). A single transmission can contain any number of blocks (ending with ETB) or messages (ending with ETX). An EOT following the last ETX block indicates a normal end of transmission. Message blocking without line turnaround can be accomplished by using ITB (see paragraph 25.6.5 and Figure B-4F, Control Character ITB - End of Intermediate Transmission Block).

Control characters or sequences within a block of text are not allowed. Any station receiving a control character within a text block treats the control character or sequence as data and waits for the block check character (BCC) to detect a possible error. If an error is detected, normal recovery procedures are used. If no error is detected, the transmission is treated as valid data.

A block of text data can be terminated prematurely by using an ENQ character, which signals the receiver to "disregard this block". NAK is always the reply in this situation, since the block ended with a forced error condition. An example is shown in Figure B-4C, Control Character NAK - Negative Acknowledgment.

25.13 SWITCHED-NETWORK (DIALUP) OPERATION. For switched-network operation, the point-to-point connection can be established by either manual or automatic means. At the PSN the call will be answered automatically by TCMS. Dialed connections are operated as point-to-point lines with contention. Both stations start in the "circuit-assurance mode". Once circuit assurance is established and identified, the stations use the normal BCS procedures required for operation (switched point-to-point). When both stations have completed their message transmissions, a disconnect signal is normally sent.

The "circuit-assurance mode" is entered when the called station goes "off-hook". At this time the calling station is notified by a signal from its data set that a connection with another data set has been established. Once this indication is received, the calling station sends either of the following messages:

WRU - Who are you (the transmitted sequence is SYNC SYNC ENQ). This requests the called terminal to identify itself.

IAM/WRU - (the transmitted sequence is SYNC SYNC (ID) ENQ where ID = station identification sequence). This message identifies the calling station and requests the called station to identify itself.

Either message is then followed by an identification message from the called station as follows:

ID ACK0 - (the transmitted sequence is SYNC SYNC (ID) ACK0, where ID is optional).

NOTE

If the received ID sequence is unsatisfactory, then either station can initiate a disconnect sequence.

Additional signals available as a reply to the WRU or the IAM/WRU message are:

NAK - This indicates that a "not ready" condition exists at the called station.

WACK - (optional) This indicates that "temporary not ready to continue" condition exists at the called station.

Refer to Figure B-5 for Mode IB Switched - Network Dialup Operation.

All stations must provide the capability to transmit identification sequences in order to permit several stations to operate on the same switched line. An identification (ID) sequence can be from 2 to 15 characters long. The minimum 2-character sequence consists of the same character transmitted twice.

ID sequences may precede ENQ, ACK1, ACK0, and NAK in the control mode. A receiving station must be able to recognize the above control characters when preceded by an ID sequence. WACK must not be preceded by an ID sequence.

Both stations exit from the circuit-assurance mode following satisfactory initialization when any of the following sequences are sent or received:

a. SYNC SYNC EOT - Returns the data link to normal operation, control mode

b. SYNC SYNC SOH - Initiates a block of header data

c. SYNC SYNC STX - Initiates a block of text data

All signals other than those just described are considered to be errors. If a valid reply is not received by the calling station (following either a WRU or an IAM/WRU) within the receive timeout period, the request message can be retransmitted. However, the data link continues in the circuit-assurance mode until the circuit-assurance sequence is satisfactorily completed.

The call between stations can be terminated by the disconnect timeout or by transmission of the disconnect sequence: SYNC SYNC DLE EOT. This sequence may be initiated by either station when operating on a switched-network basis. When operating with a control station, the control station normally initiates the disconnect sequence. As this sequence is transmitted and received, each station returns to an on-hook condition and the line is dropped.

Although the switched network (dialup) operation is supported, the dialout is not permitted.

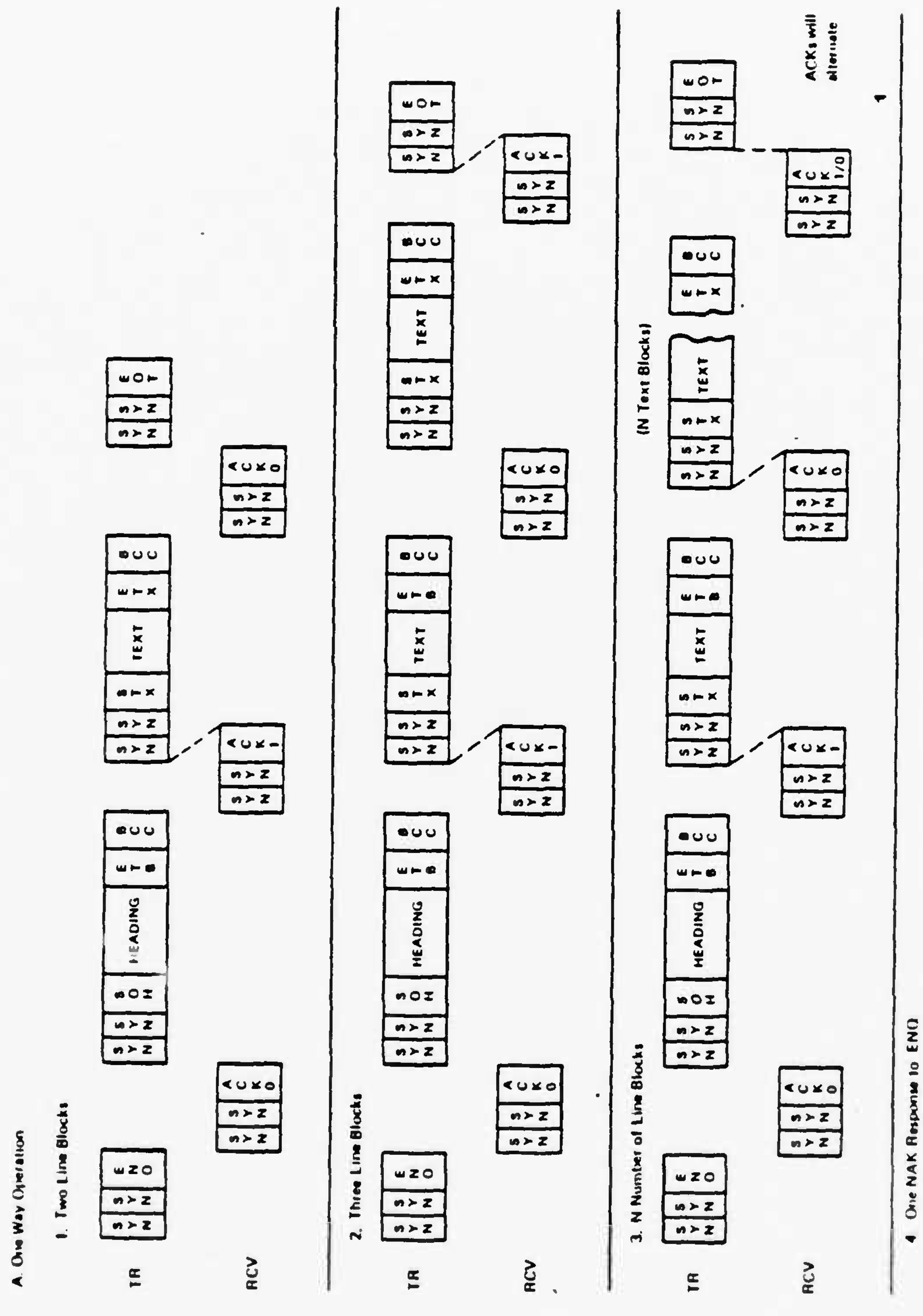


Figure B-4. Mode IB Link Protocols
(Sheet 1 of 11)

15

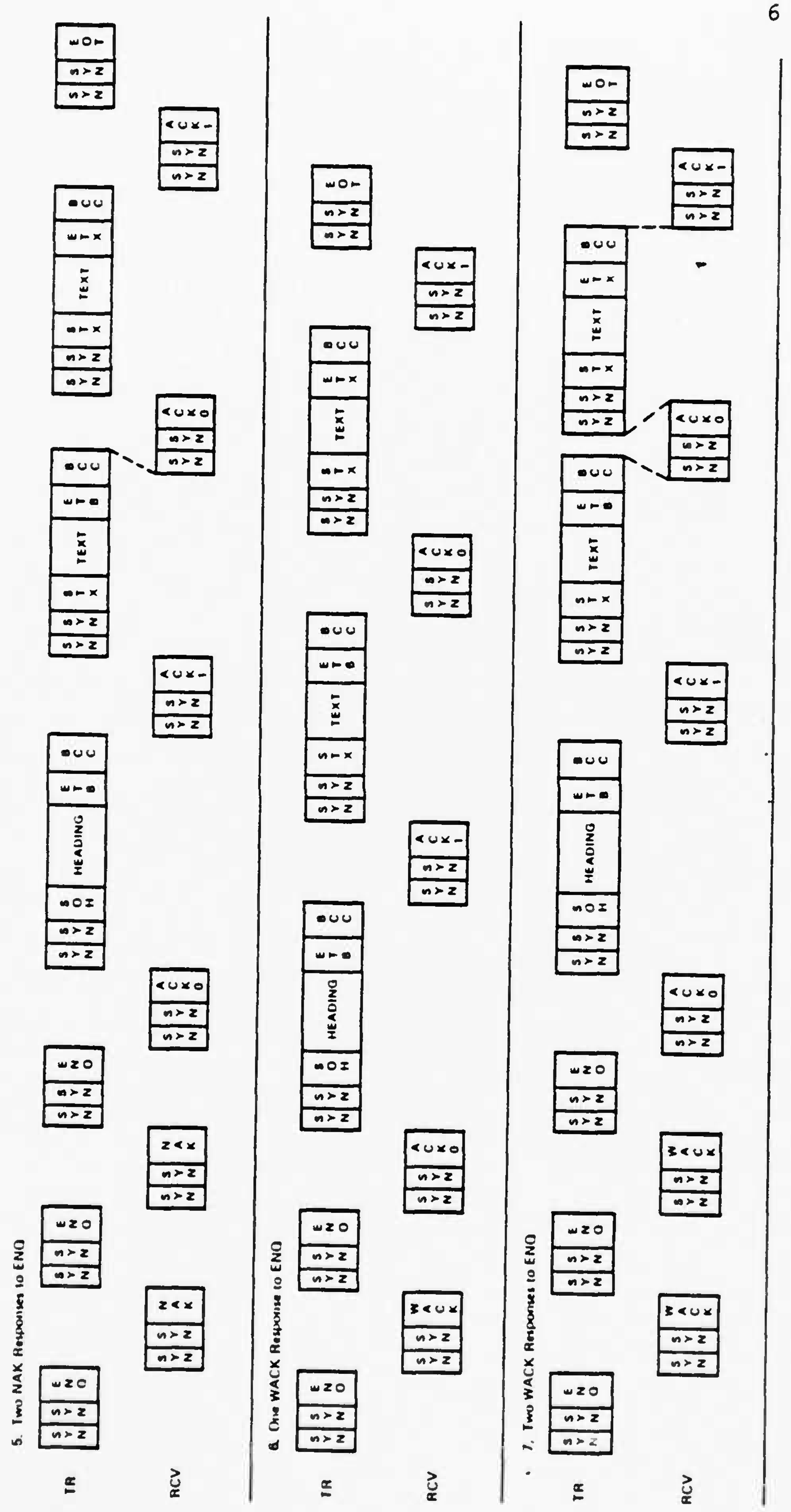

5. Two NAK Responses to ENQ
6. One WACK Response to ENQ
7. Two WACK Responses to ENQ
TR
RCV
SYN
SYN
ENQ
NAK
WACK
SOH
HEADING
ETB
BCC
STX
TEXT
ETX
ACK0
ACK1
EOT

Figure B-4. Mode IB Link Protocols
(Sheet 2 of 11)

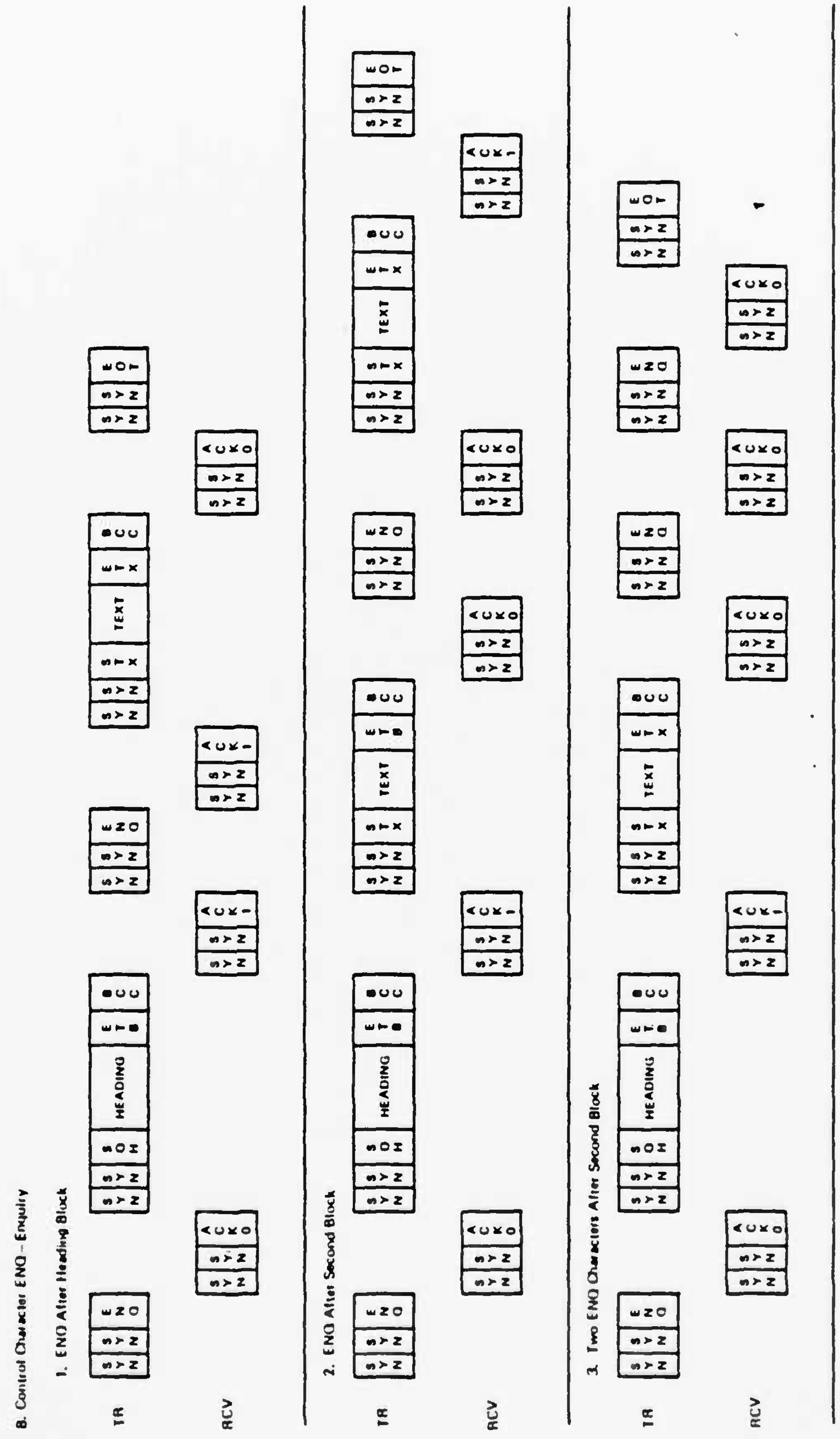


Figure B-4. Mode IB Link Protocols
(Sheet 3 of 11)

17

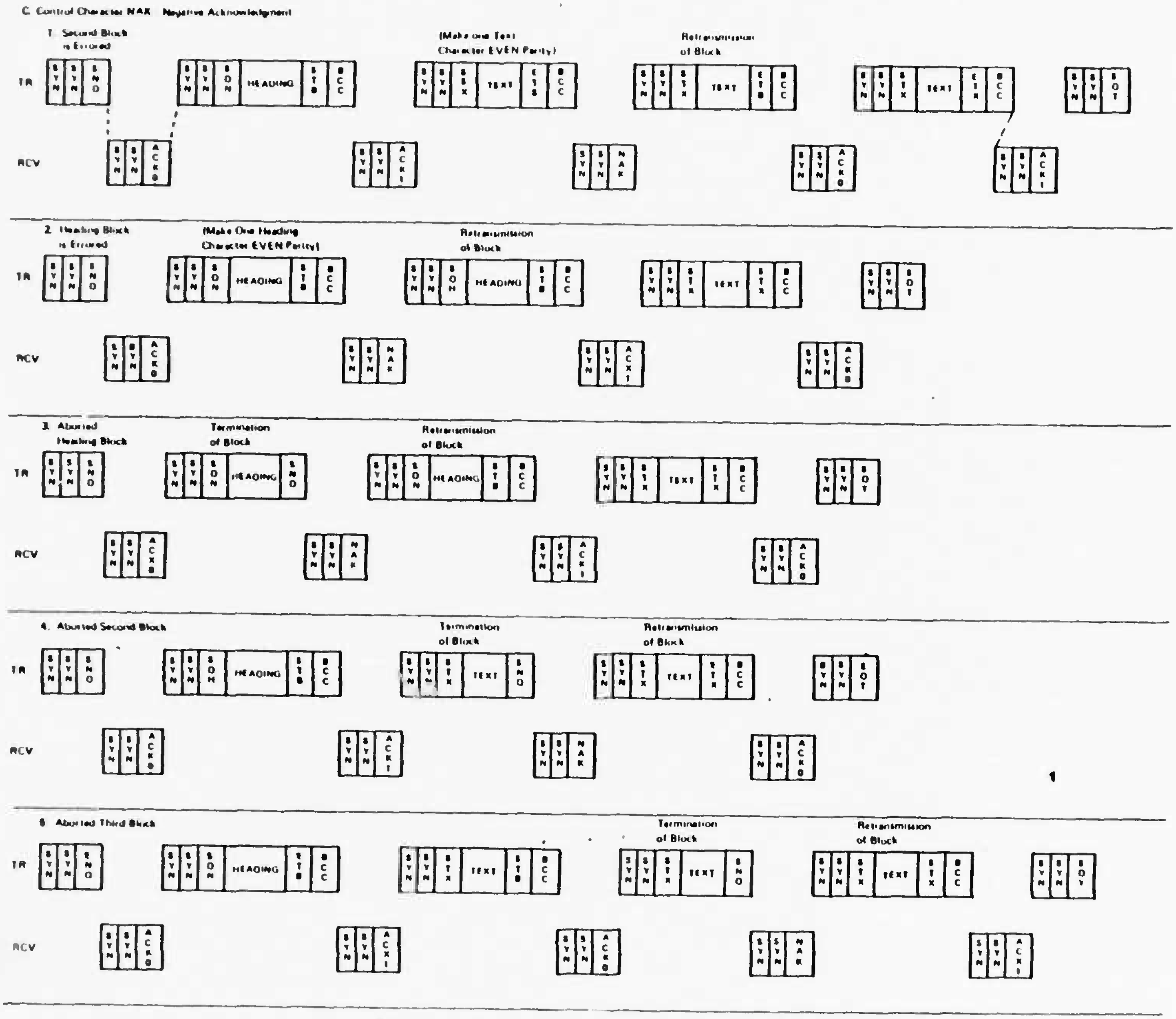


Figure B-4. Mode IB Link Protocols
(Sheet 4 of 11)

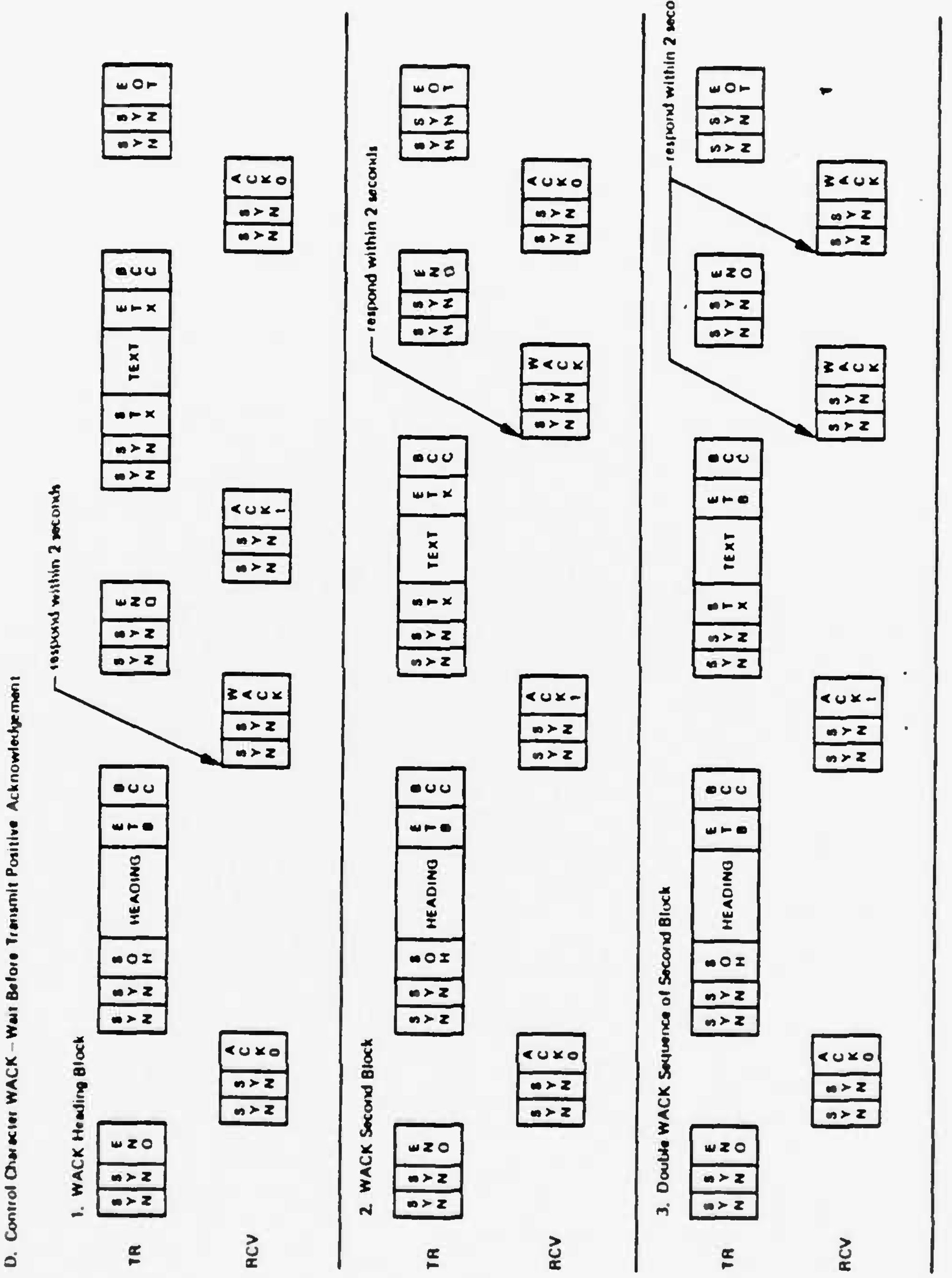


Figure B-4. Mode IB Link Protocols
(Sheet 5 of 11)

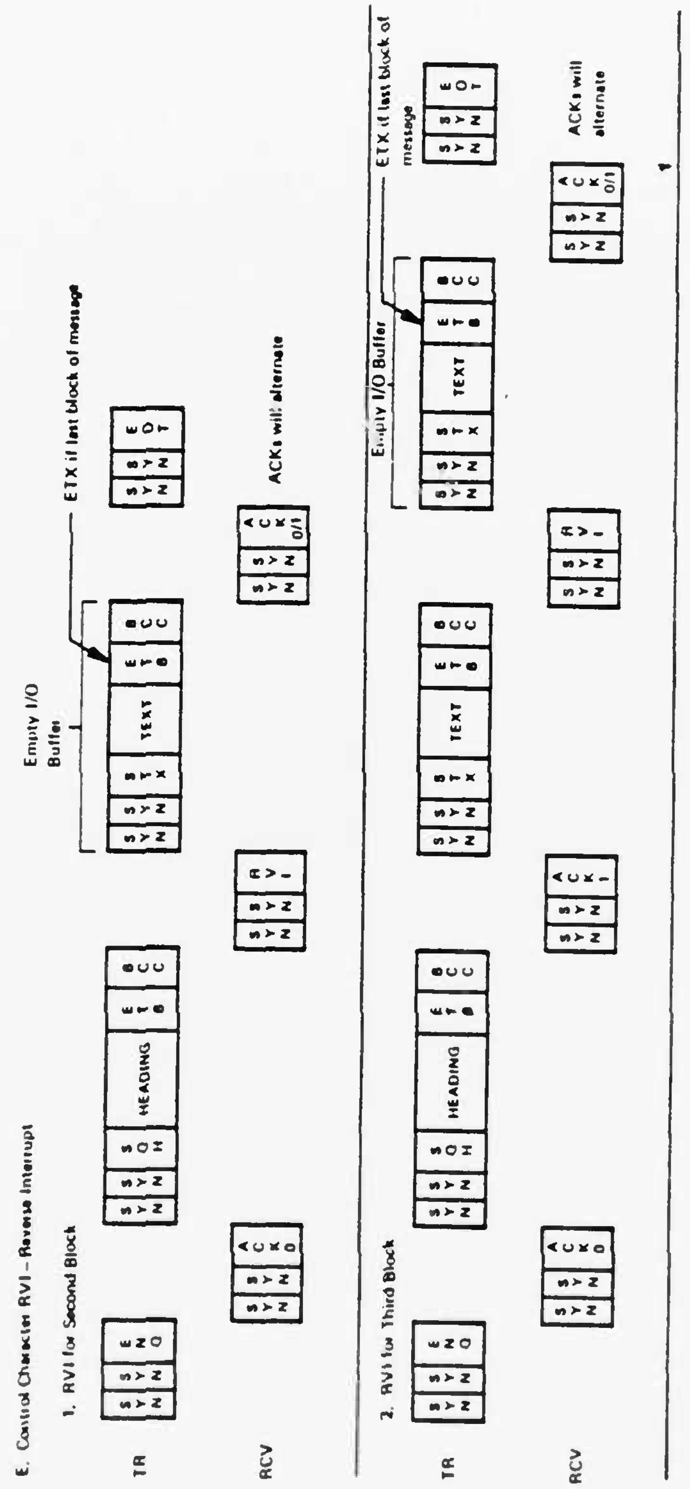


Figure B-4. Mode IB Link Protocols
(Sheet 6 of 11)

20

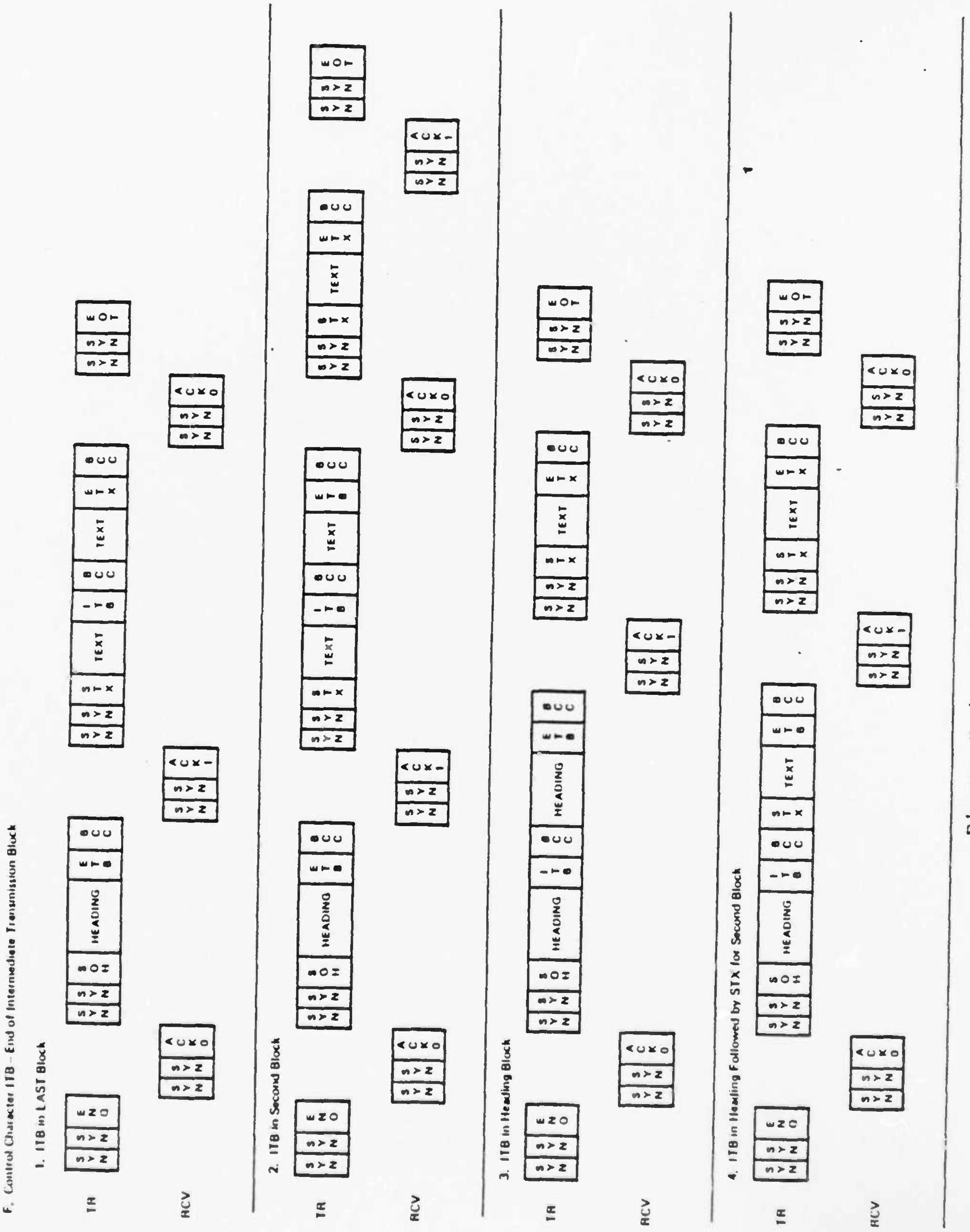


Figure B-4. Mode IB Link Protocols
(Sheet 7 of 11)

