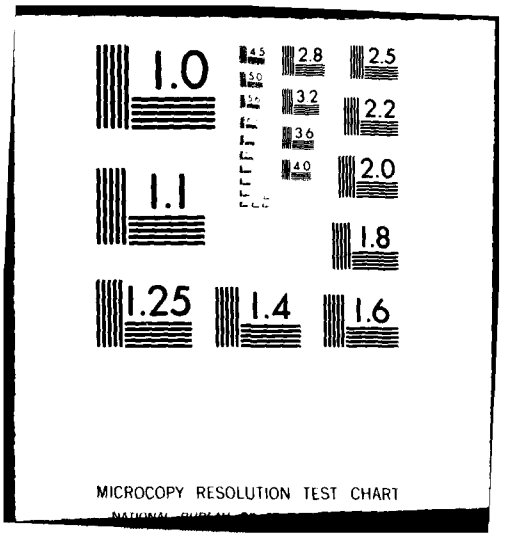
AD-A090 363 ARMY ELECTRONIC PROVING GROUND FORT HUACHUCA AZ F/G 17/2
TESTING OF THE ARMY'S INTEROPERATING NETWORK OF TACTICAL C3I SY--ETC(U)
JUN 80 G H BANISTER

UNCLASSIFIED NL

END
DATE FILMED
11-80
DTIC


1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.5
2.8
3.2
3.6
4.0
4.5
5.0
MICROCOPY RESOLUTION TEST CHART

TESTING OF THE ARMY'S INTEROPERATING NETWORK OF TACTICAL C^{3}I SYSTEMS

10 GRADY H. BANISTER, MR.
US ARMY ELECTRONIC PROVING GROUND
FORT HUACHUCA, ARIZONA 85613

INTRODUCTION

The Army has embarked upon a coordinated program to develop and field a collection of automated command control, communications, and intelligence (C^{3}I) systems to provide the effective battle management that is required if we are to overcome the numerical superiority of the Soviet Block. The Army Battlefield Interface Concept 1979 (1) describes the basic architecture for integrating these systems into a functional and interoperating network. The purpose of this paper is to discuss some of the voids in current information science technology as it relates to the testing of individual systems and the network to insure that each system and the network will properly perform their functions under the stress of combat. To fully appreciate the technical nature of the problems anticipated in testing this network, let us examine three major aspects of the situation.

(1) The nature and size of the network
(2) The environment in which the network must function
(3) The purpose of and information required from the test.

THE NETWORK

The network will be composed of numerous automated systems and subsystems which can be grouped into five basic functional areas: (1) Administrative and Logistics, (2) Intelligence and Electronic Warfare, (3) Field Artillery, (4) Air Defense, and (5) Command and Control.

There is, in fact, a sixth area required to complete the

network -- the communications system. Each of these areas may be composed of various systems and subsystems (see Fig. 1). For example, the field artillery area consists of TACFIRE (Tactical Fire Direction System), BCS (Battery Computer System), FAMAS (Field Artillery Meteorological Acquisition System), RPV (Remotely Piloted Vehicle,) FIRE-FINDER (Artillery and Mortar Locating Radar), plus other support systems. These systems, in some cases, are a subnetwork; for example, TACFIRE consists of processing centers or nodes at Corps, Division, and Battalion level, with terminals at various locations from the forward observers to the Corps Headquarters.

The Army tactical C^3I network must also interconnect and interoperate with the other services as well as our allies. Thus, there is a super network even before we consider the theater or national level interfaces. To assist in visualizing the size of the Army tactical C^3I network, a Corps with four Divisions may have in excess of 200 processing nodes, and this does not include communications nodes. The communications support to this network will consist of various data transmission media, from dedicated point-to-point wideband circuits provided by multichannel systems, to dial-up voice grade data circuits, to combat net radios (shared with voice traffic), to time division multiple access systems.

A very significant aspect of this network is that it is evolving with time. Each system or subsystem is being developed and tested on its own schedule and may or may not be available at a specific time so that its interface with another system can be tested. For example, TACFIRE is in production now but its interfaces with other field artillery systems could not be tested prior to the production decision because the other systems were not available and some will not be available for at least another three or four years. In addition, the communications system which the processing systems will depend on for communications is also changing during the same time frame that these systems are being introduced.

