AD NUMBER
ADB010431
LIMITATION CHANGES
TO: **Approved for public release; distribution is unlimited.**
FROM: **Distribution authorized to U.S. Gov't. agencies only; Test and Evaluation; 19 MAR 1976. Other requests shall be referred to Air Weather Service, Attn: CSE, Scott AFB, IL 62225.**
AUTHORITY
AWS ltr, 8 Jul 1976

(18) SAMSO (19) TR-76-88

SDC-TM-(L)-5613/005/01

(6) AIR FORCE GLOBAL WEATHER CENTRAL
SYSTEM ARCHITECTURE STUDY.

FINAL SYSTEM/SUBSYSTEM SUMMARY REPORT.

VOLUME 5.

SYSTEM DESCRIPTION.

SYSTEM DEVELOPMENT CORPORATION
2500 Colorado Avenue
Santa Monica, California 90406

(11) 1 Mar[redacted]76 (12) 128p.

(9) Final Report [redacted] 1 Feb[redacted]75 — 1 Mar[redacted]76.

Distribution Statement

Distribution limited to U.S. Government Agencies only. Other requests for this document must be referred to Air Weather Service/CSE, Scott Air Force Base, Illinois, 62225.

(15) F04701-75-C-0114

Prepared for:

DEPUTY FOR DEFENSE METEOROLOGICAL SATELLITE PROGRAM OFFICE
H.Q. SPACE & MISSILE SYSTEMS ORGANIZATION
AIR FORCE SYSTEMS COMMAND
LOS ANGELES, CALIFORNIA 90009

339 900

Unclassified

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE

READ INSTRUCTIONS BEFORE COMPLETING FORM

1. REPORT NUMBER: TM-(L)-5613/005/01
2. GOVT ACCESSION NO.:
3. RECIPIENT'S CATALOG NUMBER:
4. TITLE (and Subtitle): AIR FORCE GLOBAL WEATHER CENTRAL SYSTEM ARCHITECTURE STUDY, FINAL SYSTEM/SUBSYSTEM SUMMARY REPORT, VOLUME 5 - SYSTEM DESCRIPTION
5. TYPE OF REPORT & PERIOD COVERED: Final Report for Period 1 Feb 1975 - 1 Mar 1976
6. PERFORMING ORG. REPORT NUMBER:
7. AUTHOR(s):
8. CONTRACT OR GRANT NUMBER(s): F04701-75-C-0114
9. PERFORMING ORGANIZATION NAME AND ADDRESS: SYSTEM DEVELOPMENT CORPORATION, 2500 Colorado Avenue, Santa Monica, California 90406
10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS: PE35167OF
11. CONTROLLING OFFICE NAME AND ADDRESS: DEPUTY FOR DEFENSE METEOROLOGICAL SATELLITE PROGRAM OFFICE, HQ SPACE & MISSILE SYSTEMS ORGANIZATION/YDA, LOS ANGELES, CALIFORNIA 90009
12. REPORT DATE: 1 March 1976
13. NUMBER OF PAGES: 125 (this volume)
14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office):
15. SECURITY CLASS. (of this report): Unclassified
15a. DECLASSIFICATION DOWNGRADING SCHEDULE:
16. DISTRIBUTION STATEMENT (of this Report): Distribution limited to U.S. Government Agencies only. Other requests for this document must be referred to Air Weather Service/CSE, Scott Air Force Base, Illinois, 62225.
17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report):
18. SUPPLEMENTARY NOTES:
19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

data system
computer system
computer architecture
weather data processing
Air Force Global Weather Central
meteorological data processing

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

This document has been prepared in partial fulfillment of CDRL line item A004 of System Development Corporation's Air Force Global Weather Central System Architecture Study contract. Efforts for this report were expended under Task 6, "Conceptual Design and Development Plan", performed under contract F04701-75-C-0114 for SAMSO, under the direction of Col. R. J. Fox, YDA.

The purpose of this study has been to optimize the entire AFGWC data process-

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE

Unclassified

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered) ing system from the vantage point of current and future support requirements, addressing the AFGWC data processing system over the 1977 through 1982 time frame. This study was performed under a unique plan which allows complete traceability between user requirements, Air Force Global Weather Central operational functions, requirements levied upon the data system, a proposed component configuration which meets the data system requirements, and a system specification designed to acquire a system which meets these requirements.

The resultant system described has a number of unique features, including total hardware authentication separation of security levels, load leveling accomplished by assigning main processors in accordance with a dynamic priority queue of tasks, and a system-wide network control capability. Other key features include a central data base processor to fill requests for data from other processors, computer operations centers, the use of array processors for accomplishing difficult numerical problems, and sophisticated forecaster console support. These elements have been designed to provide 99.5% reliability in meeting user requirements.

The proposed system architecture consists of five dual processors each of which is about 3.5 times as powerful as an existing AFGWC processor (a Univac 1108). Each dual processor has an array processor which will be capable of very high performance on vector arithmetic. The array processors are used to assist on the difficult numerical problems, including the Advanced Prediction Model for the global atmosphere, as well as very fine grid cloud models and cloud probability models. Some of the new requirements that will be supported with this system are [illegible] one minute response to query interface, reentry support for Minuteman, and limited processing of high resolution (0.3 nautical mile) meteorological satellite data. In addition, cloud cover prediction for tactical weapon systems, ionospheric prediction for radio frequency management, and defense radar interference prediction will be supported by this system.

Volumes of this final System/Subsystem Summary Report are as follows:

- Volume 1 - Executive Summary
- Volume 2 - Requirements Compilation and Analysis (Parts 1, 2, and 3)
- Volume 3 - Classified Requirements Topics (Secret)
- Volume 4 - Systems Analysis and Trade Studies
- Volume 5 - System Description
- Volume 6 - Aerospace Ground Equipment Plan
- Volume 7 - Implementation and Development Plans
- Volume 8 - System Specification

ABSTRACT

This document has been prepared in partial fulfillment of CDRL line item A004 of System Development Corporation's Air Force Global Weather Central System Architecture Study contract. Efforts for this report were expended under Task 6, "Conceptual Design and Development Plan", performed under contract F04701-75-C-0114 for SAMSO, under the direction of Col. R. J. Fox, YDA.

The purpose of this study has been to optimize the entire AFGWC data processing system from the vantage point of current and future support requirements, addressing the AFGWC data processing system over the 1977 through 1982 time frame. This study was performed under a unique plan which allows complete traceability between user requirements, Air Force Global Weather Central operational functions, requirements levied upon the data system, a proposed component configuration which meets the data system requirements, and a system specification designed to acquire a system which meets these requirements.

The resultant system described has a number of unique features, including total hardware authentication separation of security levels, load leveling accomplished by assigning main processors in accordance with a dynamic priority queue of tasks, and a system-wide network control capability. Other key features include a central data base processor to fill requests for data from other processors, computer operations centers, the use of array processors for accomplishing difficult numerical problems, and sophisticated forecaster console support. These elements have been designed to provide a 99.5% reliability in meeting user requirements.

The proposed system architecture consists of five dual processors each of which is about 3.5 times as powerful as an existing AFGWC processor (a Univac 1108). Each dual processor has an array processor which will be capable of very high performance on vector arithmetic. The array processors are used to assist on the difficult numerical problems, including the Advanced Prediction Model for the global atmosphere, as well as very fine grid cloud models and cloud probability models. Some of the new requirements that will be supported with this

system are a one minute response to query interface, reentry support for Minuteman, and limited processing of high resolution (0.3 nautical mile) meteorological satellite data. In addition, cloud cover prediction for tactical weapon systems, ionospheric prediction for radio frequency management, and defense radar interference prediction will be supported by this system.

Volumes of this final System/Subsystem Summary Report are as follows:

- Volume 1 - Executive Summary
- Volume 2 - Requirements Compilation and Analysis (Parts 1, 2, and 3)
- Volume 3 - Classified Requirements Topics (Secret)
- Volume 4 - Systems Analysis and Trade Studies
- Volume 5 - System Description
- Volume 6 - Aerospace Ground Equipment Plan
- Volume 7 - Implementation and Development Plans
- Volume 8 - System Specification

This volume (Volume 5) contains a description of the system design by SDC. It is the last and most detailed step in an expanding design description which begins in the Executive Summary (Volume 1) which should be taken by the reader as a predecessor to this volume. The final portion of this document defines how individual functional tasks will be accomplished within the proposed architecture.

TABLE OF CONTENTS

TABLE OF CONTENTS (Contd)

TABLE OF CONTENTS (Contd)

LIST OF FIGURES

LIST OF TABLES

INTRODUCTION

The purpose of this document is to describe the architecture and develop insight into its proposed use in accomplishing AFGWC functions. In a few instances, this information is the same as is provided in the Tradeoff Analysis Study or in the AGE Plan, but redundancy seemed necessary for completeness.

An integral part of this document is the overview of the system which is contained in Volume 1, The Executive Summary. We suggest that the reader complete Volume 1 to develop a more general understanding of the concepts and components of the AFGWC architecture before reading the detailed discussions.

The first part of this document is organized according to the architectural domain for easy reference to and compatibility with other volumes. The last part which describes how functions are accomplished using the architecture is organized according to the functional domain. Use of the requirements/function matrix in Volume 2 provides the link to determine how individual requirements have been fulfilled by this architecture.

In developing the proposed AFGWC data system architecture, numerous technical working papers were generated by SDC to document the results of various related analyses. SDC will supply summaries of these working papers under separate cover, as a list of appendices to this design description to this design description volume. Topics to be included in this supplementary publication are as follows:

- Appendix A - AFGWC Hardware Baseline
- Appendix B - Emerging Technology
- Appendix C - Hardware Component Documentation
- Appendix D - Special Purpose Hardware, State-of-the-Art Synopsis
- Appendix E - Comparative Performance Analysis of High Performance Computers
- Appendix F - Miscellaneous Memos
- Appendix G - Bibliographies
- Appendix H - System Simulation and Related Topics

1.0 ARCHITECTURAL DESCRIPTIONS

Many of the discussions presented to describe the AFGWC architecture are accompanied by illustrations and figures which have a basic design in common. The basis for this common ground is illustrated in Figure 1 which is a very basic schematic representation of the entire system architecture. Each set of major system components, (a subsystem such as a main processor or operations console), is represented by a unique symbol on the diagram. As we proceed through this system description, Figure 1 will be introduced frequently but the subsystem being discussed will be highlighted and illustrated more prominently than the others. This technique will not only he to identify the unique aspects of each particular subsystem, but will also allow the relationships with the remainder of the architecture to be established.

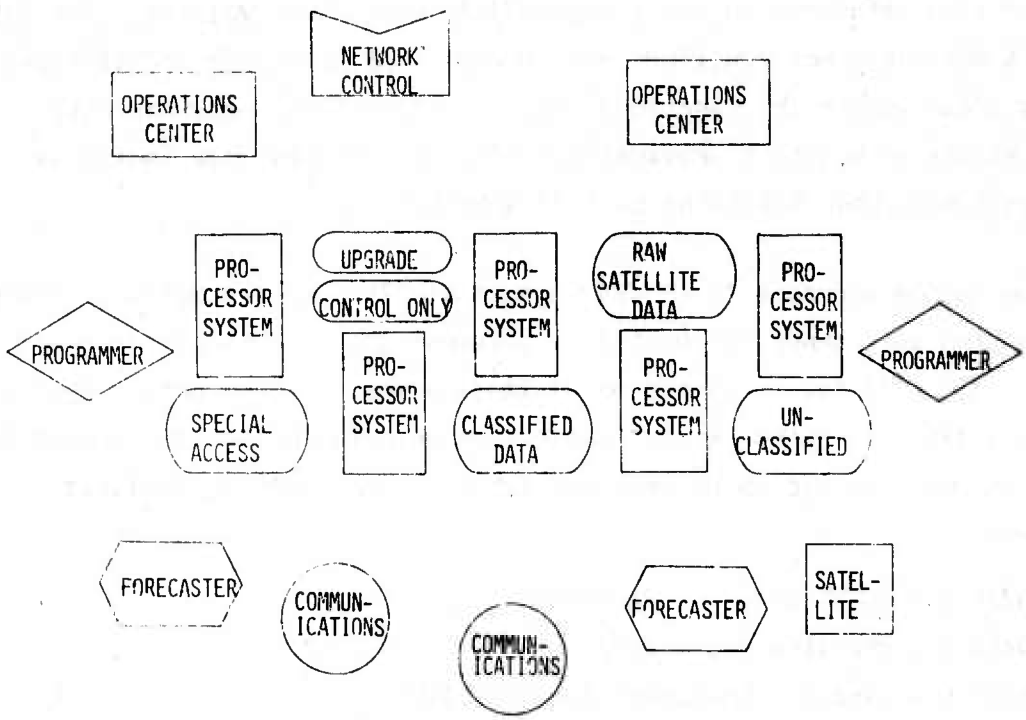

Figure 1. System Architecture (Master Schematic)

1.1 DATA STORAGE (A10)

The data storage section is divided into two segments. The first, storage devices that retain data on a rather permanent basis, and second, storage devices which retain data on a very transient basis, e.g., processor memory.

1.1.1 Storage Devices (A11)

Figure 2 shows the overall data storage structure of the enhanced architecture. These data base subsystems have been described already in the overview and this section will concentrate on the details that were omitted in the Executive Summary (Volume 1).

Tape units are connected to disk units rather than to processors for the following reasons:

a. The process of writing tapes at any given level of security would require a processor to remain at its designated security level until the tape output was complete, thus preventing the rapid redistribution of the processor resources to other security levels;

b. It enables the centralization of the tape storage which is less expensive than dedicated tape systems; and

c. It enables the centralization of tape mounting and dismounting thus minimizing the number of operator positions required.

It is anticipated that disk storage will be used as a buffering device to hold data sets which are normally written directly to tape.

In an effort to avoid dedicating tape drives to processors due to the expense of this approach and in order to centralize tape mounting and dismounting to minimize operator positions, tape units are connected to disks storage rather than to processors. It is anticipated that disk storage will be used as a buffering device to hold data sets which are normally written directly to tape.

Tape control units would then destage the data from these areas onto tape. Tape control units themselves may be a combination of a support processor and a tape control unit or may be a control unit similar to the control units used in the automated mass storage facilities which will be discussed shortly. Figure 3 shows a standard tape control unit and tape drive configuration. Note that the tape drives are connected to the control units through a swtiching arrangement which pools the tape drives and allows them to be separated onto control units according to the demands of the moment. This switch is security verifiable in that once tape drives are established in their linkage to control units there is no possibility for inadvertent access from another control unit.

Control units are dedicated to security levels, due to the fact that they must be attached directly to security level dedicated data bases. The tape drives will have visible indicators which provide a means for the operator to identify the security level at which they are being operated.

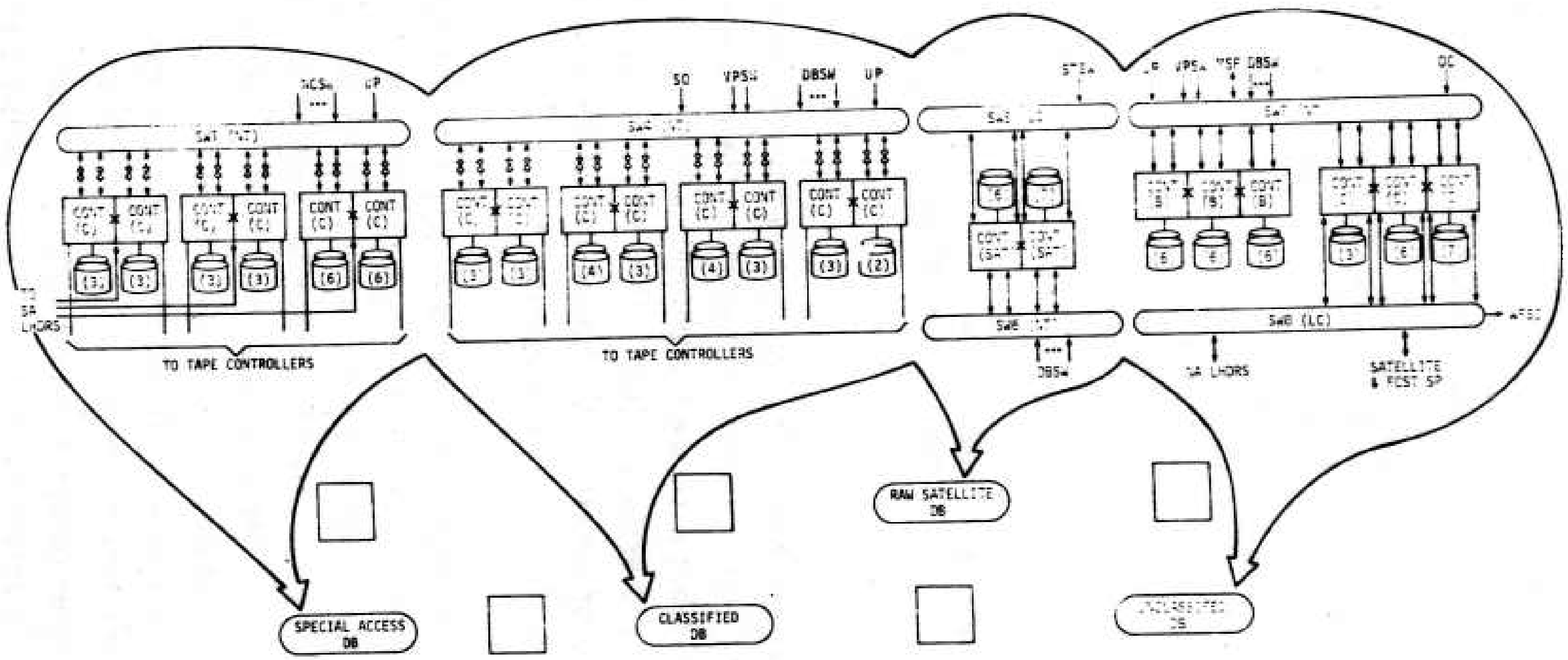

Figure 2. Data Storage Subsystems

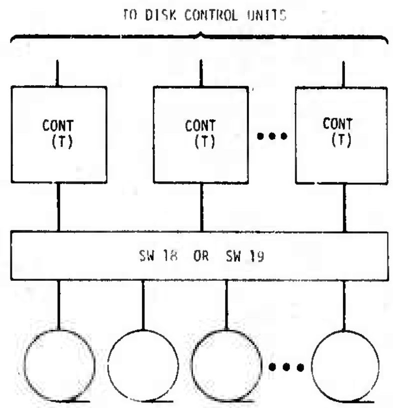

Figure 3. Standard 10-1/2 Inch Tape Data Storage, Normal or Special Access

These tape drives are manually loaded and unloaded using standard 10-1/2 inch reels of magnetic tape. In each perimeter the tape drives will have a mixture of densities available with the predominant density being the highest available today, that is 6,250 bytes per inch. This high density minimizes tape storage requirements. Lower densities are needed to provide compatibility between AFGWC and other facilities when exchanging tapes.

In the event that a centralized tape pool utilizing the types of control units already discussed is not feasible or cost effective for a given vendor, he may propose an alternative which consists of dedicating tape drives to processor systems and remoting them from the processor systems into a central location. Manually mounted and dismounted tapes have been chosen for the classified levels because the volume of data used at these levels did not provide sufficient cost justification for the use of an automated mass storage facility. It may be, however, that an individual vendor can provide a mass storage facility for the automated mounting and dismounting of tapes on a cost effective basis. The specifications for the architecture allow this possibility; however, the interchangeability of tapes between facilities still requires the use of standard 10-1/2 inch tapes unless other facilities can conform to the use of whatever tape media is required for an automated mass storage facility.

Figure 4 shows a block diagram of a typical mass storage facility which will be used in the enhanced architecture for unclassified tape data storage.

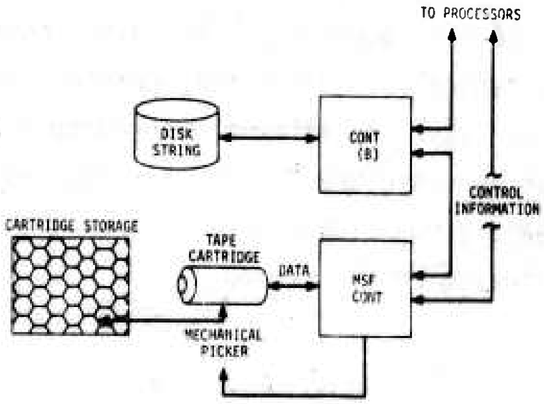

Figure 4. Mass Storage Facility, Unclassified Tape Data Storage

The mass storage facility control unit is interfaced directly to the disk control units and to the processor which controls the mass storage facility by executing mass storage facility software. The location of data sets, on disks and within the mass storage facility, is kept on disk tables which are redundantly recorded and updated on separate disk strings. The mass storage facility itself contains no single point of failure. Data are recorded on disks by processors and are then taken from the disks (disk destaging) and written onto tape cartridges. The tape cartridges correspond to approximately 50 million bytes of data in a typical situation so that two tape cartridges comprise one single density disk or four tape cartridges comprise one double density disk of 200 million bytes. The tape cartridges are stored into a cartridge storage bin by a mechanical picking device. There is a redundant mechanical picking device in the event of failure.

Data can be restored to disk if requested by main processor software. The data cartridge is removed from its storage location, the tape is taken out of the data cartridge and wrapped around a read/write head and the data is written directly to the disk control unit without going through the processor. The processor is then notified of the availability of the data set. This mass storage facility is under the control of a centralized data base manager.

Figure 5 shows a typical disk string and control unit configuration which has been "cross-latched" for reliability purposes. This disk control unit and disk string configuration is typical for satellite, combination, support and bulk disks. To provide reliability and additional throughput by alternative paths, both control units can access either of the strings under their control. The disk string switching feature may either be a part of the control unit or part of the disk pack distribution on the string.

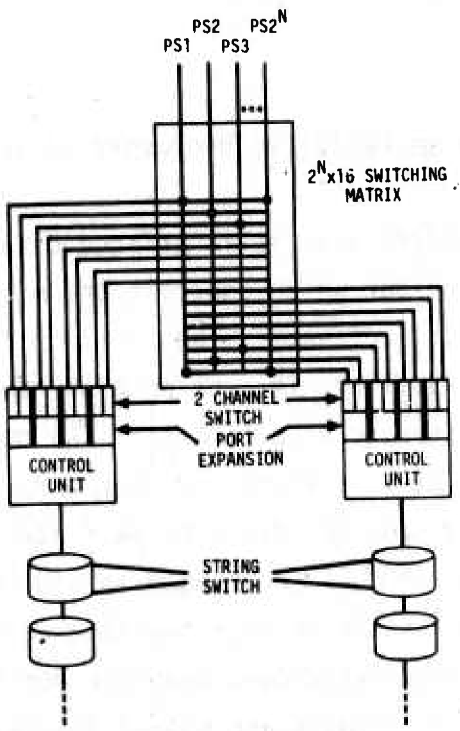

Figure 5. Cross-Latched Disk Strings Attached to Multiple Processors

Control units normally contain only one port which may be attached to a single channel. Disk ports may be increased via port expansion features, typically, up to four ports per control unit. Thus with the port expansion feature, four processors could access the control units redundantly or eight processors could access the disk strings without the redundancy of control units. The port expansion feature can usually be extended via a two-channel switch which allows each port to access either of two channels. This extends the maximum accessing capability to 16 processors without redundant control units or eight processors with redundant control units.