21

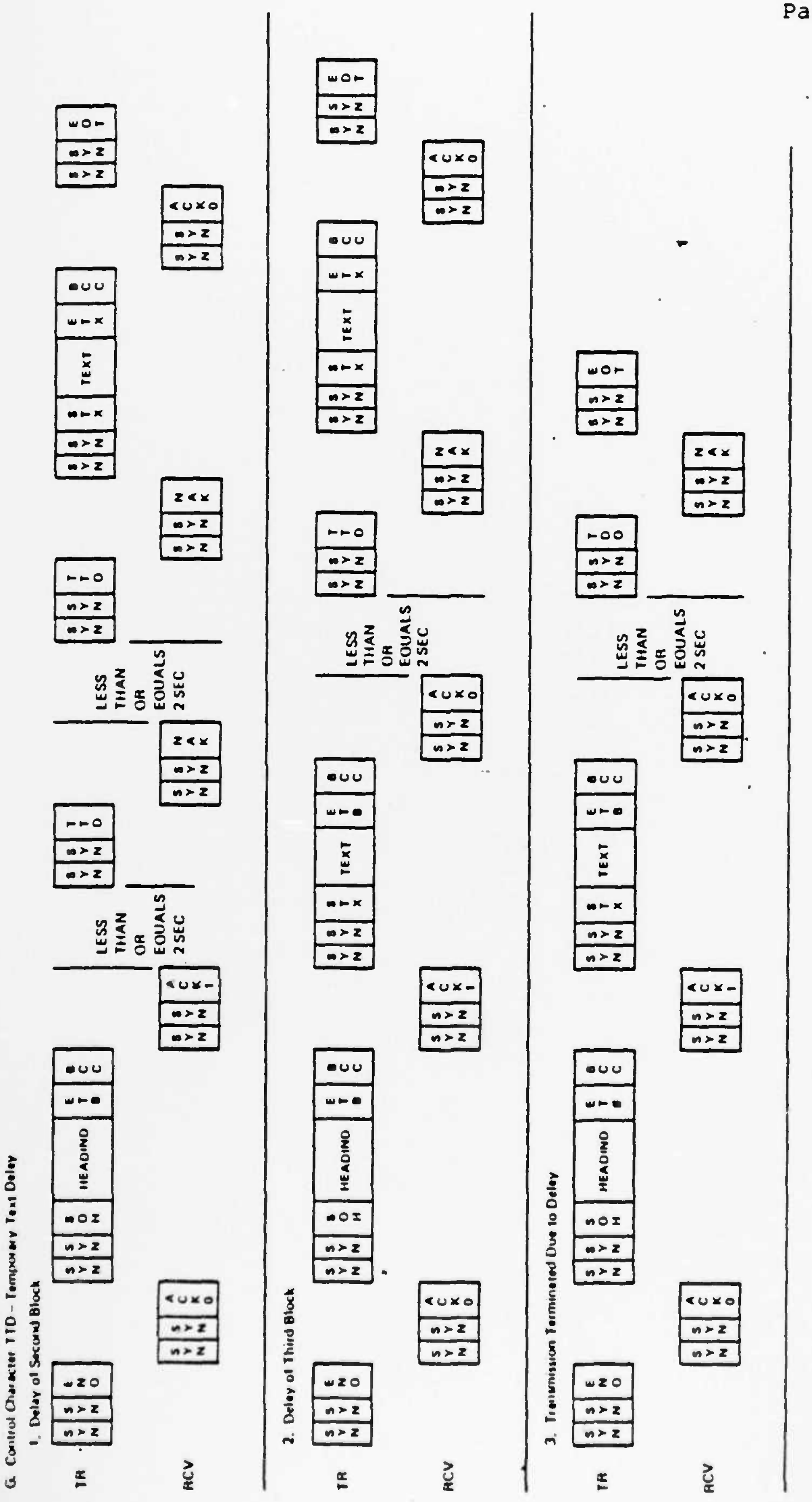

G. Control Character TTD – Temporary Text Delay
1. Delay of Second Block
2. Delay of Third Block
3. Transmission Terminated Due to Delay
TR
RCV
SYN
SYN
ENQ
SOH
HEADING
ETB
BCC
ACK0
ACK1
STX
TTD
NAK
TEXT
ETX
EOT
LESS THAN OR EQUALS 2 SEC

Figure B-4. Mode IB Link Protocols
(Sheet 8 of 11)

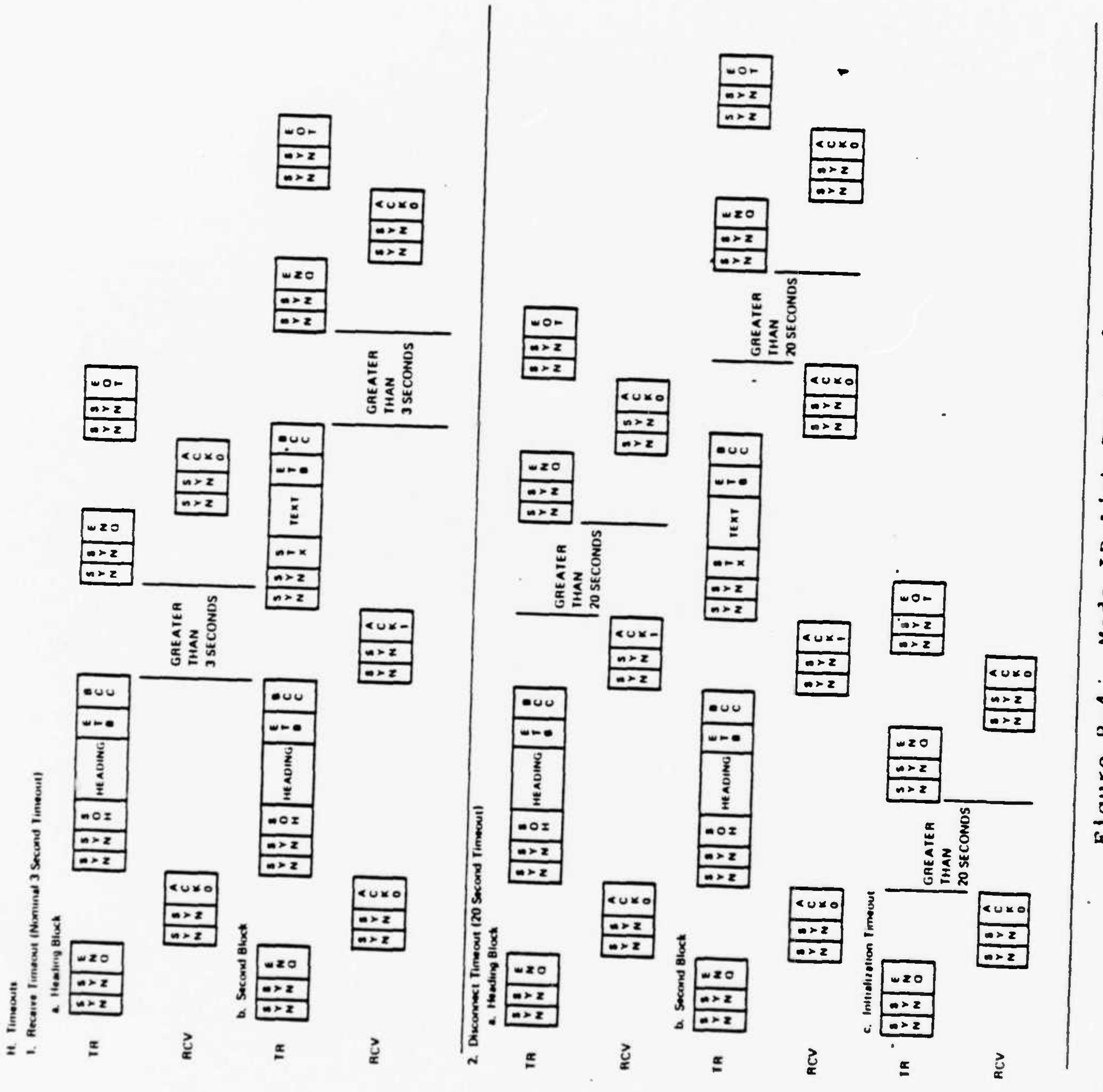
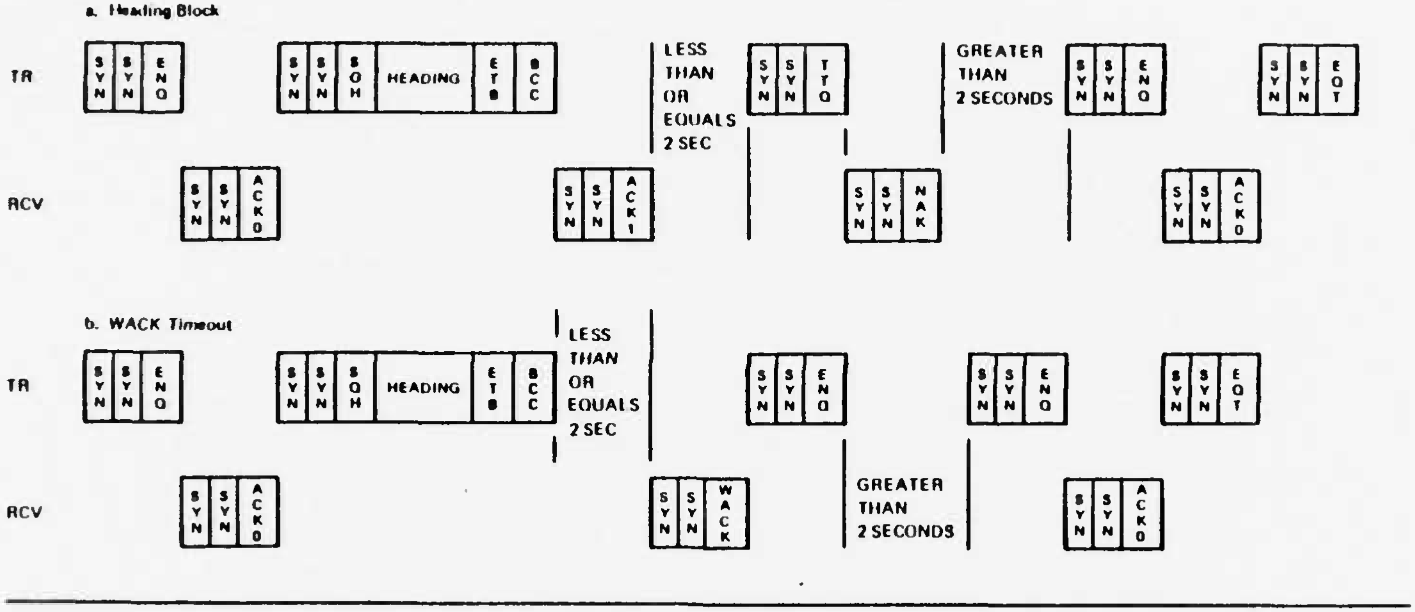


Figure B-4: Mode IB Link Protocols
(Sheet 9 of 11)

H. Timeouts (continued)

3. Continue Timeout (Nominal 2 seconds)


a. Heading Block

b. WACK Timeout

Figure B-4. Mode IB Link Protocols
(Sheet 10 of 11)

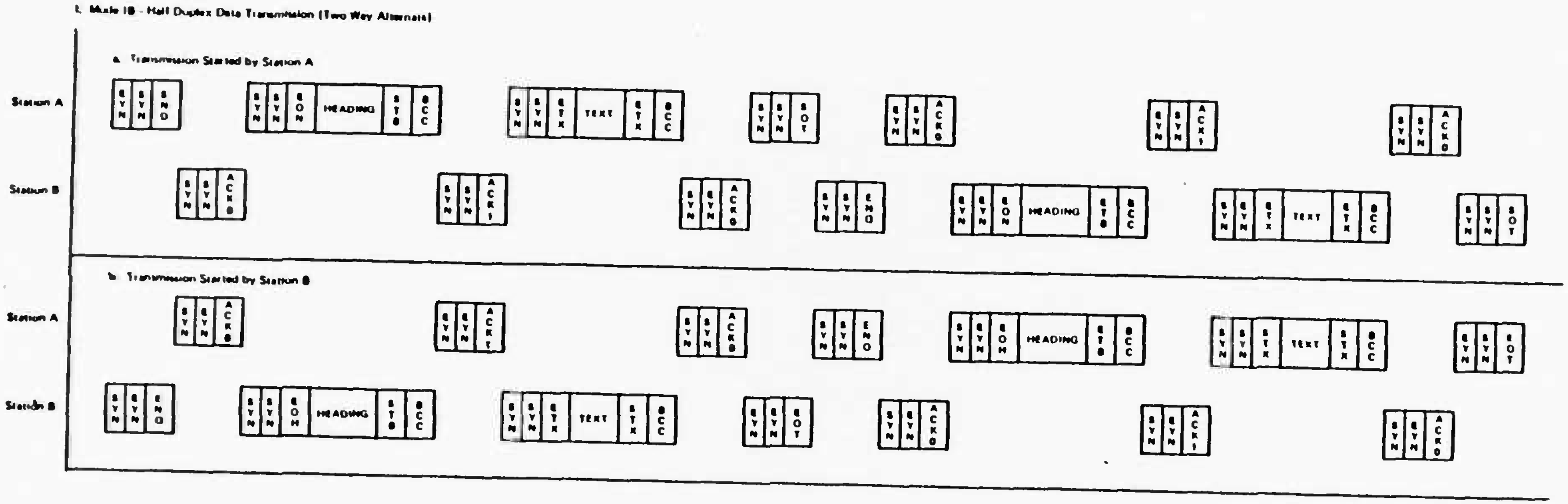


Figure B-4. Mode IB Link Protocols
(Sheet 11 of 11)

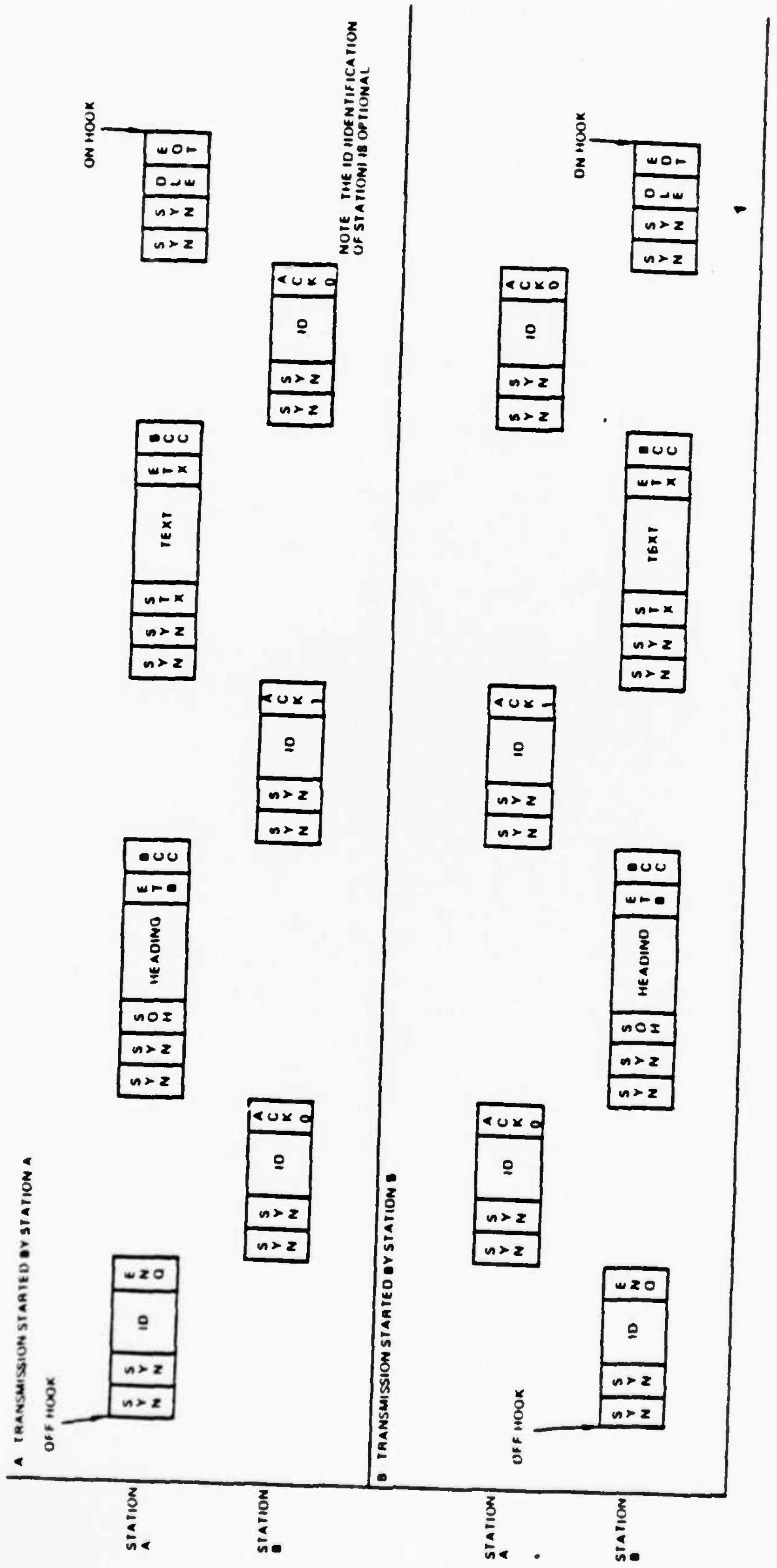


Figure B-5. Mode IB - Switched Network Dialup Operation

APPENDIX B: AMPE-MART/MATE Interface Criteria

AMPE - MART/MATE

INTERFACE CRITERIA

1. MART Requirements.

1.1 General. This section establishes the requirements for an I/SA AMPE to interface with Modular AMME Remote Terminal (MART) and to provide LINE signaling/supervision, data exchange, and message processing in accordance with the applicable System Design.

1.1.1 The AMPE will provide AUTODIN MODE I line signaling and supervision IAW DCAC 370-D175-1.

1.2 Message exchange between the AMPE and MART will be correlated to a unique select (SEL) character matrix for each MART. This matrix will cross reference, by terminal ID, the DCAC 370-D175-1 SEL characters with assigned MART unique SEL characters (ANNEX 2). Alterations to this matrix will be made by an on-line table change, addressable by terminal ID. Pending AMPE transmit to a MART, the AMPE will interrogate the received SEL character and substitute an appropriate MART SEL character from the matrix. During AMPE receive from a MART, the AMPE will interrogate the device SEL character and substitute an appropriate DCAC 370-D175-1 character from the matrix. Select character matrices shall delineate unique hardware configurations for each terminal.

1.2.1 Messages transmitted to the MART, other than system control messages and Local Circuit Switch (LCS) mode traffic, will be in JANAP 128 format. The MART will not interpret the LMF code of received messages.

1.2.2 All AMPE generated service messages will be in plain English text to permit non-communication trained personnel to clearly understand action required.

1.2.3 All AMPE generated system control messages will be formatted IAW ANNEX 1.

1.3 Message received from the MART may be of three formats: JANAP 128, DD 173, and System Control. Complete header validation is required in all instances except when in LCS mode.

1.3.1 The format will be identified by a unique encoded MART transmit SEL character.

1.3.2 DD 173 requires formatting to JANAP 128, PLA to RI conversion, local distribution, paging and (when applicable) sectioning.

1.3.3 Comeback copies and/or receipt of transmission are required.

1.3.4 The AMPE will accept and respond to a MART generated RM control characters IAW DCAC 370-D175-1.

1.4 Limitations of the MART.

1.4.1 LMF will not be interpreted in determining device selection.

1.5 Detailed Requirements.

1.5.1 Interface. The AMPE shall provide interface to the MART in accordance with the following provisions:

1.5.1.1 Line Control. Communications line control will be in accordance with DCAC 370-D175-1, with the following exceptions:

a. Chapter 7, all references to CSU mode operations.

b. All references to ASC operational restriction.

c. References to AUTOVON terminal procedures.

d. Chapter 5, paragraph 7, reference to "difference between the tributary and ASC procedures."

1.5.1.1.1 Line control shall consist of AUTODIN Mode I, block-by-block and continuous. Continuous will be used on high volume circuits. Line code will be in American Standard Code for Information Interchange (ASCII).

The communications link (AMPE to MART) will consist of the following: full duplex, four wire, synchronous, dedicated circuits. Line speeds are fixed at either 300 BPS, 600 BPS, 1200 BPS, 2400 BPS, 4800 BPS, 9600 BPS, or 19.2K BPS.

1.5.1.2 AMPE Response to MART RM.

1.5.1.2.1 A MART shall have the capability to generate and transmit RM sequences. RM sequences will normally be initiated by the MART operator due to nonavailable MART output device(s).

1.5.1.2.2 Upon receipt of each RM from the MART, the AMPE will respond with a "CAN" control character sequence IAW Chapter 3, paragraph 4b, DCAC 370-D175-1. The AMPE will make one attempt to retransmit the rejected message. If two consecutive RM's are received for the rejected message, the AMPE shall automatically respond by routing the message to intercept (by MART SEL CHAR and terminal ID).

1.5.1.2.2.1 AMPE shall respond to an RM IAW para 1.5.1.2.2 above and by providing and advisory message to the AMPE system console. This advisory will include as a minimum the following information:

a. Terminal identifier/3 positions.

b. Select character/output device/1 position.

c. System time/4 to 7 positions.

d. PAN number/4 positions.

e. Precedence of message/1 position.

f. LMF/2 positions.

1.5.1.2.3 The MART may advise the AMPE console operator of a MART output device malfunction via a system control message. AMPE will provide for interception/altroute by SELECT CHAR of message traffic addressed to malfunctioning output devices.

1.5.1.3 Circuit Reinitialization. AMPE shall provide for automatic reinitialization of the MART communications link as specified for Mode I operations in DCAC 370-D175-1.

1.5.1.4 Local Circuit Switching (LCS) Mode. AMPE will provide a fully automated local circuit switching capability wherein one MART may establish a circuit-to-circuit link with another MART having the same host AMPE.

1.5.1.4.1 Requesting LCS Mode. The MART will request the circuit switch connection to a specific terminal via a system control message transmitted to the AMPE. (See ANNEX 1)

1.5.1.4.2 AMPE Acceptance of LCS Request. The AMPE will notify the concerned MART of the validated request and connection via a system control message. (See ANNEX 1)

1.5.1.4.3 AMPE Rejection of LCS Request. The AMPE will notify the originating MART of the rejected request via system control message. (See ANNEX 1)

1.5.1.4.4 Line Protocol. SEL character "Y" will be inserted in the second framing position of each line block transmitted in LCS mode. An exception is the system control message requesting disconnection. In this case, SEL character "V" is used.

1.5.1.4.5 Termination of LCS Mode. Either terminal in LCS mode may request termination by transmitting a system control message to the AMPE (See ANNEX 1). Termination of LCS mode may be initiated by the AMPE upon receipt of a Flash or ECP message for either terminal.

1.5.1.4.5.1 High Precedence Pre-emption. Upon AMPE receipt of a Flash or ECP message that is destined for one of two LCS connected terminals, the AMPE will terminate the LCS connection and transmit the high precedence message to the appropriate terminal.

1.5.1.4.5.2 The AMPE will notify the concerned MARTS of terminated LCS mode via a system control message. (See ANNEX 1)

1.5.1.4.5.3 When the LCS disconnect is made either by AMPE pre-emption, terminal request or loss of circuit continuity, the LCS connect procedure must again be initiated at the terminal if further LCS operation is required.

1.6 AMPE Receive.

1.6.1 Message format types. A variety of formats are transmitted from the MART to the AMPE. Specifically, formats DD 173, JANAP 128 and Systems Control message, are generated by the MART. The format of each message transmitted is identified by a unique encoded MART transmit SEL character. A detailed discussion of SEL characters is provided in ANNEX 2.

1.6.1.1 DD 173 formatted messages are prepared at the MART VDU or OSU. The MART line output will comply with ANNEX 3.

1.6.2 Message media. A variety of message media are transmitted from the MART. The unique MART transmit SEL characters is correlated to message format, MART peripheral devices and LMF. ANNEX 2 provides further discussion of SEL character identification.

1.7 AMPE transmit requirements. The AMPE will transmit all message traffic to the standard remote terminal in JANAP 128 format, with the exception of a uniquely formatted systems control message. (See ANNEX 1)

1.7.1 Circuit Security Level Validation. A comparison of the circuit security level with message classification must be accomplished by the AMPE. Delivery of messages with classification in excess of the addressed circuit will not be allowed.

1.7.2 High Precedence Pre-emption. AMPE will provide for high precedence pre-emption of lower priority messages in accordance with JANAP 128.

1.7.3 In-Service Message/Optional Feature. The AMPE shall automatically transmit a plain text JANAP 128 service message to a MART subsequent to circuit initialization and immediately following the in-service command execution. This message will advise the terminal that the circuit is now in service with the AMPE.

1.7.4 Comeback Copies/Data Message Acknowledgement. The AMPE will provide comeback copies for narrative messages transmitted from the MART. The decision to transmit a comeback copy shall be based upon the SEL CHAR and may be different for each MART.

1.7.5 System Control Messages. AMPE shall recognize and respond to systems control messages. These messages are designed to provide a means of requesting AMPE action and for the conveyance of information. The systems control message will be restricted for use within the AMPE network and for exchange, between AMPE and MART, but not between MARTS. System control messages are uniquely formatted IAW ANNEX 1.

1.7.5.1 Systems control message will be originated by AMPE or MART as required.

1.7.5.2 These messages will be identified by select character "V" present in the second framing character position of the line block. The select character bit configuration found in data blocks originated by the MARTS is unique in that the first five bits identify the select character and bits 6 and 7 identify the format of the message being transmitted. AMPE will interpret the first five bits of the character present in the second framing position of the line block, if that character is an ASCII "V ",the remaining two bits shall be ignored. Upon receipt of systems control messages, AMPE shall shift format position #9 to the right four places and insert the three letter originating MART routing indicator and a space. The routing indicators will be extracted from the AMPE circuit table.

1.7.5.3 Systems control messages shall fall into two categories. The first category covers those systems control messages requiring an automatic response from the AMPE. The second category covers those messages requiring operator intervention. The second type is utilized by the AMPE systems' operator to originate and transmit advisories to the MARTS. Formats are defined in ANNEX 1.

1.7.5.3.1 Systems control messages requiring automatic response by AMPE shall be identified by command field entry positions 5 through 7 on input and responded to by AMPE. upon receipt of task request and/or completion of task, AMPE will provide an advisory formatted IAW existing protocol to the AMPE system console of action taken or to be taken.

1.7.5.3.2 Systems control messages originated at the MART for the purpose of information and routed by command field entry "NAR" and "SVC" in format character positions 5 through 7. On input AMPE shall concurrently route "NAR" option messages to the AMPE system console VDU and systems console printer. "NAR" option messages which exceed 3 lines in length shall default to the AMPE service position. "SVC" option messages shall be routed to the AMPE service position in all cases.

1.7.5.3.3 AMPE operators shall originate systems control messages from the systems console.

1.7.5.3.4 MART generated systems control messages will be restricted in length to 1,920 characters or a full screen. When the MART generated systems control message is rejected on input for illegal/invalid formats, a canned plain language service message specifying reason for rejection will be generated and transmitted to the originating terminal.

1.7.5.4 Systems control messages will not be accountable nor are they to be included in systems statistics.

1.7.6 Plain Language Service Messages. AMPE will create plain language service messages formatted IAW JANAP 128 abbreviated plaindress for use within the AMPE system. Service messages exchanged with the MART will be identifiable by a unique SEL character (U). SEL character (U) will be placed in the appropriate SEL character framing position.

1.7.7 Header/EOM Validation. Header and trailer validation of field entries (to preclude ASC rejection) will be accomplished by AMPE prior to format conversion. Canned plain language service messages reflecting the classification and precedence of the referenced message shall be transmitted to the originating terminal citing illegal/invalid field entries. Delivery responsibility for rejected message traffic shall lie with the originating MART. AMPE will RM the MART upon receipt of invalid security at time of input and transmit a canned plain language service message citing the reason for rejection to the MART

1.7.8 SEL Character Matrix. AMPE will provide a unique SEL character matrix to interface with each MART. This matrix will be utilized for SEL character conversion on incoming message select characters to the unique device SEL character required by the MART for processing of the received message traffic. AMPE shall review the following fields in order to ascertain the correct substitute select character for MART output.

a. Precedence.

b. Language Media Format (LMF).

c. Select Character.

d. Content Indicator Code.

1.7.8.1 Select character conversion of AMPE bound MART input shall require stripping of bits 6 and 7 of the select character and reconfiguration to a valid DCAC 370-D175-1 bit select character. Select character matrix shall be constructed in such a manner as to allow for future enhancement.