THE ENVIRONMENT

The Army tactical C^3I network must survive and provide the capability to continue to function in spite of the environment of the battlefield. Three aspects of the environment must be considered: (1) physical, (2) communications/traffic stability, and (3) radio electronic combat.

The physical environment includes shock and vibration and the physical damage, destruction, or capture of portions of the network by enemy action in addition to the disruption and reconfiguration of the network due to the movement and relocation of nodes. The

(212)

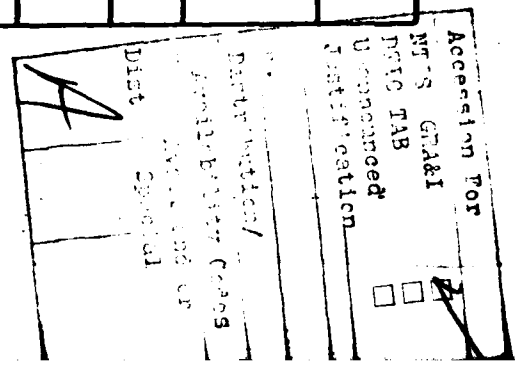
(213)

BATTLEFIELD AUTOMATED SYSTEM CATEGORIZATION

BATTLEFIELD FUNCTIONAL SYSTEM / SYSTEM LIFE CYCLE STATUS	ADMIN AND LOG		INTEL AND EW		FA	ADA	C^2	COMMO	ENGR
CATEGORY I CONCEPT/ DEFINITION	(MEDMIS) MEDREG* PAR* MEDLOG* WHOLE BLOOD MGMT* JACS*		ELOCARS HAALS RAWS ASAS ATRN AMS* REMBASS	U/E ECM	APPS II FAMAS BSTAR		CTOS	PACKET RADIO JTIDS MSE ADDS SDA(DLOED) CEOI PROD FACILITY ATFES	ARTINS+
CATEGORY II VALIDATION/ DEVELOPMENT	(CS3) TUFMIS	DAS3 DS4 SAMS SAAS	AGTELIS SOTAS TACELIS ENHANCED GUARDRAIL TEP	MULTEWS-A QUICK FIX TACJAM CAS ECM	TPQ-36 TPQ-37 APPS-PIP (PHOTO-LOCATOR) PADS BCS RPV	CCS	DTOS NBDS	TTC-39 TYC-39 TCCF PLRS GPS TEMLY/ SEELY	
CATEGORY III APPROVED PRODUCTION/ INSTALLATION	STANFINS** (CS3) SIDPERS	NCR 500 SAILS (CS3) DLOGS MMM	MAGIIC QUICKLOOK II TRAILBLAZER COMFAC GUARDRAIL V INTERIM SLAR DATA LINK		TACFIRE	TSQ-73			

*SOFTWARE ONLY - NO HARDWARE IDENTIFIED
**OPERATES IN CORPS (EUROPE) DURING PEACETIME ONLY
+EAC - BAND WILL TRACK DEVELOPMENT

Figure 1



communication/traffic stability aspects of the environment include the effects of the physical environment on the data flow between nodes that may cause rerouting of messages, reallocation of circuits, and create dynamically varying workloads at the processing nodes. The effects of enemy radio electronic combat may reduce the quality of existing circuits, deny us the use of circuits, and introduce confusion by injecting false messages into our communications system. In addition, the network must be secure so that information being exchanged is not available to the enemy and he cannot exploit the network even with captured equipment.

THE TEST

The testing of automated C^3I systems must be designed to completely exercise all functions of the item under test, stress the system in accordance with the environment, determine the system's ability to protect itself and the network from hostile activities, and insure that it will continue to function in an error prone communications environment. With the introduction of each new or modified system, the test must also determine what is the impact on the network and the other processing nodes. While doing all of the above, the testing procedure must provide a high degree of repeatability as to the content (including error cases) and timing of the stimuli presented to the system under test to aid the developer in the diagnosis of failures and the validation of corrections. The tests must also be designed so that all of the network is not required to test a single node. It may not be possible to collect and operate the entire network except during major exercises and actual combat.