To further provide physical paths to disks, a switching matrix can be used in addition to the port expansion feature or the port expansion and two-channel switch feature. This switching matrix provides a means of extending the number of physical paths to disks beyond 16. Processors are multiplexed among ports by the switching matrix as is indicated by the fact that processor systems PS1 and PS2 are on the same port of both control units.

The disk configuration is not intended for high-traffic volumes on disks; that is, it is not intended that 16 or more processors would be active at any given time, but rather that 16 or more processors could be wired to the disks with only a few active. For example, in the enhanced architecture, the fact that the main processor systems are run as multiprocessors allows in the normal access area a maximum of three processors to be active on any one data base. Normally, there will be no more than one processor active on a data base.

Processors are permanently configured to data bases to avoid switching transients and the need to quiesce input/output on systems prior to switching. If it were necessary to quiesce all input/output on disk subsystems before switching this would create several operational bottlenecks in the process of trying to bring additional resources to bear under peak load. In addition, it would raise the possibility of an input/output error creating a system failure on already running main processor systems. To avoid this, of course, all processor systems have been configured to data bases on a permanent basis and their access by security level is limited through authentication devices.

The one by sixteen switching matrices can be computed from several two by four or two by eight or two by sixteen switches. Or they can be custom built as a single unit. These switches have an extremely high reliability. Each node is a isolated solid state switching device which can be removed as a unit and replaced. Each node also has a fail safe mode in which it prevents access of data. When this failure occurs, normally, a light provides visual indication of the failure at a local configuration control panel, however, this light can readily be remoted to the network control console to provide the status of the switching devices. Switching devices such as these require no preventive maintenance.

A low capacity storage device (LCSD) configured on the support processors for data downgrade can be either cassette type devices or "floppy" disk devices. The "floppy" disk devices are prevalent in the industry today.

A typical unit is the IBM 3540 Diskette Input/Output Unit. In the 3540 model B2, each dirve operates independently. Each drive has a separate hopper and a separate stacker holding up to 20 diskettes. Under program control, diskettes are automatically fed, one at a time from the hopper and mounted on the dry spindle for a read/write operation. At the end of the operation, the diskette is automatically removed from the spindle and stacked, thus permitting uninterrupted processing. Less elaborate diskette read/write devices are available for a lesser price. In either case the diskettes are a industry standard in form and can be obtained from a number of vendors. They are protected against contamination by an outside cover. Each diskette consists of a number of tracks which can be directly addressed thus permitting the reading and writing of messages from different locations without sequential processing of the entire tape, a disadvantage of the cassette approach. The diskettes have high reliability and high data integrity characteristics.

1.1.2 Processor Memory (A12)

1.1.2.1 Main Processor Memory (A121)

Main processor systems have been costed in the Tradeoff and Analysis Volume 4 with full main memory. This is due to the fact, that calculations based on requirements indicated that typical memory requirements plus operating system areas come very close to the maximum main memory allowed on processors. Of course, for processor systems with virtual memory, individual vendors must propose a tradeoff between the use of virtual and real memory.

The fact that full main memory is required on processor systems can be seen intuitively from several factors. First, the average job at AFGWC is a meteorological model which requires large scratch pad areas in memory for data matrices. Secondly, the main processor systems are multi-processors where, in effect, we have two CPUs executing out of the same memory thus requiring twice as much memory to provide a high CPU utilization. Thirdly, the main processor systems are acting as hosts to a very fast array processor which, although it has its own local memory, must use the host as an interface to the rest of the data system. Fourthly, the main processor systems must have sufficient main memory to accept the functions already being performed on another processor system which may have failed. Thus recovery in a degraded mode requires that these functions be accepted by other main processors. And, finally, it will be necessary to provide a means by which functions can be kept in memory to provide sufficient responsiveness for requirements such as in query/response. If main memory on the multiprocessor system was split so that half of the multiprocessor ran classified communications and the other half ran unclassified numerical models, the uniprocessor running numerical models would probably be given more main memory than the other half which ran communications oriented responses.

Special and normal access perimeters have been specified as having different main memory requirements with the special access having a smaller main memory requirement. Because the variable access perimeter spans both of these requirements it must have the larger of the two, i.e., the normal access requirement. In addition, because all three processors in this normal access perimeter can take on any of the roles required, each of these main processor systems, along with the variable access processor system, must have the same amount of memory.

1.1.2.2 Support Processor Memory (A122)

Support processors will probably be million instruction per second "mini" computers with 32 bit word length. These processing units provide approximately the same computing power as the 1108 in a 19 inch rack mounted physical space. Their memory capabilities today extend up to a million characters. And in the future will probably go up beyond that.

1.1.2.3 Array Processor Memory (A123)

Array processors have a locally attached memory on the order of a million characters. This local memory is necessary to keep the arithmetic elements of the array processor busy, particularly when doing applications such as meteorological models. Without it the array processor would develop severe data path bottlenecks in an attempt to access atmospheric parameters. The array processor and its local memory can be switched between each side of the uniprocessor or run off of the multiprocessor system.

1.1.2.4 Auxiliary Memory (A124)

Because of the variety of capabilities and the fact that no vendor supplies capabilities identical to any other vendor, our concepts about auxiliary memory are mixed and not precise. Two capabilities stand out which appear important to us. Each has to do with the availability of memory larger than that adressable by the CPU. Two concepts exist. The first is the immediate redefinition of active memory which is capable of input/output staging in the inactive portion while the CPU is working with the active portion. This reduces the effective input time on jobs that can be restaged to be equal to the change over time. The other capability which we found to be available was that of moving large amounts of data into a staging memory while utilizing the main memory for CPU activity. Then, through an addressable scheme which identifies blocks, data can be transferred very rapidly from the staging memory to the main memory and the effective time of input is the time required for this transition.

1.1.3 Data Base (A13)

1.1.3.1 Data Base Structure (A131)

The meteorological data base structure at AFGWC is the product of an evolving set of requirements. The result is that it may now resist growth and may not be able to adjust to additional requirements. Its adaptability to change, requires investigation. The SDC approach is to modify the meteorological data base structure so that it can more easily accommodate new requirements.

The structure is based on three vectors: a time vector, a vector in which each element is a box in 3 space and a vector for which each element is the value of meteorological parameter in that space at that time. Even though the three important vectors will remain in the same in post 1977 versions, their nature changes.

Starting first with the time vector, in the present data base the structure depends to some degree on the assumption of only a few convenient intervals (older data are purged). It assumes purge of all data simultaneously for a given time and point in 3-space. It assumes no two sets of data can be represented at a single point in time. With the existence of three input satellite systems updating the data base when the data are available and the possibility for purging only part of the data for a given point, the time dimension takes on more of a continuous nature rather than being discrete and cyclic.

The dimension which describes a solid in 3-space also is changing in the era of the new architecture. Presently only one grid scale is accommodated with all others treated as exceptional. With the mesoscale support of tactical systems sometimes for prespecified target areas, it seems the data base must accommodate a variable grid structure or at least provide an equally simple and efficient structure for each system as well as a useful interrelationship.

We envision the parameter set associated with a single-space time point accommodating more variables, but on the other hand allowing a wider variation in the number of variables represented at a single point. This may be due to the need for identification of data source and data reliability. For example, input parameters are needed in the probabilistic line of sight problem. We see the expansion of trend variables or trend statistics as possible parameters. The new structure must accommodate an expansion, even though we cannot currently identify exactly what that expansion will be.

There are cascading effects associated with the changes mentioned above. For example, AFGWC can no longer necessarily afford to automatically duplicate the meteorological data base on all systems if the time update is on an almost continuous scale. The structure of the system may be so complex in storage that both users and user programs must have a simpler visualization of the strucuture than that actually incorporated. Thus, data base management routines and an "apparent structure" must be developed.

SDC's proposed solution in the architecture is: 1) the use of overlay data bases which are classified and contained within a security level environment, and 2) the ability of higher level environments to request data from lower level environments.

Also, we are proposing the use of staging techniques which allow data to be moved from slower to more rapid access devices (e.g., from tape to disk to auxiliary memory to main memory).

The additional storage and the availability of fast array processors allows preprocessing into applications-peculiar formats. It allows redundancy for overlapping storage to ensure rapid sequential read for contiguous areas. It allows sequential read and filter as opposed to memory search.

1.1.3.2 Data Base Management (132)

First one must recognize there are multiple and somewhat conflicting objectives in defining a data base structure. Some of these objectives are:

a. it is desirable to achieve an organization that possesses order, simplicity, and homogenity as well as consistency in the structural hierarchy;
b. data bases are built and organized according to program usage, even to the point where redundancy in organization is allowed to achieve utility;
c. data bases which are user filled or used for storage of formatted output data are structured according to the user interface;
d. often the structure is oriented towards efficient use of the hardware component;
e. depending on the degree to which timing necessitates radical actions, data records are made compatible with disk pack characteristics, i.e., organized to reduce rotation rate, packed to reduce storage or to speed up access time, and sometimes structured to minimize sequential search time.

In the development of data base management, new factors are introduced, destroying old concepts. Some of these considerations are itemized below:

a. With a data base management concept utilizing data base interference routines, the application program characteristics need not be a consideration in data base structuring. Programs are isolated from the data structure and therefore changes to data structure can be transparent to application code.

b. Logical addressing can be used since executive routines can keep track of location through pointer tables, obviating the need for routines to know real, physical storage location.

c. Many techniques can be used to increase the efficiency of the hardware systems, such as ping-ponging of data between disks and random scatter on multiple disks to reduce head movement, which need not be a consideration to the application program.

d. The concept of staging has a great impact on data base structuring, i.e., depending on the predictability of the movement of data, the most restricted or "input/output bound" data flow is given the greatest design consideration.

e. The designs must consider the optional use of fixed head or movable head disk capability as well as the use of tape devices or mass storage facilities.

f. With extended memory (working memory with rapid transfer from auxiliary memory elements), redefinition can take place rapidly (in the case of certain designs) where data structure considerations become obvious.

g. Designs can optionally use array processor memory or host memory. The vectorization and the rapid transfer of data must also be considered.

The above considerations should be made, a design criteria written and the data base restructured based on results. This design analysis should be done concurrent with the investigation of program modifications which can accommodate the enhancement of the data flow.

Data base access can be broken down into categories for the AFGWC architecture: central meteorological classified overlay raw satellite, host/array processor (numerical model), support processor or communications LHDR interface, fixed head disk (as part of the main processor subsystem), and the tape staging area. Each of these categories will be addressed in turn in the following paragraphs.

The central meteorological data base is managed by a main processor subsystem with a ready backup located on another main processor subsystem. The central data base manager must queue requests for data base elements, must utilize redundant (backup) copies of the data base in answering requests, must discern duplicate requests for a data base element and combine them, and must be coded in such a way that both halves of the multiprocessor can be utilized to decrease response time to requests. The central data base manager must use files shared with the backup for queues and stack vectors so that the backup can assume processing with minimal description if the primary fails. Furthermore, the central data base management routines should be capable of recovering from a failure of a uniprocessor and continuing in a degraded mode with only half of the main processor active. Network control should be notified and, if necessary, an orderly transition to the backup should be accomplished. The central data base manager should be capable of using one copy of a data base element to answer read-only requests while the backup copy is being updated, and then switching to update the other copy. The switch should not be made during satisfaction of a request due to the discontinuities in the data that might result.

Classified processors must have a minimal data base management capability to maintain point or area overlays to segments of the unclassified data base and to filter data segments (requested over a wide area from necessary to camouflage the request) down to the needed amount.

The raw satellite data base needs minimal management and this is provided by network control via the assignment of function to processors. Network control establishes the satellite data ingestion support processor who will store data into the satellite raw data files by vehicle as it arrives from downlink receiving sites. In addition, the network controller will allocate quarter orbit tasks to main processors for mapping and gridding. The hardware of the disks and disk controllers and the allocation of files will allow concurrent data ingestion and mapping.

Host/array processor (numerical model) data base management concerns itself with the allocation of host (3.5 RP main processor) memory and local array processor memory in such a way as to optimize the overlap of processing and data transfer. Because this timing is highly dependent on problem characteristics, individual programs will have responsibility for accomplishing this data base management using standard subroutines. The array processor is not multi-programmed, making data base management a relatively straightforward task.

The support processors, LHDR's and main processors interface with the combination disks and compete for access (at any given security level). It is therefore important that any single processor tie up the disk for a minimum amount of time. For this reason, high activity data sets or their indexes will be located on the fixed head portion of the disks. Individual files may have reserve keys to indicate ownership during update. Management is thus very simple, with service on a first-come-first-served basis.

The fixed head disk areas will be used for operating system areas and model staging areas. The management will be accomplished by standard executive routines with application programs reserving files through executive allocation services.

The tape staging area will be managed as a set of fixed areas that are wrap around data sets of chained records with the capability to chain multiple fixed areas together. Tape controllers and main processor compete for access to disk but must reserve areas via the volume table of contents.

1.2 DATA TRANSFER AND ROUTING (A20)

This portion of the system can be thought of as the internal system interface. It is the vehicle by which the security, network control, master data base, and outer subsystem maildrop philosophy are implemented. This portion of the design must accommodate all required data volumes and response times while giving adequate security protection, appropriate integrity for system control, and appropriate protocol for a system where virtually all components are interlinked either directly or indirectly. This portion of the design is extremely critical since it dictates the abilities and the constraints of system usage with respect to interaction of system components.

The probability is great for the acquired system to be different in the areas of data transfer and routing than what we have envisioned in our design. There are several reasons for this: a) contractors have specific capabilities with respect to number of ports, transfer rates, component distances and controller intelligence; so that each individual configuration allows options which are different than another configuration, (b) the only requirement in the system design for new hardware development in the use of new technology is in the authentication and delimiter devices which must operate at channel speed (e.g., approximately 5 megabits per second) for the hub of the control-only and secure component intercommunication network.

1.2.1 Hardware Linkage (A21)

The decision was made very early to utilize the capabilities of authentication (including data path encryption) rather than automatic physical switching because of the difficulties encountered in the system quiescence and initialization. In our investigations no vendor seemed to have the ability to interface properly with a physical switch system, which was in direct opposition to our ability to satisfy one or two minute time requirements associated with query/response.

This led to the concept of two types of data lines: those secured by virtue of their authentication and coding and those which were unsecured. We wanted to minimize the number of secured data lines because of the cost and engineering impact. This was accomplished by identifying all the links which were always at the same security level and also controlling the security level of links which did not require the rapid time response dictated by requirements. We also dedicated storage devices which could not be cleaned rapidly, as well as communication line specific minicomputers, to individual security levels leaving only the main processors with the flexibility to quickly change security levels. As a backup we also used authentication to double-check operator action where the option existed to rapidly switch between security levels.

The problem was encountered as to whether to require that a single authentication device accommodate a single security level plus all lesser security levels or whether it need to treat data at a single level. The latter solution was felt to be simpler and less costly in design. Using headers and other protocol we determined that if the receiving device did not recognize the data being transferred, it would immediately assume non-validity. In this case, data transmission would be stopped and network control immediately notified. This technique essentially made security compromise impossible (since we are only worried about the inadvertent passage of data and not malicious espionage).

The third class of linkage considered in our design was that of the one-way data line. This we feel could be accommodated by a simplex data path with a sender on one end and a receiver on the other. Certification of data receipt could be via simple data encoding schemes, or if required, the use of a control-only data link in addition to the one-way link allowing only the passage of acknowledgement or nonacknowledgement data. Software intelligence can accommodate the time delay of acknowledgements so as not to slow down the maximum data rates required in this system. (The control-only data link is discussed in the subsequent paragraphs.) We feel that the one way data concept is viable because of its current implementation in the AFGWC data system structure.

The next type of data link required in this complex system is perhaps the most shaky in terms of security control, but we feel it is mandatory from the standpoint of network control and to solve the problem of data requests from a higher security level. This requires a hardware control assurance that only certain recognizable pieces of information are passed from a higher security level to a lower level with a monitor capability as additional verification to certify that that link was indeed being used in a manner consistent with the system design philosophy. SDC feels that an isolated protected programmable device can accomplish this function and although not requiring significantly high data rates, it can supply the response times consistent with the time limited requirement of the AFGWC system.

The concepts identified above led to the conceptual application of an upgrade data link in which data may travel to an equal or a higher level of security and there be utilized in computation as needed. The upgrading of data was required many places in the system especially in utilization of the unclassified meteorological data base for classified applications. The solution also allowed the capability for a lower classification console to initiate a run at a higher classification level or for data to assume a higher pseudo classification for efficient printout purposes where it was known that the human interface accomplished certification and subsequent downgrade to the appropriate level.

Intuitively we felt that in no place within the system could we allow either hardware or software to assume the responsibility of downgrade of classified information. We did however assume the reliability of hardware and software to assign a level of security consistent with the security assignment of the hardware and software components and to trust this assignment in the form of security headers for the purposes of communications routing over a line of equal or greater security level.

Several places within the current or future system we saw the requirement for certification/downgrade of data but in all instances these data were small in quantity and in a form easily viewed by the human element. We therefore created a security downgrade position in which data were written on a low capacity storage device, manually removed from the hardware data path, viewed by security downgrade monitor, and through switching, transferred to the appropriate security level.

With these basic data routing tools we could then assign to the main processors of the system certain basic interfaces:

a. A two-way control-only data link for requesting data from the master data base subsystem and receiving job assignment information from the network control computer.

b. A one-way data link to allow upgrading of data to a higher classification level or transfer of data to an equal security level.

c. A means by which the network control computer or the network control console could provide a particular security level to the security key memory of the computer without intervention by the computer or from outside sources.

d. A means to communicate via one-way data link to the operations console which would accommodate all computers no matter which security level.

e. A way of accommodating the interface between the computer operations position and the computer in question.

f. A secured two-way path to the storage subsystem which had been assigned the same security level as the computer in question.

In the case of the network control computer it could interface directly with the network control console and via the network control console could load authentication memory. The backup network control computer could maintain the same links as the network control computer and in addition interface directly with the highest classification level programmer subsystem.

The master data base processor could utilize the upgrade data capability to pass unclassified information to unclassified or higher security levels. We proposed maximizing the number of data links between the data base processor to optimize this vital interface. The backup data base management processor would interface with the unclassified programmer subsystem. In all cases we used authentication encoding where the potential exists for lower level data recipients to interface with higher level computers. It was extremely important based upon our design concept for the master data base processor to interface with every main processor as well as data bases of each classification level.

1.2.2 Security Separation (A22)

Now we shall get into the details of the vital interfaces within the proposed system. The basic authentication encoding scheme consists of chips that effect some algorithm such as the Bureau of Standards data encryption standard (DES) which is unique and repeatable according to the same key. (Since this was in truth an authentication rather than encryption problem we felt it did not warrant the use of NSA approved cryptographic devices. It was determined, however, that such devices were available to satisfy our application.) Encoders which have a common security level will contain the same key. The key is loaded by the network control computer or as a backup from the network control console. The only authentication devices accommodated by the key change capability are those associated with the main processors of the system. The key change capability is limited by the fact that a lockout exists with respect to any main processor: a) until cleaning (writing random 1's and 0's in all memory components three times) prior to downgrade or b) where the processor has been assigned a permanent unclassified position. The keys are associated with a dual processor in that configuration or with each uniprocessor if they are separate. Both decoding and encoding chips shall be associated with a single key memory.

We have specified a cascading encoder/decoder device. Although this device is part of the upgrade component it operates independent of its software. The cascading encoder/decoder can take data, encode it at any level (even non-encoded at the classified level), and upgrade it to any specified classification level. This capability shall be accomplished at channel speed for any single request and shall have the capability to handle multiple requests.

The basis for the control only data link is a device which probably is not available in the current market. This device, which we call an "information delimiter", will compare incoming data words against a prespecified set of acceptable words and if the comparison is not valid will notify network control. This device also recognizes patterns and logical sequences of data received over the control-only data line and it checks the rate at which data are transmitted to ensure compatibility with normal line usage. In all cases if a violation results then network control shall be notified.

1.2.3 Controllers (A23)

Standard controllers are used for disk interfaces with the exception of the tape controller. Our primary design approach is to have the tape controller write data in a prespecified area of a disk which is compatible with the security level assigned to the tape. Processor activation can specify that any data on the disk can be written on the tape assigned the appropriate security classification level and linked to the disk in question. We felt that specification of this capability was not unreasonable from the standpoint that most vendors had designed a controller associated with the mass storage facility which has these capabilities. If our assumption is not valid, we have offered the alternative of direct tape interface with processors where encoding decoding devices will assure consistency between the classification level which the operator felt he had loaded and the classification level of the computer. In our design, headers will be utilized to ensure appropriate classification level on tapes being entered into the system and such headers will be written by processors assigned to a given security classification level.

1.2.4 Interface (A24)

The principle connections within the system are from each of the external subsystems (e.g., forecaster console, satellite data) and the appropriate disk pack data system. The exceptions are the programmer consoles, network control area and operations consoles which interface directly with the computers. The two principal interconnection data links are the control-only data link and the upgrade data link which, like the spokes of a wheel, interconnect to almost all parts of the system (see Figures 6-7). As mentioned before tapes interface directly with disks, as does the mass storage system, with no intervention by the main processor. There is a link which distributes security keys throughout the system from the network control console and interconnections of the line handler/decoder routers with each other and with the communications console as well as with the appropriate external data line and internal disk.

The design has attempted to judiciously use the minimum of input/output ports associated with computer and data base systems although this is extremely difficult in the case of the latter. In our design more basic connections exist than are actually required in a given system state. Once a computer system has been specified and we know the number of ports, data transfer characteristics and computer interface associated with transfer pertaining to the individual ports, the design can be optimized. Refinement will be primarily in the area of assuring appropriate band width for peak load data transfer circumstances, especially in the areas of: a) transfer of data from the master data base to all parts of the system, b) transfer and processing of satellite data for gridding and mapping, c) transfer and storage of video images to and from forecaster consoles, and d) high response associated requirements.

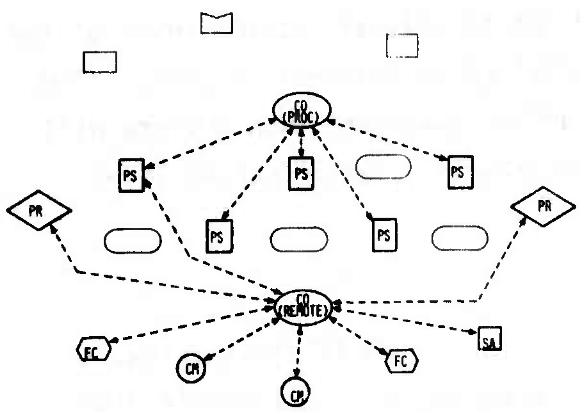

Figure 6. Control Only Data Links

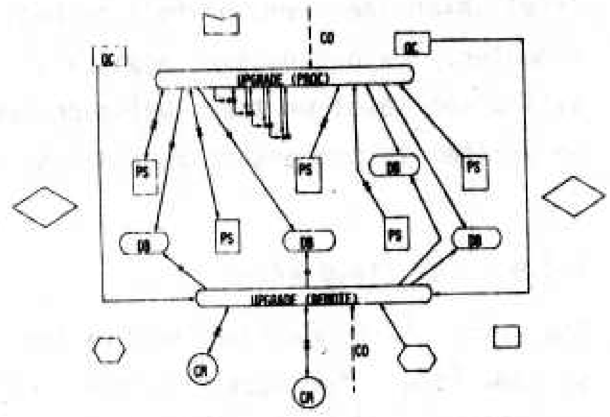

Figure 7. One-Way Upgrade Data Links

1.2.5 Routing (A25)

Under the subject of routing, we would like to treat in more detail the specific characteristics of the control-only and upgrade data links. The upgrade data link (see Figure 8) is a combination of hardware/software components. As we see it, this link has a very important function of receiving data on one security level, decoding at that level, upgrading (and therefore reencoding) these data to the level of the recipient (never downgrading) and, forwarding the data. All of this must take place at channel rates so as not to destroy the natural intercommunication between a computer and a disk pack subsystem. This device must handle many data requests simultaneously and must itself be secure.