1.7.8.2 Select character matrix shall be alterable via systems console command while system is on-line.

1.7.8.3 The following table demonstrates the correlation between DCA and MART unique select characters.

(* asterisk denotes those select characters requiring conversion)

DCA SEL CHAR	MART SEL CHAR	MART TRANSMIT TO AMPE
A	A	5 LEVEL Baudot
D	D	card, hollerith (JANAP 128)
H	H	narrative (OSU, VDU, 8 level paper tape) (JANAP 128)
A or H	*U	Service
-	V	Systems control message
-	Y	Local circuit switching
		MART RECEIVE FROM AMPE
A	A	5 level, Baudot
D	D	card, hollerith (JANAP 128) (ASCII)
		MART TRANSMIT TO AMPE
F	F	Card, flash (JANAP 128)
*S	G	8 level ASCII, flash
H	H	8 level ASCII, narrative (JANAP 128)
S	S	5 level Baudot, flash
*H	T	8 level ASCII, immediate, priority

TABLE (Cont'd)

-	U	Service
-	V	Systems Control Message
-	X	Logging Information

1.7.8.4 The following table demonstrates the relationship of DCA and MART unique select characters in a typical MART narrative configuration. Message format fields containing information necessary to correct the select character conversion are identified under column heading "fields". As a minimum, one or more of the following fields must be interrogated by AMPE to accomplish select character conversion.

a. Select Character

b. Language Media Format

c. Precedence

d. Content Indicator Code

e. Routing Indicator

f. Classification

TABLE I (Cont'd)

FIELDS	DCA SEL CHAR	MART SEL CHAR	MART TRANSMIT TO AMPE
a	A	A	5 level, Baudot
a	B	B	8 level, ASCII
a/b/e	A or B	U	8 or 5 level, service message
	-	V	Systems Control Message
	-	Y	Local Circuit Switching

FIELDS	DCA SEL CHAR	MART SEL CHAR	MART RECEIVE FROM AMPE
a	A	A	5 level, Baudot
a/c	B	B	8 level, ASCII
a/b	S	G	8 level ASCII, flash
a/b	S	S	5 level Baudot, flash
a/c	B	I	8 level ASCII, immediate or priority
	-	U	Service Message
	-	V	Systems Control Message
	-	Y	Local Circuit Switching

TABLE`NO. 1

	A. CLAS	B. S P	C. PREC	D. S P	E. 3 LTR DEST RI	F. S P	G. COMMAND FIELD	H. S P	I. VERB OPTION
1.	*		**	****	XXX		ICS		CONNECT: (Distant RI)
2.	*		**	****	XXX		ICS		DISCONNECT
3.	U		R	****	XXX		RPT		(NO ENTRY IN THIS FLD)
4.	U		R	****	XXX		DPT		STAT: (DPT RI) (File Code)
5.	U		R	****	XXX		DPT		XMIT: (DPT RI) (File Code)
6.	U		R	****	XXX		NAR		NARRATIVE (Max 1920 Characters) Free Form
7.	U		R	****	XXX		SVC		NARRATIVE (Max 1920 Characters) Free Form
8.	U***		R	XXX	XXX		ICS		CONNECTION MADE TO TERM (3 LTR RI)
9.	U***		R	XXX	XXX		ICS		DISCONNECTION MADE AT (Time)
10.	U***		R	XXX	XXX		ICS		REQUEST REJECTED A. Hi-Precedence Busy B. Term Down C. Non-Compatible Security Level.

TABLE NO. 1 (Cont'd)

11.	U****	R	XXX	XXX	DPI	A. File (DPI File Code) Released. B. File (DPI File Code) Request Rejected C. Stat Request Rejected
12.	U	R	XXX	XXX	NAR	NARRATIVE (Max 1920 Characters) Free Form

LEGEND

* REFLECTS THE HIGHEST PRECEDENCE OF MESSAGE TRAFFIC TO BE SENT VIA LCS MODE.

** REFLECTS THE HIGHEST CLASSIFICATION OF MESSAGE TRAFFIC TO BE SENT VIA LCS MODE.

*** AMPE SYSTEMS GENERATED RESPONSE TO MART SYSTEMS CONTROL MESSAGE.

**** THIS FIELD CONSISTS OF A SINGLE SPACE IN THE MART FORMATTED SYSTEMS CONTROL MESSAGE. AMPE UPON RECEIPT, EXPANDS THE FIELD AND INSERTS THE ORIGINATORS 3 LTR ROUTING INDICATORS, FOLLOWED IMMEDIATELY BY A SPACE.

TABLE #2

SYSTEMS CONTROL MESSAGE DEFINITIONS

1. LCS (local circuit switching). Request for establishment of LCS mode to a distant MART.

2. LCS (local circuit switching). Request for disconnection of LCS mode to a distant MART.

3. RPT (report). Request for terminal statistics. (See TABLE 1 for STAT format)

4. NAR (narrative). Verb/option field is free form.

5. SVC (narrative). Verb/option field is free form.

6. LCS (local circuit switching). Notification of establishment of LCS mode to a distant terminal.

7. LCS (local circuit switching). Notification of disconnection of LCS mode to a distant terminal.

8. LCS (local circuit switching). Notification of rejection of request to establish an LCS mode connection and reason for rejection.

9. NAR (narrative). Verb/option field is free form.

10. SVC (narrative). Verb/option field is free form.

ANNEX 1

1. Systems control message formats and required/optional field entries are defined below.

2. Format:

a. MARF Line Output to AMPE.

(See para 3)	A	B	C	D	E	F	G	H	I
	C		P						
	L	S	R	S	R	S	C	S	VERB
	A	P	E	P	I	P	M	P	OPTION
	S		C				D		
POSN	1	2	3	4	567	8	` 91011	12	13-1920

b. Format received at AMPE VDU. NOTE. Field D is expanded, the OSRI and a space is added to this field.

	A	B	C	D	E	F	G	H	I
	C			3					
	L	S	P	L	R	S		S	VERB
	A	P	R	T	I	P	C	P	OPTION
	S		E	R			M		
			C				D		
				R					
				I					
POSN	1	2	3	567	8910	11	121314	15	16-1920

3. Field Definition:

a. Classification Field. In the case of ICS message, this field reflects the highest classification of message traffic to be transmitted in ICS mode. In all other instances classification assigned will be commensurate with security level of information entered in the verb option field.

b. Space

c. Precedence Field. In the case of "LCS" message, this field reflects the highest precedence of message traffic to be transmitted in LCS mode. In all other instances, precedence assigned is optional.

d. Space. (FROM: Originators 3 letter routing indicator. This field is added by AMPE on input from the MART. Originated system messages will include this field on input from the AMPE message entry position.)

e. Three letter destination routing indicator will always be the same 3 alpha characters sent from the MART. This field will contain variable alpha characters when originated by AMPE.

f. Space.

g. Command Field. Three alpha characters designating requested function.

h. Space.

i. Verb Option Field. Entries in this field are fixed IAW attached table No 1.

ANNEX 2

SELECT (SEL) CHARACTERS

1. A MART/AMPE SEL character contains three elements:

A.	Device Character	(bits 1-5)
B.	Format Identification Code	(bits 6, 7)
C.	Even Parity Bit	(bit 8)

2. Device Character Determination. The peripheral device which inputs the message text will define the proper device character to use for message transmitted by the MART. Minimal parameters for the matrix are: DCAC 370-D175-1 SEL CHAR, RCV LMF, Precedence, Content Indicator Code routing and authorized Receive Device Character.

MART TRANSMIT DEVICE CHARACTER

Code	Device
(bits 1-5) of the following ASCII characters):	
A	5 LEVEL PAPER TAPE (MART CONVERTS ITA2 to ASCII)
B	RESERVED
C	9 TRACK MAG TAPE RESERVED
D	CARD HOLLERITH
E	RESERVED
H	NARRATIVE (OSU, VDU, AND 8 LEVEL PAPER TAPE)
U	SERVICE MESSAGE
V	SYSTEM CONTROL MESSAGE
Y	LOCAL CIRCUIT SWITCH (LCS) MODE TRAFFIC

MART RECEIVE DEVICE CHARACTER

A	5-LEVEL: PAPER TAPE (MART CONVERTS ASCII TO ITA2)

ANNEX 2 (cont'd)

B	RESERVED
C	RESERVED
D	CARD, HOLLERITH
E	RESERVED
F	CARD, FLASH PRECEDENCE
G	8-LEVEL ASCII NARRATIVE, FLASH PRECEDENCE
H	8-LEVEL ASCII NARRATIVE
S	5-LEVEL PAPER TAPE, FLASH PRECEDENCE (MART CONVERTS ITA2 TO ASCII)
*T	8-LEVEL ASCII NARRATIVE, IMMED OR PRIORITY PRECEDENCE
U	SERVICE MESSAGE
V	SYSTEM CONTROL MESSAGE
X	LOGGING INFORMATION
-	Undefined, Spare
-	Undefined, Spare

* Device Character "T" is restricted for use with message review terminal.

3. FORMAT IDENTIFICATION CODE (FIC) DETERMINATION. Bits 6 and 7 of the MART/AMPE SEL Character are derived from a code indicating the type format of the message. The code will be referred to as the format identification code (FIC). The FIC will be one of the following:

TYPE FORMAT	BIT	
	7	6
Reserved	1	1
DD 173	0	1
JANAP 128	1	0

ANNEX 2 (cont'd)

4. EXAMPLE OF SEL CHARACTERS.

Message Format	BIT							
	8	7	6	5	4	3	2	1
CSU DD 173	0	0	1	0	1	0	0	1

5. The proper device character and its associated device is determined from interrogating the DCAC 370-D175-1 SEL CHAR, RCV LMF, Precedence, CIC, DSRI and Authorized Receive Device Characters. There are two exceptions to this rigid cross-reference.

a. All flash Precedence Service messages default to 8-level ASCII narrative, flash Precedence (SEL "G").

b. All flash Precedence Data Traffic, regardless of RCV LMF or CIC, default to card, Flash Precedence (SEL "F").

ANNEX 3

DD 173 Message Formatting

1. This Annex prescribes the data line output in DD 173 format for a MART. The traffic is orgiinated at an OSU or VDU message entry position. In either case, the data line output will be standardized IAW Appendix A.

2. If the message is prepared for entry via the OSU, the following rules apply:

a. DD 173 forms will be prepared using 10 pitch, OCR type set, A or B font.

b. The first character read from the DD 173 form will define the left margin of the form (character position 1). In this case, page numbering information in the upper left corner of the DD 173 form will alwys be the first characters(s) read. Each line is limited to 69 characters including positioning spaces.

c. A set of two carriage returns and one line feed will be inserted by the MART after reading each line of the DD 173 form.

d. The beginning of text is indicated by an alpha character classification other than a predefined address prosign, being detected in character position 1 (after two or more sets of two carriage returns and one line feed are sensed following detection of an address field).

e. The word "SUBJ" or "SUBJECT" (on new line - left justified) will follow the end of internal instructions. These instructions will be placed at the beginning of each section, as required IAW JANAP 128 during AMPE message reformatting.

f. An example of a properly prepared DD 173/1 form is attached at Appendix B. TABLE #3 contains descriptions to specific fields. Note that the page scan is limited to 20 lines:

(1) The positioning indentations in the address fields provides specific information of continuation lines and multiple addresses.

(2) The prosign "XMIT" is not valid unless preceded by an AIG number in the TO address field or a Collective Address Indicator in the TO or INFO address feidls.

(3) The optional progisn "DIST" is used to indicate automatic routing by local distribution information. Each entry is separted by a slant (/). End of field is indicated by a double slant (//). Both the prosign and addressee entries will be stripped during AMPE JANP 128 message reformatting prior to transmission.

(4) The operating signal ZEN, if used, will immediately precede the PLA. The PLA will begin in character position 20.

(5) The prosign "ACCT" is used to indicate accounting and group count information. This prosign, if used, will follow all other prosigns. During AMPE JANP 128 message refomatting, the "ACCT" and accounting information is placed JANAP 128 format line 10.

(6) Continuation of text on second and succeeding pages begins on line 2. Although entries are made in line 1 of all message form pages, only line 1 entries from page 1 are transmitted to the AMPE. Text is limited to a maximum of 20 lines, 69 characters per line on all continuation message form pages.

g. The MART senses the last message form page from the intregration of the page count field.

g. Subsequent to sensing the last page, the MART detects EOM upon reading 20 lines of data or four consecutive blank lines (three lines per inch), whichever occurs first.

TABLE #3 EXPLANATION OF TERMS TO DD FORM 173/1

ITEM NO.	TAB POSITION**	NUMBER & TYPE OF CHARACTERS	DESCRIPTION OF ENTRY
*1	1	2 - NUMERIC	Page number.
2	5	2 - NUMERIC	Total page count.
3	9	6 - NUMERIC 1 - ALPHA	First two digits represent the day of the month, next two digits represent the hour of the day using the 24 hour clock, and the last two digits represent the minutes. It will be contain the suffix "Z" indicating time in GMT.
4	18	3 - ALPHA	Authorized abbreviation of the current month.
5	23	2 - NUMERIC	Last two digits of the current year.
*6	27	2 - ALPHA	Action precedence.
*7	31	2 - ALPHA	There must be an info precedence entry if action field was not used.
*8	35	4 - ALPHA	Classification repeated 4 times.
*9	41	5 - ALPHA	SPECAT or SHD designator repeated 5 times.

TABLE #3 EXPLANATION OF TERMS TO DD FORM 173/1

ITEM NO.	TAB POSITION**	NUMBER & TYPE OF CHARACTERS	DESCRIPTION OF ENTRY
10	48	2 - ALPHA	Language media format (LMF information.) Leave blank unless specific LMF is required.
11	52	4 - ALPHA	Content indicator code (CIC), normally "ZYUW." Other CICs may be used as prescribed in applicable directives.
*12	58	ALPHA NUMERIC up to 12	A unique sequence assigned by the Orig for positive message identification.
*13	1	0 or 3 - ALPHA	Book message information. If "YES" is used, the CIC field must contain "ZEXW" or "ZYQW."
14	5	VARIABLE. To end of line	Message handling information.
15	15	VARIABLE	Start of From PLA with office symbol, if available.
16	15	VARIABLE	Start of TO PLA with office symbol, if available. If no ACTION address, item 19 applies.

TABLE #3 EXPLANATION OF TERMS TO DD FORM 173/1

ITEM NO.	TAB POSITION**	NUMBER & TYPE OF CHARACTERS	DESCRIPTION OF ENTRY
17	20	VARIABLE	PLA continuation line(s) applies.
18	15	3 - ALPHA Type in "AIG" and number.	Start of address indicating group information.
19	10	4 - ALPHA Type in prosign "INFO."	Start of information line.
20	15	VARIABLE	PLA for INFO addressees.
21	15	Type in operating signal "ZEN."	Start of ZEN information.
22	19	VARIABLE	Start of PLA(s) to be delivered by other than electrical means.
23	11	Type in prosign "XMT."	Exempt prosign.
24	15	VARIABLE	Any exempted PLA when AIG(s) are used in the TO line.
25	1	VARIABLE	Start of classification line.
26	1	4-ALPHA	End of classification indicator
27	1	VARIABLE	Start of text.

*NOTE: These entries must be made on all subsequent pages for proper handling.

**The first character to appear on the DD Fo m 173 will define the left margin (character position 1). In this case, page numbering information in the upper left corner of the form. Each line is limited to 69 characters including positioning blanks, correction signs, and spaces.

2. MATE Requirements.

2.1 General. This Section establishes the requirement for an I-S/A AMPE to interface with a Modular AUTODIN Terminal Equipment (MATE) and to provide line signaling/supervision, data exchange, and message processing using DCAC 370-D175-1 MODE I and JANAP 128 procedure.

2.2 Message exchange between the AMPE and the MATE will utilize the standard set of select characters identified in DCAC 370-D175-1.

2.2.1 Messages transmitted to the MATE will be in JANAP 128 format.

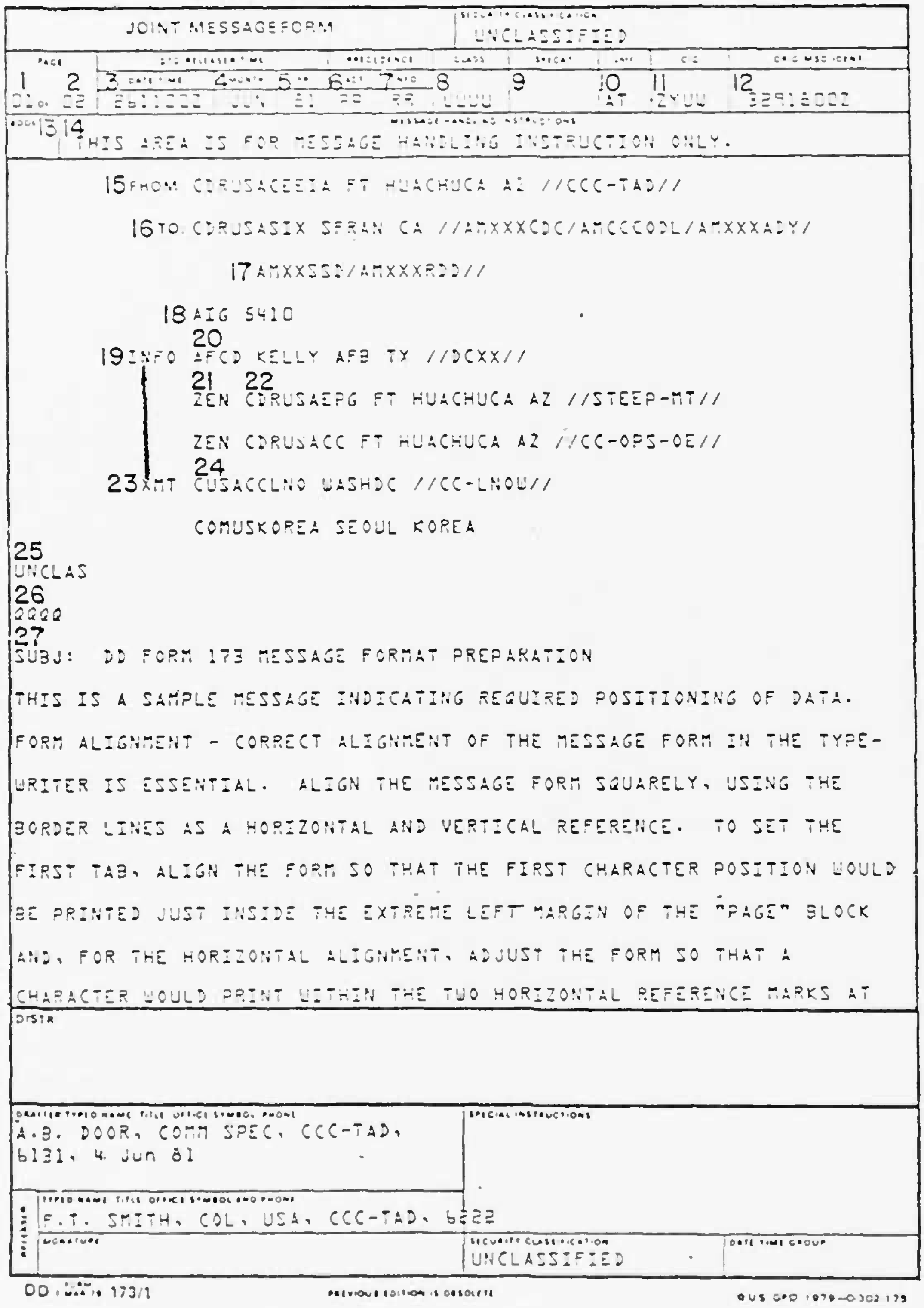
2.2.2 There are no special requirements for service message text. Standard communications service procedures will be supported by the MATE.

2.3 Messages received from the MATE will be in JANAP 128 format.

2.3.1 The MATE will perform PLA-RI lookup and DD173 to JANAP 128 conversion.

2.3.2 The AMPE will accept and respond to MATE generated RM control characters IAW DCAC 370-D175-1.

2.4 The AMPE will send/receive all media to/from the MATE.



JOINT MESSAGEFORM

SECURITY CLASSIFICATION
UNCLASSIFIED

PAGE		DTG RELEASER TIME			PRECEDENCE		CLASS	SPECAT	LMF	CIC	ORIG MSG IDENT
1	2	3 DATE-TIME	4 MONTH	5 YR	6 ACT	7 INFO	8	9	10	11	12
01 of	02	261122Z	JUN	81	RR	RR	UUUU		AT	ZYUW	3291800Z

BOOK 13 14 MESSAGE HANDLING INSTRUCTIONS
THIS AREA IS FOR MESSAGE HANDLING INSTRUCTION ONLY.

15 FROM CDRUSACEEIA FT HUACHUCA AZ //CCC-TAD//

16 TO CDRUSASIX SFRAN CA //AMXXXCDC/AMCCCODL/AMXXXADY/

17 AMXXSSD/AMXXXRDD//

18 AIG 5410

19 INFO 20 AFCD KELLY AFB TX //DCXX//

21 ZEN 22 CDRUSAEPG FT HUACHUCA AZ //STEEP-MT//

ZEN CDRUSACC FT HUACHUCA AZ //CC-OPS-OE//

23 XMT 24 CUSACCLNO WASHDC //CC-LNOW//

COMUSKOREA SEOUL KOREA

25 UNCLAS

26 QQQQ

27 SUBJ: DD FORM 173 MESSAGE FORMAT PREPARATION

THIS IS A SAMPLE MESSAGE INDICATING REQUIRED POSITIONING OF DATA.

FORM ALIGNMENT - CORRECT ALIGNMENT OF THE MESSAGE FORM IN THE TYPEWRITER IS ESSENTIAL. ALIGN THE MESSAGE FORM SQUARELY, USING THE BORDER LINES AS A HORIZONTAL AND VERTICAL REFERENCE. TO SET THE FIRST TAB, ALIGN THE FORM SO THAT THE FIRST CHARACTER POSITION WOULD BE PRINTED JUST INSIDE THE EXTREME LEFT MARGIN OF THE "PAGE" BLOCK AND, FOR THE HORIZONTAL ALIGNMENT, ADJUST THE FORM SO THAT A CHARACTER WOULD PRINT WITHIN THE TWO HORIZONTAL REFERENCE MARKS AT

DISTR

DRAFTER TYPED NAME, TITLE, OFFICE SYMBOL, PHONE
A.B. DOOR, COMM SPEC, CCC-TAD,
6131, 4 Jun 81

SPECIAL INSTRUCTIONS

RELEASER TYPED NAME, TITLE, OFFICE SYMBOL AND PHONE
F.T. SMITH, COL, USA, CCC-TAD, 6222

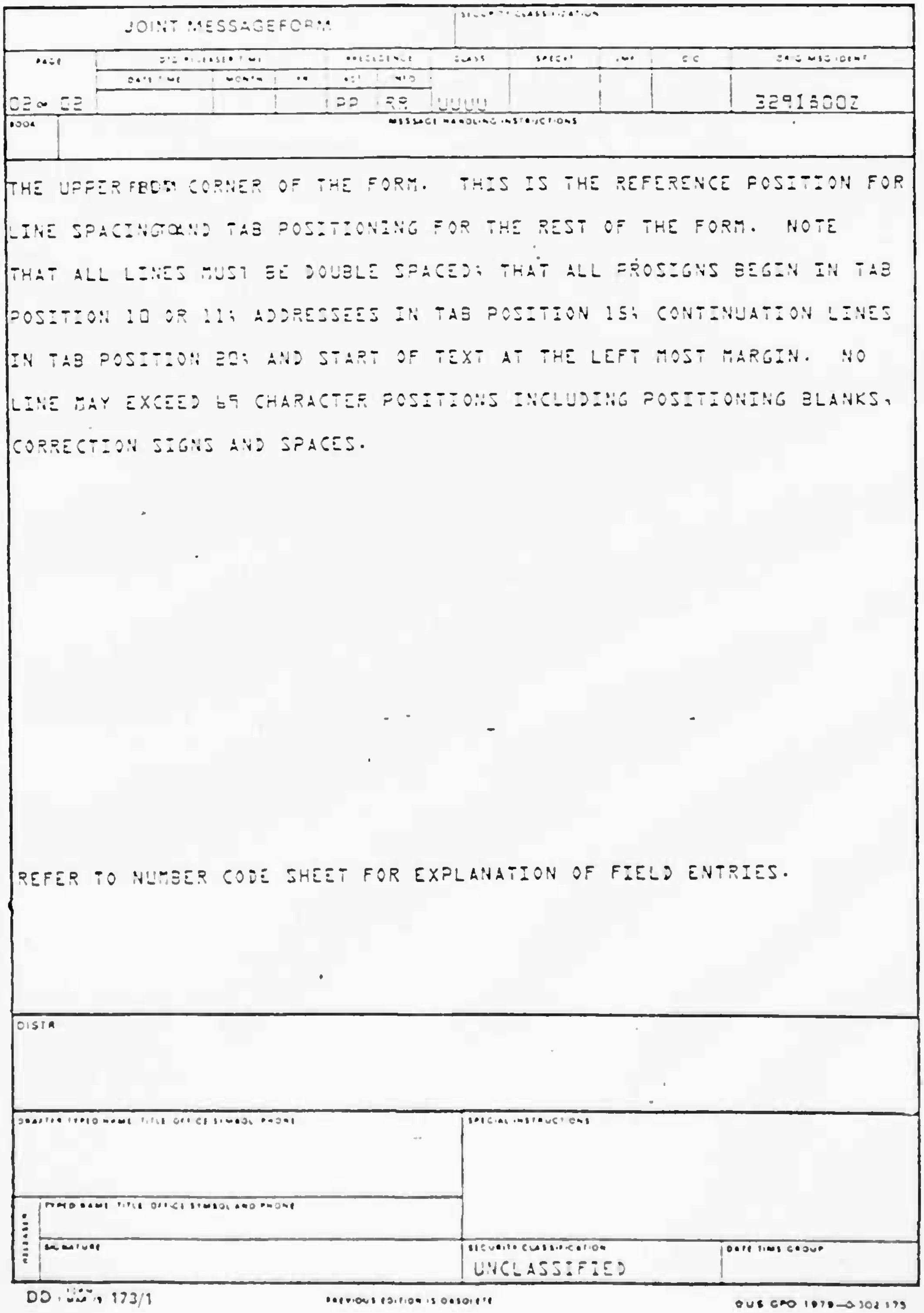
SIGNATURE

SECURITY CLASSIFICATION
UNCLASSIFIED

DATE TIME GROUP

DD FORM 1 MAY 79 173/1 PREVIOUS EDITION IS OBSOLETE ☆US GPO 1979—O-302-175

APPENDIX B Sample DD Form 173/1.



JOINT MESSAGEFORM

SECURITY CLASSIFICATION

PAGE	DTG/RELEASER TIME: DATE TIME	MONTH	YR	PRECEDENCE: ACT	INFO	CLASS	SPECAT	LMF	CIC	ORIG MSG IDENT
02 ~ 02				PP	RR	UUUU				3291600Z

BOOK

MESSAGE HANDLING INSTRUCTIONS

THE UPPER ~~FBDM~~ CORNER OF THE FORM. THIS IS THE REFERENCE POSITION FOR LINE SPACING AND TAB POSITIONING FOR THE REST OF THE FORM. NOTE THAT ALL LINES MUST BE DOUBLE SPACED; THAT ALL PROSIGNS BEGIN IN TAB POSITION 10 OR 11; ADDRESSEES IN TAB POSITION 15; CONTINUATION LINES IN TAB POSITION 20; AND START OF TEXT AT THE LEFT MOST MARGIN. NO LINE MAY EXCEED 69 CHARACTER POSITIONS INCLUDING POSITIONING BLANKS, CORRECTION SIGNS AND SPACES.

REFER TO NUMBER CODE SHEET FOR EXPLANATION OF FIELD ENTRIES.

DISTR

DRAFTER TYPED NAME, TITLE, OFFICE SYMBOL, PHONE

SPECIAL INSTRUCTIONS

RELEASER

TYPED NAME, TITLE, OFFICE SYMBOL AND PHONE

SIGNATURE

SECURITY CLASSIFICATION

UNCLASSIFIED

DATE TIME GROUP

DD FORM 173/1

PREVIOUS EDITION IS OBSOLETE

☆U.S. GPO 1979—0-302-175

APPENDIX B Sample DD Form 173/1.

PRINT
EXPANSION
CRITERIA

1. REQUIREMENTS

1.1 General. The AMPE when connected to the MART is responsible for performing the print expansion requirements for various users. The AMPE will receive compressed reports via AUTODIN in 80-column card message format. It will provide the capability to expand and forward the expanded reports for printing on the MART printer in 132-character format in a real-time on-line fashion. The reports to be printed will be recognized by combinations of CIC and RI. Recognition logic shall be based on any combination of a maximum of 2 RI and CIC pairs.

1.2 Detailed Requirements. Reports to be printed will be received on-line via AUTODIN. They will contain a continuous string of delimeter characters, control and count characters, and characters to be printed. Strings of three or more blanks in the message will have been suppressed by the transmitting station. The AMPE must then scan the string of received characters, insert the blanks, construct the print lines, insert the proper select characters, and transmit the data to the MART for printing.

1.3 Control Characters.

1.3.1 Delimiter Character. The delimiter character will be a "less than" sign. This is a 12-4-8 Hollerith punch which has the 7-bit ASCII binary code 0111100.

1.3.2 Printer Control Character. All printer control character (PCC) will be immediately preceded by one delimiter character, e.g., PCC. Printer control characters are defined as follows:

Character	Interpretation
b(blank)	Space one line before printing
0(zero)	Space two lines before printing
- (hyphen)	Space three lines before printing
1	Skip to channel 1 before printing (advance to top of page - line 5)
9 or c	Skip to channel 9 before printing (advance to bottom of page - line 61)

1.3.3 Count Character. The character representing the count will be one of the ASCII characters represented by the 7-bit binary code 1000100 through 1011010. The five low order bits will be utilized to correspond to decimal values 3 through 25. Note that the corresponding binary value is one greater than the decimal value. The minimum number of blanks to be reinserted by this technique is 3, the maximum is 25. All count characters will be immediately preceded by one delimiter character, e.g., cc. The count characters are defined as follows:

Binary Count	ASCII Character	Decimal Count
1000100	D	#
1000101	E	4
1000110	F	5
1000111	G	6
1001000	H	7
1001001	I	8
1001010	J	9
1001011	K	10
1001100	L	11
1001101	M	12
1001110	N	13
1001111	O	14
1010000	P	15
1010001	Q	16
1010010	R	17
1010011	S	18
1010100	T	19
1010101	U	20
1010110	V	21
1010111	W	22
1011000	X	23
1011001	Y	24
1011010	Z	25

Note that in defining the printer control characters and the count characters, care was taken to insure that there would be no chance for misinterpreting the intent of the control character.