AN APPROACH

USAEPG has developed a concept for testing automated C^3I systems which has the potential to solve a large part of the test community's problems. This concept is embodied in a program to provide USAEPG with an advanced test capability covering all phases of USAEPG's test mission. Emphasis is on the application of automation and simulation technology to meet the challenge of complete systems performance and interoperability testing of automated C^3I systems. This overall program is called MAINSITE which is the acronym for Modular Automated Integrated Systems/Interoperability Test and Evaluation (Fig. 2). The MAINSITE concept has evolved from earlier efforts by the Army Security Agency Test and Evaluation Center and Program Manager, Army Tactical Data Systems, to solve portions of the overall testing problem. USAEPG has combined and extended these earlier concepts and now is in the process of implementing them.

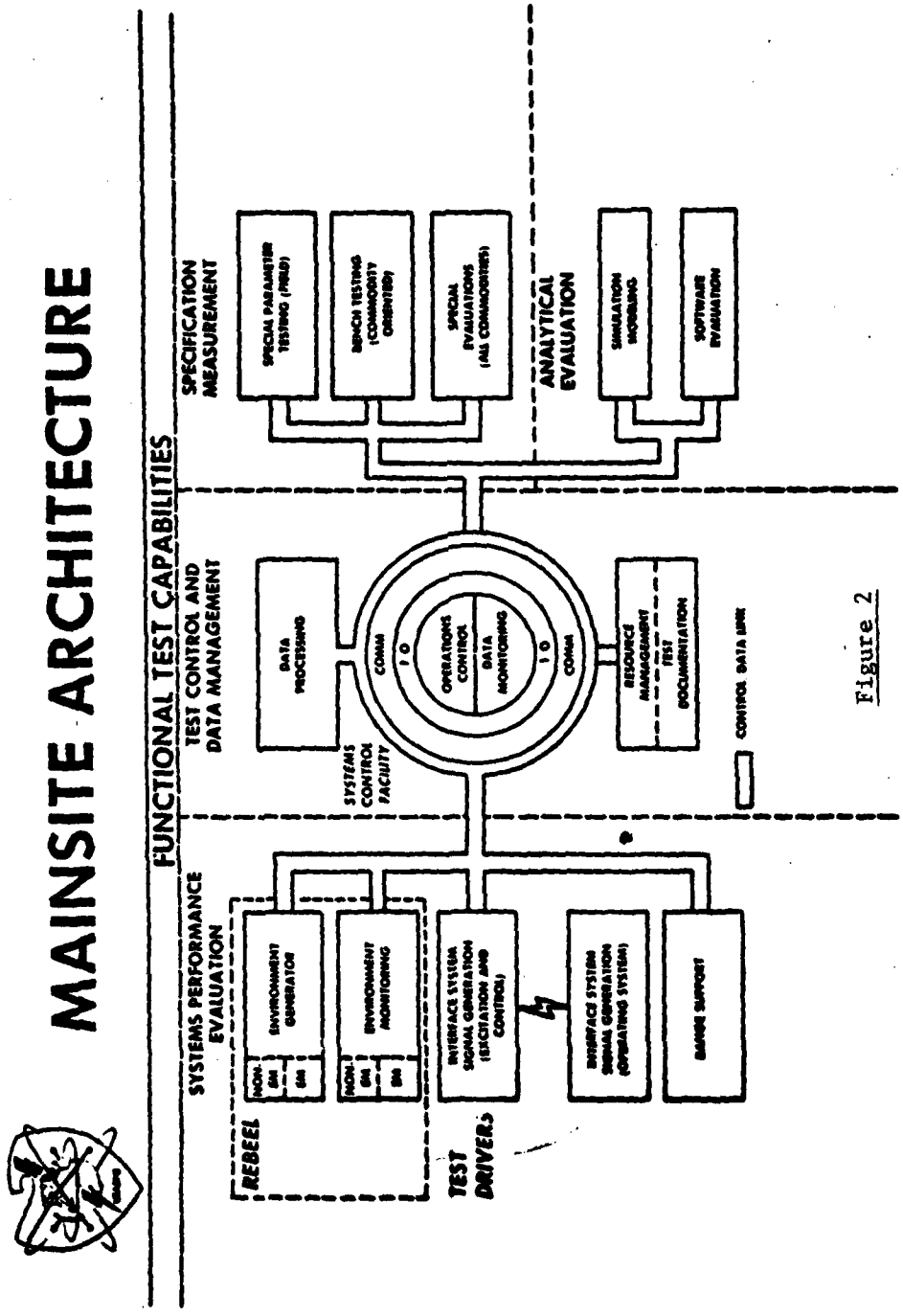

MAINSITE ARCHITECTURE
FUNCTIONAL TEST CAPABILITIES
SYSTEMS PERFORMANCE EVALUATION
TEST CONTROL AND DATA MANAGEMENT
SPECIFICATION MEASUREMENT
ANALYTICAL EVALUATION
SPECIAL PARAMETER TESTING (FIELD)
BENCH TESTING (COMMODITY ORIENTED)
SPECIAL EVALUATIONS (ALL COMMODITIES)
SIMULATION MODELING
SOFTWARE EVALUATION
DATA PROCESSING
SYSTEMS CONTROL FACILITY
COMM
I/O
OPERATIONS CONTROL
DATA MONITORING
RESOURCE MANAGEMENT
TEST DOCUMENTATION
CONTROL DATA LINK
ENVIRONMENT GENERATOR
ENVIRONMENT MONITORING
INTERFACE SYSTEM SIGNAL GENERATION (EXCITATION AND CONTROL)
INTERFACE SYSTEM SIGNAL GENERATION (OPERATING SYSTEM)
BARGE SUPPORT
REBEL
TEST DRIVERS

Figure 2

(215)

The key elements of the USAEPG approach are:

(1) Automated presentation of stimuli (messages) to the system under test.

(2) Automated control of the electromagnetic environment around the system.

(3) A flexible, modular design approach applicable to the testing of all C^3I systems.

(4) Transportability of the basic elements to permit use at other locations as required.

(5) Central control to extend the capability when required.

THE CONCEPT OF TEST

The Concept of Test which has established the capability requirements for the MAINSITE program is based on subjecting the system to three progressively more difficult phases of testing. These phases are:

(1) Test the System Logic

(a) Single Thread -- Each function is tested independently of other functions to provide control of the relationships of responses to stimuli to include error conditions (Step 1).