The problem as you might have realized, is with the data being encoded there is no way for the upgrade device to know what routing is to be accomplished. We thought about decrypting just a header word for such information or trying to bypass the authentication device with the routing information but decided that these solutions held too great a security risk. The solution we chose was communication via the control-only data link; the sending device will, simultaneous to transmission, send over the upgrade data link a message which indicates present security level, destination, and destination security level. The security level upgrade shall be accomplished with the cascading decoder/encoder hardware device which is isolated. It shall be designed such that the software portion of the upgrade data component has no access to the data during the time it is decoded. The upgrade component also has a task of simple serialization and presentation of requests for resources to the network control data base.

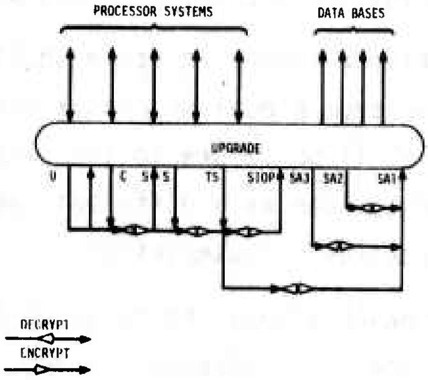

Figure 8. Upgrade Data Processing

The control-only data link is a device (probably a small processor) which shall be isolated and kept secure from tampering or software intervention. The device shall recognize initial header messages as any messages being sent which identify both the sender and the addressee. The total information content of any single computer word sent over this data line shall be limited to a very small subset of all possible combinations of bits. We felt that the best way to accomplish this was by comparison of a memory of legitimate codes. However, consideration of a specific subset of bits requiring all others to be a fixed pattern is also a possibility. Whenever data are sent which are not recognized to be valid, violations are reported to network control; the sending device is notified of the error, and transmission is terminated awaiting network control release. The control-only data link will also recognize the frequency of messages from a particular source and shall treat as a violation any cases in which the frequency exceeds a predefined threshold. In addition, it will consider the relationships of successive words to one another since only certain sequences of word transmissions are legitimate.

1.2.6 Switching (A26)

With the use of authentication encoders/decoders, there is no requirement for automatic switching within the system. Places within the system within which a manual switching capability shall exist are as follows:

a. A switch at the network control console shall allow configuration of a main processor from a dual processor mode to a uniprocessor mode. The switch shall be secure to the extent that each side of the multiprocessor can operate at a different security level with no physical data connection or interaction.

b. There is a switch which allows the assignment of the array processor to either side of the dual processor system. The results of the switching must be available to network control for appropriate task assignment.

c. At the network control console there will be a switch (actually a gang switching capability) which allows hooking the variable perimeter processor system to either the normal or special access perimeter. There is a lock-out capability associated with the switch which does not allow downgrading to the normal access perimeter until the cleaning function has been completed and certified.

d. There are local switches which allocate memory to processors, allocate disks to controllers, allocate tape drives to tape controllers, identify support processors with support functions, assigns line handler/decoder routers to appropriate circuits and finally switches the assigned uniprocessors to a maintenance console while simultaneously disconnecting it from the rest of the system.

e. There are selector switches on several consoles which allow the operator to select the data routing classification level. These are included on the operations consoles, the data downgrade consoles, the special operations console and the communications consoles.

f. There is a switch at network control which puts processors in an independent mode separating them from the overall control of the network control computers. This is used as a backup in case the automatic network control capability fails completely.

g. There are switches at the network control console which identify the network control computer and the backup computer for network control as well as assign special access programmer support processing to the backup network control computer. Similarly, a switch assigns the master data base processor, assigns the backup and links the normal access programmer consoles to the backup computer.

As we had mentioned before, the gang switching capability applies to the variable perimeter, network control assignment, backup network control assignment, master data base processor assignment, and backup master data base processor assignment.

1.2.7 Compatibility (A27)

Considering the question of compatibility, SDC has tried to provide a design that allows several large computer manufacturers to respond with standard equipment. However, the design might for many reasons be a mixed vendor system especially in the area of array processors and mini computers. We feel that it will be up to each of the vendors to propose the best solution to the compatibility problem. It is important if the systems specifications is split into several different procurements that the compatibility responsibility be identified with a specific procurement.

1.2.8 Merging (A28)

A detailed analysis of the proposed equipment and data rates (perhaps even simulation) will show relative line usage. It may be desirable from a cost standpoint to multiplex data where shown to be cost effective and on the other hand to double and triple other lines to provide adequate bandwidth for peak load transmission conditions.

1.2.9 Conceptual (A29)

SDC feels very strongly that the final system design will benefit from studying and adopting protocol and interface standards for AFGWC. The components which are retained in the 1977 baseline will not necessarily be equipped to comply with the standard but the exception should be specified and modifications made where required. The philosophy taken in the design is to require that more linkages exist than will be actually used at some point in time and in fact some linkages will be invalid from the standpoint of security compatibility authentication. Therefore, processors must assume an appropriate linkage as they are operating with the software designed to protect against the usage of the inappropriate linkages with notification and recovery procedures when inappropriate linkages are violated.

Disk control shall be processed on a first-come-first-served basis, however, since multiple users are utilizing disks, standards must be adopted which minimize the tying-up of a disk pack by a device while avoiding thrashing. This can be accommodated by computers setting up their calls before they command the disks, accomplishing all the work that needs to be done judiciously and efficiently, and then releasing the disk. If disk usage is over a maximum period of time then the disk input/output will be time-sliced for communications for other subsystems to write on the fixed head portion of the disk.

The disk and processor system will be treated by all outside interfaces as a service bureau where they provide the data, notify network control, and wait for a control-only data response to indicate when their request has been fulfilled. Once data are sent to an upgrade level, the sending system shall monitor for a retransmission request on the control-only data link. A large file of interactions shall be maintained, along with saving the data (on the order of one minute) that has been transmitted. All data transfer and routing operations will identify the security level of the data involved; the data transfer and routing will be made in a manner that makes physical violation of the security level impossible.

In terms of routing, the control-only data link will automatically know the sender and will be capable of identifying the recipient using part of the data message. In the upgrade data link, when data is sent, there will also be a control-only message which identifies data routing classification level of the data, and classification level of the receiver. Inter-computer communications data strings shall always identify the sender of the data.

Acknowledgement of data sent over the upgrade data link shall be over the control-only data link. Acknowledgement from non-smart devices such as disks, shall be over the return data link. In all such cases there is two way compatibility at the appropriate security level. Acknowledgement should be phased so as not to delay the passage of the data.

Parity checks and checksums shall be generated associated with the transmission of data and only higher level coding techniques will be used where for some reason acknowledgement cannot be accomplished because of security level. There will be a closed loop path on all data sent between components to ensure that no data are lost.

1.3 COMPUTATION AND SOFTWARE (A30)

1.3.1 Processors (A31)

1.3.1.1 Main Processors (A311)

Because main processors have been treated in the Executive Summary and the main processor memory section 1.1.2, and because the main processor capabilities are familiar to AFGWC due to the similarities to 1108's and 1110's, they will not be treated in very much depth. However, there are a few features which are important.

The main processor system that has been specified is unique to the extent that it is a dual processor, which when operating in the uniprocessor mode must be separable to the extent of satisfying security requirements, i.e., there must not be any electronic connection between the two halves and previous connections must have been severed via a switch certified to be secure.

A discussion of computer size is important. The design is based on a 3.5 RP (A Univac 1108 is one RP) computer throughput power. The important criteria in our selection is not only the total system computer power but also the segmentation of that power to be able to handle multiple and conflicting jobs. Under normal conditions, five processors of a 3.5 RP rating (operating in a dual processor mode) can handle the job; however, under high conflict conditions and/or conditions of a degraded system, the ten uniprocessors (of a capacity of 2 RP each) can handle all situations.

The advantages of having the multiprocessors is the added reliability resulting from the self-repair and recovery capability of the dual processor system. Almost all single points of failure are recoverable immediately and without intervention by the network control system.

If in a procurement a bidder specifies a higher RP computer, he will still have to provide the same number of systems unless the compute capability is so great as to nearly eliminate the possibility of conflict. (Remember that the security conflict will exist no matter what the speed, its only the time overlap conflict that will be reduced.)

The main processor must, of course, have the capability to perform input/output interface functions without degrading the simultaneous computation. The satellite mapping and gridding problem benefits considerably from a very large memory, which these systems will have.

The processor systems must be able to operate from a centralized remote console but will have dedicated, local maintenance equipment. A maintenance position associated with each main processor has been specified because it is the least expensive option since standard hardware/software components are already available and because of the necessity for providing diagnostic information at the mainframe.

1.3.1.2 Array Processor (A312)

The array processor is a satellite to a general purpose host computer, is closely coupled to the host, and behaves very much as if it were another CPU in a multiprocessor system; it shares memory and is as autonomous as possible in its activities.

The computation performed by the array processor is controlled by a FORTRAN program in the host. The FORTRAN program uses subroutine calls (to machine language routines, possibly) as its interface to the array processor. Computation in the host and in the array processor are highly overlapped.

Ideally, the host would be refining and storing on disk results of the array processor's calculation while the array processor was working on another segment of the problem; simultaneously, the array processor would be loading the next segment to be worked on and transferring the results of a previous segment to the host. In this way, all overhead would be basically hidden behind the necessary calculation.

The array processor uses the host as its interface to the remainder of the data system. This allows the use of existing interfaces, e.g., host to disk, and the extensive software support already written for general purpose machines. At the same time, the array processor need only contain enough logic to perform the requisite calculations and share memory with the host, minimizing its internal complexity and hence its cost. The host also performs those calculations requiring longer precision than is present in the array processor, and does data manipulation.

The host and array processor run asynchronously, as mentioned previously. Control and coordination are attained in two ways. First, the host can command (and sense the status of) the array processor via a normal input/output channel interface. Second, the host can establish a queue (in host memory) of operations to be performed by the array processor. The array processor will then be triggered via the channel interface to begin the operations listed in the queue. Upon exhaustion of the queue, the array processor can interrupt the host and notify it of completion of activities, again via the channel. Due to the time constraints and security requirements of AFGWC, it may be necessary for the host to interrupt the array processor prior to completion of the list of operations. At this point, the array processor must be able to halt processing at some convenient point in such a manner that intermediate results can be saved and the activity restarted again later. It is also vital that the host be able to quickly sense a failure of the array processor so that the job can be restarted and still meet deadlines.

Because the requirements of AFGWC will change with time, flexibility is a highly desired attribute for the array processor. This is reflected in the microcoded rather than hardwired control, and in the elimination of as many data path bottlenecks as possible. Such bottlenecks might occur between the host and the array processor, or within the array processor. The use of a local memory on the array processor, for example, should minimize conflict problems arising from using the host memory and also minimize the overhead due to host/array processor communication. Flexibility is also specified in the expandability of local memory, control microstore, and the number of processing elements.

1.3.1.3 Support Processor (A313)

Support processors have been patterned after units similar to the Interdata 8/32, the PDP 1170, the Data General ECLIPSE, and the SEL 32. Each of these processors today provides roughly the computer power of a UNIVAC 1108 with a growth path into further compute power. The software base of these processors is increasing as acceptance grows. Today there are standard operating systems for both real-time and batch applications and a wide variety of compilers. In some cases, data management systems exist.

1.3.2 Software (A32)

The software component and its proper development is vital to the success of the enhanced AFGWC architecture. The nature of the homogenity of the main processor backbone and the rapidity with which they are scheduled and upgraded/downgraded to the necessary security level implies certain capabilities in the software elements. The following section will describe these elements, their role in the enhanced architecture and special software needs for a successful implementation of the architecture.

1.3.2.1 System Software (A321)

The function of the system software is to provide scheduling, job control, and resource interface within a main processor system. The main processor system can exist as either a uniprocessor, uniprocessor with an array processor or a dual processor with an array processor. The system software must provide its capabilities in all of these configurations. Since all of these processor configurations exist at a single security level the system software will be required to operate with a single security level and will not be required to handle mixed mode security. During a single processor security level assignment, a disk interface will exist only with a disk assigned to that security level. The system software must provide an interface to the upgrade data link. The system software will have to accommodate the interface to the network control software. This interface will receive job requests from network control and provide network control periodic status on executing jobs and processor resources.

Since some of the processor system will be accessing mutual disk storage facilities (especially the unclassified processors accessing the unclassified disk units) along with support processor, the competition for these resources will be high. The software must provide efficient techniques for guaranteeing that access to these mutual disk resources is equitable between the competing main and support processors.

1.3.2.2 Support Software (A322)

The support software will provide the AFGWC architecture with all required functions normally associated with utility and maintenance operations. For optimum operation of the AFGWC architecture all support software will run in the normal scheduled environment of the main processors. There are currently several utility functions that were designed by AFGWC which produce management aids. They will be modified, if necessary, to perform in the new system.

1.3.2.3 Applications Software (A323)

The application software performs the many product and mission specific functions at AFGWC. An extensive library of software programs exist for the Univac 1108/1110 AFGWC system. If modification is required for these programs to execute on the new main processors it will occur after a survey of the applicabiility of their function of the enhanced architecture and the updated mission requirements. The survey will establish the programs for modification and the relative priority to the enhanced architecture. All application software that is to be implemented on the enhanced system will be developed to take advantage of the new system architecture elements: multiprocessors, array processor, distributed tasks, central data base, mass storage facility, automated forecaster consoles, etc.

1.3.2.4 Numerical Models (A324)

The numerical models will provide AFGWC with advanced numerical techniques utilized in the analysis and forecasting function. Numerical models designed for use in the enhanced architecture will make maximum use of the features of the architecture, i.e., multiprocessors and array processors. Due to the complexity and extended execution periods of many of the advance models, full exploration of such features as checkpointing should be guaranteed. Further, more, the coding complexity and subsequent difficulty in program checkout requires absolute adherence to the accepted technique of structured programming.

1.3.3 <u>Purchase Software</u> (A33)

1.3.3.1 Programmer Interface (A331)

This first portion of the purchased software deals primarily with the programmer interface software. This software is under the purchased software division since it will most likely be vendor-supplied as part of the hardware system for a minimum additional cost. Programmer interface software specifications are patterned after the capabilities of such software systems as the IBM Time Sharing Option (TSO) or the Univac Conversational Terminal Systems, i.e., Univac 1100 CTS. The capabilities offered by such software breaks down into three categories, the ability to enter and edit ability to submit jobs, and the ability to do online debugging of programs. These are the three primary capabilities required for increased programmer productivity.

1.3.3.2 Data Oriented Language (A332)

The primary applications computer language used at AFGWC is FORTRAN. It has obvious shortcomings when it comes to data transfer and handling. It is possible to augment or replace FORTRAN where these processes are concerned.

Data management statements which explicitly represent the data management action desired by the data base user provide for easy use, easy understanding, and easy modification. This improvement over the present data base access method derives from the explicit form of the data manipulation statements in that the user can define in such a statement exactly what he wants done with a specific set of data (rather than setting up a subroutine call to a data management routine where any data reference is implicit and must be constructed using documentation describing the call and the parameters). These program development advantages will become system advantages which facilitate standardization and management control of both the data base and programs which access the data base in an environment such as AFGWC where there is an ongoing requirement for the data base, a requirement for modification of programs which use this data base, an immediate requirement for the development of additional applications programs which access the data base, and a high probability for long-range development of additional programs which utilize the data base.

Data declaration statements oriented for design and construction of the data base will provide for improved data processing in a manner similar to the data manipulation statements discussed previously. The data base controller or the data base design maintenance group will be provided with tools (data base design declaration statements) which facilitate the definition and construction of a data base specific to the needs of the system of data base users.

SDC recommends the continued use of FORTRAN for development of AFGWC applications programs due to cost considerations. Such use minimizes reprogramming of current applications software, since most of the current programs are written in FORTRAN, and increase the transferability of future applications software.

The design decision that a data base management system be developed at AFGWC and the conclusion that FORTRAN will continue to dominate as the language for applications software dictate the development of support software to process data-oriented statements. The structure and capability requirements of such support software are therefore relevant.

A requirement exists for a processor that is capable of receiving mixed Data Management Language (DML) and FORTRAN source statements which: a) describe (for design or construction) the data base, or b) constitute a FORTRAN application program with a capability to refer to data base data using DML statements. Representative processors capable of making such transformations include: a) a preprocessor developed by General Research Corporation, ENLODE, which combines some elements of a higher-order language suited for specifying Ballistic Missile Defense (BMD) engagement logic with elements of a higher order, data oriented language suited for translation to FORTRAN source code which effects the interface with a centralized BMD data base; and b) the UNIVAC 1100 DMS preprocessor which accepts combined Data Manipulation Language (DML) and Cobol source statements and produces (Cobol source statements which include subroutine calls to the Data Management Routine (DMR) in order to implement the action of the DML statement. Such preprocessors are not overly complicated, and development of like processors can be accomplished using standard compiler development context analysis, syntax driven, or macro processing techniques.

In addition to implementing the desired data management extension to FORTRAN, the processor using macro processing techniques provides an ongoing capability to supplement FORTRAN through the use of macro declarations and macro calls. Such a capability can be used to add new data management capabilities to the baseline data management language, provide AFGWC language extensions to FORTRAN which would be consistent with structured programming (e.g., if-then-else, do while, and case macros), and to develop Higher Order Language constructs suitable for the analysis, development, and/or construction of AFGWC systems. An operational example of this type of processor is the SDC-developed AMPLE (an Adaptable Macro Processor for Language Extensions) which processes macro declarations written in FORTRAN, retrieves canned FORTRAN macros from a macro library and translates programs containing AMPLE macro calls into FORTRAN source programs. A macro processor of this type could be used for developing experimental language forms suitable for consideration as higher order language forms tailored to AFGWC processing needs.

The baseline specification suitable for use in developing a data-oriented language for AFGWC is available. The CODASYL data base task group has produced specifications for a data-definition language which should be an industry standard and specifications for a data manipulation language (which augments cobol) which can serve for guidance in the development of a data manipulation language to augment FORTRAN. The CODASYL data base task group recommendations for a data-oriented language are the result of a long and concerted effort by leaders in data management techniques. Their specification represents the best in current thinking langauge forms relevant to present-day hardware.

1.3.4 Developed Software (A34)

Three major software subsystems (master data base management, network control, and communication data routing) are integral to the design of the enhanced AFGWC architecture. All three of these subsystems will, to various degrees, be developed as custom AFGWC software packages. The following section addresses these three subsystems.

1.3.4.1 Master Data Base Management (A341)

The data base is composed of observational, gridded meteorological, and satellite-sensed parameters. It is the central storage of both the input and output fields of the analysis and forecast functions at AFGWC. The data base approach associated with the enhanced architecture is based on centralization of the data base with a main processor acting as the Master Data Base Manager which controls the simultaneous use of the data base by all of the main processors. In addition to the Master Data Base Manager there will be a backup data base manager which will be on-line and in a continuous monitoring posture; this data base manager has been called the "bull pen" data base manager. The computer program that provides this primary and redundant function is the master data base program. The master data base program must provide both data management and system interface functions.

The data management function provides the internal system data base function. The AFGWC data base structure, and management thereof, present some unique problems. The present system accommodates only one grid scale and treats all the others as exceptions. With the meso-scale support of tactical system (sometimes for prespecified targets), the data base must accommodate a variable grid structure. The parameter set associated with a single space time point will in the future have to accommodate more variables while allowing a wide variation in the number of variables represented at a single space point. An example would be the expansion of trend variables or trend statistics. The new data base management scheme must accommodate this type of expansion, however, the exact nature of this expansion is not at this point in time clearly defined. The data base management system must also provide the capability to extract selected fields in formats that are customized to the user needs.

The system interface function must provide all of the interface between the primary and back-up data base managers, the primary data base manager and the main processor environments and the primary data base manager and the mass storage facility. The interface between the primary and the main processor environments will exist as a direct communications link (between all unclassified processors) or a control-only link (between classified processors and the data base manager). The data base program must provide an optimum response to both interface type; the control-only request path from the classified processor will be somewhat more restrictive due to the limited volume of request parameters that can be transferred on this type of link.

1.3.4.2 Network Control Program (A342)

The network control program is the central scheduling and network manager for all components of the AFGWC architecture. The program will reside as the primary on a special access processor and as a combined backup on a second special access processor. The program will perform the following functions:

a. System Scheduling. This function will respond to scheduling requests; maintain status on all scheduled jobs and subsystem components; perform "look-ahead" analysis in order to maintain optimum system loading, flexibility, and responsiveness; and maintain system performance statistics.

b. Contingency Management. This program portion will provide system management in the event system failures occur; the backup network control program will respond to the failure of the primary by assuming the primary role and insuring a main processor is scheduled for replacement of the backup.

c. System Interface. This program portion will provide system interface of the upgrade processor for receiving scheduling requests and system/subsystem status; the control-only data path used for output of network control parameters to other system components; the network control console (output of status and action items; input of control parameters from the network controller).

d. Security Management. This subprogram will perform all management functions associated with the switching of components, upgrading and downgrading of processor systems, and all control of the data path authentication system.

1.3.4.3 Communication Data Routing (A343)

The communication data routing software will reside and execute in the line handler/decoder routers. The function of the data routing will selectively route all incoming messages according to security level. In performance of this function the line handler/decoder routers will be the only mixed mode security processors in the architecture. When messages are received on a specific security level communications line they are either (1) routed to the disk maildrop associated with the line handler/decoder router that received it provided the security level is the maximum level allowed on that line; (2) routed to the line handler/decoder router which interfaces with the disk maildrop which is at the security level of the incoming traffic or (3) the message is routed to the communication console for action by the communication controller, e.g., the header was unintelligible or the routing code did not agree with those of AFGWC. Outgoing traffic is retrieved from the maildrop and set up as outgoing traffic.

The data routing software is one of the two major software elements of the line handler/decoder routers; the other being the communication link handler which performs line protocol and transfer functions. The data routing software will be implemented on a non-homogenous set of line handler/decoder routers. Its design should be as modular and structural as is feasible to enable maximum use of design and code transferability.

1.4 TERMINAL INTERFACE (A40)

There is a wide variety of external communications that will be handled through the terminal interface of AFGWC. These range from analog transmission to data rates as high as 200 kilobits per second. These communications are portrayed in Figure 9.