1.4 Printer Report. The integrity of the reports is the responsibility of the originator and will contain integral report pages. No report page will be divided between two or more separate reports. Each report page is to be printed on a page that has the following characteristics:

1.4.1 Sixty-six lines per page.

1.4.2 Six lines per inch.

1.4.3 Each page will be 11 inches long.

1.4.4 Line 5 will be the position of the first print line on each page. Line 61 will be the last line on the page. Thus 57 print lines are available per page.

1.5 Operational Requirements.

1.5.1 Delimiter Sequence. The technique of data expansion uses a group of two control characters; the first is always a single delimiter character denoting the start of control sequence. The second character defines the necessary action to be taken. The control character (second character) can be:

a. Printer control character - denotes beginning of a print line.

b. Count character - denotes number of blanks to be inserted.

c. "Less than" character - denotes end of report.

1.5.2 Report Expansion. When scanning for the start of report, the first character of the report should be a <. After the start of the report delimiter has been found, the report will expanded using the control characters, count characters, and data characters until the end of the report delimiters (<<) have been found. The sequence is then repeated as necessary.

1.5.3 Error Procedures. Upon the detection of an error in the input data, the following procedures shall be followed to continue printing the report. If no printer control sequence is detected after all 132-print positions are accounted for, a print control sequence of Ø shall be inserted to preclude printing over the previous line. In the event the character following the delimiter cannot be identified as one of the defined characters, e.g., printer control character, count character, or end of report character, the logic shall cause the printer to print a row of asterisks as the next line, advance to the top of a new page, print an "invalid control character", substitute a blank for that character and continue the line expansion and printing process. The blank expansion of the format print buffer over 132 or an invalid character will cause "Blank Expansion Error" to be printed. More than 132 printer line columns formatted without a following delimiter/control character combination will cause the message "Print Line Exceeds 132". When one of the three errors is detected causing the error will be printed on a new line and underscored with asterisks for 132 positions. The appropriate error message is printed and a skip to channel 1 is performed. The report processing will continue.

APPENDIX C: IRT Interface Requirements

IRT INTERFACE

REQUIREMENTS

1. MCP Remote Terminal Line Handler (MCPIRT)

The IRT MCP line handler is used to communicate in a full duplex, synchronous manner with the IRT via MCP.

1.1 Detailed Description

a. The IRT MCP line handler is a full duplex, block-by-block communications interface. All input messages are framed by four control characters and message text is 80 characters in length, as shown in Figure 4-8.

b. The IRT is not a pollable device; it transmits to the AMPE when it has data available and is in a constant ready to receive mode. It is controlled by data acknowledge (ACK) sequences passed between the IRT and the AMPE and by recognition of the EOM sequence. After each block is transmitted, no further data is sent until the correct control sequence is received. If a negative acknowledge (NAK) sequence is received, the same block is retransmitted. If a wait before transmit (WBT) is received, a three second timer is set; and after the timer expires, the same block is retransmitted. If no answer is received after three seconds, the block is retransmitted. Whenever an ACK is received, the next block is sent.

c. At initialization, a delete message (DM) is expected and sent. The correct control sequence response is ACK and the alternating duplicate block protect bit is set to its initial state. A reject message (RM) control sequence is then sent. In normal operation, the alternating duplicate block protect in the select (SEL) character is toggled for each block.

d. If the IRT circuit is up and in idle state, the line handler initiates a DM control sequence to determine the current status of the IRT and its communications line. If the IRT does not respond with an ACK control sequence, the operator is notified that this circuit did not respond and the circuit is logged down.

e. When receiving, the line terminal is looking for sequential synchronous (SYNC) characters before the start of header (SOH). All leading and trailing SYNC characters are stripped off by the line terminal. When SOH is detected, the line terminal passes data until the end of text block (ETB) or

```
S S S                                            E

O E T          TEXT      (80 characters)    B     T
                                                   B
H L X                                       P


                                                 E

                                                  T
                                                   X
```

FIGURE 4-8. IRT LINE HANDLER BLOCK FORMAT

end of text (ETX) is encountered. The input block is checked for correct control character sequences and block parity. If the input data block is received in error, a NAK is sent. If buffer space for the next block is temporarily unavailable, a WBT is sent and a one and one-half second timer is set to acquire the buffer. If the input data block is received correctly and it does not contain an EOM, an ACK control sequence is sent. If the input block contains an ETX, the IRT line handler waits for EOMIN to set send ACK for the trailer. The IRT line handler also checks if any of the control sequences transmitted have been received. If so, the operator is notified that this IRT circuit is in loopback and the circuit is logged down.

f. All message characters, including the block parity character (BPC), and all control characters have odd character parity. The BPC produces block parity for bits one through seven of all characters except the SYNC and SOH characters. A description of the IRT control character is listed in Table VIII.

g. Figure 4-9 is a schematic illustration of the IRT traffic flow through the AMPE System.

1.2 Buffer Formats. MCPIRT uses the standard MCP communications buffers and standard SQ buffers.

1.3 System Module References. MCPIRT checks CMOD and COMMON.

1.4 Queues. MCPIRT uses MCP's cueues.

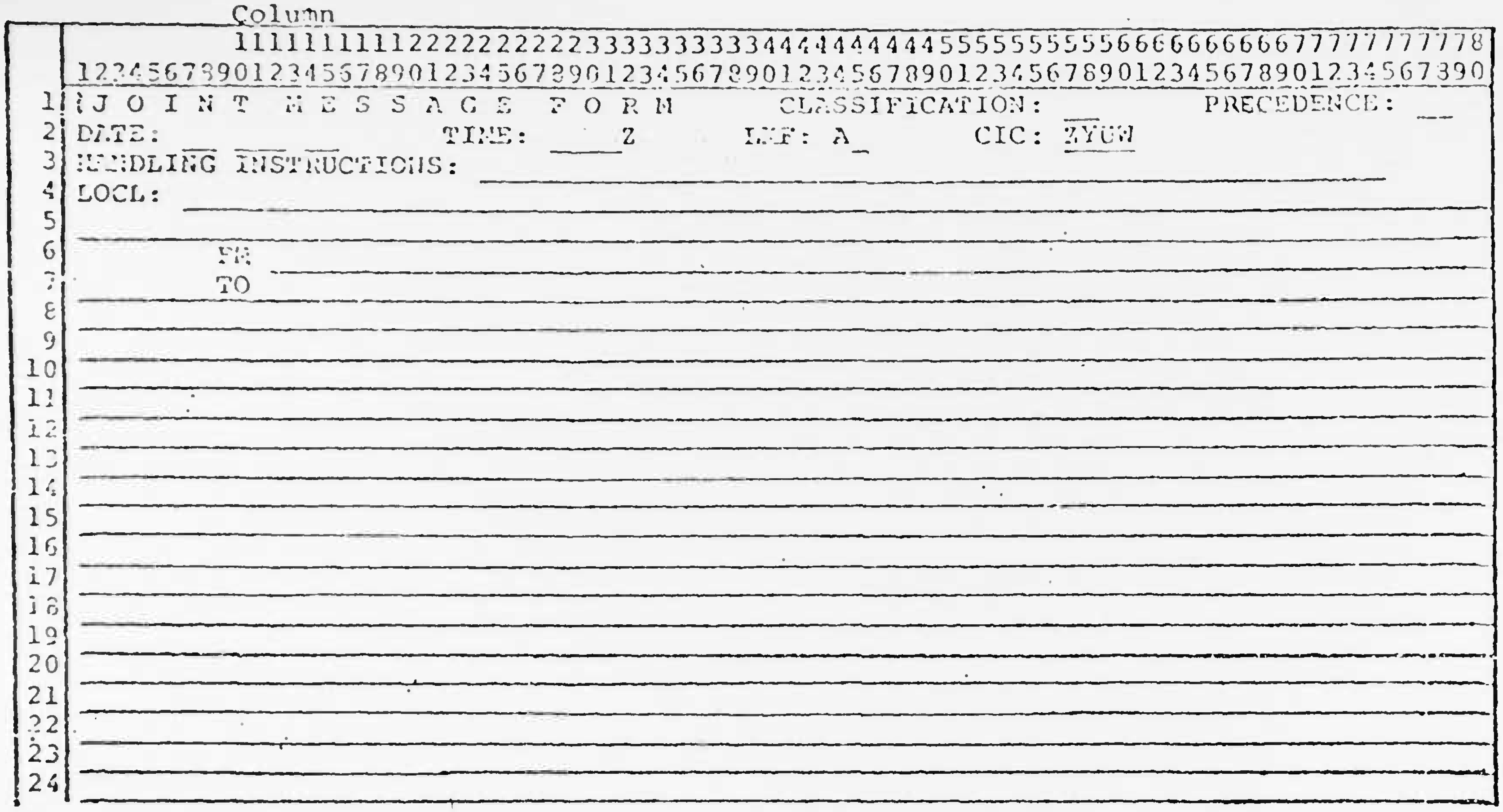
1.5 Interfaces. MCP gives control MCPIRT, and control is released to MCP.

TABLE VIII - IRT CONTROL CHARACTERS

Control Character	Hexadecimal Value	Description
SYNC	16	Character synchronization; hardware generated and hardware stripped
SOH	01	Start of header
SEL		Select character; may have any of the following parameters: P 0 1 B M X X X P is parity bit B is alternating duplicate block protect bit M is marked punched card XXX is 000 if output is printer 001 if output is punched card 010 if output is VDU
STX	02	Start of text

TABLE VIII - IRT CONTROL CHARACTERS (Cont'd)

RM	12	Reject message; sent by receiver to cause transmitted message to cancel current message being transmitted.
ETX	03	End of data for card messages or end of screen for VDU entries and control sequences.
ETB	17	End of physical block for card messages or end of physical line for VDU entries.
ACK	06	Positive acknowledge; dual sequence (ACK ACK) response for valid message.
NAK	15	Negative acknowledge; dual sequence (NAK NAK) response for message in error.
WBT	1E	Wait before transmit; response to a valid data block to inform transmitter that receiver can no longer accept data.
DLE	10	Data link escape; defines next contiguous character as resulting from IRT operator depressing one of 16 auxiliary function keys.
DM	18	Delete message; sent by the transmitter to cause the receiver to cancel the current message being received.



```
Column
            11111111112222222222333333333344444444445555555555666666666677777777778
   12345678901234567890123456789012345678901234567890123456789012345678901234567890
 1 J O I N T   M E S S A G E   F O R M     CLASSIFICATION:            PRECEDENCE: __
 2 DATE:                 TIME: ____Z      LMF: A_       CIC: ZYUW
 3 HANDLING INSTRUCTIONS: ____________________________________________________
 4 LOCL: ___________________________________________________________________________
 5 ________________________________________________________________________________
 6         FM
 7         TO _____________________________________________________________________
 8 ________________________________________________________________________________
 9 ________________________________________________________________________________
10 ________________________________________________________________________________
11 ________________________________________________________________________________
12 ________________________________________________________________________________
13 ________________________________________________________________________________
14 ________________________________________________________________________________
15 ________________________________________________________________________________
16 ________________________________________________________________________________
17 ________________________________________________________________________________
18 ________________________________________________________________________________
19 ________________________________________________________________________________
20 ________________________________________________________________________________
21 ________________________________________________________________________________
22 ________________________________________________________________________________
23 ________________________________________________________________________________
24 ________________________________________________________________________________
```

NOTE: _ indicates fields to be filled in by the operator - does not show on screen

Figure 1-1. Initial header preparation mask.

```
   Column
            11111111112222222222333333333344444444445555555555666666666677777777778
   12345678901234567890123456789012345678901234567890123456789012345678901234567890
 1 Line 23 of previous mask
 2 Line 24 of previous mask
 3
 4
 5  C O N T I N U A T I O N   P A G E   N O   X X   O S S N   C L A S S I F I C A T I O N
 6 ________________________________________________________________________________
 7 ________________________________________________________________________________
 8 ________________________________________________________________________________
 9 ________________________________________________________________________________
10 ________________________________________________________________________________
11 ________________________________________________________________________________
12 ________________________________________________________________________________
13 ________________________________________________________________________________
14 ________________________________________________________________________________
15 ________________________________________________________________________________
16 ________________________________________________________________________________
17 ________________________________________________________________________________
18 ________________________________________________________________________________
19 ________________________________________________________________________________
20 ________________________________________________________________________________
21 ________________________________________________________________________________
22 ________________________________________________________________________________
23 ________________________________________________________________________________
24 ________________________________________________________________________________
```

NOTES: _ indicates fields to be filled in by the operator - does not show on screen.
@@ page number of this message.

Figure 1-2. Continuation mask.

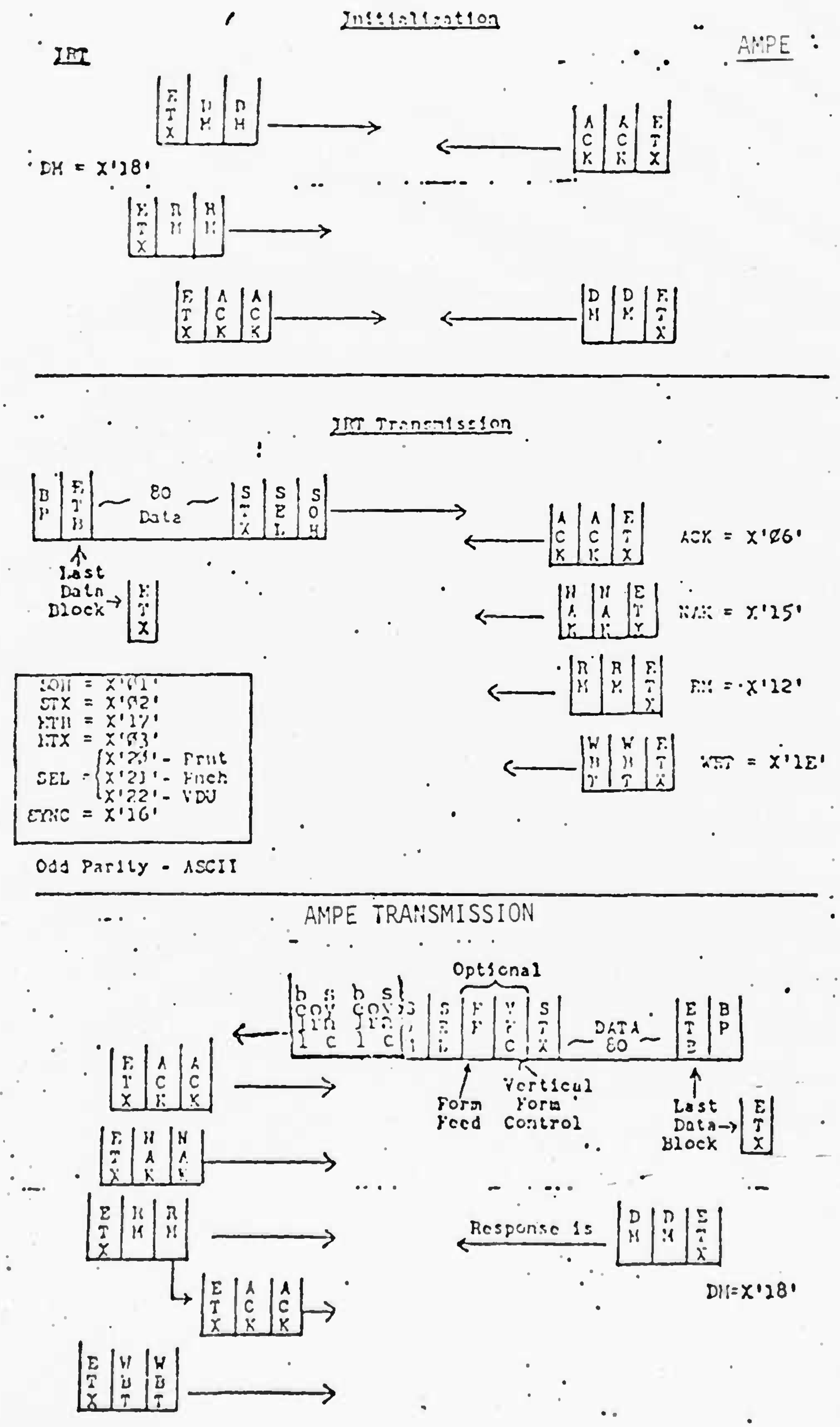


Figure 4-9 IRT/AMPE Traffic Flow

APPENDIX D: DPI Interface Requirements

DPI INTERFACE REQUIREMENTS

1. MCP DPI Handler (MCPDPI)

The MCP DPI handler provides a full duplex, synchronous communications interface to the DPI (360/65) using modified binary synchronous communications protocol.

1.1 Detailed Description.

a. The MCP DPI line handler ensures that all data being transmitted and received to or from the DPI has the correct block format, parity, length, and control framing characters.

b. Block parity is computed in accordance with nontransparent binary synchronous procedures. The block parity character is generated to include the first data character after the SOH or STX character and also the ETC or ETB character. All characters transmitted and received are ASCII characters with ODD PARITY.

c. All data transmissions are verified by control messages; i.e., ACK/NAK/ENQ. No idle characters are generated between data transmissions.

d. At initialization, an EOT control sequence must be transmitted and detected before any processing can occur.

e. When receiving input, the line terminal looks for two sequential SYNC characters before any input is passed to the DPI line handler, and all SYNC characters are deleted. For an input header, SOH is the first valid character. SOH indicates an 80 byte data buffer (plus control characters) containing a message header. After receiving the SOH block, STX is the first character of each succeeding block until either ETX or EOT is received. Each intermediate data block will end with an ETB control character; the last data block is indicated by an ETX. After the ETX block, the next data block must be header.

f. Data block sizes vary from a minimum of 80 character (plus framing characters) to a maximum of 2000 characters (plus framing characters). To ensure line synchronization, SYNC characters are suffixed to each data block. After each block is transmitted or received, no further data blocks are sent until the proper control sequence is received.

g. See Table IX for a list of the DPI control characters and their use.

h. Timeouts are used to prevent indefinite data link hangups, by providing a fixed time within which all responses must occur. Transmit timeouts will be one second; receive timeouts will be three seconds; and continue timeouts (WACK) will be two seconds.

TABLE IX - DPI CONTROL CHARACTERS

Control Character	Hexadecimal Value	Description
SOH	Ø1	Precedes a header block
STX	Ø2	Precedes a block of text characters
ETB	17	Indicates end of text block
ETX	Ø3	Indicates end of message that has one or more blocks
EOT	Ø4	Indicates end of transmission
ENQ	Ø5	Enquiry; used to obtain a repeat transmission or a bid for the line
ACKØ	1Ø3Ø	Positive acknowledgment
ACK1	1Ø31	Positive acknowledgment
WBT	1Ø3B	Wait before transmit
NAK	15	Negative acknowledge; indicates a previous block received in error
STICK	1Ø35 .	Initiated by the DPI to allow AMPE to transmit

i. All DPI circuits are defined in a unique AMPE system manner by four characters.

(1) The first character of the circuit module name is II.

(2) The second character defines the particular DPI in the the AMPE system. The system reserves the characters C, Q, R, and Y.

(3) The third character can be any alphabetic character.

(4) The fourth character can be any alphabetic character except A, P, or S. These characters are reserved as follows:

(a) A defines the DPI active circuit.

(b) P defines the DPI problem batch files.

(c) S defines the DPI service file.

j. On outbound DPI messages, a SOH framed packet is 83 characters in length. A STX framed packet can be a maximum of 2003 characters, including framing character, and a minimum of 83 characters in length. Figure 4-11 is an example of two outbound messages; the first is 25 line blocks in length and the second is 48 line blocks.

k. On inbound DPI messages, a SOH should only be placed on packets containing preamble or JANAP 128 headers. A unique character follows; e.g., an ASCII lower case m. An example of a 500 line block message would be framed and packeted as shown in Figure 4-12.

l. File request and statistics request control messages outbound from the DPI to AMPE consist of single line block messages which are framed as shown in Figures 4-13 and 4-14, respectively.

m. In order to accommodate IBM 2701 hardware requirements, two synchronous characters are added to all line blocks transmitted from AMPE at the required frequency. Frequency is determined by line speed and data blocking factor.

1.2 Buffer Formats. MCPDPI uses standard MCP communications buffers.

1.3 System Module Reference. MCPDPI accesses circuit modules and AMPE common.

1.4 Queues. MCPDPI uses MCP queues.

1.5 Interfaces. MCPDPI interfaces with MCP.

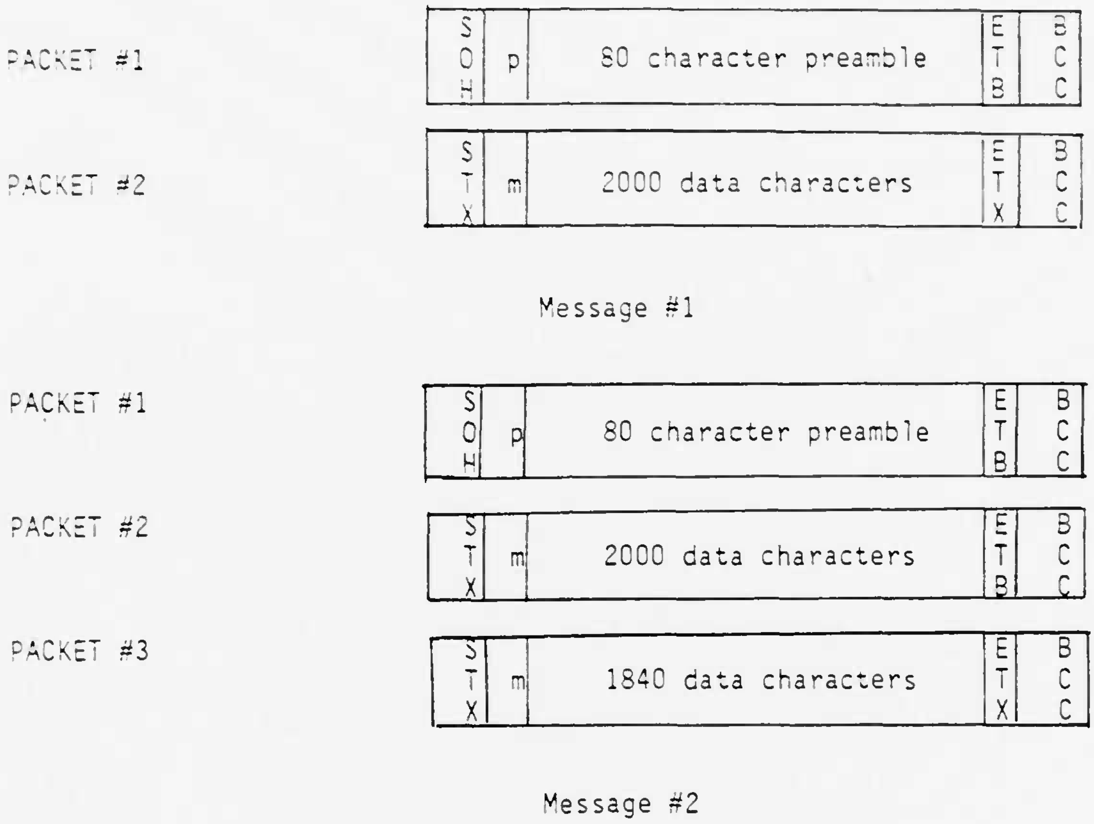


Figure 4-11. Outbound DPI message formats.

PACKET #1	S O H	p	80 character JANAP 128 header	E T B	B C C
PACKET #2	S T X	m	2000 data characters	E T B	B C C
PACKET #3	S T X	m	1840 data characters plus 80 character JANAP 128 trailer	E T X	B C C

Figure 4-12. Inbound DPI message format.

S O H	f	80 character preamble	E T X	B C C

Figure 4-13. DPI file request format.

S O H	s	80 character preamble	E T X	B C C

Figure 4-14. DPI statistics request format.

Appendix E

Deleted

APPENDIX F: NACE Protocol for Remote Computer Interface

COMMAND AND CONTROL TECHNICAL CENTER

NACE Protocol

For

Remote Computer Interface

May 31, 1977

SUBMITTED BY:

NORTON BRAGG
Project Officer

APPROVED BY:

R. E. HARSHBARGER
Acting Deputy Director
NMCS ADP

Copies of this document may be obtained from the Defense Documentation Center, Cameron Station, Alexandria, Virginia 22314.

~~Distribution limited to U. S. Government agencies only pending further study of this system which is subject to modification; 31 May 1977. Requests for this document must be referred to the Director, NMCS ADP Directorate, (C300), The Pentagon, Washington, D.C. 20301.~~

CONTENTS

CONTENTS (Continued)

ILLUSTRATIONS

SECTION 1. GENERAL

1.1 Purpose

The objective of this document is to provide a programming guide for attaching a Remote Computer to the Honeywell DATANET 355 (DN-355) Remote Terminal Supervisor (GRTS) under the Remote Computer Interface/Direct Access Convention (RCI/DAC) for subsequent inclusion to the NMCS Automated Control Executive (NACE). This document is not intended to replace existing documentation on this subject but is to supplement them in areas which are not clearly defined.

1.2 Equipment Configuration

In order for a remote computer to send or receive message traffic from/to NACE, the remote computer must be physically connected (hard wired) to a port of the DN-355. Remote computers must be configured in the DN-355 Startup (BOOT) deck. The DN-355 can handle up to 200 remote computers or terminals simultaneously with varying rates of transmissions ranging from 110 bits per second to 50,000 bits per second.

1.3 Protocol Convention

The communication line discipline (protocol) used by the DN-355 and NACE is the RCI/DAC convention. In the convention, the remote computer operates in a message response mode. Only the operations defined within the RCI/DAC interface can be used by the remote computer, operating with the DN-355, to communicate with NACE.

The benefits of RCI/DAC are that it provides error checking and recovery procedures to assure that no data are handled more than once and are error free when received. This interface also allows NACE and the remote computer to communicate directly with each other via the DN-355.

SECTION 2. SYSTEM DESCRIPTION

Remote computers must satisfy the requirements of the RCI/DAC interface. Basically, RCI/DAC requires that information and control records transmitted be in the format specified in Figure 1. Where applicable, the remote computer must acknowledge (either positively or negatively) each message sent by the DN-355.

2.1 General Description

Remote computers which are to be used to send/receive message traffic to NACE via the DN-355 must initially send to the DN-355 a SELECT command which will logically connect the line to the DN-355. The DN-355 will respond by acknowledging the SELECT with a "Clear to Send" message. The remote computer must respond with the log-on USERID$PASSWORD that was issued for that remote computer. The DN-355 will validate the USERID$PASSWORD and send to the remote computer an acknowledgement. Upon receipt of the acknowledgement, the remote computer must issue the DAC NACE-U command. This command instructs the DN-355 to logically connect the communication line from the remote computer to NACE. The DN-355 will then send a security message (25 words) which the remote computer must acknowledge (ACK). The DN-355 will also send the Terminal ID of the line to NACE which will verify that the remote computer is known to it. If the Terminal ID is not known to NACE, it will disconnect the line. If the Terminal ID is known to NACE, it will issue a READY command to the remote computer. The remote computer must acknowledge with the appropriate command to which the DN-355 must ACK. With this ACK, both the remote computer and NACE are in the Active RCI/DAC mode (see paragraph 2.1.2.2). This two-way exchange of messages continues until termination by either NACE or the remote computer.

2.1.2 Modes of Operation. Under the RCI/DAC interface, there are two modes of operation. They are the Idle mode and the Active mode.

2.1.2.1 Idle Mode. In the Idle mode, no messages are exchanged; but the remote computer line remains logically connected to the DN-355. If the line remains idle for seven minutes, the DN-355 will disconnect the line. While in the Idle mode, the remote computer must be ready to transmit a "SELECT" or "Ready for Disconnect" control message.

2.1.2.2 Active Mode. When both lines of the remote computer and NACE are logically connected, and a "READY" control message is received by the DN-355 from either the remote computer or NACE, the Active mode of Operation is entered.

During the Active mode of operation, the remote computer must be prepared to accept any of the following messages:

- Information messages with or without data.

SYN	
SYN	Synchronization Character
SYN	
SYN	
SOH	Start of Header
FC	Format Code
SC	Sequence Code
AC	Address Code
OC	Operation Code
IC	Identification Code
STX	Start of Text
DATA 324 CHARACTERS	Data (not to exceed 324 characters)
ETX	End of Text or End of Text Block (ETB)
BCC	Block Check Character

FIGURE 1. Control Record Format

* Special control messages

* Service messages

  - Terminate

  - Ready for disconnect

  - Disconnect

After transmitting a message to the remote computer, the DN-355 begins a 7-second timeout. If no response is received from the remote computer within seven seconds, the DN-355 retransmits the last message with the same Sequence Code and a negative acknowledgement (NAK). A "Terminate Service" message from either NACE or the remote computer initiates a return to the Idla mode. A Terminate message may be sent at any time during Active mode.

2.1.2.3 Line Disconnection. When the disconnect function is sent to the DN-355, the following service messages are sent:

* Ready for Disconnect (RFD) - No reason for the disconnect is sent to the DN-355. The DN-355 responds with a RFD with the message "LINE DISCONNECTED CP" and the line is logically disconnected.

* Disconnect - If the DN-355 receives a disconnect, the line is immediately disconnected without answering the message.