(b) Multithread -- All functions are tested in combination to the maximum practical extent to expose negative effects of synergism and interaction (Step 2).

(2) Test the System Capacity

(a) Required Load -- Loading of the system up to the stated requirements to determine performance versus requirement (Step 3).

(b) Saturation Load -- Multithread load is increased to systematically saturate system resources so that throughput, response time, and degradation effects may be determined (Step 4).

(216)

(3) Test the System in a Realistic Communications Environment

(a) Without Radio Electronic Combat -- Communications by automated systems over less than optimal communications channels requires additional processing and the retransmission of digital messages, both of which adversely affect system timing (Step 5).

(b) With Radio Electronic Combat -- Step 5 is repeated but in the degrading EM environment produced by threat radio electronic combat to insure that the system and network are capable of surviving despite disrupted communications (Step 6).

It should be noted that phases 1 and 2 are conducted with error free communications and therefore provide a baseline for evaluating the effect of the real world communications on system performance.

The System Control Facility, the Realistic Battlefield Environment-Electronic, and the Test Driver portions of the MAINSITE program are essential to this concept of test.

THE SYSTEM CONTROL FACILITY (SCF)

The SCF is the USAEPG real time test control and data management facility consisting of a large central computation center, test operations control centers, and communications to the mobile remote test facilities. In addition to providing real time control to multiple test facilities, the SCF will be capable of simulating on a real time dynamic basis the responses of other systems not physically present for a test.

THE REALISTIC BATTLEFIELD ENVIRONMENT - ELECTRONIC (REBEEL)

The REBEEL is a collection of mobile simulators, replicas, and actual emitters which create a controlled electronic environment to represent the radio electronic combat threat, targets for our electronic sensor systems and the electronic environment representing friendly emitters. The REBEEL will be automatically controllable from the SCF permitting rapid, repeatable execution of complex test conditions. Wherever possible the emitter simulators will be designed to permit preprogrammed sequences of operations to be executed without dependence on the SCF for use at locations other than Fort Huachuca.