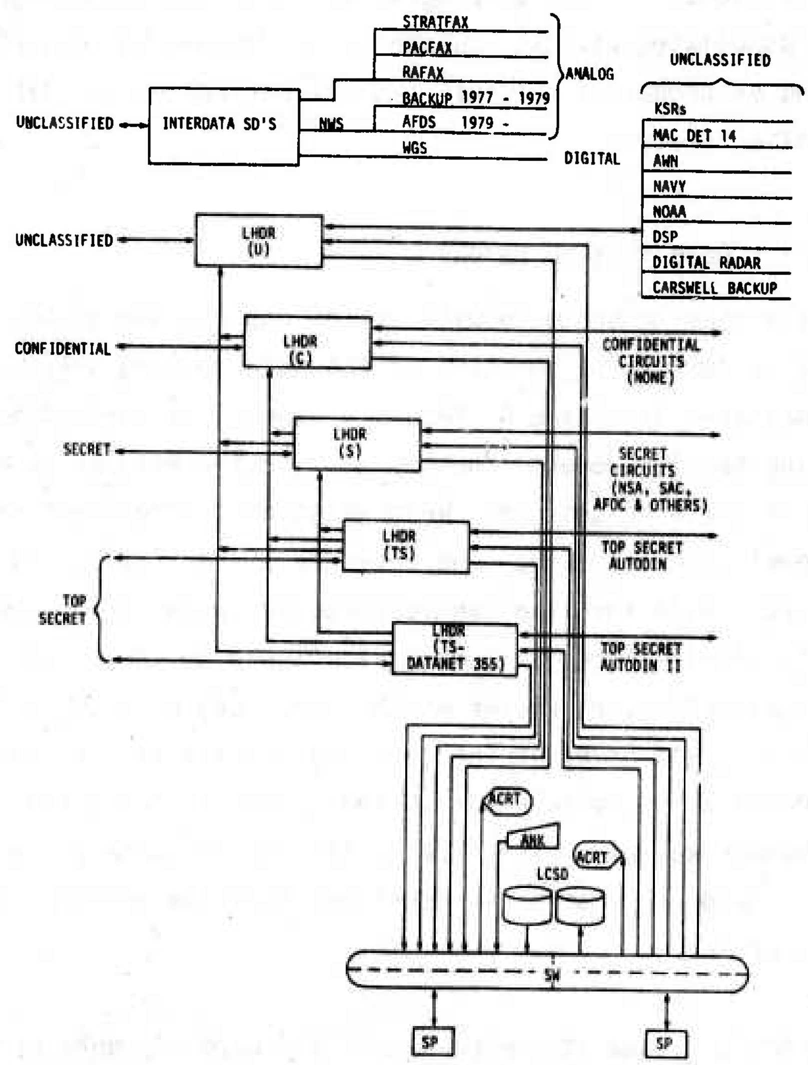

Figure 9. Terminal Interface

Each communication line coming into AFGWC is terminated in a modem or other device such as the Data Link Terminals (DLTs) for AUTODIN. Each of these then is connected to a line handler/decoder router. The line handler/decoder router is responsible for the following:

a. Line protocol and maintaining communications over each of the lines;

b. Formatting the message headers and messages so as to comply with the line protocol for the appropriate communications link;

c. Identification of incoming messages as to security level and message type;

d. Message recognition/validation, such as start of message and end of message flags;

e. Store and forward; and

f. Notification of network control of message existence and type for assignment of priority in establishing a queue within each security level.

The line handler/decoder routers must be consistent with the various levels of messages which can arrive or be originated at AFGWC: Unclassified, Confidential, Secret, Top Secret, SA1, SA2 and SA3. The philosophy followed in this design is to determine the classification of the message as soon as possible in the processing and to switch it into the appropriate path or if message classification cannot be determined, to output it on the communications console. This reduces the mixed mode processing and the exposure of one level of classification to other levels of classification in the data base and the computer programs. Doing this results in less chance for compromise due to either hardware error or to malicious action through software. In the same vein, output messages are not switched to the data line until the last possible minute. The switching function is independent, and is performed by an isolated hardware/software function.

The communications console is a vital element of this structure. It must interface with the line handler/decoder routers in order to receive and validate incorrect and garbled messages, both incoming and outgoing.

1.4.1 Normal Access (Classified) (A41)

There are Secret dedicated external data communications lines to SAC, NSA, and other customers. The AFOC line will also be upgraded to Secret in the future. In addition, both the current AUTODIN and the future AUTODIN II will carry information through Top Secret and SPECAT. It is particularly important that the various categories of security classification be separated as soon as possible as they enter AFGWC to minimize the possibility of security violation. All unclassified information coming in or going out over the various classified lines, passes through a disk interface box retained at an unclassified level. There is an indirect interface with the main processor through a disk system which is also maintained at the unclassified level.

The dedicated circuits which are designated for Secret information first interface with the line handler/decoder router. This line handler/decoder router determines the classification of the incoming data and routes it to the appropriate disk interface which is maintained at the proper security level: Unclassified, Confidential, or Secret. Each of these disk interface boxes interfaces indirectly with a main processor via a disk system retained at the same security classification level. The current AUTODIN lines are connected to a similar type of line handler/decoder router. Again, this unit determines the security classification of the incoming messages and routes it to the appropriately classified disk interface which is Unclassified, Confidential, Secret, or Top Secret. These are the same disk interface boxes used by the line handler/decoder router connected to the Secret lines with the addition of a disk interface box at the Top Secret level tied to a main processor via a disk system at the security level.

With the advent of AUTODIN II, a Datanet 355 computer will be installed which acts as a line handler/decoder router and performs the same functions of determining the classification of the data and routing it to the corresponding disk interface box as previously described. After AUTODIN II becomes operational, the current AUTODIN lines are to be phased out and the line handler/decoder routers associated with the current AUTODIN will no longer be required.

1.4.2 Normal Access (Unclassified) (A42)

Most of the external data communications lines are in this category. Conventional data and astrogeophysical data is received from the Carswell ADWS, via the Automated Weather Network. Dedicated circuits are provided for the National Oceanic and Atmospheric Administration (NOAA), Defense Support Program (DSP), MAC Detachment 14, Navy Fleet Numerical Weather Center, plus 17 additional ASR/KSR circuits. AFGWC must maintain the capability to backup the Carswell ADWS, and, beginning in FY 80, Digital Radar Data will be an additional input.

All of the input information handled by the unclassified communications lines is received by a line handler/decoder router maintained at the unclassifed level Network control decides which main processor will process which type of unclassified data, thus determining which combination disk will be used. The line handler/decoder router then passes the Unclassified data to the appropriate disk controller.

Outgoing Unclassified data to be transmitted over the Unclassified lines will follow the reverse path.

1.4.3 Special Access (A43)

Three line handler/decoder routers provide the interface with the special access circuits. Data are passed to the appropriate disk controller for reading into a combination disk.

1.4.4 Satellite Data (A44)

Satellite primary and special data are ingested through the satellite support processor. This processor consists of a mini computer capable of handling the ingestion of data from all supported vehicles. The satellite support processor is identical to the forecaster support processor.

The satellite support processor is capable of handling up to six DMSP links from the DMSP Site 3 Ground Station plus data from the GOES and TIROS-N satellites through their respective dedicated ground stations. Upon receipt of this data, the satellite support processor performs data cleaning and formatting functions as required by the particular satellite program before writing the data onto mass storage in the proper format.

AFGWC must distribute satellite imagery products to a variety of users in a timely and accurate manner. This will be accomplished by the Satellite Imagery Distribution system (SID). The satellite support processor will interface with the SID Console as well as the communication links utilized for SID.

1.4.5 Routing (A45)

1.4.5.1 Line Handler/Decoder Router (A451)

In the architectural design there is a requirement for a line handler/decoder router computer which interfaces with all lines of a given maximum security level. In some instances the computers have already been specified (for example, the Data-Net 355 for AUTODIN II). The functions to be performed by the line handler/decoder router include:

a. Line specific interfaces which for non-intelligent line termination includes all line protocol and syncronization tasks and for lines with intelligent terminals it includes prespecified interfaces.

b. System specific message decoding to determine message security level and to ensure message begin and end conditions.

c. Routing which includes selecting a channel corresponding to the correct security classification, authentication of the channel, gaining access to the appropriate disk on which the message is to written and finally writing the message onto the disk.

d. Interfacing with the communications console. When it recognizes that messages are to be manually processed or that security checking is not satisfactory, it automatically routes the message to the communications console.

1.4.5.2 Satellite Data Router (A452)

The Satellite Data Router function resides in the satellite support processor. It receives and identifies the data from a particular type of satellite (DMSP, GOES, or TIROS-N). The data is then input and buffered to the satellite ingest dedicated mass storage where it is written on one of four dedicated disk subsystems.

1.4.6 General (A46)

1.4.6.1 Protocol (A461)

Line protocol affects the complexity of the software required to operate on the incoming messages and format the outgoing communications. In addition, the multitude of external links use different protocols which compound the problem. A standardized message protocol for all external AFGWC messages would greatly simplify the communications software.

On all the existing communications links, the protocol has already been established and is in operation. Therefore, little can be done to change it except for future possibilities with new requirements. However, on new systems such as AUTODIN II, there is a possibility that AFGWC can influence protocol to be established on the line. This would be particulary important with high data rates such as the AUTODIN II at 50 kilobaud and even more so on the digital radar which is expected to have data burst rate of 200 kilobaud. There is a strong effect of protocol on the software involved in the communications processor.

1.4.6.2 Control (A462)

No capability will exist for external sources to generate software instructions or to activate any software instructions within the AFGWC system.

1.4.7 Other (A47)

1.4.7.1 Teletype (A471)

A dedicated line provides teletype data directly to the SESS area from the Carswell ADWS. This is a continuing function. In addition, a stand-alone TTY circuit between WPE and HQ AFCS, which will include a paper tape capability, will still be employed. Also, TTY circuits for direct communication between WPF and the COMET networks will continue to be used as alternates to the COMET links input to AFGWC via Carswell.

1.4.7.2 Facsimile (A472)

A centralized CONUS weather facsimile facility interfaces with all external facsimile circuits. This automated facility is known as the Weather Facsimile Switching Center (WFSC). The WFSC replaces the manual facilities at AFGWC and at the National Meteorological Center, Suitland, Maryland. The WFSC receives digitized weather facsimile maps. These maps and charts are relayed to users on a predetermined schedule. The WFSC is a store and forward system, where products are produced in digital form and converted to an analog signal compatible with customer facsimile recorders. An intermediate storage device is used for map storage. A schedule of transmission requirements is kept on this same storage device. The WFSC transmits maps and/or subsets of maps to subscribers as specified in the predetermined transmission schedule. These transmission schedules are executed automatically under network control.

Two new Interdata Model 50 type mini computers are to be procured for installation at the WFSC. In addition, the Interdata Model 50 currently installed at the National Meteorological Center is to be relocated to the WFSC and will function as a program assembler and will provide backup to the other two Model 50s.

The Interdata Model 50 interfaces to the current analog facsimile circuits which continue in existence. These are the STRATFAX, PACFAX, and RAFAX. In addition, this provides a backup facsimile capability for the National Weather Service during the 1977 to 1979 time frame. After that period, AFGWC will interface with NWS through the Automation of Field Operations and Services (AFOS) network. The Interdata 50 will also be the interface to the digital weather Graphics System when WGS comes into operations in 1976.

Within AFGWC, the forecasting consoles will have a data path to the Interdata 50. The facsimile products prepared at the forecasting consoles are digitized and passed to the Interdata 50 for storage until the proper time for transmission to the external facsimile circuits. In addition, manually-prepared products within AFGWC are hand-carried to the WFSC to be digitized and again stored on the intermediate storage device until the proper time for transmission over the appropriate facsimile circuit.

1.5 CONSOLES (A50)

In most cases, an interface processor will be associated with each console, coordinating functions between hardware components. These mini computers will in turn be connected to support processors which will link the consoles of similar classification and application to the main processor system.

The design of all consoles will allow for as much modularity of components as is possible, so they may be added or deleted as requirements dictate.

1.5.1 <u>Mission Support</u> A51)

The mission support consoles are characterized by the autonomous control they exert over either a segment of the system or the entire system.

1.5.1.1 Network Control (A511)

Network control shall be provided two alphanumeric CRTs and two alphanumeric keyboards. A network switch panel will allow for switching of the variable access perimeter and the primary and backup support processors. A configuration display panel will provide network control with information necessary for adequate monitoring of support and main processors, disk systems, line handler/decoder routers, consoles and other subsystems. Additional selector panels will be provided for data base and network control processor selection. (See Figures 10 and 11).

1.5.1.2 Operations (A512)

Each operations console will be provided with two alphanumeric CRTs and two alphanumeric keyboards. These components and a status panel will be used to determine system configuration and monitor the status of equipment, operation, schedule, user authorization, system file, and data base maintenance. (See Figures 12 and 13.)

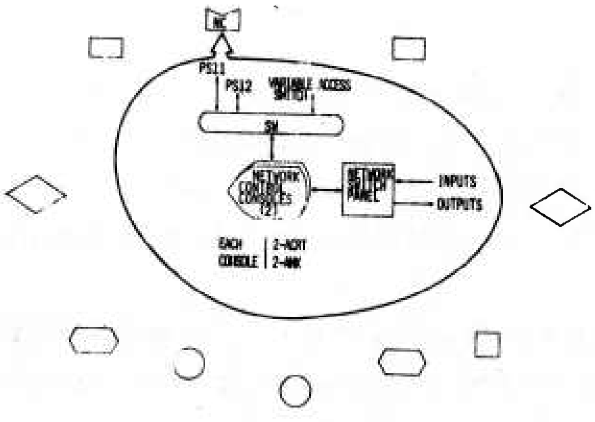

Figure 10. Network Control Schematic

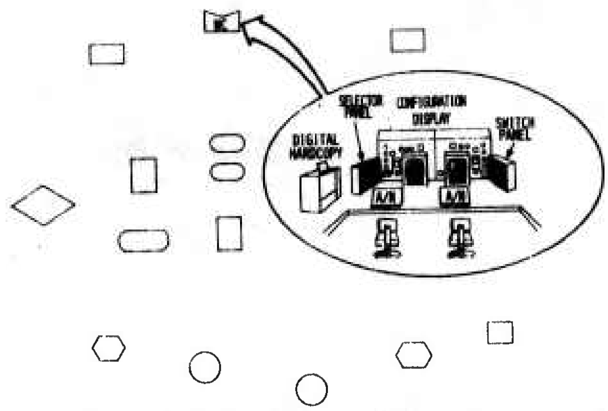

Figure 11. Network Control Hardware Components

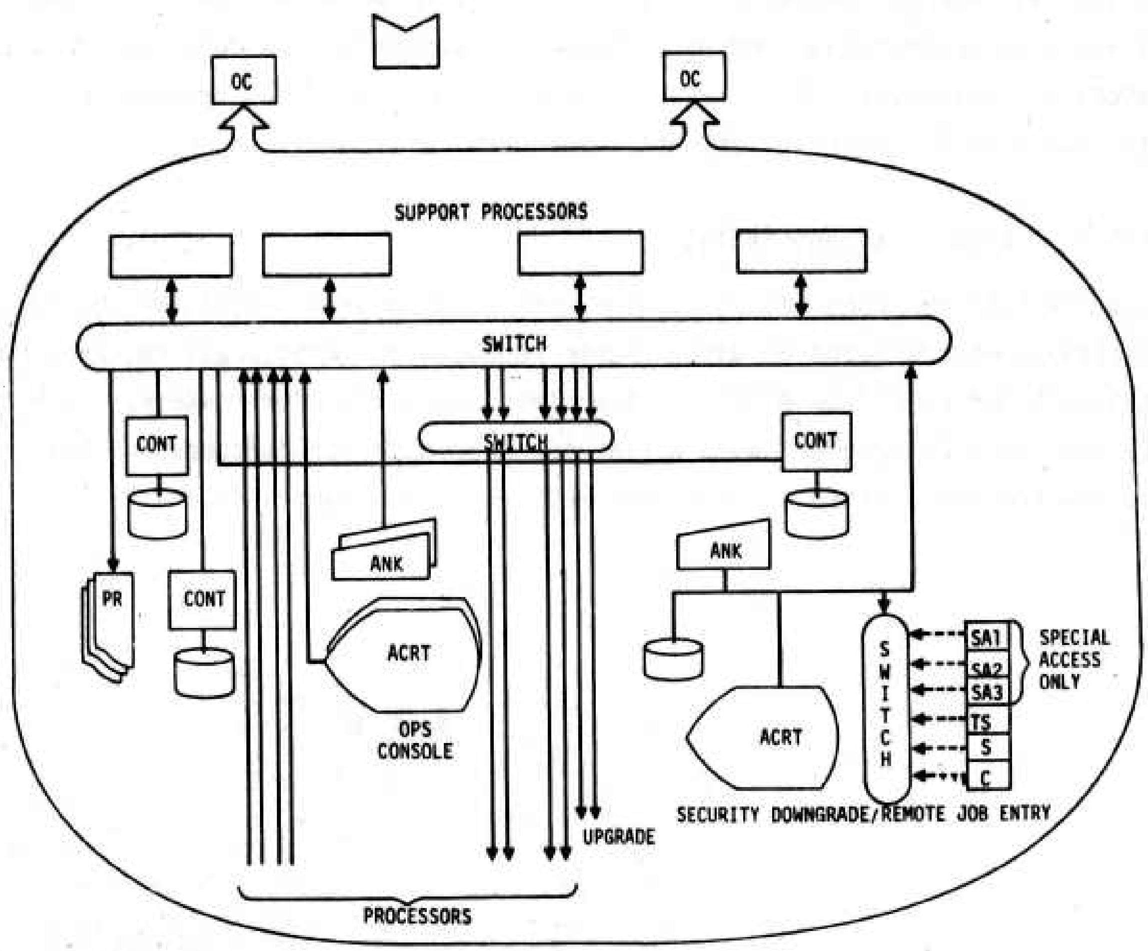

Figure 12. Operations Center Schematic

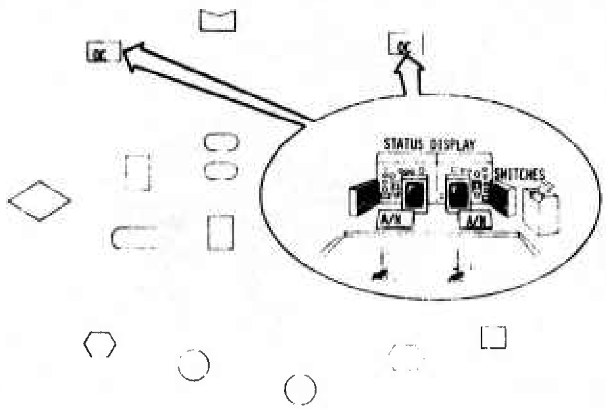

Figure 13. Operations Control Hardware Components

1.5.1.3 Security Downgrade (A513)

The security downgrade/remote job entry console will contain an alphanumeric CRT for data presentation and an alphanumeric keyboard, low capacity storage devices for temporary data archival, a low speed printer for messages and data sets, and a card reader for job entry purposes.

1.5.1.4 Communications (A514)

The communications consoles associated with each security perimeter shall use one alphanumeric CRT and an alphanumeric keyboard to monitor all messages being received by or sent from AFGWC via the line handler/decoder routers. Each console will also be provided with a slow speed printer for hardcopy and low capacity storage devices as a storage medium. (See Figures 14 and 15.)

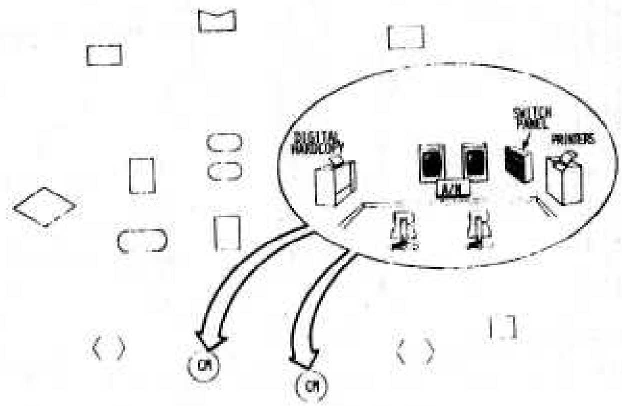

Figure 14. Communications Console Hardware Components

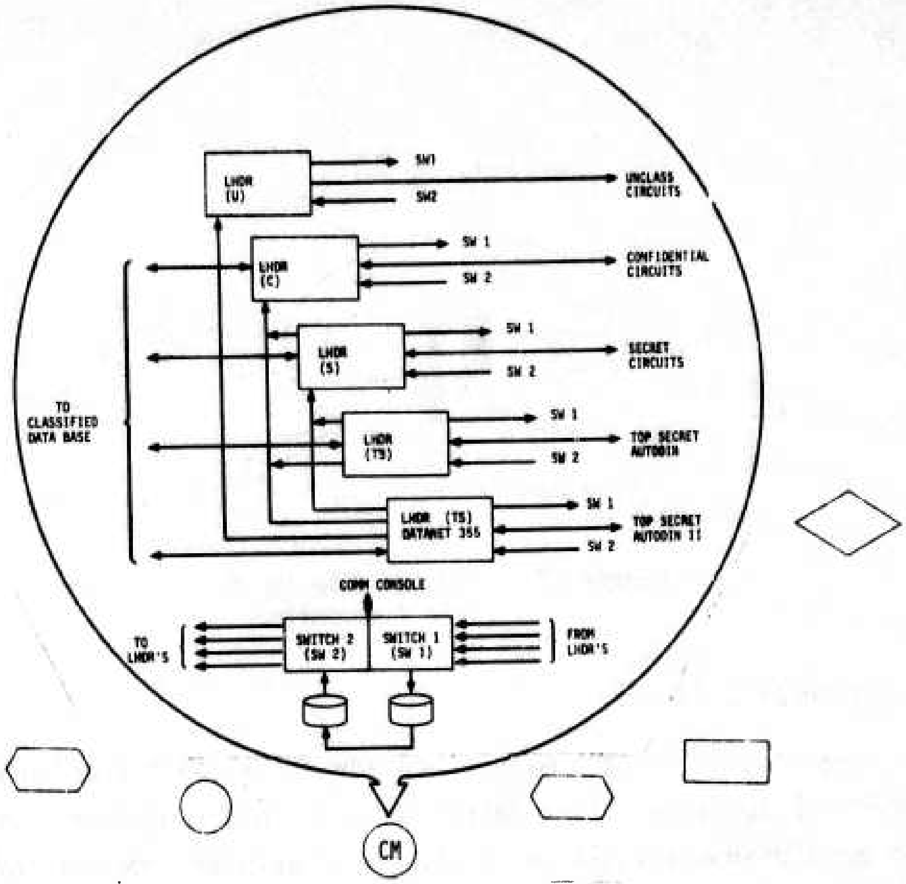

Figure 15. Communications Subsystem Schematic (Normal Access)

1.5.1.5 Satellite Imagery Dissemination (A515)

The Satellite Image Dissemination (SID) console will be provided with a black and white high resolution CRT for quality control of satellite data, an alphanumeric CRT for message generation and receipt, and an alphanumeric keyboard. This equipment will be directly interfaced with the satellite support processor. (See Figures 16 and 17.)