When the disconnect is received from NACE, the DN-355 ensures that the line is disconnected from NACE and that any activity on the line (input or output) is destroyed.

2.2 Detail Description

Once logically connected to NACE via the DN-355, all communications are carried out in the form of Information and Control records. Information messages may be sent with or without text. Text refers to a message with data between the Start of Text (STX) and End of Text Code (ETX).

2.2.1 Information and Control Record Format. All messages must be transmitted in the format as depicted in Figure 1.

2.2.1.2 Synchronization Character (SYN). Two or more consecutive synchronization characters (octal 026) must be recognized by either the remote computer or the DN-355. This assures that the two systems are synchronized before data transmission begins, thus reducing the possibility of lost or erroneous data. It is recommended that at least four SYNs be used.

2.2.1.3 Start of Header (SOH). The SOH (octal 001) indicates the beginning of the message.

2.2.1.4 Format Code (FC). The FC specifies the purpose and the format of the text in the message. The FC directs the DN-355 as to what action is required to handle the message.

2.2.1.4.1 Control Record, No Compression. This FC (octal 104) is used by either the remote computer or the DN-355. The text of the message is not compressed and contains only one control record.

2.2.1.4.2 Control Record, Compression. This FC (octal 105) is only used by the remote computer. The text may be compressed and may contain one record.

2.2.1.4.3 Information Message, No Split, No Compression. This FC (octal 110) when used specifies that the text must not be compressed. The text may contain multiple records, but all of them must be complete within the message. Each record must be enclosed by a Message Media Code (MMC) and a Record Separator (RS). See Figure 2. A MMC must follow the STX and a RS (octal 036) must precede the ETX.

2.2.1.4.4 Information Message, No Split, Compression. This FC is octal 111. The text of a message with this FC may be compressed, but the text must contain complete records. The text may contain multiple records. Each record must be enclosed by a MMC and a RS. A MMC must follow the STX and the RS must precede the ETX.

2.2.1.4.5 Information Message, Split, No Compression. This FC (octal 112) specifies the text is not compressed, but records in the text may be split across messages. An incomplete record at the end of the message is continued after the STX of the next message. The text may contain multiple records.

2.2.1.4.6 Information Message, Split, Compression. This FC (octal 113) specifies the text may be compressed and records in the text may be split across messages. An incomplete record at the end of a message is continued after the STX of the next message. The text may contain multiple records.

2.2.1.4.7 Information Message, User-Defined Text. This FC (octal 115) specifies the text of a message may be in any format agreeable between the remote computer and NACE. NACE, to properly perform its designed functions in the area of message routing, needs more control information about the message being received. This information is provided in the form of Message Media Codes (MMC). See Figure 2. These MMC codes will be the first characters transmitted after the STX and RS characters.

2.2.1.5 Sequence Code (SC). This code is used to insure that data is neither lost nor used more than once. This code alternates between octal 101 and 102. A changed SC indicates new text when text is present. The following rules concerning the use of SC apply equally to the remote computer and the DN-355. After transmitting a message to the remote computer, the DN-355 begins a seven-second timeout. If no response is received from the remote computer within seven seconds, the DN-355 retransmits the last message with the same SC and a negative acknowledgement (NAK).

Receiving Messages with the Same SC

a. When the text of the message is received in error, retransmit the last message with a NAK and the same SC.

b. When the SC is the same, the message was received error-free with an ACK, and the text of the message has already been processed, alter the SC and transmit the next message (with or without message text) with an ACK.

FIRST CHARACTER		SECOND CHARACTER	
MEDIA CODE	DESCRIPTION	MEDIA CODE	CONTROL CHARACTER DESCRIPTION
A	SINGLE-CARD MESSAGE	A	STATUS REQUEST
B	HEADER	B	STATUS INFORMATION
C	CARD IMAGE DATA	C	SUPER ACK
D	TRAILER	D	SUPER NAK
E	VARIABLE LENGTH - TEXT	E	NO BUFFER
F	CONTROL INFORMATION	F	CANCEL
G	TTY MESSAGE	G	READY
N	OPERATOR MESSAGE	N	DISCONNECT
		I	NO DATA

Media codes (A) and (B) will be followed by the AUTODIN SEL character

Media codes (C), (D), and (E) will be followed by the Security Classification Code

Media code (F) will be followed by the second character to describe the control function

Figure 2. Message Media Codes

c. When the SC is the same, the message was received error-free with an NAK and the text of the message has already been processed, retransmit the last message with the same SC with an ACK.

d. When the SC is the same and the received message is in error and contains no text, retransmit the last message with a NAK and the same SC.

e. When the SC is the same and the received message is error-free, contains no message text and contains an ACK, alter the SC and transmit the next message with an ACK and new message text.

f. When the SC is the same and the received message is error-free, contains no message text and contains an NAK, retransmit the last message with the same SC and an ACK.

Receiving Messages with Different SC

a. When the SC is different and the received message text is error-free and contains an ACK, process the message text, alter the SC and transmit the next message with an ACK.

b. When the SC is different and the received message text is error-free and the received message contains an NAK, process the message text, alter the SC and transmit the next message with an ACK. (The message text, being transmitted in one direction was received error-free).

c. When the SC is different and the received message is error-free, contains no message text and contains an ACK, change the SC and transmit the next message with an ACK and new message text.

d. When the SC is different and the received message is error-free, contains no message text and contains an NAK, retransmit the last message with the same SC with an ACK.

2.2.1.6 Address Code (AC). Although the AC (octal 100) is not used by either the DN-355 or NACE, it is a part of the standard interface and must be included in the message format.

2.2.1.7 Operations Codes (OC). The OCs specify the operations to be performed and describe the acknowledgements which may be given. Bit 7, the Most Significant Bit (MSB), is always a one. Bits 4-6 contain the acknowledgement code. The DN-355 will only send a positive acknowledgement (ACK) 000, or the negative acknowledgement (NAK) 001. The DN-355 will, however, recognize all NAK codes. Bits 1-3 define the instructions which specify the operations to be performed.

a. Acknowledgement Codes

BIT POSITION

6	5	4	Description
0	0	0	Positive Acknowledgement
0	0	1	Negative Acknowledgement
0	1	0	Negative - BCC in error
0	1	1	Negative - Char Parity error
1	0	0	Negative - SC in error
1	0	1	Negative - OC in error
1	1	0	Negative - STX missing
1	1	1	Negative - ETX missing

b. Operations Codes

BITS 3 2 1	OPERATION INSTRUCTION	OPERATION SPECIFIED
0 0 0	No Request	This instruction neither requests nor inhibits the sending of message text. (Used to send an ACK with new message text).
0 1 0	Select (Send Data)	Indicates the remote computer is ready to transmit data. After the DN-355 has accepted a SELECT, all preceding SELECTs are ignored until the line is placed in an Idle Mode.
0 1 1	Terminate	Informs the received that no more messages are to be transmitted, but the line is to remain connected (Idle mode). Both NACE and the remote computer must remain ready to receive messages.
1 0 0	Ready for Disconnect	Informs the receiver that the sender is going to disconnect the line.
1 1 0	Disconnect	Informs the receiver that the sender is disconnecting the line. No reply is expected and both stations are to disconnect the line.

2.2.1.8 Identification Code (IC). The IC (octal 100) is not used by NACE or the DN-355 but is part of the standard interface and must be included in the message format.

2.2.1.9 Start of Text (STX). The STX (octal 002) defines the beginning of the textual portion of the message.

2.2.1.10 End of Text (ETX). The ETX (octal 003) defines the logical end of the textual portion for the message. (Not necessarily the physical end of the text).

2.2.1.11 Block Check Character (BCC). The BCC is an exclusive OR of the message characters following the SOH and up to and including the ETX. Since the DN-355 checks for odd pairty, the BCC must also be odd parity.

2.2.2 Data Compression. When the message text contains three or more of the same data characters, these characters may be compressed to reduce the number of characters to be transmitted. The format used to compress consectuive characters are as follows: X, US and CC.

where, X - is the character to be compressed
US - Compression indicator (octal 037)
CC - A count of the number of times the character is to be repeated. (Maximum of 63)

This data compression technique permits compression of the multiple occurrence of any character and also allows for compression of multiple occurrences of sets of characters within the same record. When compression is specified, the DN-355 checks each input character to determine if it is the compression character. This character is used to expand the input for transmission to NACE.

2.2.3 Message Media Codes (MMC). The MMC's used by the remote computer and NACE are described in Figure 2. The MMC's are a sub-level of the RCI/DAC interface and as such are of little concern to the DN-355. The MMC's describe the type of message being received, i.e., single-record or AUTODIN, the security classification of the message and other control information. Through the use of NNC's, NACE and remote computers coordinate the sending/receiving of message data such as WAITS, NO DATA NOW, and CANCEL.

2.2.3.1 Message Format. Message text will be broken down into message segments. (A message segment is construed to be all characters after the synchronization (SYN) and before the BCC and must contain no more than 1272 characters). A segment will contain a maximum of 16 line blocks of 80 text characters. Each message segment will contain complete line blocks. Compression of text and the truncation of trailing blanks is permitted. Each line block within a segment will be preceded by a MMC and will be followed by a record separator (octal 036). The MMC will contain information about the line block that follows.

2.2.4 Ready Messages. This message is sent when either NACE or the remote computer has messages to transmit. The format of this control message is as follows:

SYN, SYN, SYN, SYN, SOH, FC, SC, AC, OC, IC, STX, FG, NULL, RS, ETX, BCC

where, FC = 115
OC = 100
FG = MMC denoting Ready
NULL = 100
RS = 036

After each command sequence is completed, the remote computer places his communication line in the receive position and waits for the next command from NACE. The assumption here is that NACE always has something to do. This is not always true as NACE may be waiting to receive more data.

2.2.4.1 Auxiliary Field. The purpose of the auxiliary field is to indicate to the DN-355 which message data formats are to be used for message data from the remote computer to the DN-355. The auxiliary field is used only in the SELECT and DAC control messages and only one auxiliary field is permitted per control message. The DN-355 does not transmit any auxiliary fields. When no auxiliary field is used, the message data to the remote computer will be compressed and edited, and may be split across message segments. The auxiliary filed is as follows:

Codes in ASCII

RECEIVE	TRANSMIT	COMPRESSION	EDIT	SPLIT RECORDS
100	113	Yes	Yes	Yes
101	111	Yes	Yes	No
102	113	Yes	No	Yes
103	111	Yes	No	No
104	112	No	Yes	Yes

RECEIVE	TRANSMIT	COMPRESSION	EDIT	SPLIT RECORDS
105	110	No	Yes	No
106	112	No	No	Yes
107	110	No	No	No

2.2.4.2 Special Control Messages. The Special Control Message enables the remote computer to transmit instructions or operational information to the DN-355 and NACE. They are used for initiating, acknowledgement and terminating information. The format for Special Control Messages are as follows:

2.2.4.2.1 Special Control Message, No Auxiliary Field.

SYN, SYN, SYN, SYN, SOH, FC, AC, OC, IC, STX, ETX, BCC

This format may be used for all Special Control Messages to the DN-355.

2.2.4.2.2 Special Control Messages, Auxiliary Field.

SYN, SYN, SYN, SYN, SOH, FC, AC, OC, IC, AUX FIELD, STX, ETX, BCC

This format may optionally be used by the remote computer when sending a SELECT to the DN-355. The DN-355 never sends this message. The FC used in a SELECT message is octal 103.

SECTION 3. INPUT/OUTPUT DESCRIPTION

3.1 General Description

Users of the RCI/DAC interface must be aware that the remote computer is subordinate to the DN-355 and NACE. Once logically connected to NACE, the remote computer responds to commands from the DN-355 and NACE. The remote computer must send acknowledgements for all control messages sent to it by the DN-355 and must execute any commands contained in the message. Additionally, the remote computer, through the use of Message Media Codes (MMC), must acknowledge the messages sent from NACE. NACE usually with send/receive all messages through the use of write/read, courtesy call driven sequence. The DN-355 will then pass the message from NACE to the remote computer. Upon receipt of the message from NACE, the remote computer sends an ACK to the DN-355 to let the DN-355 know that it has received it. The DN-355 will then send to the remote computer a transmit message (clear to send). The remote computer can then send/receive message data. The DN-355 expects a response every seven seconds from the remote computer (to remain in the active mode). If the remote computer has no data to send, the remote computer may either send a No-Data message or a Disconnect message.

3.2 Initiation Procedures

In order to receive from or transmit message data to NACE, the DN-355 must be alerted to the remote computer wishes to sign-on. Input is initiated by the remote computer by a SELECT message. This message may or may not have the defined auxiliary field (see paragraph 2.2.4.1). The SELECT accomplishes two purposes:

a. The DN-355 is made aware that the remote computer is ready to enter the Active mode of operation.

b. With the auxiliary field defined, the DN-355 is told what format in which the remote computer expects to receive/transmit its message data.

3.2.1 SELECT Format. The format of the SELECT command with and without the defined auxiliary field, is depicted in paragraph 2.2.4.2.

3.2.1.1 SELECT Acknowledgement. The DN-355 on receipt of the SELECT command, will place the remote computer line in the Active mode and transmit an ACK in the following format:

SYN, SYN, SYN, SYN, SOH, FC, SC, AC, OC, IC, STX, ETX, BCC

where, SYN - 026
SOH - 001
FC - 110
SC - 101 or 102
AC - 100
OC - 102
IC - 100
STX - 002
ETX - 103
BCC - Exclusive OR of all characters following the SOH up to and including the ETX.

3.2.2 Log-On Procedure. Upon receipt of the ACK from the DN-355, the remote computer transmits the log-on identification as follows:

```
    SYN, SYN, SYN, SYN, SOH, FC, SC, AC, OC, IC, STX, H, $*SLOGXXUSERID$PASSWORD,
    ZZZ, RS, ETX, BCC

    where, FC - 104
           OC - 100
           H  - 110
           XX - Terminal Identification Code Assigned
           USERID$PASSWORD - Security USERID$ Password Assigned.  The XX and
                             USERID$PASSWORD are ASCII equivalents.
           RC - 026
```

3.2.2.1 Log-On Verification. If the Terminal ID and/or USERID$PASSWORD was incorrect, the DN-355 will transmit a line disconnect message. Upon verification of the Terminal Identification and USERID$PASSWORD, the DN-355 will transmit an ACK in the following format:

```
    SYN, SYN, SYN, SYN, SOH, FC, SC, AC, OC, IC, STX, ETX, BCC

    where, FC = 102, and all other character configuration is the same as
                other examples.
```

3.2.3 Direct Access Mode. When the remote computer receives the ACK from the DN-355 in response to its log-on, it is then necessary to inform the DN-355 that it wishes to be connected to NACE in the DAC mode.

This is accomplished by issuing the following command:

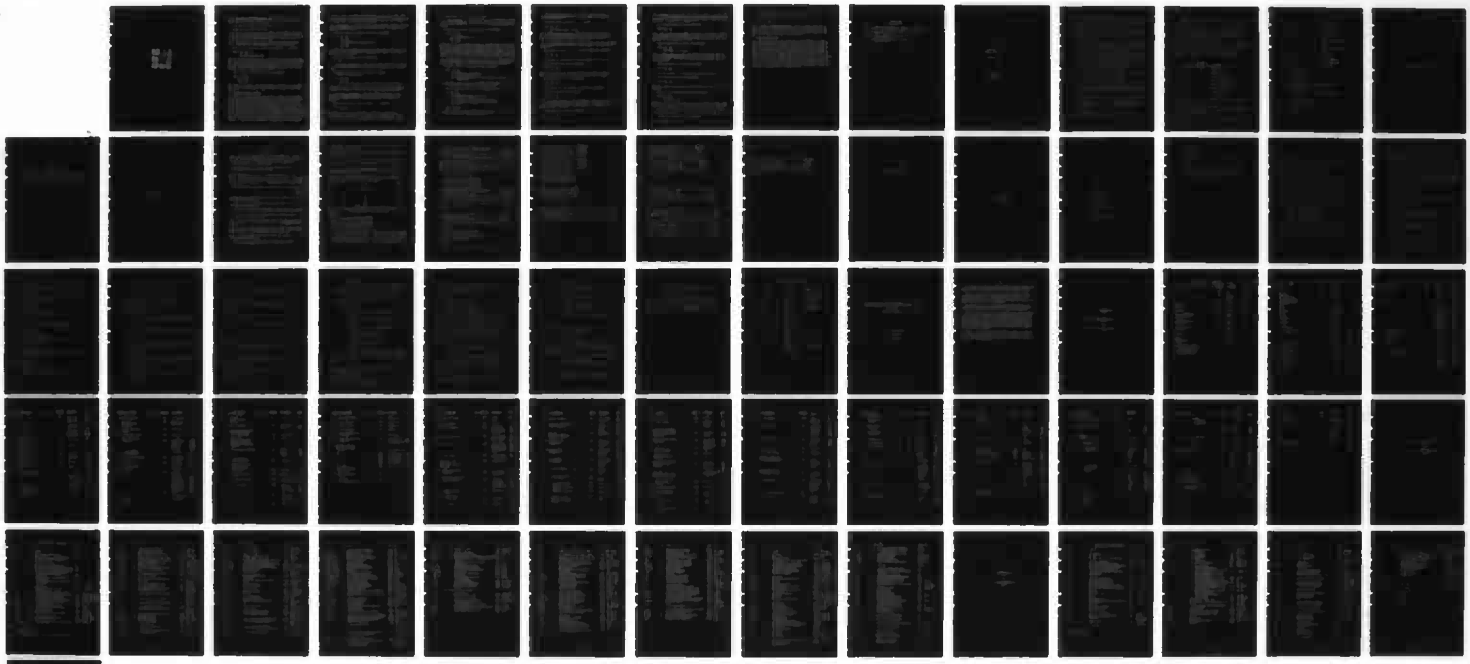
```
    SYN, SYN, SYN, SYN, SOH, FC, SC, AC, OC, IC, STX, H, $*$DACNACE-U, RS,
EXT, BCC

    where, FC = 104
           OC = 100
            H = 110
           $*$DACNACE-U is the octal equivalent.
           RS = 036
```

3.2.3.1 DAC Acknowledgement. When the DN-355 receives this command from the remote computer, the DN-355 will pass on to NACE the Terminal Identification of the remote computer to NACE. If NACE is incorrectly spelled or not in core, the DN-355 will transmit to the remote computer the message "XXXXNOT KNOWN". If the Terminal Identification is not known to NACE, the line will not be connected. If the DAC command was issued incorrectly, the remote computer will have to begin again at the SELECT command. If the DAC command was submitted correctly and the terminal code was known to NACE, the DN-355 will transmit an ACK with message data. This message data will include the security classification of the remote computer and the data. The size of this message is 25 words or 100 characters in the following format:

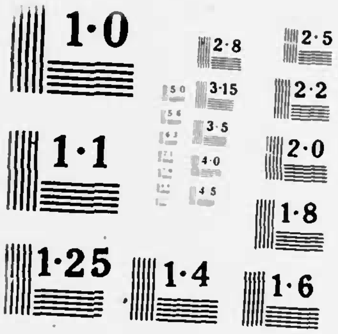
```
    SYN, SYN, SYN, SYN, FC, SC, AC, OC, IC, STX, Message data, ETX, BCC

    where, FC - 115
           OC - 100
```

AD-A134 884 INTER-SERVICE/AGENCY AUTOMATED MESSAGE PROCESSING 7/7
EXCHANGE PROGRAM FUNCTI..(U) DEFENSE COMMUNICATIONS
AGENCY ARLINGTON VA 01 NOV 83

UNCLASSIFIED F/G 17/2 NL



END
DTIC
7-86



NATIONAL BUREAU

MICROCOPY RESOLUT

3.2.3.2 Remote Computer Acknowledgement. When the remote computer receives this message from the DN-355, the remote computer must (as always) acknowledge the receipt of it in the following format:

SYN, SYN, SYN, SYN, SOH, FC, SC, AC, OC, IC, STX, ETX, BCC

Where, FC - 104 for ACK, 114 for NAK

When the DN-355 receives this ACK from the remote computer, NACE is effectively in control and the remote computer will respond only to requests from NACE; but the remote computer must acknowledge the receipt of all messages from the DN-355 and expect an ACK if transmitting message data.

3.2.4 Ready from NACE. When the security message is ACK'ed by the remote computer, NACE will issue a Ready message (FG) in the following format:

SYN, SYN, SYN, SYN, SOH, FC, SC, AC, OC, IC, STX, FG , ETX, BCC

where, FC = 115
OC = 100
FG = MMC indicating ready

The receipt of the FG must be ACK'ed in the same format as in paragraph 3.2.3.2. When the DN-355 receives this ACK, it will return the ACK (with the same sequence code). The return of the ACK from the DN-355 is a "clear to send" indication. The remote computer must either transmit message data or transmit a No Data (FI) message to NACE to complete its write/read sequence from the FG that was sent. The format of the NO Data message is as follows:

SYN,SYN,SYN,SYN,FC,SC,AC,OC,IC,STX,FI,NULL,RS,ETX,BCC

where, FC = 315
OC = 100
NULL = 100
RS = 036

NACE will ACK the receipt of the No Data message with another write/read sequence with no MMC. This completes the initiation sequence required by the RCI/DAC interface.

3.3 Message Transmission to NACE.

Because NACE is providing message routing service to other users concurrently, it cannot dedicate buffers to any one user source. NACE uses a buffer management routine that will allocate buffers among the active users. Therefore, before transmitting data to NACE, the remote computer must transmit a No Buffer, or No Data MMC. NACE, upon receipt of these commands, will attempt to find a buffer that is free for use. If none can be found, NACE will issue a wait MMC. If one is found, NACE will respond with a write/read command for the data. NACE must forware (route) the messages that it receives to the processors' message queues that are to receive them. However, there are times a message cannot be identified for routing. When this occurs, NACE will NAK the message, but will accept the message in its entirety for possible correction through other NACE facilities. The remote computer, if it is acting as a message concentrator, must also be prepared to preempt transmission of a current message to transmit one of a higher message precedence. This is accomplished by transmitting a "cancel" MMC to NACE. NACE will then "forget" the current message, and transmit an ACK to the remote computer. The remote computer should then relink the current message for later transmission, and transmit the one of higher message precedence.

3.3.1 Readv Message. To initially request a buffer from NACE, the remote computer transmits a "Ready" MMC to complete the write/read of NACE. The format of the Ready message is as follows:

```
SYN,SYN,SYN,SYN,SOH,FC,SC,AC,OC,IC,STX,FG, DC,5,RS,ETX,BCC

Where, FC = 115
       OC = 100
       FG = Ready
       DC = Data compression character 037
        5 = 065
       RS = 036
```

When NACE receives this Ready message from the remote computer, NACE will respond by transmitting a write/read (write 0 words/read large) sequence with no MMC. The format of this message is:

```
SYN,SYN,SYN,SYN,SOH,FC,SC,AC,OC,IC,STX,ETX,BCC

FC = 100
```

3.3.2 Message Data Transmission. After receiving the ACK from NACE in paragraph 3.3.1, the remote computer may begin transmitting message data in the following format:

```
SYN,SYN,SYN,SYN,SOH,FC,SC,C,OC,IC,STX,MMC,-----RS,MMC,---
----RS,MMC--------RS,ETX,BCC

where, FC = 115
       OC = 100
       RS - 036
      MMC = will depend upon the type of data message being transmitted.
```

Assuming there were no line errors, NACE will ACK or NAK the message (depending on whether the message was identified or not) with the next write/read sequence.

3.3.3 No Buffer Available (Wait). When this message is received by the remote computer, it indicates that NACE does not have any available buffer. NACE will transmit this message as a Write three words/Read Small. The format of this message is:

```
SYN,SYN,SYN,SYN,SOH,FC,SC,AC,OC,IC,STX,FE       ,RS,ETX,BCC

where, FC = 115
       OC = 100
```

The remote computer must transmit an ACK to the DN-355 to complete the write/read sequence of NACE and let its timer run-out. The remote computer may restart its transmission by transmitting thr Ready message in paragraph 3.3.1. The format for this ACK is the same as paragraph 3.2.3.2. The DN-355 will return the

ACK (same sequence code) to the remote computer.

3.3.4 Cancel Messages. It may become necessary to stop transmission of message data because of preemption by another message with a higher routing precedence or after encountering too many line errors. The format for this message is as follows:

```
SYN,SYN,SYN,SYN,SOH,FC,SC,AC,OC,IC,STX,FF,NULL,RS,ETX,BCC

where, FC - 315
       OC = 100
       FF - MMC denoting cancel
     NULL = 100
       RS = 036
```

NACE, upon receipt of the cancel message, will determine whether it must purge the portion of the message that was already received or "forget" that it ever received that portion. In either case, NACE will ACK the receipt of the cancel. The remote computer must relink the message for later transmission, time out, and then transmit a Ready message for the data message with the higher routing precedence. In the case of multiple errors, the remote computer must time out and either transmit a No Data or Disconnect depending on the condition of the line.

3.3.5 Status Request. The remote computer, because of the response made of the RCI/DAC, never requests the operational status of NACE, but always replies to the Status request from NACE. The format of the Status request from NACE is:

```
SYN,SYN,SYN,SYN,FC,SC,AC,OC,IC,STX,FAddeee ,RS,ETX,BCC

where, FC = 102
       OC = 104
       FA = MMC denotes Status request
       dd = Terminal identification
      eee = Message communication if remort computer is a message
            concentrator
```

When the remote computer receives this message, it must determine the condition of its line and transmit a response in the following format.

```
SYN,SYN,SYN,SYN,SOH,FC,SC,AC,OC,IC,STX,FBddeeef,RS,ETX,BCC

where, FC = 115
       OC = 100
       FB = MMC denoting Status information
       dd = Terminal identification
      eee = Communication line of message concentrator
        f = U for Up, D for Down and N for Not Configured
       RC = 036
```

3.4 Line Disconnect

This message is of two types, a Ready for Disconnect and a Disconnect, and each may be sent by the remote computer, the DN-355 or NACE.

3.4.1 Remote Computer Disconnect. When the remote computer determines that it has no more data messages to send, it transmits a Disconnect message to NACE in the following format:

```
SYN,SYN,SYN,SYN,FC,SC,AC,OC,IC,FH,NULL,RS,ETX,BCC

where, FC = 115
       OC = 100
       FH = MMC denoting Disconnect
```

3.4.1.1 NACE Response to Disconnect. NACE, upon receipt of the Disconnect, will assure that, if a message was in progress when the Disconnect was received, it will be purged and then a Disconnect will be transmitted to the DN-355. The format of this message is the same as paragraph 3.4.3.

3.4.1.2 DN-355 Response to Disconnect. The DN-355, upon receiving the Disconnect message from NACE, will transmit the Disconnect message to the remote computer in the format of:

```
SYN,SYN,SYN,SYN,SOH,FC,SC,AC,OC,IC,STX,NLINE DISCONNECTED--CP,RS,ETX,BCC

where, FC = 104
       OC = 100
```

This message must be acknowledged by the remote computer in the following format:

```
SYN,SYN,SYN,SYN,FC,SC,AC,OC,IC,STX,ETX,BCC

where, FC = 104
       OC = 100
```

When the DN-355 receives this ACK, it will remove the terminal ID from its DAC terminal table and transmit another Disconnect in the following format:

```
SYN,SYN,SYN,SYN,FC,SC,AC,OC,IC,STX,ETX,BCC

where, FC = 102
       OC = 104
```

The remote computer will then transmit its final ACK in the format of:

```
SYN,SYN,SYN,SYN,FC,SC,AC,OC,IC,STX,BCC

where, FC = 102
       OC = 104
```

3.4.1.3 Disconnect Immediately. When this message is received by the DN-355, it will Disconnect the line without responding (ACK) to the message. Any messages (input or output) destined for the remote computer will be destroyed and NACE will be notified. the format is:

```
SYN,SYN,SYN,SYN,FC,SC,AC,OC,IC,STX,ETX,BCC

where,  FC = 102
        OC = 104
```

3.4.2 Disconnect from the DN-355. The DN-355 will transmit a Disconnect when the line is too bad (hardware problems) to properly handle a Ready for Disconnect. Upon receipt of this message, the remote computer disconnects immediately without responding. The format of this message is:

```
SYN,SYN,SYN,SYN,SOH,FC,SC,AC,OC,IC,STX,ETX,BCC

where, FC = 102
       OC = 104
```

3.4.3 Ready for Disconnect from NACE. When NACE is at an End-of-Job condition, it will determine if there is a message in progress, if so, NACE will allow the message in progress to be completed, before transmitting a "Ready for Disconnect". The format of this message is as follows:

```
SYN,SYN,SYN,SYN,SOH,FC,SC,AC,OC,IC,STX,FH,ETX,BCC

where, FC = 102
       OC = 100
       FH = Ready for Disconnect
```

3.4.3.1 Remote Computer Response. When the Ready for Disconnect message is received, the remote computer should relink all remaining messages for later transmission and ACK the receipt of the Disconnect to the DN-355, with the following message:

```
SYN,SYN,SYN,SYN,SOH,FC,SC,AC,OC,IC,STX,ETX,BCC

where, FC = 104
       OC = 100
```

The DN-355 will respond to the ACK with the following Clear to Send message:

```
SYN,SYN,SYN,SYN,SOH,FC,AC,OC,IC,STX,ETX,BCC

where, FC = 110
       OC = 102
```

The remote computer must then ACK the receipt of the FH to NACE with the following message:

```
SYN,SYN,SYN,SYN,SOH,FC,AC,OC,IC,STX,FC,NULL,RS,ETX,BCC

where, FC = 115
       OC = 100
       FC = denotes ACK
```

NACE, upon the receipt of this ACK, will send to the DN-355 a Disconnect message. The DN-355 will then transmit a Ready for Disconnect in the following format:

```
SYN,SYN,SYN,SYN,SOH,FC,SC,AC,IC,STX,N LINE DISCONNECTED --CP,RS,ETX,BCC
```

The message must be ACKed by the remote computer with the following message:

```
SYN,SYN,SYN,SYN,SOH,FC,SC,AC,OC,IC,STX,ETX,BCC

where, FC = 104
       OC = 100
```

The DN-355 will then accomplish the Disconnect with the final message:

```
     SYN,SYN,SYN,SYN,SOH,FC,SC,AC,OC,IC,STX,ETX,BCC

     where, FC = 102
            OC = 104
```

3.4.3.2 Disconnect Immediately from NACE. If one of the NACE modules aborts, NACE will attempt to save as much of its operating environment as possible, and therefore, has little time to perform the nicety of the formal RCI/DAC interface. NACE will immediately disconnect the line without notifying the remote computer and expects no response as a result of the disconnect.