THE TEST DRIVER

Each Test Driver (Fig. 3) will consist of a rugged minicomputer with sufficient storage for messages (stimuli) to be trans-

(217)

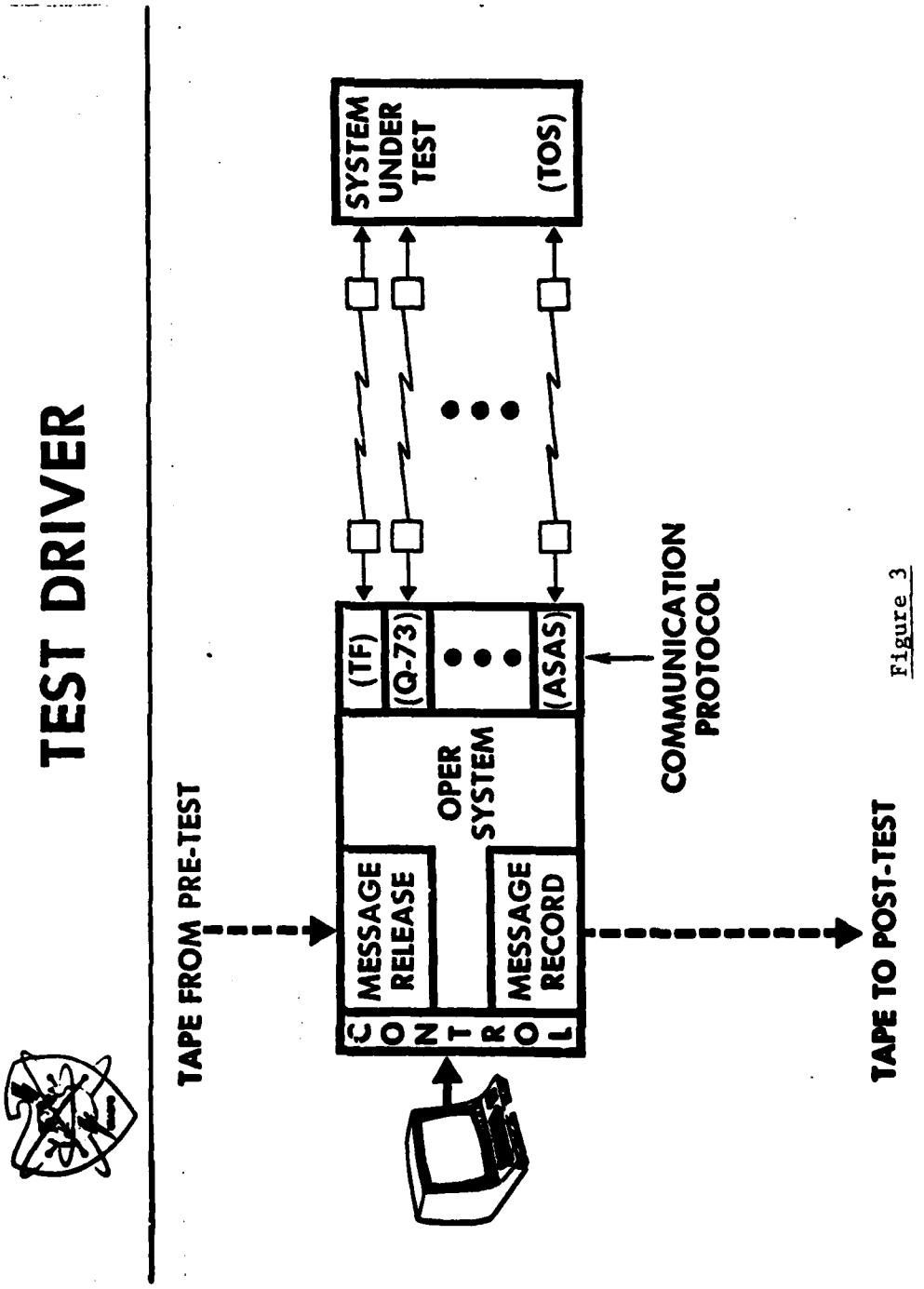

TEST DRIVER
TAPE FROM PRE-TEST
CONTROL
MESSAGE RELEASE
OPER SYSTEM
MESSAGE RECORD
(TF)
(Q-73)
(ASAS)
COMMUNICATION PROTOCOL
SYSTEM UNDER TEST
(TOS)
TAPE TO POST-TEST

Figure 3

(218)

mitted and the recording of all traffic across the interface. Facilities for both remote and local test monitoring and control as well as a communications interface with the SCF will be included.