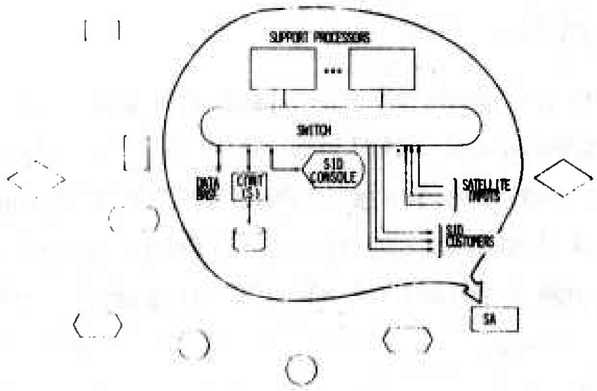

Figure 16. Satellite Data Processing Schematic

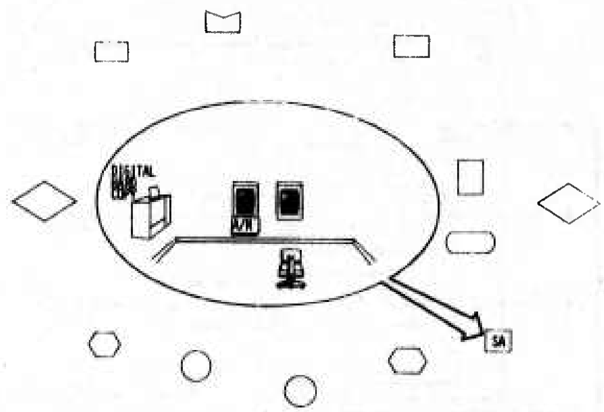

Figure 17. SID Console Hardware Components

1.5.1.6 Maintenance (A516)

The maintenance console on each main processor system will provide all the resources necessary for stand-alone maintenance of that processor system. This may include an alphanumeric CRT and keyboard, a printer, and card or tape handling equipment. This equipment will also be adequate to allow the assumption of computer operation functions in the event of a failure of the operations console.

1.5.2 Mission Operations (A52)

The mission operations consoles provide general and special services to various users.

1.5.2.1 TAF/METWATCH (A521)

The TAF/METWATCH console will provide two black and white high resolution CRTs for display of weather charts and satellite data and two alphanumeric CRTs for editing of bulletins and data lists. The TAF/METWATCH console will have two alphanumeric keyboards, a lightpen for data modification and access to a device which will produce hardcopy versions of all CRT displays. (See Figure 18.)

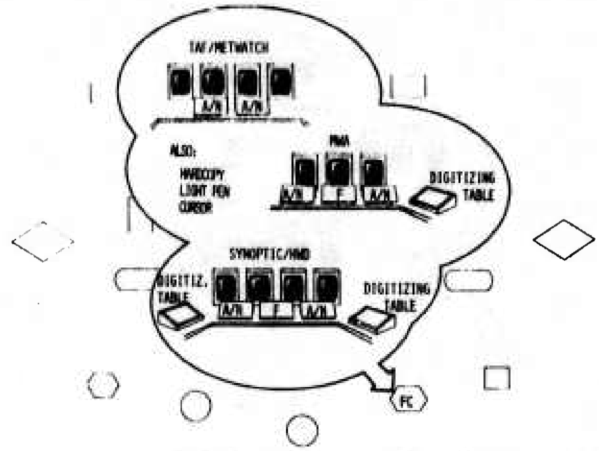

Figure 18. Forecaster Console Hardware Components

1.5.2.2 Military Weather Advisory (A522)

The military weather advisory console will be made up of two black and white high resolution CRTs and one color CRT for data presentation. Two alphanumeric keyboards, one function keyboard, and a digitizing table will be provided as a means of modifying or entering data to the system, primarily the CRTs. The military weather advisory console will have a lightpen for data modification and access to a device which will produce hardcopy versions of all CRT displays. (See Figure 18.)

1.5.2.3 Synopticion (A523)

The synoptic console will have essentially the same components as the military weather advisory console with an additional color CRT and digitizing table. (See Figure 18.)

1.5.2.4 Forecaster (Special Access) (A524)

The forecaster consoles dedicated to forecaster functions will have three CRTs for data presentation - one alphanumeric and two black and white high resolution (to be used especially for displays of satellite data). These CRTs will be controlled by two keyboards, one alphanumeric and the other for special functions. The special access forecaster console will have a lightpen for use in data modification and the ability to produce hardcopy versions of all CRT displays. A digitizing table will provide a means of high resolution data modification, especially that displayed on CRTs. (See Figure 19.)

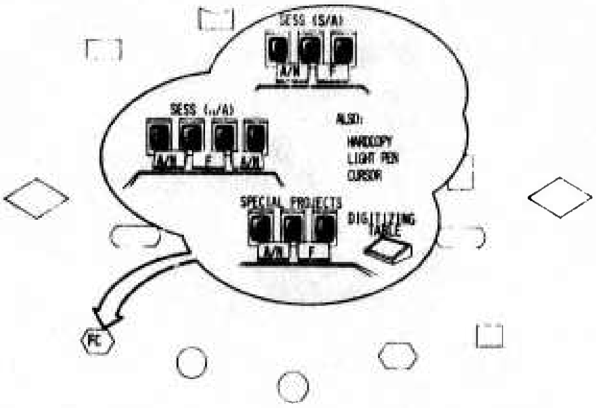

Figure 19. Forecaster Console Hardware Components

1.5.2.5 SESS (Special Access) (A525)

The special access SESS console will have the same capabilities and components serving the geophysical forecaster in the normal access perimeter. This means the normal access SESS console has an extra alphanumeric CRT and keyboard which serves the data base monitor not found in special access. (See Figure 19.)

1.5.2.6 SESS (Normal Access)(A526)

The forecaster consoles dedicated to forecaster functions will have: three CRTs for data presentation - one alphanumeric and two black and white high resolution (to be used especially for displays of satellite data); two keyboards - one alphanumeric and the other for special functions. The special access forecaster console will have a lightpen for use in data modification and the ability to produce hardcopy versions of all CRT displays. A digitizing table will provide a means of high resolution data modification, especially that displayed on CRTs. (See Figure 19.)

1.5.2.7 Quality Assurance (A527)

Two alphanumeric CRTs and two alphanumeric keyboards will provide the quality assurance console with the ability to monitor and control the quality of the AFGWC data base. A hardcopy device and lightpen will be available for data archival and modification respectively.

1.5.2.8 Programmer (A538)

Programmer consoles will support normal software development and maintenance as well as studies and analysis functions. They will be located in both the normal and special access perimeters and will require an alphanumeric CRT display and keyboard. There will be audio alarms and status indicators at the programmer consoles to indicate the availability of required resources. The ability to produce a hardcopy version of CRT displays will be provided. The programmer consoles used for studies and analysis functions will be equipped with a plotter in addition to the other components. (See Figures 20 and 21.)

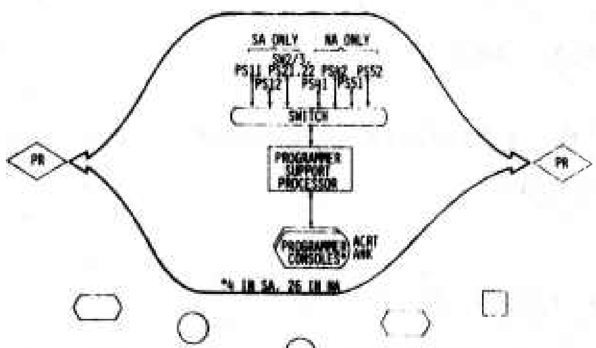

Figure 20. Programmer Support Schematic

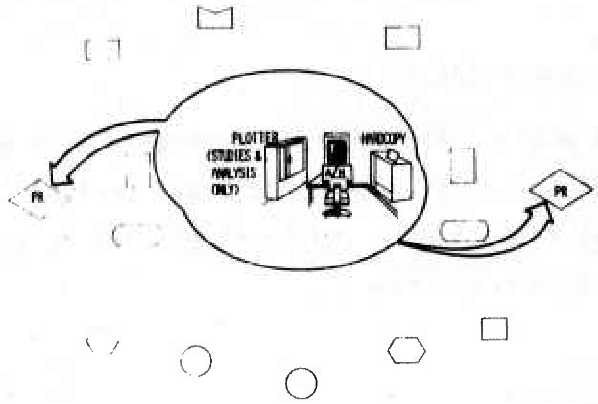

Figure 21. Programmer Console Hardware Components

1.5.2.9 Special Operations (A529)

Forecasting functions associated with special operations require both an alphanumeric and black and white high resolution CRT, plus an alphanumeric keyboard and a second keyboard for special functions. This console will also require a card reader, a printer, and access to a device which will produce hardcopy versions of all CRT displays.

1.6 DATA INPUT/DISPLAY (A60)

This category includes those hardware components used for data manipulation primarily found at consoles.

1.6.1 Rapid Response Visual (A61)

The rapid response visual displays provide console operators with displayed information (tabular, graphic, and imagery) without the normal time lag associated with hardcopy devices. Three CRTs are classified under this heading: alphanumeric, color, and high resolution black and white. All the CRTs should have the full range of ASCII characters, meteorological and special symbols, and program control functions. The high resolution CRT will have a 63 gray shade capability. All CRTs should be of a medium size with the following resolution:

a. Alphanumeric - 24 lines x 80 characters/line

b. Color - 512 x 512

c. Black and white, high resolution - 1024 x 1024

1.6.2 Documentary Visual (A62)

Documentary visual devices include those which will be used to produce information (tabular, graphic and imagery) in a hardcopy form. Specifically, they consist of a programmable character printer, a 2,000 line per minute standard printer, a plotter with an active area of about 2' by 3' and a device which will produce black and white hardcopy of CRT displays. All these devices should be able to reproduce the full range of ASCII, meteorological, and special symbols.

1.6.3 Miscellaneous Status (A63)

There are two miscellaneous status displays which will provide network system and subsystem status to the control areas of AFGWC. A configuration display panel will provide the network control console all the status information necessary for the performance of its normal and fall-back responsibilities. A security level display will be provided to all operation center printers, tape devices and other devices that may have occasion to be configured at various security levels.

1.6.4 Selection (A64)

This category includes those components designed to provide a major switch or selection capability. Specifically, this consists of a network switch panel for manipulation of the variable perimeter and support processors, a unit switch panel for tape and disk units, a data base selector panel for assigning data base associated components, and a processor selector panel. With the exception of the unit switch panel, the others shall be remoted to the network control console.

1.6.5 Miscellaneous Communications (A65)

Miscellaneous communications currently includes only the card reader/punch. This device will be capable of handling cards at a speed of at least 1000 cards per minute.

1.6.6 Manual Inputs (A66)

Manual input components provide console operators with the ability to manually enter instructions or enter or modify data in the AFGWC system. Associated with the CRTs are the alphanumeric and fixed function keyboards primarily used to enter instructions. A lightpen and magnetic cursor provides the primary means of entering new data and modifications to information displayed on the CRTs. They are also the primary tools to be used on another manual input device: the digitizing table. This table should have a minimum active area of 2' by 3' and an effective nominal resolution of 2000 by 2000 positions.

1.7 PERSONNEL (A70)

A distinct need exists to automate the operations of AFGWC as much as is feasible. This is especially important in light of the possibility of reduced manning levels and the need to accommodate ever-increasing user requirements. To fill this need, the concept has been developed of automated work center consoles dedicated to specific man/machine interface functions. These consoles and the personnel associated with them are classified as belonging to one of two categories: mission support or mission operations. This will be presented for consideration here under those two headings, followed by the related topic of training.

1.7.1 Mission Support Positions (A71)

Mission support centers are characterized by the autonomous control they effect over either a segment of the system or the entire system. Specific consoles include:

a. Network control,

b. Operations,

c. Security,

d. Communications,

e. Satellite imagery dissemination, and

f. Maintenance.

Consoles dedicated to all these functions will each provide two personnel positions except for the security position. In each of these two man teams, activities will be shared between skilled technicians of approximately equal capabilities with one acting as the senior man in charge. (These functions, except for security downgrade, are judged to be sufficiently complex to warrant two men per console to adequately monitor and control required consoles. When manned as a backup to the operations console they will each require two personnel. When being used for maintenance functions they will be manned by military and/or civilian personnel as the situation demands. As might be expected, however, the maintenance consoles will remain unmanned throughout most operations. The personnel requirements for mission support positions (along with mission operations and training) are summarized in Table 1.

1.7.2 Mission Operations Positions (A72)

Mission operations centers provide general or special services to various users in both the normal and special access perimeters. Specific consoles include:

Table 1. Console Personnel Allocation.

Work Center Category	Function	No. of Consoles	Personnel Per Console	Slots Per Shift	Total Slots	Primary GWC Org
Mission Support Positions	Network Controller	1	2	2	10[1]	WPD
	Operations Controller	2	2	4	20	WPD
	Security Controller	2	1	2	10	WPD
	Communications Controller	2	2	4	20	WPD
	SID Controller	2	2[2]	4	20	WPP
	Maintenance	5	<1[3]	2	10	WPD
Mission Operations Positions	TAF/METWATCH	15	2	30	150	WPF
	Military Weather Advisors	1	2	2	10	WPF
	Synoptician	5	3	15	75	WPF
	Forecaster (special/access)	3	1	3	15	WPJ
	SESS Forecaster (normal/access)	1	2	2	10	WPE
	SESS Forecaster (special/access)	1	1	1	5	WPE
	Quality Assurance	1	1	1	5	WPD

Table 1. Console Personnel Allocation (Continued)

Work Center Category	Function	No. of Consoles	Personnel Per Console	Slots Per Shift	Total Slots	Primary GWC Org
Mission Support Positions (Cont)	Programmer	30	---[4]	---	---	WPD, WPP, WPA
	Special Operations	2	2	4	20	WPF
Training	Data System	---[5]	---	---	2	WPD
	Console Position	---[5]	---	---	1	WPD
	Programmer	---[5]	---	---	2	WPD

[1] Personnel are assumed to be required for five shifts per day.

[2] Plus use by WPD and S & A personnel.

[3] An average loading of two men for the five maintenance consoles is assumed.

[4] Although these consoles will be used by programmers, use will be non-scheduled and personnel will not be assigned to individual consoles.

[5] Only personnel totals are indicated since training will most likely be accomplished with available personnel during normal work day.

a. TAF/METWATCH,

b. Military weather advisory,

c. Synoptic,

d. Forecaster (special access),

e. SESS forecaster (normal access),

f. SESS forecaster (special access),

g. Quality assurance,

h. Programmer, and

i. Special operations.

The majority of these consoles (the first six and the last one) are dedicated to meteorological forecasting functions and therefore require personnel adept in that discipline. The size of individual forecasting teams will vary from one type of console to another (see Table 1.) but will generally consist of personnel of similar ability and rank. One exception involves the normal access SESS forecaster where the two personnel assigned will be a data base monitor and geophysical forecaster, positions requiring different backgrounds and levels of knowledge. The quality assurance controller will be responsible for a continued level of excellence in the AFGWC data base. He does not need a forecasting background but will require a knowledge of statistics and data base structure. No manning has been associated with programmer consoles since they are only tools, will be used on periodic schedules, and do not have specific personnel assigned to them.

1.7.3 Training (A73)

Personnel will be required for training in the following topics:

a. Data system,

b. Console positions, and

c. Programming.

A routine schedule will be selected to insure that appropriate personnel are given the proper instruction. A total training force of five personnel will be needed for this eductional function. The training assignments suggested by Table 1 are made according to the complexity of the areas. Study of the data system and programming techniques should require more time and careful attention to these console operations. This is particularly true since a good portion of console operation training must by its nature be done on the job.

1.8 MANAGEMENT (A80)

1.8.1 Control (A81)

1.8.1.1 Organization (A811)

An assessment has been made of the AFGWC organizational structure by evaluating the impact of major new requirements on AFGWC operations. Consideration has also been given to the effect of the new data system architecture, including the implementation and integration process, on staff and line operations personnel. Most 1977-82 requirements can be accommodated with modest changes to the current AFGWC organizational structure (see Figure 22). Greater emphasis should be placed on acquisition and integration activities in the operations staff (now recommended to be reporting to the commander of all AFGWC operations), on the input and output of satellite data in the current Data Acquisition and Processing Branch, and on new responsibilities in the Data Automation Branch. While the nature of activities within other branches may be greatly affected by the new architecture, these new tasks can be accomplished within current organizational frameworks.

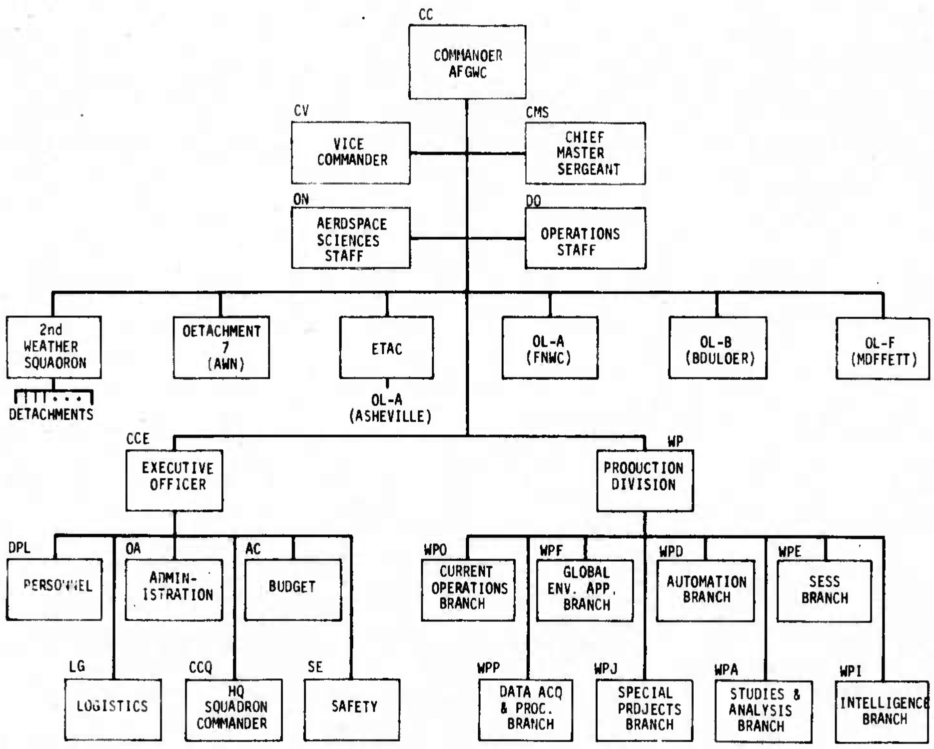

Figure 22. Current AFGWC Organizational Structure

Except for DO, no consideration was given to restructuring of AFGWC liaison or staff organizations. Most of the functions of these units are employed to maintain administrative efficiency within AFGWC, and do not require changes as a result of a new data system architecture. DO, however, will realize an expanded role as new data system components are acquired, integrated, and validated. Thus, as illustrated in Figure 23, distinct responsibilities should be set up within DO for acquisition/integration and configuration control (configuration control is often structured as one subset of integration activities, but since these kinds of hardware and software maintenance activities are so critical to AFGWC, this function should be given key prominence in the DO staff). The day-to-day functions of Production Division operations support, as well as requirements analysis and planning activities, will remain as primary responsibilities of DO, as shown in Figure 23. In keeping with this new long-term emphasis on data system integration, a suggested new title for this entity is the "Operations and Integration Staff".

It should be noted that in accomplishing software configuration control, DO will be involved with both in-house and outside contractor personnel. DO will therefore be in the position of enforcing established Air Force configuration management guidelines on contractor personnel, as well as controlling the production and maintenance of in-house software. All products should be documented, produced, and maintained according to a consistent set of standards, with the enforcement of these rules being the responsibility of DO. To enable this configuration control and contractor management, DO may require a staff that is more oriented towards the computer sciences and systems engineering. This increased emphasis on computer systems analysis backgrounds will not only ensure the success of computer systems implementation, but will also further guarantee the success of other related long-term planning efforts.

Most of the Branch organizations in the Production Division will not necessarily undergo realignment because of the new requirements or because of a new architecture. While some requirements and proposed hardware and software components may profoundly affect the ways in which activities are accomplished, these tasks can, for the most part, still be done under current personnel hierarchies. The

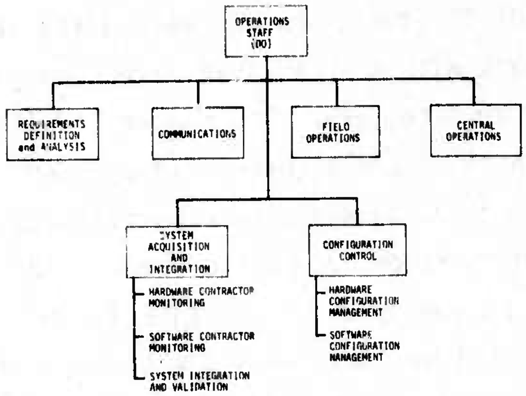

Figure 23. Operations Staff Organization

Studies and Analysis Branch, for example, will be involved in the development of numerous new models over the next several years, but as is the case now, there will be much overlap between computer scientists, mathematicians, and meteorologists in this area, many of whom will simultaneously be involved with more than one computer program. A rigid structuring, therefore, of this branch does not appear to be justified.

The same is true of the Special Projects, Space Environmental Support, and Intelligence Branches: activities within these organizations, even considering the impact of the new architectures, should still be feasible within current organizational frameworks. Similarly, while forecaster consoles, new models, and new user requirements may greatly change the methods by which observers and forecasters execute their duties, these methods should be accommodated by the present structure. That is, teams of observers and forecasters, generally allocated to geographical areas, should still be a reasonable way to operate.

The Data Acquisition and Processing Branch, however, can benefit from some reorientation at the lower levels to reflect the impact of satellite data input and output requirements. As shown in Figure 24, Operations and Program Development sections are logical divisions of responsibility within the Branch, but within each section, processing of new data sources and the semi-automated dissemination of this processed data should receive special attention. A more descriptive title for this Branch, "Satellite Data Processing Branch", is suggested.

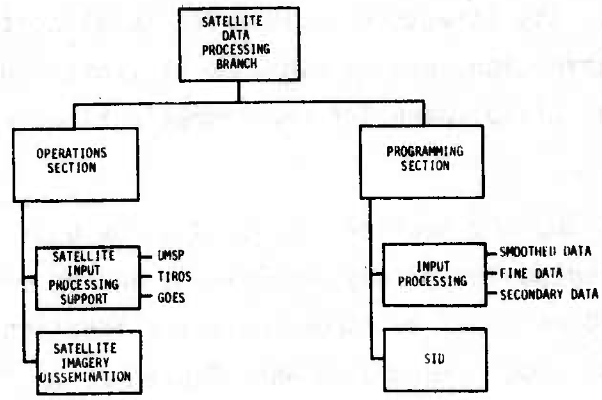

Figure 24. Revised Data Acquisition and Processing, Branch Organization

Figure 25 illustrates several suggested changes to the Data Automation Branch structure:

a. Machine Operations Section. This new structure reflects the advent of numerous Automated Work Centers that will be used by machine operations personnel.

b. Computer Flight Plans Section. No changes anticipated--this function will take on more importance with the influx of new CFP requirements in the 1977-82 time frame.

c. Mission Applications Section. This section has been structured to emphasize some of the major new software development and maintenance efforts that will be required.

d. Environmental Data Systems Section. No basic changes, although this section's substructure has been set up in part to emphasize the large development efforts that are expected in data base software and in executive program conversion.

e. Data Handling Section. This entity was retitled from its former name of "Data Processing Section" to more accurately describe its proposed functions. Its structure is intended to allocate personnel to the coding, conversion, and maintenance of front-end decoders and to the development of software for new communications processing functions.

f. Operations Support Section. This is a new unit within this Branch, and is oriented toward any development and/or maintenance that will be required of AFGWC to accommodate the functions of the system control and system support Automated Work Centers. In the more distant future, this group could develop software for other specialized operations, such as unique support for the Interactive Processing and Display System, that might supplement contractor efforts.