3.5 Operational Deviations

The RCI/DAC interface, with its user defined format, was designed to interface with the NMCS AUTODIN Terminal Subsystem (NATS). However, other remote computers can (and have been) also be configured to operate within the interface without adhering to all formal rigidity required by the RCI/DAC interface. An agreement must be reached between the users of the remote computers and the NACE support staff as to the format and volume of the message data that is to be transmitted/received. The format and volume must satisfy the basic requirements of the RCI/DAC and DN-355 interface. The DN-355 must first of all be satisfied as to the SELECT and DAC that must be issued in order to be connected to NACE. Once connected to NACE, the remote computer must be prepared to either send or receive message data, or to send a wait command to prevent timing out. The minimum MMC that can be used are: Ready, No Data, No Buffer, Disconnect and Acknowledgements (positive or negative). NACE can be modified to handle a variety of messages even though they do not conform to the format of the current NACE users.

BIBLIOGRAPHY

Honeywell, Remote Terminal Supervisor (GRTS), DB40B, July 1976

Honeywell, NATS IOC Interface, Task HIS 620, Subtask 1, Undated

Honeywell, I/O Programming, DB82A, January 1975

Honeywell, RNP/FNP Interface, DB92A, January 1975

SPECTRA 70 WWMCCS

INTERFACE SPECS

SUBCONVENTION

SECTION

The following is a detailed description of the formats of each message as viewed by the NATS and NACE and a description of the control information necessary to communicate with the DN355 and the H6000.

As a prelude, a description of the NATS/NACE subconvention specifications is necessary. The following paragraphs define the specification for the NATS/NACE subconvention.

1. There will be a logical and/or physical link for traffic from NATS to NACE. This line will handle all data, control sequences and protocol required to facilitate the transfer of data from NATS to NACE.

2. There will be a logical and/or physical link for traffic from NACE to NATS. This link will handle all data, control sequences, and protocol required to facilitate the transfer of data from NACE to NATS.

3. Each link will appear as a separate port to both NACE and NATS and will require no cross talk between ports for operation.

4. Basic security features are being developed by the Government for the NATS/NACE subconvention. The security features are:

a. RCI/DAC log-on and access level check.

b. Security code labeling of output (to NATS) adequate to allow for security caveat development at the final destination output device.

These security features are projected to be available in a subsequent version of WWSR6.0.

5. To insure positive control of the link, log on to a direct access program will be a log-on with no wait. If DAC program has not issued a "CONNECT" MME GEROUT for the terminal, a message "DAC" NOT KNOWN will be transmitted.

6. NACE will set status bit to place 355 in listen mode to NATS terminal for duration of connect.

7. Messages transmitted across the link, either way, will confirm to the following:

a. Messages will be broken down into message segments with each segment containing a maximum 16 lineblocks of 80 data characters each. Each message segment will contain complete lineblocks. Compression of data and truncation of trailing blanks will be allowed.

b. Each lineblock within a segment will be preceded by a media code character and will be followed by a record separator - (Octal 36 - Hexidecimal 9E). The media code character will contain information about the link block that follows. The following media codes (NOTE - ALL CODES ARE IN ASCII) will be used:

	MEDIA	CODE	CHARACTER	
	OCT	HEX	ASCII	DESCRIPTION
1	101	C1	(A)	* Single card message
2	102	C2	(B)	* Header
3	103	43	C	** Text - Card Image
4	104	C4	D	** Trailer - End of Message
5	105	45	E	*** Text - Variable Length
6	106	46	F	**** Control Information
7	107	C7	G	Operator Message

* NOTE: MEDIA CODES (A) AND (B) WILL BE FOLLOWED BY THE AUTODIN SEL CHARACTER (FRAMING CHARACTER TWO).

** NOTE: MEDIA CODES (C) AND (D) WILL BE FOLLOWED BY THE SECURITY CLASSIFICATION

*** NOTE: A PROVISION HAS BEEN MADE WITHIN THE SUBCONVENTION FOR VARIABLE LENGTH BUT THE NACE PACKAGE CANNOT HANDLE IT.

**** NOTE: MEDIA CODE (F) WILL BE FOLLOWED BY ONE OF THE FOLLOWING CHARACTERS TO DESCRIBE THE CONTROL FUNCTION

	OCT	HEX	ASCII	DESCRIPTION
1	101	C1	A	[1]Status Request
2	102	C2	B	[2]Status Information
3	103	43	C	Super ACK
4	104	C4	D	Super NAK - may not be sent to core only systems
5	105	45	E	WAIT
6	106	46	F	Cancel Current Message
7	107	C7	G	Pseudo Break
8	110	C8	H	Terminate
9	111	49	I	No Data (sent by transmitter only for handshaking)

[1] A status request will be in the following format:

F A dd eee

F = Control Information

A = Status Request

dd = Generic Device Type

NOTE: COMMUNICATION GENERIC DEVICE TYPES TO BE DEVELOPED.

eee = Unit Number

[2] A status request will be answered in the following format:

F B dd ee f

F = Control Information

B = Status Information

dd eee - Echo of Status Request

f = Status

RAMSTEIN WWMCCS PROTOCOL SPECIFICATIONS

	ASCII	
1	N	Not on System
2	U	Up
3	D	Down
4	R	Requested down

The following flows, narrative descriptions and data examples are provided to thoroughly explain operation of not only the NATS/NACE interface, but also the inner-protocol of the RCI-DAC interface to the DN355.

MESSAGE FORMATS SECTION

MESSAGE FORMATS

This is a description of the message formats and the DN355 control information necessary to pass these massages. The complete DN355 protocol will not be described in this paper. A supplemental will be added in the future to describe the entire DN355 protocol (i.e., NACK procedures, DN355 time-out procedures, etc.) for the benefit of the remote computer.

The following is a description of the control information block necessary to effect communications with the DN355 and H6000.

CONTROL INFORMATION-------------------CONTROL RECORD OR DATA---------

1				2	3	4	5	6	7	8	9	10	11a/11b	12
SYN	SYN	SYN	SYN	SOH	FC	SC	AC	OC	IC	AUX	STX	Data (Maximum 324 ch. or 16 LBs)	ETX/ETB	BCC

End of Block
Control
Information

1. SYN - This is the SYNchronization character and is a HEX'16' (OCT '026'). This character remains constant.

2. SOH - This is the Start of Header character and is HEX '01' (OCT '001'). This character remains constant.

3. FC - This is the Format Code character which varies with tye type of message to be passed. The four types are Info, Special Control Record, Data and Service.

4. SC - This is the Sequence Code character which alternates between a HEX 'C1" (OCT '301') and a HEX 'C2' (OCT '302').

5. AC - This is the Address Code character which is not used but must be in the control information. It is a HEX '40' (OCT '100'). This character remains constant.

6. OC - This is the Operation Code character and is used for ACKnowledgements and NonACKnowledgements. ACKnowledgements are recorded as HEX '40' (OCT '100') and NonACKnowledgements can very dependent upon existing conditions.

7. IC - This is the Identification Code character and is a HEX '40' (OCT '100'). This character remains constant.

8. AUX - This is the AUXiliary fields code character and is normally present only in a SELECT SERVICE message. When used, it is a HEX 'C7" (OCT '307').

9. STX - This is the Start of Text character and is a HEX '02' (OCT '002'). This character remains constant.

10. DATA - This is the DATA or control record field. Further discussion of Data formats will be discussed in the respection portions of this paper, Transmit or Receive.

11a. EXT - This is the End of Text character and is a HEX '83' (OCT '203').

11b. ETB - This is the End of Transmission Block character and is a HEX '97' (OCT '227').

12. BCC - This is the Block Check Character and is a cumulative exclusive OR operation with each character following the SOH and up to and including the ETB/ETX. The BCC must be odd parity.

All information must be odd-parity and all but SYN, SOH, STX, ETB/ETX, and 3CC are valid ASCII characters. The following translations are provided for the ASCII characters used in the control information.

HEX	OCT	ASCII
C1	101	A
C2	102	B
43	103	C
C4	104	D
45	105	E
46	106	F
C7	107	G
C8	110	H
CD	115	M
40	100	@

The following messages are the messages to be expected on Transmit and Receive. They will be referenced by message number in the expansion of the narrative descrip.ions of the Transmit and Receive sections of this paper.

MESSAGES

1.

SYN	SYN	SYN	SYN	SOH	FC	S*C	AC	OC	IC	AUX	STX	ETX	BCC
					C	B	@	B	@	G			

*Sequence Code must always be initialized as a "B".

2.

SYN	SYN	SYN	SYN	SOH	FC	SC	AC	OC	IC	STX	ETX	BCC
					B	B	@	@	@			

SYN	SYN	SYN	SOH	FC	SC	AC	OC	IC	STX	ETX	BCC
				H	B	@	B	@			

3.

SYN	SYN	SYN	SYN	SOH	FC	SC	AC	OC	IC	STX	CONTROL RECORD	R*S	ETX	BCC
					D	A	@	@	@		H $ * $ 3 B* ECA* $NACE*			

*3B is a channel designator. This designator will identify input/output device. 3B used for demonstration purpose only.

ECA is a USERID. ECA used for demonstration purposes only.

NACE is a Program ID. It will identify the using program designated to receive input or send output to or from the H6000.

RS -- This is the Record Separator. It is a HEX '9E' (OCT '036').

```
4.  H $ * $ 3 B  ECA $ N A C E R
                               S
```

5.

SYN	SYN	SYN	SYN	SOH	FC	SC	AC	OC	IC	STX	ETX	BCC
					H	B	@	B	A			

6.

SYN	SYN	SYN	SYN	SOH	FC	SC	AC	OC	IC	STX	CONTROL RECORD	RS	ETX	BCC
					D	B	@	@	@		H $ * $ D A C* $ N A C E			

*DAC - This is the Direct Access ID which connects the H6000 with no wait.

```
7.  H $ * $ D A C $ N A C E R
                            S
```

8.

SYN	SYN	SYN	SYN	SOH	FC	SC	AC	OC	IC	STX		ETX	BCC
					D	B	@	@	@		N LINE DISCONNECTED -- XXX		

XXX is variable.

9.

SYN	SYN	SYN	SYN	SOH	FC	SC	AC	OC	IC	STX	ETX	BCC
					B	A	@	F	A			

```
10. XX*R
       S
```

*XX represents the NATS/NACE subconvention control characters.

11.

SYN	SYN	SYN	SYN	SOH	FC	SC	AC	OC	IC	STX		RS	ETX	BCC
					M	A/B	@	@	@		X X			

12.

SYN	SYN	SYN	SYN	SOH	FC	SC	AC	OC	IC	STX		RS	ETB	BCC
					D	A/B	@	@	@		H 1			

SYN	SYN	SYN	SYN	SOH	FC	SC	AC	OC	IC	STX	ETX
					D	A/B	@	@	@		

13.

SYN	SYN	SYN	SYN	SOH	FC	SC	AC	OC	IC	STX	ETX	BCC
					H	A/B	@	@	@			

14. X X D A T A RS - - - - - - - - - - - - D A T A RS

15.

SYN	SYN	SYN	SYN	SOH	FC	SC	AC	OC	IC	STX		ETX	BCC
					M	A/B	@	@	@		X X, D A T A RS X X - - - - - - D A T A RS		

16. X X X X X X X RS

17.

17.

SYN	SYN	SYN	SYN	SOH	FC	SC	AC	OC	IC	STX		ETX	BCC
					M	A/B	@	@	@		XXXXXXX RS		

18

SYN	SYN	SYN	SYN	SOH	FC	SC	AC	OC	IC	STX		ETX	BCC
					M	A/B	@	@	@		XXXXXXXX RS		

19. XXXXXXXX RS

20. G NACE DISCONNECT RS

21.

SYN	SYN	SYN	SYN	SOH	FC	SC	AC	OC	IC	STX		ETX	BCC
					M	A/B	@	@	@		G NACE DISCONNECT RS		

22. Send no characters.

23.

SYN	SYN	SYN	SYN	SOH	FC	SC	AC	OC	IC	STX		ETX	BCC
					M	A/B	@	@	@		XXDATA RS XX DATA RS		

24.

SYN	SYN	SYN	SYN	SOH	FC	SC	AC	OC	IC	STX		ETX	BCC
					M	A/B	@	@	@		XXDATA RS XX DATA RS		

```
25.  X X D A T A R X X         D A T A R
                   S                     S
```

26. GNATS DISCONNECT

27.

S Y N	S Y N	S Y N	S Y N	S O H	F C	S C	A C	O C	I C	S T X		E T X	B C C
					D	B	@	@	@		N LINE DISCONNECTED X X X		

XXX IS VARIABLE

APPENDIX G: WWMCCS RTOS

LINE DISCIPLINE

FOR

AUTODIN INTERFACE

DCT 9000 - DN 355

CONTENTS

A. MESSAGE TYPES

1. Information - used for transferring AUTODIN message data and sending acks/naks.

2. Special Control Record - used for sign on, $*$id; break message, 062; or $*$DAC, Direct Access Request.

3. Service - used to initiate or terminate communications, send instruction or operation information to the other computer, and ack/nak service messages from the other computer.

B. FORMATS

1. General Information:

a. A transmission block is made up of a maximum of 253 characters including synchronization characters. An ack/nak for the previous block transmitted is contained within the next block to be transmitted. Data is exchanged using the ASCII character set with odd parity.

b. Data format within 324-character test.

(1) Data size will be three 80-char records for a total maximum of 240 characters between STX and ETB/ETX characters.

(2) "ETB" is used to end each of the first four 240-character blocks.

(3) "ETX" is used to end the fifth or the last 240-char block. In either case, no more data blocks should be sent until after a "TRANSMIT DATA" message is received from the 355.

c. The ACK/NAK for an "output" transmission block is located in the Operations code/type character of the next "input" transmission block received. This op/type code has the following bit pattern:

BIT	7	6	5	4	3	2	1
USE	1	ACK/NAK			OP	CODE	

An ACK is denoted by bits 4, 5, and 6 being turned off and a NAK is denoted by bit 4 being on and bits 5 and 6 being off.

2. The format for all three message types is basically the same: SYN, SYN, SYN, SYN, SOH, FC, SC, AC, TYPE/, STX, CONTROL RECORD TEXT, ETB, ETX, BCC.

The four sync characters, the start of header (SOH), address code, (AC), Identification code (IC), start of test (STX), and end of transmission block (ETB)/end of text (ETX) character are constant and are always present. The format code (FC) character identifies the type of message; info, special control record, or service. The sequence code (SC) alternates between "A" and "B" with each block transmitted with the SC reverting to "A" on the start sequence. The type/operation code identifies a type of message within each of the three major types; e.g., a "select" service message, a "transmit data" information message, etc. The block check character (BCC) is a cumulative exclusive OR operation with each character following the SOH and up to and including the ETB/ETX. The BCC must also have odd parity.

3. Information Message

a. To the DN355:

(1) To transmit data and ACK the last DN355 message: SYN, SYN, SYN,

```
SYN, SOH, M, A, @, @, @, STX, TEXT, ETB, BCC
             B                      ETX
```

Use alternate sequence code.

(2) To transmit data and NAK, the last DN355 message: SYN, SYN, SYN,

```
SYN, SOH, M, A, @, H, @, STX, SAME TEXT, ETB, BCC
             B                           ETX
```

Use the same sequence code.

(3) To transmit data in answer to a NAK from the DN355: SYN, SYN, SYN,

```
SYN, SOH, M, A, @, @, @, STX, SAME TEXT, ETB, BCC
             B                           ETX
```

Use same sequence code.

b. To send a "WAIT" message to the DN355:

(1) To transmit a wait and ACK the last DN355 message: SYN, SYN, SYN,

```
SYN, SOH, H, A, @, D, @, STX, ETX, BCC
          M  B
```

Data contained between STX and ETX will not be recognized by the 355. Use same sequence code.

(2) The last 355 message can be NACKED, but when the 355 receives a WAIT, it retransmits the last message anyway.

(3) The remote computer does not send "TRANSMIT DATA" messages.

c. Data from the DN355:

(1) Receiving data with an ACK of last 9000 message: SYN, SYN, SYN,

```
SYN, SOH, M, A, @, @, @, @, STX, TEXT, ETB, BCC
             B                         ETX
```

Alternate sequence code used.

(2) Receiving data with a NAK of last 9000 message: SYN, SYN, SYN,

```
SYN, SOH, M, A, @, H, @, STX, SAME TEXT, ETB, BCC
             B                           ETX
```

Same sequence code used.

(4) Receiving data NACKED by 9000 on previous transmission:

```
SYN, SYN, SYN, SYN, SOH, M, A, @, @, @, STX, SAME TEXT, ETB, BCC
                            B                           ETX
```

Same sequence code used.

d. "TRANSMIT DATA" message from DN355:

(1) Receiving TRANSMIT DATA message with ACK from 355: SYN, SYN, SYN,

```
SYN, SOH, H, A, @, B, @, STX, ETX, BC
             B
```

Alternate sequence code used.

(2) Receiving TRANSMIT DATA message with NAK from 355: SYN, SYN, SYN,

```
SYN, SOH, H, A, @, J, @, STX, ETX, BC
             B
```

Same sequence code used.

4. SPECIAL CONTROL RECORD MESSAGE

a. To the DN 355:

(1) To transmit break control record and ACK last 355 msg: SYN, SYN,

```
SYN, SYN, SOH, D, A, @, @, @, STX, H, 1, RS, ETX, BCC
                  B
```

Use changed sequence code.

(2) To transmit break control record and NAK last 355 msg;

SYN, SYN, SYN, SYN, SOH, D, $\underset{B}{A}$, @, H, @, STX, H, 1, RS, ETX, BCC

Use same sequence code.

(3) To transmit an ID control card and ACK last 355 msg:

SYN, SYN, SYN, SYN, SOH, D, $\underset{B}{A}$, @, @, @, STX, H, $*$ id USERID

$PASSWORD, RS, ETX, BCC

Use alternate sequence code.

(4) To transmit an ID control card and NAK the last 355 msg: SYN,

SYN, SYN, SYN, SOH, D, $\underset{B}{A}$, @, H, @, STX, H, $*$id USERID$PASSWORD, RS, ETX, BCC

Use same sequence code.

(5) To transmit direct access (DAC) control record and ACK: SYN, SYN,

SYN, SYN, SOH, D, $\underset{B}{A}$, @, @, @, STX, H, $*$DACFQRTOS, RS, ETX, BCC

Use alternate sequence code.

(6) To transmit DAC control record and NAK last msg: SYN, SYN, SYN,

SYN, SOH, D, $\underset{B}{A}$, @, H, @, STX, H, $*$DACFQRTOS, RS, ETX, BCC

Use same sequence code.

b. From the DN355:

(1) Receive special control record with ACK of last 9000 msg: SYN,

SYN, SYN, SYN, SOH, D, $\underset{B}{A}$, @, @, @, STX, N, MESSAGE, RS, ETX, BCC

Alternate sequence code used.

(2) Receive special control record with NAK of last 9000 msg: SYN,

SYN, SYN, SYN, SOH, D, $\underset{B}{A}$, @, H, @, STX, N, MESSAGE, RS, ETX, BCC

Same Sequence code used.

5. SERVICE MESSAGE

a. To the DN355:

(1) To transmit a "NO INSTRUCTION" message and ACK the last DN355 service message: SYN, SYN, SYN, SYN, SOH, B, $\underset{B}{A}$, @, @, @, STX, ETX, BCC

Use alternate sequence code.

(2) To transmit a "NO INSTRUCTION" message and NAK the last DN355 service message: SYN, SYN, SYN, SYN, SOH, B, $\underset{B}{A}$, @, H, @ STX, EXT, BCC.

Use same sequence code.

(3) To transmit a "SELECT" message with ACK: SYN, SYN, SYN, SYN, SOH, C, $\underset{B}{A}$, @, B, @, G, STX, ETX, BCC

Uses auxiliary field to denote no compression, no split. Use alternate sequence code.

(4) To transmit a "SELECT" message with a NAK: SYN, SYN, SYN, SYN, SOH, C, $\underset{B}{A}$, @, J, @, G, STX, ETX, BCC

Use same sequence code.

(5) To transmit a "READY FOR DISCONNECT" message with an ACK: SYN, SYN, SYN, SYN, SOH, B, $\underset{B}{A}$, @, D, @, STX, ETX, BCC

Use alternate sequence code.

(6) To transmit a "READY FOR DISCONNECT" message with a NAK: SYN, SYN, SYN. SYN, SOH, B, $\underset{B}{A}$, @, L, @, STX, ETX, BCC

Use same sequence code.

(7) To transmit a "DISCONNECT" message with an ACK: SYN, SYN, SYN, SYN, SOH, B, $\underset{B}{A}$, @, F, A, STX, ETX, BCC

Use alternate sequence code.

b. From the DN 355:

(1) TERMINATE, READY FOR DISCONNECT, and DISCONNECT messages have the same format used for sending to the DN355. The "NO INSTRUCTION" and "NOT READY FOR DISCONNECT" messages are not sent by the DN355.

(2) To transmit a "TERMINATE" message with an ACK: SYN, SYN,

SYN, SYN, SOH, B, A, @, C, @, STX, ETX, BCC
                  B

Use alternate sequence code.

c. START SEQUENCE

(1) 9000 sends a "SELECT" SERVICE message to DN 355.

Ref B5a(3)

(2) 355 sends a "TRANSMIT DATA" INFO message to 9000.

Ref B3d(1)

(3) 9000 sends an "I.D." CONTROL RECORD message to 355.

Ref B4a(3)

(4) 355 sends "TRANSMIT DATA" message to 9000.

Ref B3d(1)

(5) 9000 sends "$*$DAC" CONTROL RECORD to 355.

Ref B4a(5)

(6) 355 sends "NO REQUEST" DATA INFO msg to 9000. (The data in this msg will be "#RDYBK" to indicate no output at this time for 9000, but input will be accepted once the 9000 sends a "BREAK" message. DAC-IDLE mode entered.)

Ref B3c(1)

7. If the 9000 does not send a "BREAK" message, it must send a NO DATA "NO REQUEST" message to ACK the 355 message.

Ref B3a(1) with no "TEXT".

The next message it can then expect from the 355 is a "NO REQUEST" DATA message containing data from the 6070 program.

Ref B3a(1)

8. 9000 must then send a NO DATA, "NO REQUEST" message to the 355.

9. If the 9000 sends a "BREAK" message, (Ref B4a(1)), the next message it can expect is a "TRANSMIT DATA" INFORMATION message from the 355.

Ref B3d(1)

d. THE "BREAK" MESSAGE.

(1) This SPECIAL CONTROL message is sent to the DN 355 by the DCT 9000. The 355 does not send this message.

(2) When the DCT 9000 has data to transmit to the DN355/H6070, it must send a "BREAK" message first. This sends a bit in the H6070. When this bit is detected as being set, the 355 will be issued a command from the 6070 such that the 355 will send the 9000 a "TRANSMIT DATA" message. After all data has been transmitted from the 9000, a SEND must be transmitted, which will reset the break bit and allow any data in the H6070 for the 9000 to be sent.

(3) Any time after the "#RDYBK" message has been send AND before any "DISCONNECT" or "TERMINATE" message AND when the "BREAK" bit is not set, any data in the H6070 for the 9000 is sent. No request for input is made.

e. Wait Sequence

(1) 9000 sends a "WAIT" INFORMATION message to the 355.

(Ref B3b(1)

(2) 355 waits 7 seconds and retransmits the last block it sent.

(3) At this point the 9000 can send another "WAIT" reinitiating this sequence. This can be repeated for up to 15 minutes (or 30 minutes if so sent by the 6070 program) before the 355 sends a "READY FOR DISCONNECT" message to the 9000.

(Ref B5a(6))

(4) The 9000 must answer with a "READY FOR DISCONNECT" Ref B5a(6) or "NO INSTRUCTION" Ref B5a(1) service message.

f. Terminate or Disconnect Sequence.

(1) "TERMINATE" issued from 355.

(a) 355 sends "TERMINATE" SERVICE message to 9000.

Ref B5b(2)

(b) 9000 sends "NO INSTRUCTION" SERVICE message to 355.

Ref B5a(1)

(2) "DISCONNECT" issued from 9000.

(a) 9000 sends "READY FOR DISCONNECT" SERVICE msg to 355.

Ref B5a(5)

(b) 355 responds with "READY FOR DISCONNECT" SERVICE

Ref B5a(5)

message to 9000

-or-

9000 sends "DISCONNECT" SERVICE message to 355.

Ref B5a(7)

The 355 drops the line. No response.

(3) "DISCONNECT" issued from 355.

(a) 355 sends a "SPECIAL CONTROL RECORD" message indicating the reason for disconnect. Ref B4a(5), with message code in "TEXT" area in place of $*$DACFQRTOS.

(b) 9000 responds with "NO REQUEST" INFORMATION message.

(Ref B3a(1) with no "TEXT" data.

(c) 355 sends a "READY FOR DISCONNECT" SERVICE message to 9000.

Ref B5a(5)

(d) 9000 must respond with either a "READY FOR DISCONNECT," Ref B5a(5), or "NO INSTRUCTION," Ref B5a(1), SERVICE message to 355.

-or-

(e) 355 sends "DISCONNECT" SERVICE message to 9000.

Ref B5a(7)

(f) 9000 disconnects, no response.

4. During the transmission of a "message" (BLOCK-ETB, BLOCK-ETB, BLOCK-ETB, BLOCK-ETX), if the "ETX" block has not been ACKED by the 355 and a disconnect or terminate occurs, the entire message must be resent when the DAC mode is resumed. The DAC mode is resumed by the "START SEQUENCE."

DEFINITIONS AND EQUIVALENTS

CHARACTER	BINARY EQUIV		DEFINITION
SYN	0010110	16	Synchronous idle
SOH	0000001	01	Start of Header
STX	0000010	02	Start of Text
ETB	0010111	17	End of Transmission Block
ETX	0000011	03	End of Text
RS	0011110	1E	Record Separator
1	0110001	31	Break Character
A	1000001	41	
B	1000010	42	
C	1000011	43	
D	1000100	44	
F	1000110	46	
G	1000111	47	
H	1001000	48	
J	1001010	4A	
I	1001100	4C	
	1001101	4D	
N	1001110	4E	
@	1000000		Space
BCC	"Exclusive OR" of SOH thru EXT, ETB Characters		Block Check Character

INTER-SERVICE/AGENCY AUTOMATED MESSAGE PROCESSING EXCHANGE

(I-S/A AMPE)

TRACEABILITY MATRICES

- o FSD TO FRD/ICD
- o FRD to FSD
- o ICD TO FSD

PREFACE

This document contains three matrices; Functional Statement Document (FSD) mapped to the Functional Requirements Description (FRD) and the Interface Control Document (ICD), FRD mapped to the FSD, and ICD mapped to the FSD.

The FSD to FRD/ICD matrix demonstrates that the validated functional requirements documented in the three volumes of the FSD (Section I - Base Level Functions, Section II - ASC Residual Functions, and Section III - Network Interface Functions) are incorporated, where they are incorporated and whether they are IOC or post IOC requirements.

The FRD to FSD and ICD to FSD matrices indicate the FSD source of the paragraph where appropriate, thus it highlights those paragraphs not having an FSD source, and whether the paragraph is applicable at IOC or post IOC.

The FSD to FRD/ICD matrix has six columns: the first is the FSD function in order from all three volumes; the second designates which volume of the FSD, I for Base Level Functions, II for ASC Residual Functions, and III for Network Interface Functions; the third indicates Y for required at Initial Operational Capability (IOC, circa 1987) and P for postulated post-IOC; the fourth indicates which document the FSD function has been mapped to FRD for Functional Requirements Description and ICD for Interface Control Document; the fifth designates the paragraph; and the sixth the page number where the FSD function has been mapped.

The FRD to FSD and ICD to FSD matrices have five columns: the first is the paragraph of either the FRD or ICD; the second indicates Y for required at IOC and P for postulated post-IOC; the third is the paragraph title; the fourth is the page number of the paragraph; and the fifth is the FSD function which pertains to the paragraph.