The Test Driver will automatically transmit digital messages over the communications channels to the system under test, receive messages transmitted by the system under test, and record all exchanges over the communications system. It will utilize pre-prepared tapes of messages representing the stimuli to the system under test from those elements of the network which interface with the system under test but are not physically present. It will utilize the same communications channels, protocol, and encryption devices as the missing systems to provide as realistic a communication interface as possible. A single Test Driver may have to represent a number of missing systems (Fig. 4); therefore, it must be capable of handling multiple communications channels, various data rates and protocols. The Test Drivers will be capable of being controlled from the SCF or of operating in a stand-alone mode. Multiple Test Drivers, controlled by the SCF, will be utilized when the test requirements exceed the capacity of a single Test Driver. The Test Drivers will be transportable to provide realistic communication distances and to facilitate their use at other locations.

THE TECHNICAL PROBLEMS

The planning for the MAINSITE test capability described above has drawn heavily on experience gained during the testing of individual real time systems. This approach provides assurance that the lessons learned in solving prior testing problems will be applied to the development of future capability, but it does not guarantee adequate solutions to problems yet to be encountered. Thus the motive for this paper -- to attempt to identify any new testing problems which can be anticipated and to generate interest in the information science community on developing effective solutions.

UNANTICIPATED DATA CONDITIONS

The vast majority of the literature on testing of automated systems concentrates on proving that the system correctly processes the expected inputs. There are even automated techniques to trace the execution of computer problems to help identify all portions of the logic exercised by the test cases. (2) A good specification will identify some of the potential error conditions and state what the program should do when these errors occur. However, there has been little, if any, effort in identifying the potential sources of errors in data inputs, determining the types of errors, and developing the

TEST CONCEPT

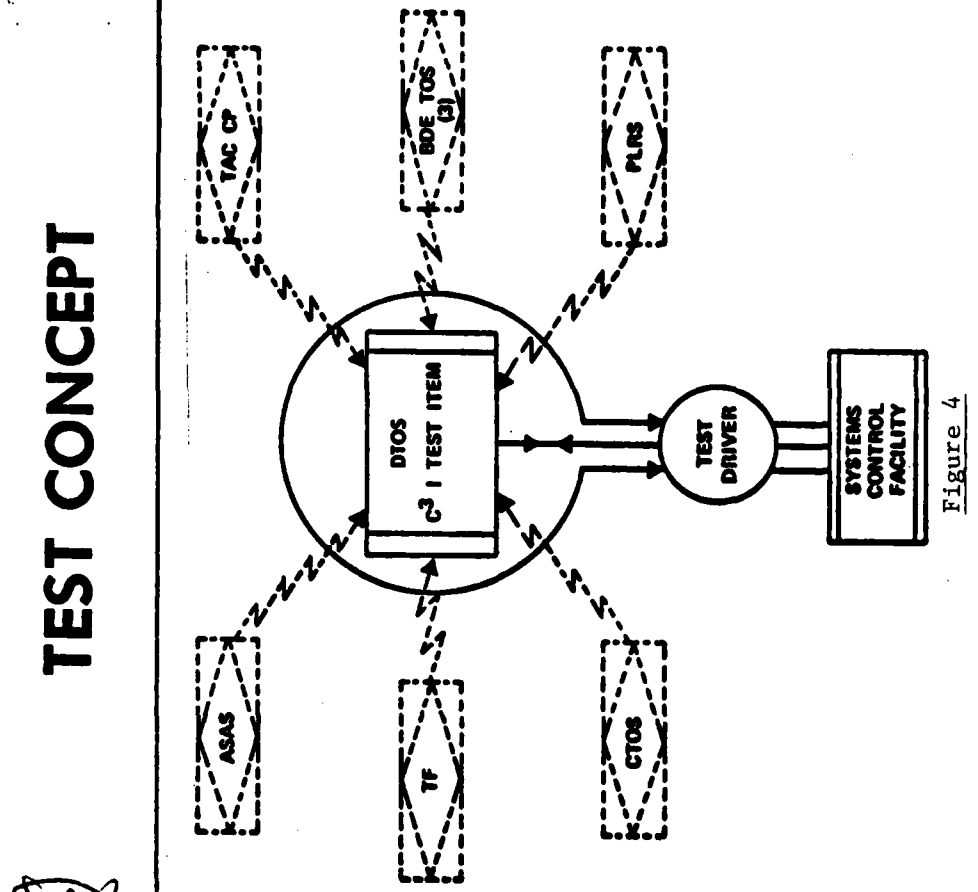


Figure 4

220

methodology required to generate and present an adequate set of input errors to the system under test.