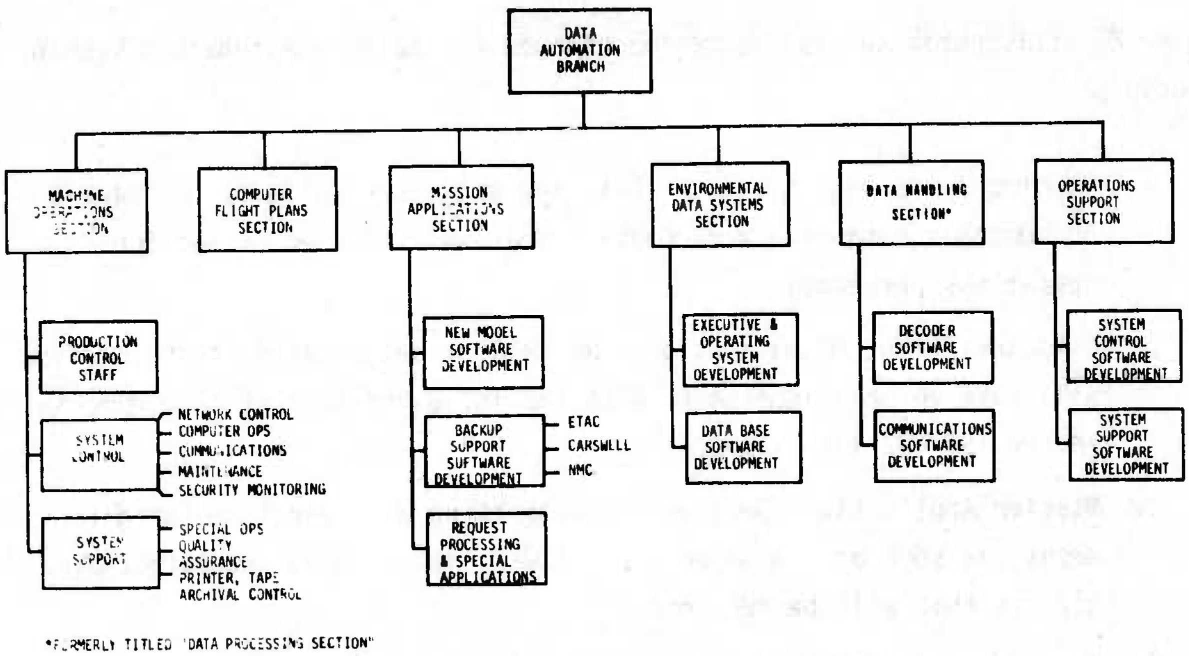

Figure 25. Revised Data Automation Branch Organization

Two technically-oriented organizations that are new to the AFGWC structure are the Aerospace Sciences Staff which will report directly to the commander and work in close conjunction with the Studies and Analysis Branch and the Current Operations Branch which will closely monitor the production efficiency of the Division (especially the operations of the Global Environmental Applications Branch) by working with all line organizations. Both of these units will further serve to guarantee the success of the AFGWC mission through efficient advanced analyses and more thorough quality control.

1.8.1.2 External Control (A812)

Very early in the architectural study it was decided that AFGWC should be considered as a service organization under its own control which would process requests for services but would not in general be a real-time arm of external organizations. The exceptions to this, of course, are the SAC requirements which currently exist and the future real-time response to the WWMCCS requests.

1.8.1.3 Network Control (A813)

External requests have considerable influence on the detailed sequence of processing and therefore on resource utilization. A key example is flight plans. We have sized the basic system such that four processor subsystems can handle the peak load operating in a dual processor configuration. This means that the requirements can be met no matter where the variable perimeter is allocated. There is further pad in the system since computers operating as uniprocessors have fundamentally more processing power than the equivalent half of a dual processor system. The dual processor system, however, does afford a higher reliability based on the advantages of a tightly coupled processing capability. The tightly coupled processors also can react somewhat more efficiently using job segmentation. Theoretically, under the worst possible configuration, there is still a processor that can be allocated to an additional job introduced into the processing queue. We feel this affords the capability to protect against heavier loading than was anticipated by us in our analysis of AFGWC.

Operational responsibility for the data system will belong to a network control function which has been identified as a single position for control of both the special and normal access areas. It has been decided that the network controller is the supervisor for all operating positions and makes the final decisions on all resource allocation. The network control function is illustrated in Figure 26.

The function will be physically located in the special access area and will control all components. The network control console is the hardware that monitors scheduling and resource allocations. These tasks are in reality performed by an on-line network control processor.

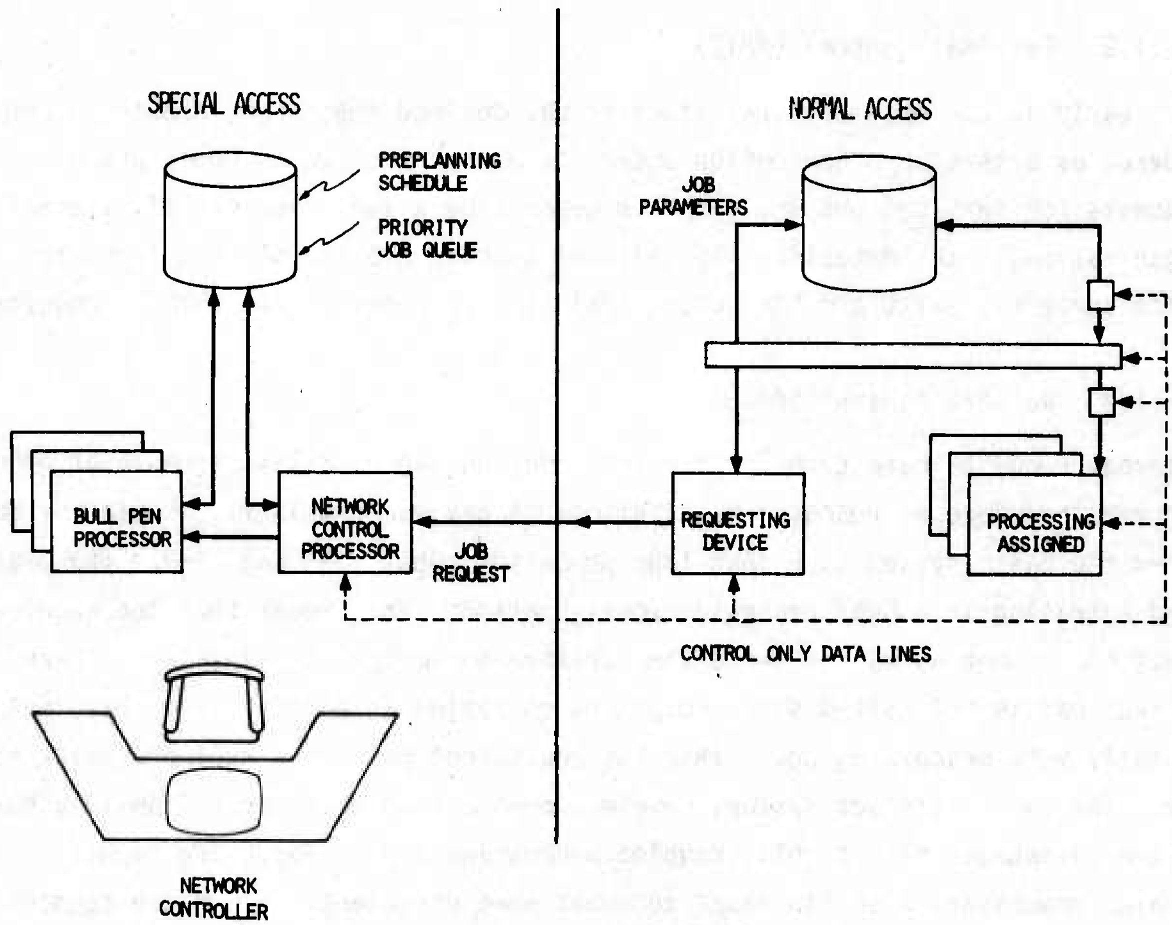

Figure 26. Network Control

The operational procedure is accomplished as follows: a device which is requesting services makes a job request through the network control processor which incorporates requests with preplanned scheduled requests in a prioritized job queue. The priorities change as a function of time as requirements become overdue. Job parameters are put onto the disk at the appropriate security level. The processor then indicates to the computer assigned the particular function that there is a job waiting in the job parameter file. Resources are allocated as required, based on maintenance and malfunction situations. If a reconfiguration or upgrade of components is necessary, this is accomplished by the network control processor. When the job is completed, network control is notified, who then notifies the requesting component.

What activities take place when a processor running at an Unclassified job level is called in to accomplish a Top Secret job and then is downgraded again to Unclassified? The first thing that we know about the processor is that it runs connected to the control units of both Top Secret and Unclassified disks. When network control gives it an unclassified task to do, the executive and support software know automatically through executive data base definition what logical configuration is to be utilized, i.e., the classified disks are to be ignored and the machine is to honor no classified requests nor is it to send out any information to these classified disks.

In the event that a system program failed and violated the software protect feature which keeps this communication from taking place, the worst that could happen would be that unclassified data would be sent harmlessly onto the classified disk. If the unclassified data were read by a classified machine, it would be encrypted at the level of the interrupting classified computer which would immediately recognize it as invalid data and cause the transmission to cease. The Unclassified disk linkup only serves to process any Unclassified jobs given to the processor by network control; the actual logical disks used for a particular job are identified in the job control parameters.

If network control has a Top Secret job to run and the classified processor, which would normally do this job, is busy with a lengthy priority Secret run, network control has the option of causing one of the multiprocessor configurations to be segmented into two uniprocessors and upgrading one of them. This would occur only in the event that another dual processor could not be made free to do the Top Secret job under the timing requirements of the Top Secret job. (The separation of the multiprocessor into two uniprocessors is a manual switching task that must be performed by the network control.)

Top Secret job. The separation of the multiprocessor into two uniprocessors is a manual switching task that must be performed by the network control.

The first thing network control does to upgrade a processor is reconfigure the authentication system when the unclassified computer notifies network control that it is through processing its jobs or has rolled out the current jobs and cleaned. The Top Secret job is then initiated and completed; when no other Top Secret runs exist for this processor, the system is cleaned and network control downgrades the processor.

An independent processor is designated to provide backup to the network control computer. That processor shall continually monitor the operations of the network control processor and when a malfunction occurs, immediately take over the network control function. The network controller is notified, and another computer is initialized as backup until the source of the problem is identified and alleviated. The network control processor and its backup have no common resource and therefore are not dependent in any way on the same component which might fail with the possible exception of common software to perform the test. If there is a software malfunction in network control, then the possibilities are high that it might also affect the backup.

To provide more efficient operation to the network control, there is a monitoring task which is associated with compiling statistics on task and resource utilization, feeding these back into the scheduling model as appropriate.

As can be seen, the network control function is very important to the operations of the entire system. It has many special protect features which disallow software interference. There is constant monitoring by the network control position. No one within the system can usurp the control authority of the network control computer except the network controller and the backup network control computer in the case of malfunction.

Even with this protection, it is necessary to provide for nonrecoverable malfunctions. Automatic functions performed by network control can also be performed manually by a combination of the network controller and the operations controller.

Also, there shall be a graceful degradation fallback mode in which computers are efficiently dedicated to functions. In this mode the system will be able to satisfy most of the normal operational requirements until the network control system is again online.

1.8.2 Operations (A82)

1.8.2.1 Security (A821)

The design of the data system has tended to centralize computer operations acting as a consolidated function servicing all computer systems rather than being oriented around a single computer system. Automation of the internal AFGWC user interfaces is provided in the form of a variety of consoles. However, the primary consideration of operations is security control.

a. Introduction. In investigating the area of hardware/software protection for a mixed mode security environment, it was found that no totally acceptable solutions currently exist in the state of the art available between the 1977-82 era. We have proposed an approach we feel to be superior to currently existing applications while at the same time providing the most efficient and flexible system. We have also managed to minimize the expenditure for security protection while not jeopardizing its integrity.

b. Physical Isolation. The proposed system utilizes physical isolation as a device to protect against malicious access to the facility. Two perimeters are established; one for special access computation and the other for normal access computation. Data flow between the two perimeters is either through (1) an upgrading of data in one direction which can be accomplished automatically by the computer, or (2) downgrade certification in the other direction which is not allowed to be done automatically, but requires manual action.

   The problems are: 1) protection of the various security levels from inadvertent classification misassignment within the closed perimeter and 2) protection from the perimeter to interfaces with the outside world. These interfaces occur through the communications links, the remote console links, and by data which must be manually taken outside the computer facility.

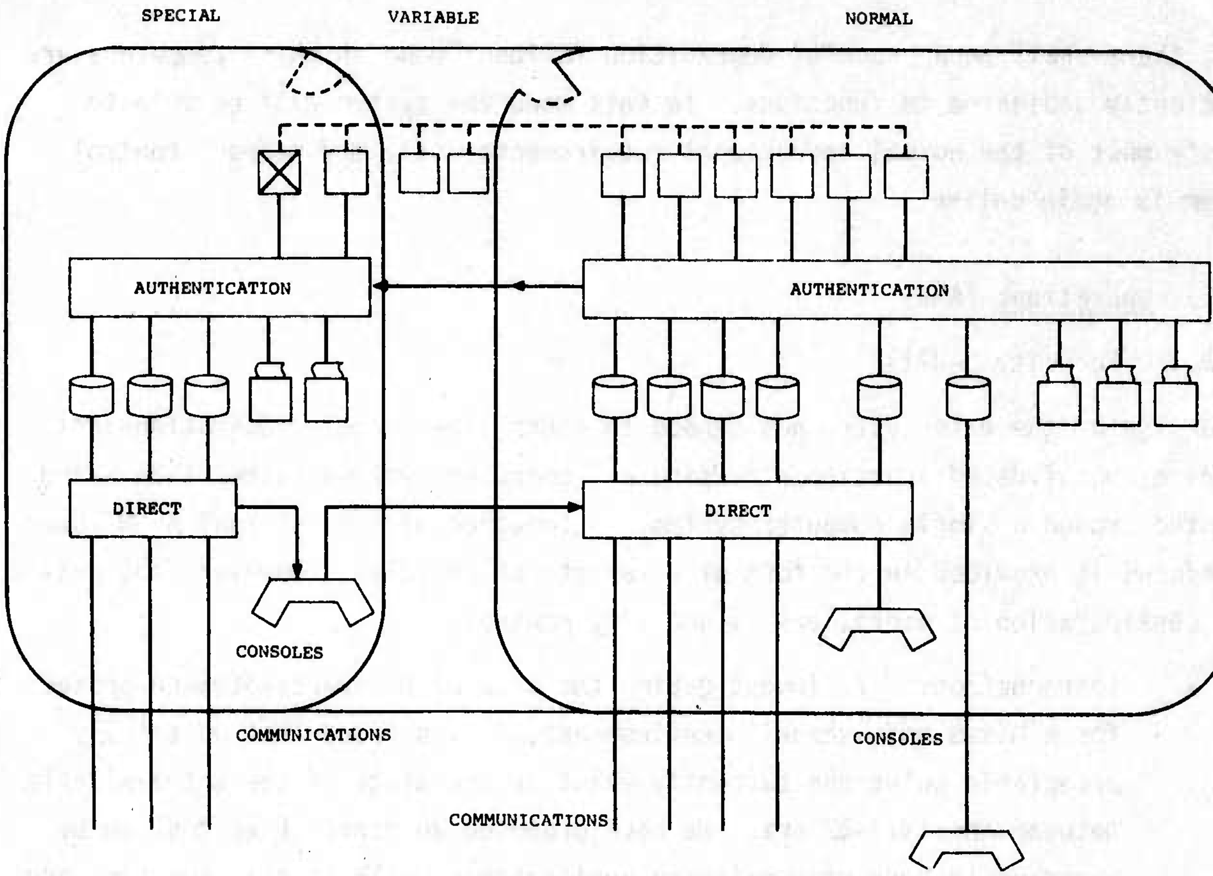

Figure 27. Security

c. Distinct Levels by Partitioning. A data path is defined as a theoretical one-directional flow of data between components electronically linked where the components are thought of as straight throughput devices. Partitioning through physical switching or authentication encoding is used within the data system to separate the data paths according to security level. The level of a path is established as the highest classification of data which has been or potentially can be interjected anywhere along the path. Notice that by this definition, segments of an extensive path can be sequentially upgraded in security level along the path.

d. Lateral/Upgrade Communications Flow. From the definition of level it follows that two-way communication can exist between components of the same level. It also follows that one-way communication can exist from a component of a lower level to a component of a higher level. Data flowing from a higher level to a lower level must do so through a manual certification/downgrade procedure with three very important exceptions:

1. Communications traffic in and out of the environment which, because of time requirements and data quantities, makes manual processing impractical;

2. Unclassified requests by a higher level to a lower level for data; and

3. Network control data which provides control of and intercommunication with components and scheduling of tasks to provide optimal processing.

e. Control-Only Data Flow. This technique prevents inadvertent passage of classified data. It does so by imposing a physical hardware requirement that the data be of a certain form, is passed at the appropriate time, and is one of a very small subset of all possible pieces of information which might be passed over the given bandwidth. For example, in the case of network control information, one of the messages indicates to a processor to go look in the pre-defined job parameter table for a job scheduled. In another case, one processor indicates to a lower-level processor that it should pass pre-defined data.

f. Mixed Mode Communications Interface. For outgoing communications, the communication line is thought of as a component existing at the level of the communication line. It can therefore accept data at a lower level, which will be appropriately marked. A special mini-computer will have the job of recognizing data coming in from a communication line and immediately routing it according to classification into the appropriate level of the computer system. Since this includes automatic downgrading, this is the single dependency on software. However, a precedent has been set by current AFGWC processing and by general communication procedures used for many years for identifying messages. By minimizing the exposure within the mixed mode environment and using special hardware and software, this function will be performed effectively. Thus, by isolating this automatic downgrade to a specific area, monitoring and checking can be performed easily, and if better procedures are developed, they can be effectively implemented.

g. Resource Allocation. The basic allocation process shall be to assign various processors to specific security levels. With this concept, most processing will be performed by computers generally held at the same security level. The only exception to this will be if the various requirements cause an abnormal imbalance of work distribution or, if extra processing is required, at special security levels. These exceptions do not often occur. When resource changes are necessary, they will be accomplished through switching/encoding of the lines and rapid clean procedures for memory elements.

h. Variable Perimeter Concept. Rather than provide processor system redundancy for both the normal access and the special access perimeter, a single area will be established. This is a separate area and is available to be easily switched to either of the perimeters, thus isolating it from the other.

i. Manual Downgrade Procedure. A viewer presentation or hard copy of data can be made available from a machine at a higher level to a security monitor position. After manual checking of the data and certifying the appropriate downgrade, the data may be rapidly re-entered into the system at a lower level by actuating switches to load the data to a lower level storage device. Data which are to be output on the printer are first sorted according to level. Then it is displayed on printers with additional manual printouts for checking and correlating the data in terms of the level at which the data were generated, the number of pages generated, and the level at which the data are to be certified.

j. Attempting to Hold Data at Lowest Level. The output from any computation once performed must remain at the level of the computation or be manually downgraded. Therefore, it is important to perform computation at the lowest practical level, especially if any of the results are not to be raised to a higher level for subsequent computation.

This also has the result of causing the majority of programs to be run at an unclassified level at AFGWC. This greatly simplifies the resource allocation problem. It also reduces the need for hard copy certification.

1.8.2.2 Quality Assurance (A822)

The two primary purposes of the quality assurance function are to check the validity of input/output data within the AFGWC system as well as to check forecast versus analysis data to monitor the degree of effectiveness of the interactive forecasting functions. The capability will exist to continually collect statistics on forecast versus analysis data; this is standard operational function with summaries and statistical analyses being available at the quality assurance console. Throughout the system there will be data base defined threshold values, functions and procedures to perform data validity checking of data input to the system and data output from the system. Depending on the level and frequency of the violations, the quality assurance console may or may not be notified.

1.8.3 Logistics (A83)

1.8.3.1 Phaseover (A831)

(The subject of phaseover is treated totally in the Implementation and Development plan, Volume 7. It will not be duplicated here.)

1.8.3.2 Spare Parts (A832)

The subject of spare parts is treated primarily in the AGE Plan. The primary requirement driving spare parts is that any failed part can be replaced within two hours of the time that a fault is isolated. Beyond that, it is dependent upon the speed and ability to replenish spare parts used.

1.8.4 Planning (A84)

1.8.4.1 Readiness (A841)

It is our opinion that there are two types of readiness preparation which apply to AFGWC. The first is readiness in preparation for the satisfaction of new requirements or incorporation of new components. The second type is readiness in preparation for peak load or abnormal conditions such as those identified in the WWMCCS crisis management requirement. The readiness functions can in general be satisfied by a simulation capability (described later). There is a mode of the data system whereby runs can be initiated through network control but with the outside influence of those runs being deactivated. (When speaking of outside in this context we speak of outside of AFGWC.) The program must have its own capability to surpass internal interfaces such as interface with the forecaster console or printer. Peak load exercises can be accomplished by inserting tasks into network control which simulate the peak load runs. The level of system degradation can then be monitored based on varying degrees of overload. Run statistics accumulated during this period will be helpful in the analysis period.

1.8.4.2 System Simulation

This capability will exist only to the degree that it can be included cheaply and effectively. SDC suggests that there be a capability to simulate the outside world to a limited degree; for example, precanned communication messages shall be able to be inserted via the data base in the period that they were received over the line handler/decoder router and likewise messages generated can be put out on the printer rather than over the communication links. To accommodate exercises, the capability will exist to operate on a pseudo time base where the network controller can control simulations and interrupt exercises in the middle if required.

1.8.4.3 Long-Term Scheduling

There should also be a simulation capability for network control whereby a run simulation will show the response and allocation of resources over long periods of time. We feel that this capability can be incorporated as a special design feature of the network control software.

1.8.5 <u>Development</u> (A85)

Provisions are made for further development of the AFGWC Data System so that the data system can maintain its capability to support the continually expanding data processing requirements. This capability will, of course, also facilitate implementation of the proposed architecture.

1.8.5.1 Hardware Augmentation (A851)

SDC's proposed architecture is designed so that performance of the data system shall not be impaired during hardware augmentation. The actions entailed in hardware augmentation (e.g., planning, system design, system simulation, system specification, hardware procurement, hardware installation, acceptance testing, and final integration of hardware in the system) should be detailed as a well-defined series of incremental steps, each of which includes preliminary reviews. Further, hardware components used to augment the AFGWC Data System should be selected (designed) to (a) insure that system reliability (MTBF) is not degraded; (b) insure that the integrity of data produced by the system or used by the system is not diminished (i.e., hardware components are not introduced which disallow data representation with sufficient significance for the computations to be performed); (c) augment the AFGWC Data System to be capable of being tested individually and as a part of the AFGWC System; (d) not degrade, but contribute to system capabilities to adjust to peak loading requirements and unusual demands on the system; (e) not be allowed to degrade system reliability due to its unavailability. Backup hardware along with procedures for switching to such backup hardware must be provided for any hardware components capable of degrading system reliability due to its unavailability.

1.8.5.2 Software Development (A852)

Augmentation of AFGWC Data System software should not adversely perturb data system operation. Augmentation activities such as planning, system design, software design, software development (or procurement), software testing and software installation should be planned such that they have no adverse effect of AFGWC Data System operation. They should be planned as a well defined series of incremental steps which reflect the continuing data system requirements for reliability, integrity, testability, adaptability, and availability.