Functional Statement Document
(FSD)

To

Functional Requirements Description
(FRD)

and

Interface Control Document
(ICD)

I-S/A AMPE FSD CROSS REFERENCED TO FRD/ICD

Functional Statement	+FSD	*IOC	FRD/ICD	Paragraph	Page
1.0 Protocols	I	Y	ICD	4.2 5.1	4-3 5-1
			FRD	3.1.5.2 3.2.1.1.1 3.2.3	3-9 3-15 3-66
DCS MODE I		Y	ICD	4.2.2.1a	4-3
DCS MODE II		Y	ICD	4.2.2.1c	4-5
DCS MODE V		Y	ICD	4.2.2.1d	4-5
Standard Remote Terminal (A.K.A. AMPE-MART) APPENDIX 1A		Y	ICD	4.2.2.2a App. B	4-6
Interim Remote Terminal APPENDIX 1B		Y	ICD	4.2.2.2b App. C	4-6
US Army DPI Interface APPENDIX 1C		Y	ICD	4.2.2.2c App. D	4-6
RIXT APPENDIX 1D		Y	ICD	4.2.2.2f Ref 2.5.a	4-6
SSMPS (Formally MRDIS) APPENDIX 1E		Y	ICD	4.2.2.2e App. E	4-6

+ I - Base Level Functions
II - ASC Residual Functions
III - Networking Functions

* Y - Yes required at 1OC
P - Postulated Post 1OC

Functional Statement	+FSD	*IOC	FRD/ICD	Paragraph	Page
DCT 2000		Y	ICD	4.2.2.2d Ref 2.5.d	4-6
WWMCCS NATS/NACE (A.K.A NMCS-NACE Protocol for Remote Computer Interface) APPENDIX 1I		Y	ICD	4.2.2.2g(1) App. F	4-7
WWMCCS RTOS APPENDIX 1J		Y	ICD	4.2.2.2g(3) App. G	4-7
WWMCCS DINDAC APPENDIX 1K		Y	ICD	4.2.2.2g(2) Ref. b,c	4-7
FACSIMILE		P	ICD	4.2.2.2h	4-7
OPINTEL Fleet Broadcast		P	ICD	4.2.2.2i	4-7
1.1 Transitional Connectivity to the ASC	II	Y	ICD	2.3 4.2.1 4.2.2.1a 5.1.2.1.1	2-2 4-3 4-3 5-1
1.2 Efficient Data Transfer	II	Y	ICD	4.2.2.1.a	4-3
1.3 TRI-TAC Interface	II	Y	ICD	5.1.2.1.2	5-2
App. II.1M TRITAC Mode I Interface Criteria	II	Y	ICD	Reference 2.5h 4.2.2.1a	 4-3
2.0 Code Conversion	I	Y	ICD FRD	4.4 3.2.1.1.3	4-10 3-17
3.0 Error Checking and Correction	I	Y		See 3.1 Thru 3.9 Below	
3.1 Undetected Bit Error Rate	I	Y	FRD	3.5.4 3.5.4.1	3-95 3-95

Functional Statement	+FSD	*IOC	FRD/ICD	Paragraph	Page
3.2 Message Accountability	I	Y	FRD	3.2.1.1	3-15
				3.2.1.1.1	3-15
				3.2.1.5.3.2	3-47
				3.2.1.6.1	3-50
				3.2.1.6.2.1	3-51
3.3 Format Validation	I	Y	ICD	4.3	4-9
			FRD	3.2.1.1.1	3-15
				3.2.1.2	3-17
				3.2.1.2.1.1	3-18
				3.2.1.2.1.1.1	3-18
				3.2.1.2.1.2	3-19
				3.2.1.2.1.3	3-20
				3.2.1.2.2.1	3-29
				3.2.1.2.2.2	3-29
				3.2.1.2.2.3	3-29
				3.2.1.2.2.4	3-29
				3.2.1.2.3.1	3-33
				3.2.1.2.3.2	3-33
				3.2.1.2.3.3	3-33
				3.2.1.3.3.2	3-36
App. 3B I-S/A AMPE Message Format Validation	I	Y	FRD	Section 20	20-1
3.4 Straggler Checking	I	Y	FRD	3.2.1.2.1.1.2	3-19
				3.2.1.2.1.2	3-19
3.5 Misrouting and Mislabeling	I	Y	FRD	3.2.1.3.1	3-34
3.6 Integrity	I	Y	FRD	3.2.1.1	3-15
				3.2.1.4.2.2.4	3-43
3.7 Channel Classmark - Message Security Level Validation	I	Y	FRD	3.1.5.3.3	3-11
				3.1.5.3.4	3-11
				3.1.5.3.6	3-12
				3.2.1.2.1.3	3-20
				3.2.1.2.1.4	3-20
				3.2.1.2.2.3	3-29
				3.2.1.2.2.4	3-29
				3.2.1.2.3.3	3-33
				3.2.1.2.3.4	3-33
				3.2.1.4.2.2.3	3-43

Functional Statement	+FSD	*IOC	FRD/ICD	Paragraph	Page
3.8 Other Error Checks	I	Y	FRD	3.2.1.1.1 3.2.1.2.3.1 3.2.1.2.3.5	3-15 3-33 3-33
3.9 Interlacing	I	Y	FRD	3.2.1.2.1.1.2 3.2.1.6.1e	3-19 3-50
4.0 FIFO by Precedence	I	Y	FRD	3.2.1.1.2 3.2.1.5.1 3.2.1.5.3.3 3.2.1.5.4	3-17 3-46 3-48 3-48
4.1 Additional DSSCS Requirements	I	Y	FRD	3.2.1.3.3.2	3-36
4.2 Exceptions to FIFO Processing	I	Y	FRD	3.2.1.5.1	3-46
4.3 Additional CRITIC Message Processing	II	Y	FRD	3.2.1.5.8.1	3-49
5.0 Flash, CRITIC, and ECP Preemption	I	Y	FRD	3.2.1.2.2.4 3.2.1.5.2	3-29 3-46
5.1 Preemption Rules	I	Y	FRD	3.2.1.5.2	3-46
5.2 Preemption Procedures	I	Y	FRD	3.2.1.5.2 3.5.2	3-46 3-93
6.0 Delivery of Single and Multiple Addressed Messages	I	Y	FRD	3.2.1.2.2.6.2 3.2.1.2.3.1 3.2.1.3 3.2.1.3.3.3	3-30 3-33 3-34 3-36
6.1 Multiple Addressing	II	Y	FRD	3.2.1.3.3.3 3.2.1.4.2.3	3-36 3-45
6.2 Collective Routing and Multiple Address Handling	II	Y	FRD	3.2.1.3.3.1	3-34

Functional Statement	+FSD	*IOC	FRD/ICD	Paragraph	Page
7.0 Media Conversion	I	Y	FRD	3.2.1.4.2.2.5	3-43
App. 7A Format and Media Conversion	I	Y	FRD	3.2.1.4.2.2.5 Ref. 2.5a	3-43
7.1 Input/Output Physical Media	I	Y	FRD	3.2.1.4.2.2.5	3-43
8.0 History Logs and Files	I	Y	FRD	3.2.1.6.2	3-51
8.1 Retrievable Message Storage	I,II	Y	FRD	3.2.1.5.8.1	3-49
				3.2.1.6.2	3-51
				3.2.1.7	3-54
				3.5.3.3	3-94
				3.7.3.2	3-101
App. 8A Message Storage Exception	I	Y		3.2.1.6.2	3-51
8.2 System Status Information	I	Y	FRD	3.2.1.6.2.1	3-51
				3.2.1.6.2.2	3-51
8.3 Reliability	I	Y	FRD	3.2.1.6.1	3-50
				3.2.1.6.2.2	3-51
9.0 Formats and Format Conversion	I	Y		Title Only	
9.1 Formats	I	Y	FRD	3.1.5.1.1	3-8
				3.2.1.1	3-15
				3.2.1.1.3	3-17
				3.2.1.2.1.1	3-18
				3.2.1.2.1.1.1	3-18
				3.2.1.2.1.2	3-19
				3.2.1.2.2.1	3-29
				3.2.1.2.2.2	3-29
				3.2.1.2.3.1	3-33
				3.2.1.2.3.2	3-33
				3.2.2.4	3-62
			ICD	4.3	4-9
App. 9A Abbreviated SI Message Format	I	Y		Information not included in FRD/ICD	

Functional Statement	+FSD	*IOC	FRD/ICD	Paragraph	Page
App. 9B Modified ACP 126 Format	I	Y	ICD	4.3.2	4-9
9.2 Format Conversion	I	Y	FRD	3.2.1.4.2.2.4 3.2.2.4	3-43 3-62
9.3 Formats/Format Conversion for Allied/NATO and Non-DoD AMPE Users	II	Y	FRD	3.2.1.4.2.2.3	3-43
App. II.9D Special Format/Format Conversion Criteria: Allied/NATO and Non-DoD Interface	I	Y	ICD	4.3.7	4-10
10.0 DSSCS Processing, App 10A	I	Y	FRD	3.2.1.1 3.4.2 3.10.1 3.12.6	3-15 3-84 3-106 3-109
11.0 Distribution of Incoming Messages	I	Y	FRD	3.2.1.4.2.1	3-37
11.1 Locating Distribution Parameters and Determining Units and Offices	I	Y	FRD	3.2.1.4.2.1.1	3-37
11.2 Determining Number of Copies	I	Y	FRD	3.2.1.1.3 3.2.1.4.2.1.2.2	3-17 3-38
11.3 Affixing Distribution	I	Y	FRD	3.2.1.4.2.2.6.1 3.2.1.4.2.2.6.2	3-43 3-43
11.4 Delivery Routing	I	Y	FRD	3.2.1.1.2 3.2.1.4.2.2 3.2.1.4.2.2.1 3.2.1.4.2.2.2	3-17 3-38 3-40 3-40
11.5 Army Distribution	I	Y	FRD	3.2.1.4.2.1.1 3.2.1.4.2.1.2 3.2.1.4.2.2.1 3.2.1.4.2.2.2	3-37 3-38 3-40 3-40
11.6 Navy Distribution	I	Y	FRD	(Same as 11.5)	

Functional Statement	+FSD	*IOC	FRD/ICD	Paragraph	Page
11.7 Air Force Distribution	I	Y	FRD	(Same as 11.5)	
11.8 NSA Distribution	I	Y	FRD	(Same as 11.5)	
11.9 DLA Distribution	I	Y	FRD	(Same as 11.5)	
11.10 DIA Distribution	I	Y	FRD	(Same as 11.5)	
12.0 Special Message Delivery Processing	I			Title Only	
12.1 Special Data Pattern Msg Processing	I	Y	FRD	3.2.1.4.2.2.7 3.2.1.4.2.2.7.1 3.2.1.4.2.2.7.2	3-44 3-45 3-45
12.2 Output (Printed or Displayed) Message Editing	I			See a thru f below	
a.		Y	FRD	3.2.1.4.2.2.6.3	3-44
b.		Y	FRD	3.2.1.4.2.2.6.6	3-44
c.		Y	FRD	3.2.1.4.2.2.6.2	3-43
d.		Y	FRD	3.2.1.4.2.2.6.2	3-43
e.		Y	FRD	3.2.1.4.2.2.6.2	3-43
f.		Y	FRD	3.2.1.4.2.2.6.2	3-43
App. 12A Navy LDMX Printed Message Format	I	Y	FRD	3.2.1.4.2.2.6.6	3-44
12.3 Print Expansion of Reports	I	Y	FRD	3.2.1.4.2.2.6.4	3-44
App. 12B Print Expansion Criteria	I	Y	ICD	App. B	

Functional Statement	+FSD	*IOC	FRD/ICD	Paragraph	Page
12.4 Sequential Delivery	II	Y	ICD	4.2.5	4-8
				4.2.6	4-8
12.5 Linked Channels	II	Y	ICD	5.1.3	5-2
13.0 PLA/RI Assignment	I	Y	FRD	3.2.1.1.1	3-15
				3.2.1.2.2.6	3-30
				3.2.1.2.2.6.1	3-30
				3.10.3	3-106
13.1 Assignment Procedures	I	Y	FRD	3.2.1.2.2.6.2	3-30
				3.2.1.2.2.6.4	3-32
				3.2.1.3.3.1	3-34
13.2 Assignment Data	I	Y	FRD	3.2.1.2.2.6.1	3-30
				3.2.1.2.2.6.3	3-31
				3.2.1.2.2.6.5	3-32
				3.2.1.2.2.6.6	3-32
				3.5.3.1	3-94
13.3 SHD Processing	I	Y	FRD	3.2.1.2.1.1.1	3-18
				3.2.1.2.2.6.2g	3-30
App. 13A Special Handling Designator Processing Procedures	I	Y	FRD	Appendix 20.0	
13.4 Address and Routing Management	II	Y	FRD	3.2.1.2.2.6.3	3-31
				3.2.1.2.2.6.5	3-32
14.0 Internal Distribution of Outgoing Messages	I	Y	FRD	3.2.1.1.3	3-17
				3.2.1.4.2.1	3-37
				3.2.1.4.2.1.1	3-37
				3.2.1.4.2.1.2	3-38
				3.2.1.4.2.1.2.2	3-38
14.1 Comeback Copies of Messages	I	Y	FRD	3.2.1.4.2.1.2.1	3-38
15.0 Readdressal and Retransmission	I	Y	FRD	3.2.1.5.8.2	3-50
				3.2.1.7	3-54
15.1 Readdressal	I	Y	FRD	3.2.1.5.8.2	3-50
				3.2.1.7.3	3-59

Functional Statement	+FSD	*IOC	FRD/ICD	Paragraph	Page
15.2 Automatic Retransmission	I	Y	FRD	3.2.1.5.8.2 3.2.1.7.4	3-50 3-59
16.0 Statistics and Statistical Report Generation	I	Y	FRD	3.3.1 3.3.3.3 3.3.5 3.3.7 3.3.8	3-66 3-69 3-70 3-76 3-79
APP. 16A Statistics and Report Generation Criteria	I	Y	FRD	Section 50	50-1
16.1 Message Traffic Information	I	Y	FRD	3.2.1.7.1 3.3.5.3.1 3.3.5.3.3 3.3.8	3-54 3-72 3-73 3-79
16.2 Message Status Information	I,II	Y	FRD	3.2.1.5.3.2 3.3.5.3 3.3.6.3 3.3.8	3-47 3-72 3-76 3-79
16.3 System Status Information	I,II	Y	FRD	3.2.1.5.3.1 3.2.1.6.2.1 3.3.5 3.3.6	3-47 3-51 3-70 3-76
16.4 Statistical Reports	I,II	Y	FRD	3.3.6 3.7.4.3 3.3.5	3-76 3-102 3-70
16.5 Additional Real-Time or Periodic Reports	II	Y	FRD	3.3.6 3.7.4.3	3-76 3-102
a. DCS Message Quality Control			FRD	3.3.6.4	3-76
b. Circuit and Equipment Outage			FRD	3.3.6.1	3-76
c. Termination Capacity			FRD	3.3.3.3 3.3.5.3	3-69 3-72
16.6 Operator Search and Retrieval of Historical, Statistical and Status Information	II	Y	FRD	3.2.1.7.1 3.2.1.7.2 3.3.5	3-54 3-54 3-70

Functional Statement	+FSD	*IOC	FRD/ICD	Paragraph	Page
17.0 Intransit Storage	I	Y	FRD	3.7.3.1	3-101
18.0 Overflow Protection	I	Y	FRD	3.2.1.5.4 3.3.3.1 3.10.3	3-48 3-74 3-106
19.0 Automatic Service Message Generation, and Other Service Message Related Functions	I	Y	FRD	3.2.1.5.8 3.10.3	3-49 3-106
19.1 Automatic Service Message Generation	I,II	Y	FRD	3.2.1.2.1.4 3.2.1.2.2.4 3.2.1.2.3.4 3.2.1.5.8.1	3-20 3-29 3-33 3-49
App. 19B Service Messages	I	Y	FRD	App 21.0	
App. II.19B Additional Service Messages	II	Y	FRD	App 21.0	
19.2 Automatic Processing of Incoming Service Messages	I	Y	FRD	3.2.1.5.8.2 3.2.1.7.2 3.2.1.7.3 3.2.1.7.4	3-50 3-54 3-59 3-59
App. 19A Operating Signals and Content Indicator Codes	I	Y		Information not included in FRD/ICD	
19.3 Manual Processing of Incoming Service Messages	I	Y	FRD	3.2.1.5.8.3	3-50
19.4 Information Protection	I	Y	FRD	3.2.1.5.8	3-49
20.0 Automation Assisted Traffic Management	I	Y	FRD	3.2.1.5.3 3.3.4 3.3.4.1	3-46 3-69 3-69
20.1 Intercept Processing	I	Y	FRD	3.2.1.1.2 3.2.1.5.3.3 3.3.4.1	3-17 3-48 3-69
20.2 History Data Information Interrogation	I	Y	FRD	3.2.1.6.3	3-54

Functional Statement	+FSD	*IOC	FRD/ICD	Paragraph	Page
20.3 Traffic Management	I	Y	FRD	3.2.1.1.2	3-17
				3.2.1.5.3.1	3-47
				3.2.1.5.6	3-49
21.0 Message Retrieval	I	Y	FRD	3.2.1.5.8.2	3-50
				3.2.1.7	3-54
				3.2.1.7.1	3-54
				3.2.1.7.2	3-54
				3.5.3.4	3-94
				3.7.3.2	3-101
22.0 Alternate Routing	I,II	Y	FRD	3.2.1.1.2	3-17
				3.2.1.5.5	3-48
				3.3.3	3-68
				3.3.4	3-70
22.1 Remote Terminals	I,II	Y	FRD	3.2.1.5.5	3-48
23.0 User-to-User Service	I	Y	FRD	3.1.5.3	3-19
				3.1.5.3.1.2	3-10
24.0 Automatic Supervision of Message Preparation	I	Y	FRD	3.1.5.1	3-8
				3.1.5.1.2	3-8
				3.2.1.2.2.5	3-30
				3.2.2.1	3-60
				3.2.2.3	3-61
25.0 Message Mask Call Up From Remote Terminal	I	Y	FRD	3.1.5.1.2	3-8
				3.2.1.5.8.3	3-50
				3.2.2.2	3-61
26.0 File Maintenance	I	Y	FRD	3.2.1.2.2.6.3	3-31
				3.2.1.2.2.6.5	3-32
				3.2.1.5.7	3-49
				3.3.2.1.2	3-68
				3.3.3.1	3-68
				3.3.9.3	3-81
27.0 System Control Activities	I	Y	FRD	3.3	3-66
27.1 Failure Recovery	I	Y	FRD	3.3.2.1.1	3-68
				3.3.9.2	3-80
				3.5.5.1	3-95
				3.7.5.2	3-103

Functional Statement	+FSD	*IOC	FRD/ICD	Paragraph	Page
a. Automatic Failure Recovery	I	Y	FRD	3.3.8.2.1	3-80
				3.5.5.1	3-95
b. Manual Failure Recovery	I	Y	FRD	3.3.8.2.2	3-80
c. Reconstruction of System Files	I	Y	FRD	3.3.8.2	3-80
				3.3.8.3	3-81
d. Message Recovery	I	Y	FRD	3.2.1.6.2	3-51
e. Error Message Purge	I	Y	FRD	3.2.1.5.6	3-49
27.2 System Reconfiguration	I	Y	FRD	3.3.2.1.1	3-68
				3.3.3	3-68
				3.3.3.1	3-68
				3.3.3.2	3-68
				3.3.9.1	3-79
				3.7.5.2	3-103
27.3 Message Trace	I	Y	FRD	3.2.1.5.3.2	3-47
				3.2.1.6.2.1	3-51
27.4 Operator Notification	I	Y	FRD	3.2.1.2.1.4	3-20
				3.2.1.2.2.4	3-29
				3.2.1.2.3.4	3-33
				3.2.1.5.3.2	3-47
				3.3.5.1.2	3-71
				3.3.5.2	3-72
				3.3.5.3.5	3-76
				3.3.6	3-76
				3.3.9.1	3-79
27.5 Error Corrections	I	Y	FRD	3.2.1.2.2.6.2	3-30
				3.2.1.2.2.6.3	3-31
				3.2.1.2.2.6.5	3-32
27.6 OPSIGS	I	Y	FRD	3.2.1.2.2.4	3-29
27.7 Fault Isolation and Equipment Status	I,II	Y	FRD	3.2.1.5.8.1	3-49
				3.3.2.1.1	3-68
				3.3.5.1	3-71
				3.3.7	3-77
				3.7.4	3-101

Functional Statement	+FSD	*IOC	FRD/ICD	Paragraph	Page
a. Internal System Control .	II	Y	FRD	3.3.5.1.2	3-72
				3.3.6	3-77
b. Circuit and Equipment Patch	II	Y	FRD	3.3.1.2	3-67
				3.3.3	3-68
				3.3.3.1	3-68
				3.3.3.2	3-68
				3.3.7	3-77
27.8 Inter-AMPE Connection	I,II	Y	ICD	2.3	2-2
				4.2.1	4-3
				4.2.2.1a	4-3
				5.1.2.1.1	5-1
27.9 Security Considerations	I	Y	FRD	3.4	3-84
a. TEMPEST Protection	II	Y	ICD	3.6	3-3
b. ALPS	II	Y	FRD	3.2.1.6.2	3-51
c. Crypto Considerations	II	Y	FRD	3.3.6.5.1	3-79
				3.4.5	3-85
d. Classification Label	II	Y	FRD	3.2.1.4.2.2.6.5	3-44
27.9.1 Authentication/ Verification	I	Y	FRD	3.1.5.3.3	3-11
				3.1.5.3.4	3-11
				3.1.5.3.5	3-11
				3.1.5.3.6	3-12
				3.2.1.2.1.3	3-20
				3.2.1.2.2.3	3-29
				3.2.1.2.3.3	3-33
			ICD	7.0	7-1
				7.4	7-2
27.9.2 Multilevel Security	I	Y	FRD	3.4.1	3-84
				3.7.3.3	3-101
				3.7.5.4	3-103
			ICD	7.1	7-1
27.9.3 DSSCS/GENSER Community Separation Hardware Considerations	I	Y	FRD	3.3.6.5.2	3-85
			ICD	7.3	7-2

Functional Statement	+FSD	*IOC	FRD/ICD	Paragraph	Page
27.9.4 End-to-End Encryption (E^3) Consideration	I	Y	ICD	4.2.2.1 5.1.1	4-3 5-1
28.0 System/Facility Design and Test Criteria	II	Y	FRD	3.3.1 3.3.2 3.3.4 3.3.6	3-66 3-67 3-70 3-76
28.1 System/Facility Design Criteria	II			Title Only	
a. System Reconfiguration Capability	II			Title Only	
(1) System/Software Modularity	II	Y	FRD	3.1.5.4.1 3.6.1b 3.6.2 3.6.3 3.6.4 3.7.2 3.8.1 3.8.2	3-12 3-97 3-98 3-99 3-99 3-100 3-104 3-104
(2) System expandability and growth	II			Title Only	
(a)	II	Y	FRD	3.7.2 3.8.1 3.8.3 3.11.2	3-100 3-104 3-104 3-107
(b)	II	Y	FRD	3.5.1.2 3.7.2 3.7.2.2. 3.8.1 3.8.3 3.10.2	3-91 3-100 3-100 3-104 3-104 3-106
(c)	II	Y			
b. Survivability/ Availability Requirement	II			Title Only	
(1) Availability Requirements	II			Title Only	

Functional Statement	+FSD	*IOC	FRD/ICD	Paragraph	Page
(a) System Reliability Requirements	II			Title Only	
1	II	Y	FRD	3.5.2	3-93
2	II	Y	FRD	3.5.5	3-95
				3.7.5.1	3-101
3	II	Y	FRD	3.5.4	3-95
(b) Connectivity Requirements	II			Title Only	
1	II	Y	FRD	3.1.5.4.2	3-12
2	II	Y	FRD	3.3.5.3.2	3-73
(2) EMI Protection	II	Y	ICD	3.5	3-2
28.2 Facility Security Testing	II	Y	FRD	3.1.5.4.4	3-12
				3.4.1	3-84
				3.4.3	3-84
				3.4.4	3-85
				4.2	4-2
				4.3	4-3
				4.4	4-5
				4.5	4-6
				4.6	4-7
				4.7	4-7
			ICD	7.0	7-1
28.3 NICS TARE AUTODIN Interface Device (AID)	II	Y	ICD	5.1.2.2.1	5-4
29.0 Integrated AUTODIN System (IAS) Functions	III	Y	FRD	3.1.5	3-6
29.1 IAS Protocol Structure and DDN Interface	III	Y		See a and b below	
a.	III	Y	ICD	4.1	4-1
			FRD	3.3.1	3-66
b.	III	Y	FRD	3.3.1	3-66
29.2 IAS Addressing	III	Y	FRD	3.1.5	3-6
a.	III	Y			
b.	III	Y			

Functional Statement	+FSD	*IOC	FRD/ICD	Paragraph	Page
29.3 Looping/Shuttling Protection	III	Y	FRD	3.2.1.2.3.1	3-33
				3.2.1.2.3.5	3-33
				3.3.3.2a,b	3-75
29.4 Data Path Control				See a and b below	
a.	III	Y	FRD	3.1.5.3	3-9
				3.1.5.3.1	3-10
				3.2.3.1	3-63
b.	III	P	FRD	3.1.5.3	3-9
				3.1.5.3.1	3-10
				3.2.3.1	3-63
29.5 Flexibility/Future Expansion	III	Y	ICD	4.1	4-1
			FRD	3.1.5.1.3	3-8

Functional Requirements Description
(FRD)

To

Functional Statement Document
(FSD)

I-S/A AMPE FRD Cross Referenced to FSD

FRD	IOC	Title	Page	FSD
1.0	Y	SCOPE	1-1	*
1.01	Y	Basis	1-1	*
1.1	Y	Interface Control Document	1-2	*
1.2	Y	Standard Definitions and Terminology	1-2	*
1.3	Y	Pre-planned Product Improvement	1-2	*
1.4	Y	Change Procedures	1-2	*
2.0				
	Y	APPLICABLE DOCUMENTS	2-1	*
2.1	Y	Military and Federal Standards	2-1	*
2.2	Y	DoD Directives, Instructions and Manuals	2-2	*
2.3	Y	Joint/Allied Communications Publications	2-2	*
2.4	Y	Service/Agency Telecommunications Instructions and Procedures	2-3	*
2.5	Y	References	2-4	*
2.6	Y	Selected Papers on Secure Systems Development	2-4	*
2.7	Y	Industry Specifications, Instructions and Manuals	2-5	*
3.0		REQUIREMENTS	3-1	Title Only
3.1	Y	General I-S/A AMPE Objectives and Concepts	3-1	I,II,III
3.1.1	Y	The I-S/A AMPE as an Element of the Integrated AUTODIN System Architecture	3-1	III.29.0,III.29.4
3.1.2	Y	The Near-Term IAS Architecture	3-2	III.29.0,III.29.4
3.1.3	Y	The Mid-Term IAS Architecture	3-2	III.29.0,III.29.4
3.1.4	Y	The Goal and Far-Term IAS Architecture	3-6	III.29.0,III.29.4
3.1.5	Y	I-S/A AMPE Concept of Operation	3-6	I,II,III
3.1.5.1	Y	I-S/A AMPE Services	3-8	I,II,III
3.1.5.1.1	Y	Formal Message Service (FMS)	3-8	I,II
3.1.5.1.2	Y	Message Editing and Preparation Service (MEPS)	3-8	24.0,25.0
3.1.5.1.3	P	Future IAS Services	3-8	III.29.5
3.1.5.1.4	P	Virtual Connection Service (VCS)	3-9	III.29.0 III.29.1b
3.1.5.2	Y	I-S/A AMPE Interfaces	3-9	1.0, II.9.3, 9.0
3.1.5.3	Y/P	I-S/A AMPE Data Path Control	3-9	23.0, III.29.4
3.1.5.3.1	Y/P	Data Flow Paths	3-10	III.29.4
3.1.5.3.1.1	Y/P	Local Subscriber (Term.) to Local Service	3-10	III.29.4

Y - required for IOC
P - required for post IOC
* - not addressed in FSD
Y/P - paragraph addresses both an IOC and a post IOC requirement

FRD	IOC	Title	Page	FSD
3.1.5.3.1.2	P	Local Subscriber (Term.) to Local Subscriber (Terminal)	3-10	23.0, III.29.4
3.1.5.3.1.3	P	User (Terminal) to Network	3-10	III.29.4
3.1.5.3.1.4	Y/P	Service to Service via the DDN	3-10	III.29.4
3.1.5.3.2	Y	Access Control	3-10	3.7, 27.9.1
3.1.5.3.3	Y	Physical Line Security Validation	3-11	3.7, 27.9.1
3.1.5.3.4	Y	Subscriber Identification Validation	3-11	3.7, 27.9.1
3.1.5.3.5	Y/P	Data Path Requests	3-11	27.9.1, III.29.4
3.1.5.3.5.1	P	Access to a Local Subscriber	3-11	27.9.1, III.29.4
3.1.5.3.5.2	Y/P	Access to a Service	3-11	27.9.1, III.29.4
3.1.5.3.5.3	Y/P	Access to a Remote Network Element	3-11	27.9.1, III.29.4
3.1.5.3.6	Y	Data Path Error Processing	3-12	3.7, 27.4, 27.9.1, III.29.4
3.1.5.4				
3.1.5.5		I-S/A AMPE Design Requirements	3-12	Title Only
3.1.5.5.1	Y	Modularity Concept	3-12	II.28.1.a,III.29.5
3.1.5.5.2	Y	Interoperability and Survivability	3-12	II.28.1b(1)(b)1
3.1.5.5.3	Y	Security	3-12	27.9, II.27.9, 28.2
3.1.5.5.4	Y	I-S/A AMPE System Objectives	3-12	I,II,III
3.2	Y	I-S/A AMPE Functions	3-15	I,II,III
3.2.1	Y	Formal Message Service Functions	3-15	Title Only
3.2.1.1	Y	Message Processing Overview	3-15	9.0, 10.0, III.29.0
3.2.1.1.1	Y	Input Message Processing Overview	3-15	1.0, 3.2.c, 3.3, 3.8, 13.0, III.29.4
3.2.1.1.2	Y	Control and Routing Overview	3-17	4.0, 11.4, 20.1, 20.3, 22.0
3.2.1.1.3	Y	Output Message Processing Overview	3-17	2.0, 11.2, 11.4, 14.0
3.2.1.2	Y	Input Message Processing	3-17	3.3
3.2.1.2.1	Y	Input Message Processing (General)	3-18	See 3.2.1.2.1.1 thru 3.2.1.2.1.4 Below
3.2.1.2.1.1	Y	Message and Format Identification	3-18	3.3, 9.0
3.2.1.2.1.1.1	Y/P	Acceptable Formats	3-18	3.3, 9.0
3.2.1.2.1.1.2	Y	Message Integrity	3-19	3.4, 3.9
3.2.1.2.1.2	Y	Message Validation	3-19	3.3, 9.0, II.9.3
3.2.1.2.1.3	Y	Security Validation	3-20	3.0, 27.9, II.27.9
3.2.1.2.1.4	Y	Error Processing	3-20	3.0, 19.1, 27.4
3.2.1.2.2	Y	Input Message Processing (Terminal)	3-20	3.3
3.2.1.2.2.1	Y	Message and Format Identification	3-29	3.3, 9.0
3.2.1.2.2.2	Y	Message Validation	3-29	3.3, 9.0, II.9.3