It is very difficult, if not impractical, to construct a complete set of expected valid inputs for testing large programs but they are at least a finite set. The error conditions represent the remainder of the universe of possible data inputs and are for all practical purposes an infinite set. In the large network environment the original source of an error may be far removed from the system that detects it; for example, an operator at a terminal connected to system "A" (see Fig. 5) may compose a message containing an error in a specific data element (field). System "A" may process the message and generate a new message for system "C" which is relayed through system "B" containing the erroneous data element. The error may not be detected until system "C" attempts to utilize the erroneous data element.

Techniques need to be developed to provide methods to identify all sources of possible errors, determine the characteristics of the errors, quantify the probability of occurrence, and generate test cases which will realistically test the network and its individual systems. An effort to analyze the error sources in a small portion of the network shown in Fig. 5 has been initiated at USAEPG to gain an insight into the complexity and magnitude of the problem.

NETWORK DYNAMICS

Unfortunately the Army's C^3I systems are evolving into an integrated network rather than having a network designed and specified into which each system must fit. It is only natural for the developer of a specific system to consider his system as the center of the universe and when confronted with the task of testing a system, the tester also considers the system under test as the center of his universe. This introspective perception of the testing task leads to a false sense of security since testing is easier if you bound the scope of the test even though major errors of omission may be committed. The real world situation is that the effect of the network on the system under test, as well as the effect of the system under test on the network, must both be tested. This interdependency is much more complex than most designers and testers realize. Let me describe a few examples of the types of network versus system relationships which must function correctly for both the system and the network to perform properly.

It is generally accepted that there must be a well defined set of messages, to include format and data elements, for information

(221)