The software design and development methodology (software engineering techniques) used for AFGWC should be analogous to the precise methodical procedures prescribed for hardware development and fabrication. A set of well publicized and strictly enforced standards and procedures should be imposed which provide guidance for all phases of the software cycle. These phases include but are not limited to: software requirements definition, software characteristics description, software functional and detailed design, coding, test, integration, operation (user-maintenance-modification and software support), retirement, and disposal.

Composite design and structured programming disciplines should be applied for AFGWC augmentations. Programs can be written using three programming structures:

a. Simple Statements. Standard assignment statements and subroutine calls.

b. Comparative Statements. If--THEN ELSE statements.

c. Iterative Statements. DO WHILE statements.

Top down design techniques should also be followed with top-level programs coded and tested first and bottom-level routines tested last. During early testing lower-level routines should be represented by dummy (or stub) programs.

A set of widely disseminated and strictly enforced standards and procedures should be made mandatory for the testing and integration of software systems. Such procedures include: publication of a test plan early in the development cycle, parallel and, if possible, independent development of test cases, testing statements, test drivers or whatever testing devices are appropriate for the application; and publication of a test report after testing and integration have been completed. Enforcement of software testing and integration can be simplified by use of automated configuration management techniques such that libraries of the baseline software and updates of that software exist, are capable of being audited, and are capable of being retrieved.

Configuration management is for the most part a documentation of the rules which are observed in developing a product. In most developments, the rules have been developed and are carried by word of mouth, but this is usually far from adequate in a major programming undertaking. Several documents associated with AFGWC should be developed to handle the configuration management task.

a. Documentation Plan. This describes each set of documentation which should be delivered, such as a top down design document, an initial programming specification, and a final programming specification as well as other documents discussed in this section. It gives a description of the content, format, and rules to follow in preparing each document.

b. Principles of Configuration Management. This document identifies baselines and the rules for moving from one baseline to the other. It tells what the error reporting schemes are and the technique used in upgrading the operational system. It usually deals with techniques for using major software changes into the system.

c. Top Down Design Document. This documents the results of the design process giving rationale and traceability to the original design requirements.

d. Initial and Final Programming Specifications. These are programmer-prepared documents which eventually become the description of the system. They provide a vehicle for detailed review. Often the final programming specification is replaced by a detailed, annotated code which has been annotated under a very strict set of guidelines.

e. Standards and Conventions Document. This document describes precisely the rules which must be followed in all areas of programming concern so that there is compatibility between approaches and program, greatly enhancing the interpretability of programs, simplifying the entire process.

f. Protocol Document. This is an interface specification which defines protocol between all component connections within the system.

g. Data Definition Specification. In order to emphasize its importance this specification, which is independent of the programming design specification, concentrates on the philosophy design and details of the data system.

h. Data Base Document. This document deals with the numbers of the data base as opposed to the structure and description. It provides controls and detailed definition to input of constants into the system. It is also a very useful user's document for understanding the fundamental constants and format.

i. Physical Model Document. In an environment such as AFGWC, where geophysical models are so important, there needs to be a separate document which is used as a reference manual and is continually updated with information pertaining to the models. It should contain notation conventions, the fundamental equations for the models, and a precise definition of the reference frames utilized within the models.

j. Glossary. SDC has found, in dealing with very large systems of this type, that the most difficult part of training for a new person is learning the esoteric terms peculiar to the unique data processing system. It is therefore essential that a complete glossary be developed and maintained. This also standardizes the usage of terminology.

The data base management function is similar in its support of all areas of operation. The most important concept in this architecture is that the nominal (constant) data base is, in and of itself, a distinct entity in the architecture with software built purely for support of this total function.

The function we can define as the task of entering software parameters into the AFGWC storage system. It should be made the task of a single group to perform this function and to effect the necessary control required in its accomplishment. The constant data base parameters should all be identified no matter how large or small, how universal or how program-unique. The ground rule should exist that no program contain internally any universal constants.

A single document should be published which identifies each item, its current value, configuring accounting information (such as who made the change and the date the change was made), formatting information associated with the input of the data, range of values, significance, nominal values, units, a complete description of each value and finally, identification of those programs which use the value. This document should be self-contained and should be designed for the system operator as well as the programmer (i.e., this means avoiding use of esoteric terms peculiar to programmers or to engineers).

It is sometimes desirable to divide the user's guide in a manner consistent with the frequency of use or change of the value in question or divide it according to the operator position most commonly associated with the value. We feel that a program should be written to produce the document automatically.

We have mentioned earlier that there was a need for a Data Definition Document which defines the structures of all files of the data system. In addition to this, there needs to be associated with each data block a philosophy of usage. This primarily involves the dynamic nature of the files and the purging philosophy/requirement associated with the data block. Association between data structures needs to be identified as well as the apparent structures as seen by programmers or console positions in using the data (even though this might be determined by the data base interface routines and is not actually the structure of the data on disk).

1.8.6 Maintenance (A86)

(Although this topic is treated in the AGE Plan introduction, it more properly belongs in the Design Description. We have therefore included it redundantly.)

This section deals with the advantages/disadvantages of various alternative maintenance approaches for the recommended architecture. (The possibilities include maintenance by a single commercial vendor, multiple commercial vendors, and full maintenance by military personnel.) In order to describe approaches to life-cycle costs, facility requirements, etc., it is necessary to define a scenario for the mixture of vendors at AFGWC. We have chosen an example which we consider the worst-case scenario; its description follows.

The system is procured in such a manner that main processors, support processors, data base elements, and major consoles are procured at different points in time. Main processor systems come from three distinct vendors. Support processors fall into two different classes and come from two different vendors. Data base elements are grouped according to major subsystems of which there are four, and hence a possible four different vendors. Consoles fall into three different categories: programmer consoles, forecaster consoles, and data system operations consoles (such as network control, operations, special operations consoles). Hence, there is a possibility of three different vendors there. Each main processor system, in addition, may consist of a host processor and an array processor which come from different vendors, and the assumption will be made that the array processor does not come from a vendor capable of providing on-site maintenance for the array processors.

Given this scenario, the following ground rules apply in calculating life-cycle cost, facility requirements, military manpower requirements, management impact, logistics requirements, operational considerations and security considerations:

a. Life Cycle Cost. First of all, consoles are not a sufficiently costly item (and they are not sufficient in quantity) that we will find vendors willing to supply on-site maintenance. Further, it is unlikely that a console vendor would be located in Omaha. Hence, it will be necessary to train military personnel to isolate faults to the plug-replaceable unit level and to replace items within the consoles. Accordingly, a spare parts inventory for consoles must be kept.

   In this case, each of the three different kinds--programmer, operations and forecaster consoles--would have different spare parts inventories. These spare parts must be kept in an environmentally controlled area to maintain their longevity. If array processors are not procured from the same manufacturers as the hosts, it may be necessary that military personnel also be able to replace pluggable units on the array processors after having isolated faults via vendor supplied diagnostics. In this case, again, there will have to be a spare parts inventory kept. The cost of spare parts should be estimated at about 10% of the cost of the unit itself in terms of a spare parts inventory and this should be proportional to the number of units. The amount of time it will take to exhaust the spare parts purchased by this 10% factor will vary with the components. In Table 2, maintenance costs are estimated for various system components over an expected 10-year life cycle. These costs are "average" since they are based on the expected system configuration in 1982, the mid-point of the 10-year period.

TABLE 2

LIFE-CYCLE MAINTENANCE COSTS

I. MAINTENANCE BASED ON PARTS COST

SYSTEM COMPONENT	SPARE PARTS COST (10% OF PURCHASE COST)	YEARS TO EXHAUST SPARE PARTS	TOTAL 10-YEAR LIFE CYCLE COST
Mass Storage Facility Media	$.175K	1	$ 2K
Switches	$24K	10	$24K
Authentication Chips	$38K	5	$76K
Array Processors	$250K	5	$500K
Forecaster Consoles	$300K	2	$1.5M
Operations Consoles	$4K	2	$20K

II. VENDOR SUPPLIED MAINTENANCE (PARTS INCLUDED)

SYSTEM COMPONENT	ANNUAL COST	TOTAL 10-YEAR LIFE CYCLE COST
Main Processors	$1.75M	$17.5M
Support Processors	$250K	$2.5M
Disks	$350K	$3.5M
Programmer Consoles	$10K	$100K

III. ANNUAL AFGWC TRAINING - $50K	$500K
TOTAL	≈ $26M

b. Facility Requirements. Facility requirements are based upon the need to keep spare parts in an environmentally-controlled area and to supply on-site maintenance areas for customer engineers. Each separate vendor should be allowed an on-site maintenance area, except in the case of the array processor or the forecaster console. Customer engineers and spare parts for each major subsystem could be contained within a room 20' by 20' on the average. Each major subsystem would require that area. In the worst case, the two different kinds of support processors would require separate rooms and each of the vendors for the host would require a separate room. Each of the distinct data base elements would not have on-site maintenance. There would be a combined single room for spare parts for on-call maintenance at the disk subsystem. This worst case would then require 6 areas of 20' by 20' for a total of 2400 square feet. This would represent about a 30% increase compared to the total area required by Univac now (1800 square feet represents a realistic expected number).

c. Military Manpower Requirements. Military manpower requirements would not change from what we had estimated because operations personnel would be trained to the use of diagnostics and in the replacement of components. There would be short training courses, no longer than one week in any case, for military personnel to enable them to replaced failed components. Failed components would be mailed back to the manufacturer for repair, replacement and restocking.

d. Logistics Requirements. Logistics requirements have already been covered as part of the life cycle cost, facility requirements and manpower requirements.

e. Operational Considerations. Operational considerations such as scheduling of preventive maintenance are straightforward. In no case can anyone take a component away from system usage for preventive maintenance unless he has cleared it with the network controller. There will be a schedule of preventive maintenance which is coordinated with the network control console, subject to modification due to unpredictable failure or unpredictable work loads.

f. Management Impact. Management approach is perhaps the most complex area with regard to the maintenance of such a large data system. There seem to be three basic possibilities: (1) Have the Air Force manage and take responsibility for the overall data system maintenance, from the standpoint that it subcontracts to each individual vendor their responsibility for maintenance of these components; (2) Give a single vendor contractual superiority such that all other hardware vendors are subcontractors to it for maintenance; and (3) Have an independent third party which could take over the bulk of the maintenance of the entire data system, in which case there would be no hardware-vendor supplied maintenance (to speak of) and a third party would come in and handle all maintenance. Each option has its benefits and its drawbacks.

Third party maintenance has the advantage that a single vendor does the actual physical maintenance of all components, thus there are no arguments with regard to interfaces and no problems about assessing blame. On the other hand, it is difficult for a third party maintenance company, in the long run, to maintain equipment as well as individual vendors, even though third-party maintenance companies make a practice of hiring employees away from the vendors. The education and background of such employees has limited periods for which it is useful. As the vendors announce new products and continue to upgrade old products, each of the customer engineers of the third party becomes more and more obsolete. There really is no good way for these third party people to continue to update the education of their people for two reasons. One is that they do not have access to as much information as the vendor has, as soon as the vendor has it, and they do not have access to the design personnel of the vendor. The other is that these third party companies can afford less time for their employees to go to school because they are selling their services at a lower cost, implying lower overhead.

Option number two, which is to have a single major vendor take over contractual obligation of maintaining the data system, has the same advantage as that of the third party maintenance: a single vendor can be held responsible for the maintenance. On the other hand, here this is a much weaker argument because the contractor does not actually perform the maintenance. He simply holds other people under contract to him. It does, however, to a large extent eliminate interfacing finger pointing problems. There are two drawbacks, however, to this approach. First, the vendor that has been given overall data system responsibility charges for that service and so it will cost more (at least in cash flow) to have an individual vendor take charge of the data system. Second, the system is not viable unless you have one vendor whose equipment dominates the system to an extremely large extent and only a few additional extraneous vendors. Thirdly, these extraneous vendors must have product lines that do not conflict with the major dominant vendor. A good example of this would be if you had a main frame manufacturer and had the telephone company supplying modems and gave the main frame manufacturer responsibility over the telephone company modem maintenance. If you have many vendors who are competing in the situation, it is too difficult for them to really maintain good working relationships despite contractual obligations.

Option number one (of having the Air Force take direct responsibility for the overall data system maintenance with contracts to each individual hardware vendor) implies either contractual or informal penalties for non-performance on the part of each individual hardware vendor. Informal penalties can arise from the competitive situations multiple vendors get into in the upgrading of data systems, and so there is an incentive for each member to perform very well in maintenance situations. It is therefore obligatory that the Air Force maintain a fair and impartial attitude at all times towards all vendors under option number one. It is also essential that the Air Force make certain that everyone feel the blame for a nonfunctioning data system rather than allowing vendors to finger-point and blame each other. A multiple vendor shop in general requires much more rigid practices with regard to vendor/Air Force relationships than the single vendor architecture of AFGWC currently permits.

A fourth option which exists in the commercial world does not appear to exist for AFGWC, and that is to award a facilities management contract to a systems house. Facilities management of the AFGWC system does not seem practical due to the military mission of the system, and due to the security clearance requirement.

g. Security Considerations. The most important impact of security considerations lies in the remote debugging of main processor systems. Hardware vendors in general appear to be trending towards the use of centralized debugging facilities, linked over high-speed telemetry lines to individual processor systems. Large processors come with maintenance support processors capable of exercising the large processor and passing the results to the remote centralized maintenance facility. This approach has several advantages. First, it allows the ready access to expertise that might otherwise be only called in after many hours of delay. Second, the centralized expertise becomes even more efficient due to the wide variety of problems that they encounter. And, third, centralized expertise allows the dissemination of individual solutions among the widest possible customer base in the shortest possible time; i.e., a problem which is solved in one location is put into a central data bank so that any other similar problem that occurs can be checked to see if the solution will work on it. Vendors are leaning in this direction because their manpower costs for maintenance have risen to a much larger proportion of their overall costs due to the inflation of salaries and lowering costs of hardware. Currently it is impossible to allow remote debugging of CPUs within the AFGWC system. The only way that this would be possible would be if the data lines themselves were secure at the highest level of classification, and that the personnel at the other end in the central facility were also cleared at that level. Both of these seems to be unlikely and enormously expensive. This is a very serious future problem in the AFGWC data system in that the alternatives are expensive and less efficient.

Another security consideration arises in the access of data base from various processors. The data base is protected against inadvertent access by improper security level main processor systems via the use of authentication chips. Primarily these authentication chips use cryptographic techniques to avoid inadvertent access. Since they are in the data and control path between processors and the disk controllers, it may be necessary to remove them or set them to "clear" before diagnostics can truly prove the existence of a problem in the controller rather than in the channel or the chip. Therefore, it will be necessary to physically isolate data base elements and data base controllers from the rest of the data system. Alternatively, vendors could propose diagnostics such that they could provide the isolation of failures without clearing the chips.

In summary, we have presented a worst-case scenario for maintenance of the proposed AFGWC architecture. It has been our intent to establish an upper bound on the resources involved and not to suggest that this will be the most probable solution to the maintenance problem.

1.9 FACILITIES (A90)

The new hardware configuration resulting from this architecture study will be adaptable to the current facility space and supporting environment.

No major structural changes to the AFGWC facility will be required for hardware components, storage, or personnel work areas. Present access routes will be adequate for the architecture. Security restraints include the entire classified data system (i.e., all primary data base storage will be in a vaulted area).

The expected impact of hardware components on facility space is illustrated in Figures 28-29. The hardware component sizes are typical of the class described by the system specification and the numbers coincide exactly with the specification. With the exception of certain consoles, all hardware is confined to areas presently designated for hardware use by Air Force personnel. Programmer consoles have been distributed evenly among those areas assumed to be occupied

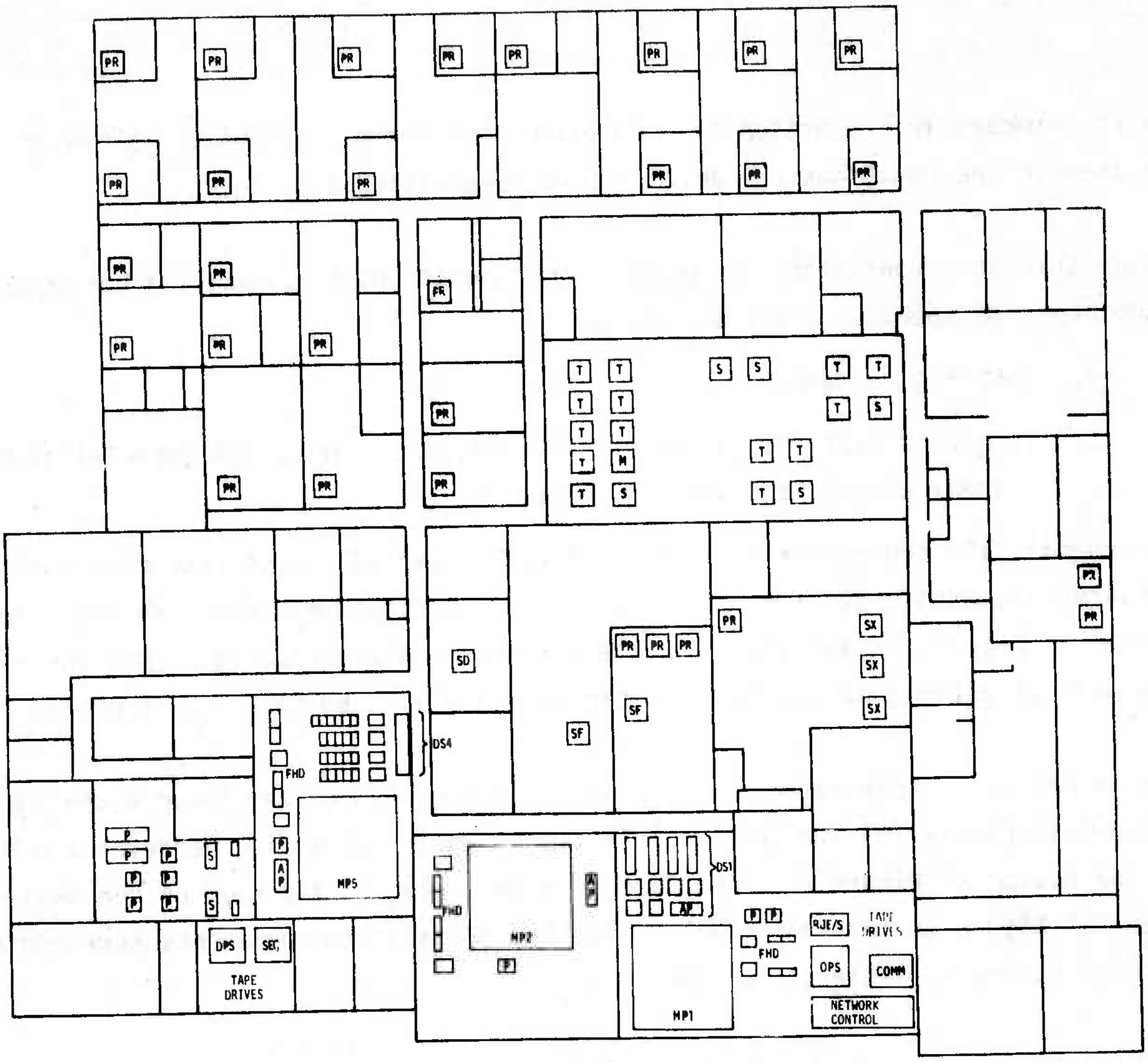

Figure 28. AFGWC Main Floor

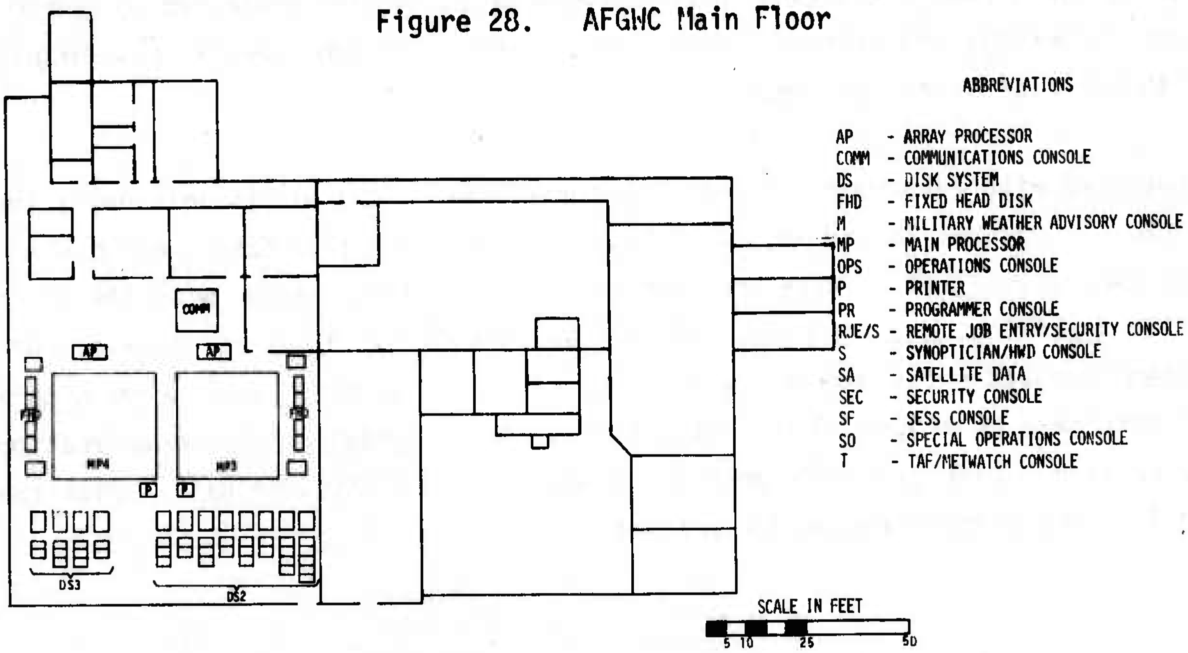

Figure 29. AFGWC Lower Floor

by programmers in proportion to the number they serve. Forecaster consoles are located in the positions now dedicated to forecasting functions.

Other than component size, the primary considerations in allocating hardware components to specific areas have been:

a. cabling distances;

b. security restrictions imposed by the three perimeters (special access, normal access, and variable access).

In general, all processors are within 50 cable feet of the storage they must use. Consoles are within 200 feet of the main processor system. Although not illustrated in Figures 28 and 29, all three perimeters are contained within the existing wall structure; no new walls or partitions will need to be constructed.

The normal access perimeter consists of the processors on the lower floor (MP3 and MP4 in Figure 29) and the three left-most rooms containing hardware and MP5 on the bottom of Figure 28. The special access area is the room on the bottom right of Figure 28 containing MP1. Finally, MP2 and the components surrounding it make up the variable access perimeter.

Each of the normal and special access areas have consoles dedicated to operations, security, and communications,with a network control console residing only in the special access perimeter.

Associated with each main processor is a maintenance console (signified by the printer in Figures 28 and 29), an array processor, and four fixed-head disks with two controllers. There are four disk systems illustrated, with the first in the special access perimeter and the remaining three in normal access. Disk system 1 provides for network control, scratch, and special access communications and data base overlays. Disk system 2 is used for normal access communications and scratch. Disk system 3 contains raw and gridded satellite data. Disk system 4 is the primary meteorological data base.