FRD	IOC	Title	Page	FSD
3.2.1.2.2.3	Y	Security Validation	3-29	3.0, 27.9, II.27.9
3.2.1.2.2.4	Y	Error Processing	3-29	3.0, 19.1, 27.4, 27.6
3.2.1.2.2.5	Y	Message Editing and Preparation Service (MEPS)	3-30	24.0, III.29.0
3.2.1.2.2.6	Y	Plain Language Address (PLA) to Routing Indicator (RI) Assignment	3-30	13.0
3.2.1.2.2.6.1	Y	Formulation of Plain Language Addresses	3-30	13.2
3.2.1.2.2.6.2	Y	Use of Plain Language Addresses	3-30	13.1, 13.3, 27.5
3.2.1.2.2.6.3	Y	Automated PLA Directory Maintenance	3-31	13.2, 26.0, 27.5
3.2.1.2.2.6.4	Y	PLA Directory Files	3-32	13.1
3.2.1.2.2.6.5	Y	File Maintenance	3-32	13.2, II.13.4, 26.0, 27.5,
3.2.1.2.2.6.6	Y	Data Base Sizing for PLAs	3-32	13.0
3.2.1.2.3	Y	Input Message Processing (Network)	3-33	III.29.0
3.2.1.2.3.1	Y	Message and Format Identification	3-33	3.3, 3.8, 9.0, III.29.3
3.2.1.2.3.2	Y	Message Validation	3-33	3.3, 9.0, II.9.3
3.2.1.2.3.3	Y	Security Validation	3-33	3.0, 27.9, II.27.9
3.2.1.2.3.4	Y	Error Processing	3-33	3.0, 19.1, 27.4,
3.2.1.2.3.5	Y	Looping Protection	3-33	3.8, III.29.3
3.2.1.3	Y	Routing	3-34	6.0, 13.0, III.29.0
3.2.1.3.1	Y	Routing Parameters	3-34	3.5
3.2.1.3.2	Y	Routing Determination	3-34	22.0
3.2.1.3.3	Y	Special Routing Considerations	3-34	See 3.2.1.3.3.1 thru 3.2.1.3.3.3 Below
3.2.1.3.3.1	Y	Collective Routing	3-34	3.3, 6.0, II.6.2, 13.1
3.2.1.3.3.2	Y	CRITIC Routing	3-36	3.3, 4.1, II.4.3
3.2.1.3.3.3	Y	Multiple Addressed Messages	3-36	6.0, II.6.1
3.2.1.4	Y	Output Message Processing	3-36	See 3.2.1.4.1 and 3.2.1.4.2 Below
3.2.1.4.1	Y	Network Outgoing Message Processing	3-36	III.29.0
3.2.1.4.2	Y	Terminating Message Processing	3-37	See 3.2.1.4.2.1 and 3.2.1.4.2.2 Below
3.2.1.4.2.1	Y	Message Distribution Function	3-37	11.0, 14.0
3.2.1.4.2.1.1	Y	Distribution Determination Parameters	3-37	11.1, 11.5-11.10, 14.0
3.2.1.4.2.1.2	Y	Distribution Determination	3-38	11.5-11.10, 14.0

FRD	IOC	Title	Page	FSD
3.2.1.4.2.1.2.1	Y	Comeback-Copies of Messages	3-38	14.1
3.2.1.4.2.1.2.2	Y	Multiple Copy Determination	3-38	11.2, 14.0
3.2.1.4.2.2	Y	Message Delivery	3-38	11.4
3.2.1.4.2.2.1	Y	Message Delivery Parameters	3-40	11.4, 11.5-11.10
3.2.1.4.2.2.2	Y	Message Delivery Determination	3-40	11.4, 11.5-11.10
3.2.1.4.2.2.3	Y	Security Validation	3-43	3.7, II.9.3
3.2.1.4.2.2.4	Y	Format Conversion	3-43	9.0
3.2.1.4.2.2.5	Y	Media Conversion	3-43	7.0, 7.1
3.2.1.4.2.2.6	Y	Message Media Services	3-43	11.0, 11.1
3.2.1.4.2.2.6.1	Y	Distribution Identification	3-43	11.3
3.2.1.4.2.2.6.2	Y	Message Identification	3-43	12.2
3.2.1.4.2.2.6.3	Y	Editing	3-44	12.2
3.2.1.4.2.2.6.4	Y	Print Expansion of Reports	3-44	12.3
3.2.1.4.2.2.6.5	Y	Classification Display	3-44	II.27.9d
3.2.1.4.2.2.6.6	Y	Special Print Out Requirements	3-44	App. 12A
3.2.1.4.2.2.7	Y	Data Pattern Delivery Processing	3-44	12.1
3.2.1.4.2.2.7.1	Y	Data Pattern Delivery	3-45	12.1
3.2.1.4.2.2.7.2	Y	Data Pattern Sections	3-45	12.1
3.2.1.4.2.3	Y	Output RI Classmarking	3-45	II.6.1
3.2.1.5		Message Processing Control	3-46	Title Only
3.2.1.5.1	Y	Precedence Processing	3-46	4.0, II.4.3
3.2.1.5.2	Y	Message Preemption	3-46	5.0, 5.1, 5.2
3.2.1.5.3	Y	Automation Assisted Traffic Management	3-46	20.0
3.2.1.5.3.1	Y	Traffic Loading	3-47	16.3, 20.3
3.2.1.5.3.2	Y	Message Timing and Overdue Notification	3-47	3.2.b, 16.2, 27.3, 27.4
3.2.1.5.3.3	Y	Intercept Processing	3-48	4.0, 20.1,
3.2.1.5.4	Y	Overflow Protection	3-48	4.0, 18.0,
3.2.1.5.5	Y	Alternate Routing	3-48	22.0, II.22.0
3.2.1.5.6	Y	Queue Management	3-49	20.3, 27.1.e
3.2.1.5.7	Y	Automated Routing/Distribution File Maintenance	3-49	26.0
3.2.1.5.8	Y	Service Messages	3-49	19.0
3.2.1.5.8.1	Y	System Generated Service Messages	3-49	8.1, 19.1, 27.7, II.4.3, II.19.1
3.2.1.5.8.2	Y	Automated Processing of Service Messages	3-50	15.0, 19.2, 21.0
3.2.1.5.8.3	Y	Manual Processing of Service Messages	3-50	19.3, 25.0
3.2.1.6	Y	Accountability and Recordkeeping	3-50	3.2
3.2.1.6.1	Y	Message Accountability	3-50	3.2.a, 3.2.b, 3.9, 8.3
3.2.1.6.2	Y	History Logs and Files	3-51	8.0, 8.2, 27.1.d, II.8.1, II.27.9.b, App. 8A
3.2.1.6.2.1	Y Y	Incoming and Outgoing Journal Entries - System Status Information	3-51	3.2, 8.2, 16.3, 27.3, II.16.3
3.2.1.6.2.2	Y	Reference Entries	3-51	8.2, 8.3
3.2.1.6.3	Y	History Data Interrogation	3-54	20.2
3.2.1.7	Y	Message Search, Retrieval, Readdressal and Retransmission	3-54	8.1, 15.0, 21.0
3.2.1.7.1	Y	Message Data Search	3-54	16.1, 21.0, II.16.6

FRD	IOC	Title	Page	FSD
3.2.1.7.2	Y	Message Retrieval	3-54	19.2, 21.0, II.16.6
3.2.1.7.3	Y	Message Readdressal	3-59	15.1, 19.2
3.2.1.7.4	Y	Message Retransmission	3-59	15.2, 19.2, 27.4
3.2.1.8	Y	Automatic Formatting, Paging and Sectioning	3-60	*
3.2.2	Y	Message Editing and Preparation Service (MEPS)	3-60	24.0
3.2.2.1	Y	Automatic Supervision of Message Preparation	3-60	24.0
3.2.2.2	Y	Message Preparation Masks	3-61	25.0
3.2.2.3	Y	Message Editing and Review	3-61	24.0
3.2.2.3.1	Y	Line Identification for Editing	3-61	24.0
3.2.2.3.2	Y	Line Editing	3-61	24.0
3.2.2.3.3	Y	Character and Word Editing	3-61	24.0
3.2.2.3.4	Y	Copy Review	3-61	24.0
3.2.2.4	Y	Format Conversion and PLA to RI Assignment	3-62	9.0,13.0
3.2.3	Y	Service Management	3-62	1.0, III.29.0
3.2.3.1	Y	Terminal to FMS Connection	3-62	III.29.4
3.2.3.2	Y	Local FMS to Distant FMS	3-62	III.29.4
3.2.3.3	Y	Management Flexibility	3-62	III.29.0
Note - Page 65 intentionally left blank				
3.3		System Control	3-66	Title Only
3.3.1	Y	System Control Concept	3-66	16.0, II.28.0 III.29.1
3.3.1.1	Y	System Control Evolution	3-67	II.28.0, III.29.1
3.3.1.2	Y	Connectivity Requirements for System Control	3-67	II.27.7, III.29.1
3.3.2	Y	Sub-Network Management and Control	3-67	II.28.0
3.3.2.1	Y	Integrated AUTODIN System Control Process	3-67	II.28.0
3.3.2.1.1	Y	Crisis Management	3-68	27.1, 27.2, 27.7
3.3.2.1.2	Y	Network Modification Control	3-68	26.0

FRD	IOC	Title	Page	FSD
3.3.3	Y	Configuration Monitoring and Control	3-68	22.0, 27.2, II.27.7b
3.3.3.1	Y	Activations/Deactivations of Subscribers and Transmission Links	3-68	26.0, 27.2, II.27.7b
3.3.3.2	Y	Subscriber and DDN Access Line Reroute and Restoral	3-68	27.2, II.27.7b
3.3.3.3	Y	Network Configuration Engineering	3-69	16.0, II.28.0
3.3.4	Y	Traffic Flow and Routing Control	3-69	20.0, II.28.0
3.3.4.1	Y	Traffic Flow Control	3-69	18.0, 20.0, 20.1
3.3.4.2	Y	Routing Control	3-70	22.0
3.3.5	Y	Status Monitoring and Performance Assessment	3-70	16.3
3.3.5.1	Y	Status Monitoring	3-71	27.7, II.27.7
3.3.5.1.1		I-S/A AMPE Status Monitoring	3-71	Title Only
3.3.4.1.1.1	Y	Impairment/Outage Condition	3-71	27.7, II.27.7
3.3.5.1.1.2	Y	Equipment Status	3-71	27.7, II.27.7
3.3.5.1.1.3	Y	Hazardous Condition	3-71	27.7, II.27.7
3.3.5.1.2	Y	Subscriber and DDN Access Line Impairment/Outage	3-71	27.4, 27.7, II.27.7
3.3.5.1.3	Y	Equipment Status	3-72	27.7, II.27.7
3.3.5.1.4	Y	Subnetwork Status	3-72	16.0, 27.0, II.28.0
3.3.5.2	Y	Performance Assessment	3-72	16.0, 27.4
3.3.5.3	Y	Traffic Header Statistics	3-72	16.0, II.16.0
3.3.5.3.1	Y	Traffic Statistics Processing	3-72	16.1
3.3.5.3.1.1	Y	Total Traffic Volume	3-72	16.1
3.3.5.3.1.2	Y	Busy Period Traffic Volume	3-73	16.1, II.16.3
3.3.5.3.1.3	Y	Multiple Addressing Factor	3-73	*
3.3.5.3.2	Y	Speed of Service Data	3-73	II.28.1b(1)(b)
3.3.5.3.2.1	Y	Network Delay	3-73	II.28.1b(1)(b)
3.3.5.3.2.2	Y	SOS & Network Delay Matrix	3-73	II.28.1b(1)(b)
3.3.5.3.3	Y	Message Length	3-73	16.1
3.3.5.3.4	Y	I-S/A AMPE Load and Throughput Data	3-76	16.0
3.3.5.3.5	Y	Access Line Backlog Data	3-76	16.3, 27.4, II.16.3
3.3.6		Reporting	3-76	Title Only
3.3.6.1	Y	DCAC 310-55-1 Reporting	3-76	II.16.5
3.3.6.2	Y	MC Reporting	3-76	II.16.5, II.28.0
3.3.6.3	Y	Subscriber Reporting	3-76	16.3
3.3.6.4	Y	DCS Message Quality Control	3-77	II.16.5
3.3.7	Y	Fault Isolation and Correction	3-77	27.7, II.27.7
3.3.7.1	Y	Circuit Configuration Data Base	3-77	II.27.7
3.3.7.2	Y	Circuit Quality Monitor	3-78	27.7, II.27.7
3.3.7.3	Y	Remote Access to Circuit Segments	3-78	27.7

FRD	IOC	Title	Page	FSD
3.3.7.4	Y	Automatic Fault Isolation	3-78	27.7, II.27.7
3.3.7.5	Y	Semi-Automated Switching	3-78	27.7, II.27.7
3.3.7.5.1	Y	Red/Black Isolation	3-79	II.27.9.C
3.3.7.5.2	Y	Subscriber Community Separation	3-79	27.9.3
3.3.7.6	Y	Interface with Technical Control	3-79	II.27.7
3.3.8	Y	Billing Data	3-79	16.0, 16.1, 16.2
3.3.9	Y	I-S/A AMPE Internal Control	3-79	Title Only
3.3.9.1	Y	Operator Control Function	3-79	27.2
3.3.9.2	Y	Failure Recovery Management	3-80	27.1
3.3.9.2.1	Y	Automatic Recovery	3-81	27.1.a
3.3.9.2.2	Y	Manual Recovery	3-81	27.1.b
3.3.9.3	Y	Data Base Management	3-81	26.0
3.4		I-S/A AMPE Security	3-84	TITLE ONLY
3.4.1	Y	General	3-84	27.9, II.28.2
3.4.2	Y	DSSCS/GENSER Integration	3-84	27.9
3.4.3	Y	Security Certification	3-84	27.9, II.28.2
3.4.4	Y	Cryptographic Security	3-85	II.27.9c
3.5	Y	Performance Requirements	3-86	See 3.5.1 thru 3.5.6 Below
3.5.1	Y	Traffic Processing	3-86	III.29.0
3.5.1.1	Y	Formal Message Service Traffic Characteristics and Traffic Loads	3-86	II.28.1, III.29.0
3.5.1.1	Y	Input Traffic Processing Capability	3-86	II.28.1
3.5.1.2	Y	Output Traffic Processing Capability	3-91	II.28.1
3.5.1.2	Y	Throughput Processing Capability	3-91	II.28.1
3.5.1.3	Y	Traffic Processing Delays	3-91	II.28.1
3.5.1.3.1	Y	Formal Message Service Processing Delays	3-91	II.28.1
3.5.1.3.2	Y	Data Transactions to the IAS Network	3-92	II.28.1
3.5.2	Y	Connection Service	3-93	II.28.1b(1), III.29.4
3.5.3	Y	Storage Requirements	3-94	8.1, 13.0, 17.0, III.29.2
3.5.3.1	Y	Plain Language Address (PLA) to RI Table	3-94	13.0
3.5.3.2	Y	RI to Logical Address Table	3-94	III.29.2
3.5.3.3	Y	On-Line FMS Storage	3-94	8.1, 17.0
3.5.3.4	Y	Search and Retrieval Access Times	3-94	21.0
3.5.3.5	Y	General Storage Requirements	3-94	17.0
3.5.4	Y	Processing Error Rates	3-95	3.1, II.28.1b(1)(a)3

FRD	IOC	Title	Page	FSD
3.5.4.1	Y	Undetected Error Rate	3-95	3.1, II.28.1b(1)(a)3
3.5.5	Y	Availability	3-95	II.28.1b(1)(a)2
3.5.5.1	Y	Recovery	3-95	27.1
3.5.6	Y	Degraded Operation	3-96	27.1
3.6	Y	Requirements for Software and Firmware Development	3-97	II.28.1
3.6.1	Y	Modifications to MIL-STD-1679	3-97	II.28.1a(1)
3.6.2	Y	Software and Firmware Management	3-98	II.28.1a(1)
3.6.3	Y	Programming Requirements	3-99	II.28.1a(1)
3.6.4	Y	Documentation Requirements	3-99	II.28.1a(1)
3.7		Hardware System Requirements	3-100	Title Only
3.7.1	Y	Hardware Definition	3-100	27.4, 27.7, II.27.7, III.29.0
3.7.2	Y	Modularity	3-100	II.28.1a(2)
3.7.2.1	Y	Reliability Through Modularity	3-100	II.28.1a
3.7.2.2	Y	Sizing	3-100	17.0, II.28.1a
3.7.3	Y	Memory	3-101	17.0
3.7.3.1	Y	In-Transit Storage	3-101	17.0
3.7.3.2	Y	Message Storage for Retrieval	3-101	8.1, 21.0
3.7.3.3	Y	Memory Access	3-101	27.9.2
3.7.4	Y	Fault Isolation and Connection Capability	3-101	27.7, II.27.7
3.7.4.1	Y	Connection Capability	3-101	27.7, II.27.7
3.7.4.2	Y	Testing	3-102	27.7, II.27.7
3.7.4.3	Y	Reporting	3-102	16.4, II.16.5
3.7.5	Y	Operational Characteristics	3-102	See 3.7.6.1 thru 3.7.6.7 Below
3.7.5.1	Y	Availability	3-102	II.28.1b(1)(a)
3.7.5.2	Y	Reliability	3-103	27.1, 27.2
3.7.5.3	Y	Maintainability	3-103	II.28.1
3.7.5.4	Y	Interrupt Structure	3-103	27.9.2
3.7.5.5	Y	Instruction Set	3-103	*
3.7.5.6	Y	Instructions in Hardware	3-103	*
3.8		Design and Development	3-104	Title Only
3.8.1	Y	Modularity	3-104	II.28.1a
3.8.2	Y	Software Design	3-104	II.28.1a(1)
3.8.3	Y	Hardware Design	3-104	II.28.1a(2)
3.8.4	Y	Commonality/Standardization	3-104	*
3.8.5	Y	Human Performance/Human Engineering	3-105	*
3.9	Y	Maintainability and Logistics	3-105	*
3.9.1	Y	Maintenance	3-105	*
3.9.2	Y	Maintenance Concept	3-106	*
3.10	Y	Precedence	3-106	*
3.10.1	Y	Security	3-106	10.0
3.10.2	Y	Flexibility	3-106	II.28.1a(2)
3.10.3	Y	Performance	3-106	13.0, 14.0, 18.0, 19.0
3.11	Y	Government Furnished Property (GFP)	3-106	Title Only
3.11.1	Y	Design Assistance	3-106	*
3.11.2	Y	Hardware and Software	3-107	*

FRD	IOC	Title	Page	FSD
3.12	N/A	Pre-planned Product Improvement	3-107	
3.12.1	N/A	Pre-planned Product Improvement Implementation	3-107	*
3.12.2	P	Additional I-S/A AMPE Services	3-107	*
3.12.3	P	Data Path Requests	3-108	29.4b
3.12.4	P	Preamble Format	3-109	9.1
3.12.5	P	Routing Table Updates	3-109	*
3.12.6	P	DSSCS and GENSER Consolidation	3-109	10.0
3.13		Training	3-109	*
4.0	Y	QUALITY ASSURANCE PROVISIONS	4-1	*
4.1	Y	Contractor Configuration/Development Reviews	4-1	*
4.1.1	Y	Configuration Management	4-1	*
4.1.1.1	Y	Configuration Management Baselines	4-2	*
4.1.1.2	Y	Engineering Change Proposals	4-2	*
4.2	Y	Contractor Validation Testing	4-2	II.28.2
4.2.1	Y	Software Testing	4-2	*
4.2.2	Y	Electromagnetic Testing Requirements	4-3	II.27.9a, II.28.1b(2)
4.3	Y	Acceptance Testing	4-3	II.28.2
4.3.1	Y	Site Testing	4-3	*
4.3.2	Y	System Testing	4-4	*
4.3.3	Y	Government Testing	4-5	*
4.4	Y	Test Documentation	4-5	II.28.2
4.4.1	Y	Test Program Outline/Plan	4-5	*
4.4.2	Y	Test Plans and Procedures	4-5	*
4.5	Y	Responsibilities for Contractor Conducted Testing	4-5	Title Only
4.5.1	Y	Contractor Test Procedures	4-5	*
4.5.2	Y	Government Responsibilities	4-6	*
4.6	Y	Equipment	4-6	II.28.2
4.7		Quality Assurance Provisions - Security Design	4-6	Title Only
10.0	Y	DEFINITIONS AND TERMINOLOGY	10-1	
11.0		COMPUTER SECURITY GLOSSARY	11-1	
20.0	Y	I-S/A AMPE MESSAGE FORMAT VALIDATION	20-1	App. 3B
21.0	Y	Service Message Appendix	21-1	App 19B,II.19B
30.0	Y	SECURITY APPENDIX	30-1	
40.0	Y	DESCRIPTION OF SNAPS BASIC DATA AUTODIN TRAFFIC	40-1	
50.0	Y	STATISTICS AND REPORT GENERATION CRITERIA	50-1	App. 16A

Interface Control Document
(ICD)

To

Functional Statement document
(FSD)

I-S/A AMPE ICD Cross Referenced to FSD

ICD	IOC	Title	Page	FSD
1.0	Y	INTRODUCTION	1-1	Title Only
1.1	Y	Scope	1-1	*
1.2	Y	Standard Definitions and Terminology	1-1	*
2.0		APPLICABLE DOCUMENTS	2-1	Title Only
2.1	Y	Military and Federal Standards	2-1	*
2.2	Y	Joint/Allied Communication Publications	2-1	*
2.3	Y	Service/Agency Telecommunications Instructions and Procedures	2-2	*
2.4	Y	Industry Specifications, Instructions and Manuals	2-2	*
2.5	Y	References	2-3	*
3.0	Y	PHYSICAL CHARACTERISTICS	3-1	Title Only
3.1	Y	Operator System Layout	3-1	*
3.2	Y	Health and Safety Criteria	3-1	*
3.3	Y	Environmental Conditions	3-1	Title Only
3.3.1	Y	Operating Temperature and Humidity	3-1	*
3.3.2	Y	Non-Operating Temperature and Humidity	3-1	*
3.3.3	Y	Noise	3-1	*
3.3.4	Y	Vibration	3-1	*
3.4	Y	Physical Criteria	3-2	Title Only
3.4.1	Y	Size	3-2	*
3.4.2	Y	Weight	3-2	*
3.4.3	Y	Maintenance Access	3-2	*
3.5	Y	Electromagnetic Interference/Compatibility (EMI/EMC)	3-2	II.28.1 b (2)
3.6	Y	TEMPEST	3-2	II.27.9 a
3.7	Y	Electrical Grounding	3-2	*
3.8	Y	Power Requirements	3-3	*
3.9	Y	HEMP Protection	3-3	*
4.0	Y	PROTOCOLS AND FORMATS	4-1	Title Only
4.1	Y	Protocols Hierarchical Layers	4-1	III.29.1
4.2	Y	Protocols	4-3	See 4.2.1 thru 4.2.6 Below
4.2.1	Y	Physical Layer	4-3	III.29.1, II.1.1
4.2.2	Y	Link Layer	4-3	Title Only

Y-required for IOC
P-required for post IOC
*-not addressed in FSD

ICD	IOC	Title	Page	FSD
4.2.2.1	Y	IAS Standard Link Protocols	4-3	Title Only
	Y	a. DCS Mode I	4-3	1.0
		b. DCS Mode IB	4-5	1.0,App 1H
Y	Y	c. DCS Mode II	4-5	1.0
	Y	d. DCS Mode V	4-5	1.0
	P	e. ADCCP	4-5	*
	Y	f. CCITT X.25	4-6	III.29.1a
4.2.2.2	Y	User Unique Link Protocols	4-6	See a. thru k. Below
	Y	a. Army AMME-MART Interface Requirements (A.K.A DCA Mode I Modified for SRT)	4-6	1.0,App. 1A
	Y	b. Army IRT Interface Requirements (A.K.A. DCA Mode I Modified for IRT)	4-6	1.0,App. 1B
	Y	c. Army DPI Interface Requirements	4-6	1.0,App. 1C
	Y	d. Navy DCT 2000 Data Communications Terminal Interface	4-6	1.0
	Y	e. Shore Station Message Processing Set (SSMPS) (Formally MRDIS)	4-6	1.0 App. 1E
	Y	f. Navy Remote Information Exchange Terminal (RIXT)	4-6	1.0,App. 1D
	Y	g. NMCS - NACE Protocol for Remote Computer Interface (A.K.A. WWMCCS NATS/NACE)	4-7	1.0,App. 1I
	Y	h. WWMCCS DINDAC	4-7	1.0,App. 1K
	Y	i. WWMCCS - RTOS	4-7	1.0,App. 1J
4.2.3	Y	Network Layer - CCITT X.25	4-7	III.29.1
4.2.4	Y	Internet Layer - Internet Protocol (IP)	4-8	III.29.1, II.12.4
4.2.5	Y Y	Transport Layer - Transmission Control Protocol (TCP)	4-8	III.29.1, II.12.4
4.2.6		Utility Layer	4-8	Title Only
4.2.6.1	P	Terminal-to-Host Protocol (THP)	4-8	III.29.1
4.2.6.2	Y	Formal Message Protocol (FMP)	4-8	III.29.1
4.3	Y	Formats	4-9	See 4.3.1 thru 4.3.6 Below
4.3.1	Y	DD Form 173	4-9	9.0
4.3.2	Y	Modified ACP-126 (NTP 4)	4-9	3.3, 9.0 App. 9B
4.3.3	Y	ACP-127	4-9	3.3, 9.0

ICD	IOC	Title	Page	FSD
4.3.4	Y	DOI-103	4-9	See a thru d Below
	Y	a. DOI-103	4-10	3.3, 9.0
	Y	b. DOI-103 Special	4-10	9.0
	Y	c. Abbreviated SI	4-10	9.0,App. 9A
	Y	d. Critic	4-9	3.3, 9.0
4.3.5	Y	JANAP-128	4-10	3.3, 9.0
4.3.6	P	Preamble Format	4-10	9.0
4.4	Y	Line Codes	4-10	2.0
5.0	Y	COMMUNICATION INTERFACES	5-1	II.12.5
5.1		Subscriber Interfaces	5-1	Title Only
5.1.1	Y	General Subscriber Terminal Interfaces	5-1	1.0, II.9.3, 9.0
5.1.2	Y	Specific Subscriber Interfaces	5-1	See 5.1.2.1 and 5.1.2.2 Below
5.1.2.1	Y	US Subscriber Interfaces	5-1	Title Only
5.1.2.1.1	Y	ASC Transitional/I-S/A AMPE Contingency Interface	5-1	1.0. II.1.1, 9.0, 27.8, II.27.8
5.1.2.1.2	Y	Tactical Interfaces	5-1	1.0, II.1.3, 9.0
5.1.2.1.3	Y	General Services Administration (GSA) Interface	5-1	1.0, II.9.3, 9.0
5.1.2.1.4	Y	WWMCCS Interface	5-2	1.0 App. 1I, App. 1J, App. 1K
5.1.2.2		Allied Subscriber Interfaces	5-2	Title Only
5.1.2.2.1	Y	NATO (NICS TARE) Interface	5-2	1.0, II.28.3, 9.0
5.1.2.2.2	Y	Allied Subscriber Formats	5-2	1.0, II.9.3, 9.0
5.1.2.2.3	Y	Australia/New Zealand Interface	5-2	1.0, II.9.3, 9.0
5.1.3	Y	Linked Channels	5-2	II.12.5
5.2	Y	Network Interface	5-3	III.29.0
5.3	Y	AUTOVON Interface	5-3	II.27.7b
6.0	Y	HUMAN INTERFACES	6-1	*
6.1	Y	Human Engineering Design	6-1	*
6.2	Y	Interaction	6-2	*
6.3	Y	Safety	6-2	*
6.4	Y	Maintainability	6-2	*
6.4.1	Y	Special Tools	6-2	*
6.4.2	Y	Modular Replacement	6-2	*
7.0	Y	Security Context	7-1	27.9.1, II.28.2

ICD	IOC	Title	Page	FSD
7.1		Functional Requirements	7-1	See 7.1.1 thru 7.1.3 Below
7.1.1	Y	Protection from Unauthorized Disclosure or Compromise of Information	7-1	27.9.2, II.28.2
7.1.2	Y	Protection from Denial of Authorized Service to Authorized Users or Subscribers	7-1	27.9.2, II.28.2
7.1.3	Y	Protection from the Undetected Unauthorized Alteration of Information Entrusted to the System	7-1	27.9.2, II.28.2
7.2	Y	Network Connection	7-1	27.9.4, II.27.9c, II.28.2
7.3	Y	I-S/A AMPE Design	7-2	27.9.3, II.28.2
7.4	Y	Terminal Data	7-2	27.9.1, II.28.2
Appendices				Appendices
B	Y	AMPE - MART		1 A
C	Y	IRT Interface		1 B
D	Y	DPI Interface		1 C
E	Y	SSMPS		1 E
F	Y	NACE		1 I
G	Y	RTOS		1 J

END

DTIC

7-86