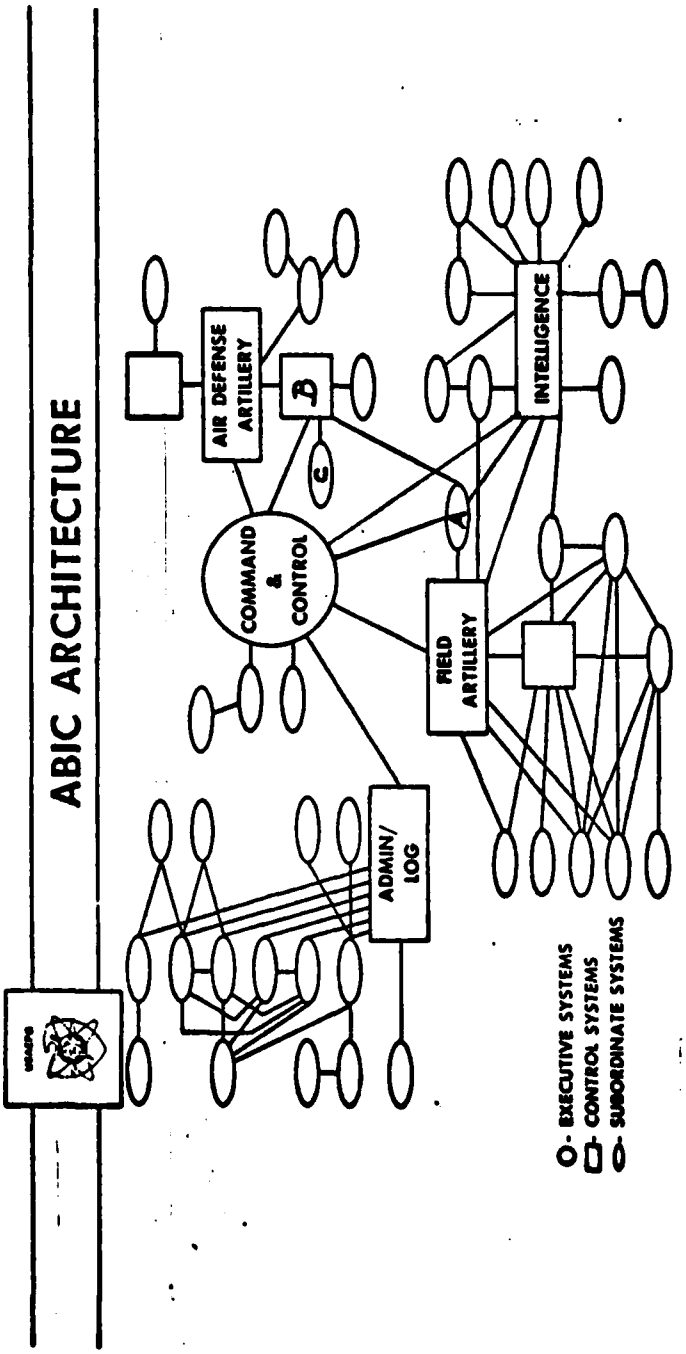

ABIC ARCHITECTURE
AIR DEFENSE ARTILLERY
B
C
INTELLIGENCE
COMMAND & CONTROL
FIELD ARTILLERY
ADMIN/ LOG
EXECUTIVE SYSTEMS
CONTROL SYSTEMS
SUBORDINATE SYSTEMS

Figure 5

(222)

exchange between interoperating members of a network. However, many of the benefits of automating the Army C^3I functions are dependent on rapid allocation of resources to solve problems. Examples are messages which task or command an air defense fire unit to engage a hostile aircraft, command a jammer to jam a specific frequency, command an artillery unit to fire a specific mission, or command a unit to execute a specific action. Thus the network is a military process control system which requires that each of the subsystems which control a part of the process provide feedback as to the status of their part of the process. A well understood principle in the design and testing of on-line process control systems is that the timing and nature of the feedback must be such that oscillations or "hunting" does not occur and that the network converges to a steady state condition. This requires that the processing of the messages which command a system to perform a task must produce the results and/or feedback (messages) which are well defined and utilized by the network to control the overall process. This aspect of the Army's C^3I network has not been defined much less tested. The use of the Test Driver with appropriate messages will permit testing of a system to determine if it responds correctly to such messages and performs the required actions to include providing the correct feedback. However, this will not necessarily prove that the processing of the feedback by the rest of the network and the time constraints involved are correct and will prevent oscillations.

In addition, there are very complex dynamic problems associated with the control of the network and its communications which also need to be tested. The Army C^3I network creates some unique network control problems. The overall network is constantly evolving by the addition of new processing nodes, the modification of existing nodes, and the changing of the type of communications between nodes. The network will not be maintained in an operational status for long periods of time except during combat. During periods of combat, the network will be changing on a very dynamic basis due to movement of forces, combat losses of communications and nodes, and the functions of individual processing nodes will change to accommodate the essential functions of inoperative nodes. All of the above presents a real challenge to both the designer of a system and the tester.

How do you generate the data and communications environment around the system under test to measure its ability to respond correctly to such a changing environment, and how do you determine the effect on the network of the systems responses when the network is physically not available? I do not have the answer to these quentions today. I do anticipate that by utilizing the processing facilities

(223)

of the SCF to simulate the network control logic, when it is defined, we will be able to at least quantify individual systems response times and predict network stability under this type of dynamic stress.

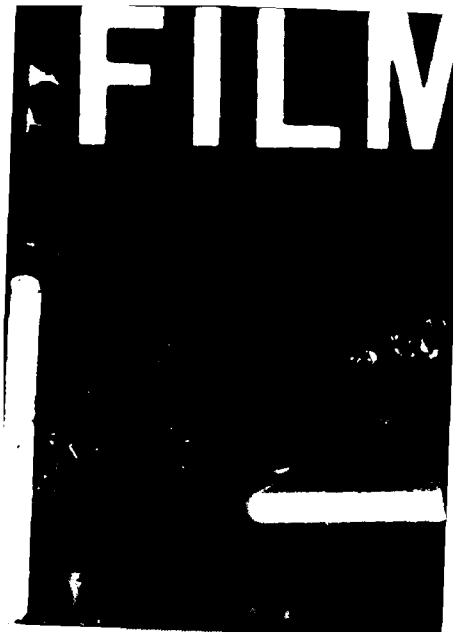
CONCLUSION

There are many problems in the design and testing of large scale distributed processing networks which are not well understood today. The purpose of performing the tests discussed is twofold; first, to find and eliminate as many errors in the system and network design as possible and, second, to assist the designers in developing the most robust, adaptive, distributed C^3I system design possible. The implementation of MAINSITE will provide a powerful tool which, if used properly, should provide significant advances in our ability to implement the Army C^3I network.

REFERENCES

1. (U) "Army Battlefield Interface Concept 1979" (U) CONFIDENTIAL Department of the Army, ACN 47635.

2. MYERS, G. J., Software Reliability, New York, John Wiley & Sons, 1976.


FILM