Backup considerations based on reliability requirements have dictated the placement of disk systems with respect to computers. In other words, not only the processor which normally has direct access to a disk system must be near it; so too must its backup. Disk system 1 must be accessible from processors 1 and 2. Processors 2, 3, and 4 are within 50 feet of disk system 2. All processors within normal access (3, 4, and 5) must be capable of reaching disk system 3. And, finally, disk system 4 must be close enough to processors 4 and 5.

Some other considerations involved in allocating facility space to hardware components include:

a. a desire to isolate printers in a single area to minimize the noise associated with them, and

b. the location of tape drives close to existing tape libraries (not shown in Figures 28 and 29).

Commercial power supplied to AFGWC is used to continually recharge a large battery system (a power repository) which provides necessary support to the computer system. It is designed to minimize the effects of power fluctuations and outages external to AFGWC, and to allow for easy switching from primary to backup power sources. Use of the basic system will be continued.

The two remaining environmental factors affecting machines are temperature and humidity. Air conditioning will be sufficient to maintain these at adequate levels.

There are five primary elements which have the most dramatic effect on the work environment of personnel. These include:

a. safety;

b. radiation hazards, nuclear, electromagnetic;

c. acoustic levels;

d. temperature and humidity control; and

e. lighting.

All these will be maintained at levels within recommended military and federal health standards.

2.0 FUNCTIONAL AREA DESCRIPTION

This portion of the document describes how the architecture previously described satisfies the functional tasks to be performed at AFGWC. This section is organized according to the functional domain for easy reference to Volume 2, Requirements Compilation and Analyses.

2.1 INPUT DATA PROCESSING (F1000)

2.1.1 SESS (F1100)

This portion of the document describes how the architecture previously described satisfies the functional tasks to be performed at AFGWC. This section is organized according to the functional domain for easy reference to Volume 2, Requirements Compilation and Analyses.

The TWX monitoring inputs and the bulk data processing inputs will both be handled automatically by the proposed data system. In both cases, data are received at the line handler/data router where it is immediately routed to a disk at an appropriate classification level (primarily unclassified). Network control is notified of the arrival of the data and type which automatically places a job request in the queue. The key event monitoring functions will have very high priority and their processing will be equivalent to the query/response operations. In the case of the event messages, there will be thresholding on queued events and the logging of event functions, including notification of the SESS operator on the SESS console as required. If required, messages will be produced and formatted for transmission. Raw data are routed to the raw data file where validation of the coding is initiated and then is stored in the process data file. Data can also be routed to printers, if desired.

2.1.2 Conventional Data (F1200)

Conventional data consists of unclassified reports received by AFGWC over the Automated Weather Network (AWN) from the Carswell ADWS. The reports include the following types of meteorological information: surface, upper air and severe weather.

These data are received by the unclassified line handler/decoder router which identifies each message as to message type, determines that the message is valid, assigns an appropriate priority, and passes the message to the appropriate combination disk controller for storage on the fixed head portion of the combination disk.

Network control, once notified by the line handler/decoder router, designates a main processor to read the message from the combination disk and perform the following functions: message decoding/correcting, message and message group validation, routing within AFGWC, initiating tasks to other processors and/or to network control, and updating the meteorological data base.

2.1.3 METSAT/Imagery Data (F1300)

One of the major design goals of the enhanced architecture study is to ingest both primary and special sensor data associated with the two polar orbiting satellite programs (DMSP and TIROS-N) and the geostationary program GOES. The design that was formulated for the ingestion of satellite data was sized to accommodate the worst-case scenario. The design will accommodate: (1) simultaneous readout from two DMSP vehicles, each of them reading out two tape recorders at a downlink rate of 2.66Mb (one recorder in smoothed playback mode and one in fine playback mode) for a duration of ten minutes; (2) simultaneous readout from two TIROS-N vehicles, each providing a single smoothed data link at 2.66 Mb; and (3) one GOES type vehicle providing approximately a 2.66 Mb downlink.

The design provides a satellite ingestion computer (satellite support processor) which receives the output from the satellite dedicated ground stations and buffers the information to a disk subsystem which is dedicated to raw satellite data ingestion. Since the band-pass of current disk units is significantly below the direct band-pass of the satellite input, the buffering will "ping-pong" between disk units. Both primary and special sensor data will be ingested and stored on dedicated disk units.

The satellite support processor is fully compatible with the direct ingestion system currently being developed for ingestion of DMSP data. If the direct ingestion device being developed is found to be acceptable and reliable, then the bandpass of the satellite support processor can simply be reduced by the bit bandwidth of the direct ingestion device or devices. The direct ingestion device can also be multiplexed into the dedicated ingestion disk system along with the satellite support processor. Since the gridding and mapping job requests will be scheduled by the satellite support processor, an operator initiated job request will be required for ingestion by the direct system.

Once the data or a subset thereof is ingested to the dedicated disk storage, network control is notified of data availability and a job request is submitted for gridding/mapping of primary data and special sensor processing.

The gridding/mapping job will be scheduled on an unclassified processor. The job will be scheduled on a dual-processor as a first choice and a uniprocessor as a second choice. The job can also be distributed by 1/4 orbit tasks to several main processors, effectively reducing the elapsed job time.

The satellite data processor software will maintain a task priority table that will contain all scheduled satellite data input and its relative priority. The priorities will be updated as operational needs are defined. When the priorities on portions of satellite readouts are changed, then the priority given to network control with the gridding/mapping job request is adjusted accordingly.

2.1.4 Product Request (F1400)

Product requests in the AFGWC architecture will be dealt with either as automated requests or manual requests. The automated requests will be responded to automatically by the AFGWC architecture, the product generated, and transmitted to the customer without human intervention. The manual request, however, will be routed to a man-machine interface such that the man can then respond with the appropriate manual or semi-automatic response and have the results again transferred to the customer. Regardless of which of the two major types of product requests is input to the system, the first exposure to the architecture will be in the line handler/decoder routers. This is the first level of interface between the outside customers and AFGWC. A specific line handler/decoder router will be determined by the classification and the interface line used into AFGWC.

Once the product request has been input and its classification level determined, it will then be routed to a "maildrop" located on the communication interface desk system. The "maildrop" will be queried on a cyclic basis by one or more of the main processors. The input processing software will determine whether the product request is an automatic or manual request. If the product request is automatic, network control will be notified of the requirement, the job will be started, and the product will be distributed. However, if the product request is manual, the product request processor will determine routing. Possible options for routing are the various forecaster consoles or the special operations console exist. The product request software will maintain a table of relative priorities between the various product requesters. The priority table will contain the time period requiring to respond to the message and a network control priority number for use in the request parameters associated with product request job initiation.

It is important to note that due to the dynamic scheduling of the components of the AFGWC architecture, no one single processor will be responsible for querying the disk that contains the product request. Product requests of a classified nature, however, will be queried by classified processor. The line handler/decoder routers will be responsible for notifying network control that a product request has been received and placed on disk storage. That request will include the priority of the product request and the classification of the job. This will be required by network control in order that the main processor can be scheduled at an appropriate security level.

2.2 DATA BASE AND RELATED COMPUTATION (F2000)

2.2.1 SESS (F2100)

Any of the SESS models can be initiated from the SESS forecaster consoles. Run control will be generalized so that functions will be similar in execution. Error messages at the SESS console will be only those directly pertaining to the model and requiring attention by the forecaster. These job requests are put in the network queue and when resources are available, they will be executed. In general, the wait time between initiation of a job request and the running of the job will be short, on the order of 30 seconds maximum. The capability will exist for the unclassified SESS console to initiate a classified job; however, the results will be on the classified printer and any operator action will have to take place at the operations console. The SESS operator will have the capability to get any hardcopy output of CRT display data.

2.2.2 Request Processing (F2200)

Request processing will be in response to messages received at AFGWC requesting either automated or manual type of products. If the nature of the requests implies an automated response, the product request software will simply notify network control of the need of a request processing job run. Network control will schedule an appropriate processor to initiate the job. Once the job is complete, the product will be tagged and distributed to the output processing maildrop.

Several elements of the AFGWC architecture have been designed specifically to handle the semi-automatic and manual product requests. This is the case of the special operations console. This console has the capacity of interfacing at all security levels with the AFGWC data system. Manual requests are received, recognized by the product request software, and distributed by one of the man-machine interfaces at AFGWC. Unclassified requests can be made to various forecaster consoles or to the special operations console, depending upon the exact nature of the request. All classified product requests will be distributed to the special operations console. The operator at the special operations console will have the capacity to start and interface with a computer job at any of the various classification levels. Available at the special operations console will be both CRT and alphanumeric keyboards, a local line printer, and a card reader. All of these inputs can interface to the AFGWC architecture at any classification level. Classification level at any one point in time will be unique.

The architecture optimizes response time to request processing by distributing the workload among many processor subsystems. The processing required in response to the request will be scheduled on an individual processor as determined by network control in accordance with the parameters passed to it as to its priority and security level.

2.2.3 Analysis (F2300)

Figure 30 shows an overview of numerical model processing. This overview is correct for both analysis and forecast programs. Network control will assign the running of the model to a host 3.5RP (a Univac 1108 is 1RP) main processor system by placing the job parameters in the job queue of the host. At the same time, network control will schedule the data base manager to provide data base fields for the running of the numerical models. The host will initialize the array processor and begin receiving analysis fields from the data base manager. These analysis fields will be stored on scratch disk areas or fixed head disk areas. Meteorological parameter arrays will be handed to the array processor along with the information required to process the queue of operations and host memory. The array processor will then begin computation using the local high speed memory for intermediate results. As final results become available, the host will return to the data base manager for data base updates. On completion of the job, network control will be notified.

2.2.4 Forecast/Prognosis (F2400)

(See section 2.2.3)

2.3 OUTPUT PROCESSING (F3000)

2.3.1 SESS (F3100)

The current teletype function can be accomplished totally at the console CRT. The message can be formulated or can be an augmentation of an automatically produced message form where the operators simply fill in the blanks. The message can be edited if required and then released to the data base and finally to be sent out via the line handler/decoder routers. The procedures can be set up so that a copy of all internally generated messages which are sent out will be available with the appropriate distribution or, if desired, a hardcopy can be made from the operator's console. External automatic requests for SESS data can be accommodated by the query response data base under standard formats. When classified messages are prepared to be checked and sent out for the unclassified data link, this is accommodated by using the security monitor downgrade position. Messages can be automatically designated for downgrade; once they are

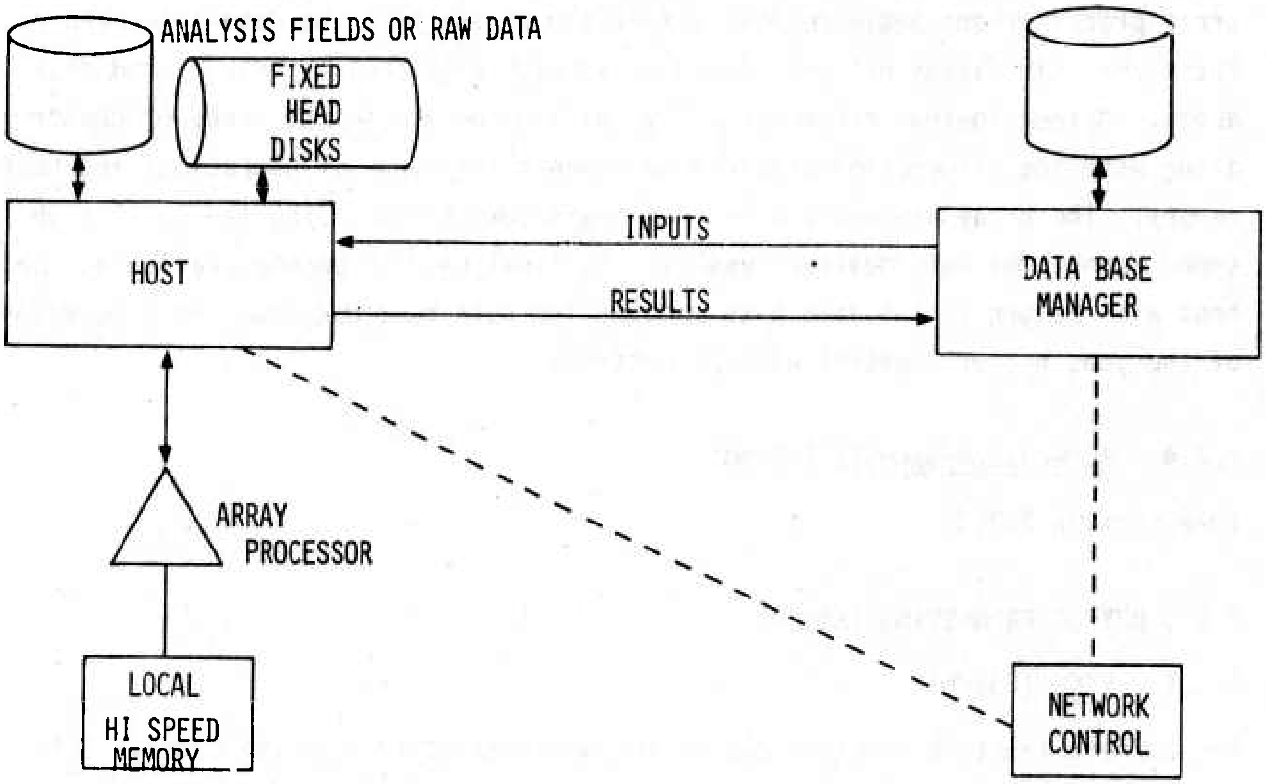

Figure 30. Numerical Model Processing

produced, they are routed to the downgrade position and introduced into the data base through output transmission or for display on the unclassified console.

2.3.2 Facsimile (F3200)

The Air Force Communications Service has proposed a weather facsimile switching center (WFSC). The purpose of the WFSC is to replace the manual facsimile operation at AFGWC and enable the weather facsimile functions at the National Meteorological Center at Suitland, Maryland, to be incorporated into the system at the AFGWC. This will provide total automation from a centralized CONUS weather facsimile facility.

In order to complete the compatibility and establish a centralized facility for the Air Force, the Air Force Communications Service is proposing the purchase of two Interdata Model 50s to be located at AFGWC for transmission of facsimile products throughout the Air Force networks. After the two Interdata Model 50s are installed and operating at AFGWC, the unit at the National Meteorological Center will be moved to Offutt as a backup to the two at that facility. Thus, the Interdata Model 50 will be utilized for all facsimile transmissions from AFGWC. Most of these transmissions will be automated and will be generated at forecaster work centers, while some will be manually prepared facsimile products which will be hand-carried to the WFSC for the AFCS personnel to digitize and then transmit through the Interdata 50s. Forecaster consoles which produce facsimile products will be connected to the Interdata 50s which will interface with all of the facsimile circuits.

Manually prepared facsimile charts are now routinely prepared by WPF for transmission on the following military circuits: EURFAX, STRATFAX, PACFAX, and RAFAX. These transmissions result from the manual preparation of 121 charts per day, some of which are sent over more than one circuit (although not simultaneously -- there is currently no capability at AFGWC to transmit FAX products to more than one circuit at a time). The 121 individual charts are comprised of a basic set of 63 types, various ones of which are produced from one to four times per day. These manually prepared charts (some of which must undergo a 50% image reduction to accommodate facsimile equipment) are either mounted on rotating drums or used by digital table-top scanners for analog transmission.

The Weather Graphics System (expected to be operational in 1976 to replace current EURFAX FAX transmissions) will be driven by essentially the same product mix as today. By 1977, however, a modest increase in the number of products disseminated through the WGS can be expected (but not to exceed 200% of present volume). Projections have been made that with modem modifications and regeneration repeater stations, WGS would operate over European communications networks at a compromise in the originally designed transmission speed. WGS equipment is expected to triple the delivery rate of the present EURFAX system. The WGS transmitter at AFGWC will digitally encode and transmit weather charts destined for eventual satellite relay to Europe.

Automatically generated facsimile charts are presently prepared by WPD personnel using the program SDMFAX, and are transmitted on the STRATFAX and PACFAX circuits. These transmissions result from the automatic generation of 25 types of charts per day, each of which is sent twice daily (20 charts on STRATFAX and 5 on PACFAX), plus one chart which is generated and transmitted once a day on PACFAX. There transmissions involve the reading of data from COMPIX equipment, which reads digital tapes produced by SDMFAX for digital dissemination.

With the advent of forecaster consoles and the facilities for totally automated generation, storage, and transmission of facsimile products, the dissemination of these products will be accomplished in highly efficient fashion. As this capability is perfected, the current "automatic" method of transmitting SDMFAX tapes through COMPIX equipment will probably be eliminated. However, manual capabilities may be retained for the occasional situations where human intervention is required for facsimile chart optimization. Eventually, AFGWC should be able to interface with all facsimile networks - STRATFAX, PACFAX, RAFAX and WGS, as well as circuits to backup the National Weather Service - through automatic or manual means.

The WFSC will consist of mini computers and peripherals capable of providing efficient facsimile service to Air Weather Service and its customers. However, while this automated facility should result in much more efficient transmission of facsimile products on the various FAX networks, the implementation of this facility will be the responsibility of AFCS, and will have little direct impact on the data system architecture. It is assumed that the capabilities listed herein, including the Weather Graphics System and implications of the Automated Data Weather Switch, will remain through 1982. A more significant impact on AFGWC could be its ability to satisfy National Weather Service requirements whenever NWS requires backup support for facsimile transmissions. However, this service should be quite infrequent (see Section 2.4.5.3).

2.3.3 Satellite Imagery Related Products (F3300)

The satellite imagery related products will be distributed through the satellite image dissemination subsystem. This is a computer based subsystem that will use the gridded satellite data bases as primary input. A secondary input will be via laser scanner devices. Satellite image dissemination software will reside in a satellite support processor. Satellite image dissemination subsystem will reside in a satellite support processor. Satellite image dissemination subsystem will be responsible first for scheduling requests for the generation of products on a main processor, and second, for the distribution of those products to the various customers.

Satellite image dissemination software will automatically notify network control when products should be generated in response to forthcoming distribution time requirements. Once the products have been generated by the main processor subsystem, the products will be maildropped, retrieved by the satellite image dissemination system and held in temporary storage until the appropriate distribution time. Depending upon the final nature of the satellite image distribution communication system, the satellite image dissemination processor will either run line protocol with the communication links themselves or distribute the imagery information to the appropriate line handler/decoder router.

Also associated with the satellite dissemination subsystem will be a console which will have the capacity of providing the man-machine interface in control to the system and also provide quality control capability in the form of a high resolution CRT. The high resolution CRT will be utilized by the SID operator to perform visual quality control. The operator will also have the capability of manually requesting certain imagery products for distribution.

2.3.4 AWN (F3400)

Prodcuts distributed through the AWN are divided into two categories: Manual (Routine TTY) and Automated (Routine TTY). Currently there are 167 products that are included.

Manual products are prepared, as required, by the observers and forecasters. These are input to a main processor for final formatting and checking which then writes the message on a combination disk and notifies network control of the product ready for transmission. Network control directs the unclassified line handler/decoder router to read the message, format the appropriate header to comply with the line protocol for the AWN and transmit the message to the Carswell ADWS.

Automated AWN products are stored on a Combination Disk after preparation by a main processor. The remaining steps are the same sf for manual products.

2.3.5 AUTODIN (F3500)

The current AUTODIN system is used to provide products prepared manually, using computer assistance and completely automated. This system, with its two lines into AFGWC, will interface with a line handler/decoder router. In 1978, the current system will be phased over to a new AUTODIN II system which will use the DATANET 355 as the line handler/decoder router. The AUTODIN II system will incorporate the WWMCCS Intercomputer Network (WIN).

Messages prepared for transmission over the AUTODIN networks will be stored on combination disks of the appropriate security classification. Network control will direct the AUTODIN line handler/decoder router or DATANET 355 to retrieve the message from the particular combination disk, format the message to conform to proper line protocol and transmit the message at the proper time.

2.3.6 Dedicated Circuits (F3600)

Products prepared for dedicated circuits are primarily unclassified. However, data up through the Secret level is required for SAC, NSA, AFOC, and other users. These products are prepared either fully automated or with computer assistance.

After preparation, the product is stored on a combination disk of the appropriate security classification. Network Control then directs the appropriate line handler/decoder router to retrieve the data, format it for proper protocol, and transmit it at the proper time.

2.3.7 WWMCCS Intercomputer Network (F3700)

Products prepared for WWMCCS users will be transmitted over the AUTODIN II System. These communications will utilize the DATANET 355 as the line handler/decoder router as described above in paragraph 2.3.5.

2.3.8 Special Projects (F3800)

Products prepared for Special Projects are stored on a combination disk which can be accessed by the Special Projects line handler/decoder router. Network Control notifies this line handler/decoder router when a product is ready. The line handler/decoder router then retrieves the data and transmits it at the proper time.

2.4 SUPPORT PROCESSING (F4000)

2.4.1 Software Development and Maintenance (F4100)

Enhanced AFGWC architecture has been provided with the total of 30 interactive programmer consoles. Four consoles will be allocated to the special access program development and 26 programmer consoles allocated to the normal access program development. The programmer consoles associated with the special access will be located and will be maintained at the security level associated with the special access perimeter. The programmer consoles associated with the normal access perimeter will be maintained at an uncalssified level.

The use of interactive terminals for program development was selected in accordance with a tradeoff analysis (see Volume 4, Final System/Subsystem Summary Report, tradeoff A52-2). A single remote program development interactive terminal will be capable of supporting several individual programmers. As was stated in the tradeoff study, this will eliminate many cumbersome procedures, such as the handcarrying of card decks, the requirements to maintain and punch card decks, and the problems associated with the submittal of these development jobs.

The gain in programmer productivity associated with the use of interactive program terminals has been estimated as high as 6 to 1. At a very minimum, AFGWC should expect an increase of about 2 to 1.

In addition to the use of interactive programming tools available in the enhanced AFGWC architecture, SDC has suggested that AFGWC plan its selection of personnel, provide periodic assignment to more rewarding tasks, and attempt to more realistically measure the productivity of individuals, train the individuals and individually tailor the motivations for individuals. SDC has also suggested the use of chief programmer teams, composite designs and structured programming techniques for use in the maintenance and program development at AFGWC.

Since interactive software development support is not a function that can be dynamically scheduled between processors, it must remain on-line continuously in support of the interactive terminals. Programmer console support, unlike other console support at AFGWC, will be directly connected to a dedicated processor. This processor will have the responsibility of interfacing and maintaining the programmer console interface. The programmer consoles will be available to perform interactive compilations and submit batch job requests to network control. Four of the programmer consoles will be associated with software development in the studies and analysis section. These programmer consoles, in addition to the normal ANK/CRT terminal, will be equipped with a plotter.

2.4.2 Special Studies and Analysis (F4200)

Special Studies and Analysis will use the programmer interface software provided already for program development and discussed under Section 1.4.3, Purchased Software. This capability will allow studies and analysis to submit jobs into the data system, develop programs for analysis of results, and save historical meteorological information using the mass storage faciltiy.

2.4.3 Data System Management (F4300)

The purpose of this section is to discuss how data base management functions can be supported using the architecture defined by the previous description. Network control and quality assurance are discussed in earlier sections.

The hardware validation capability is satisfied primarily by the maintenance console areas, the data system monitoring capability, the diagnostic software which will be supplied by the vendor, and overall system simulation. With the concept of the homogeneous system of components, the concept can exist to pull any one of the components out of the mainstream of operations for specific attention. The capability also will exist within network control to force jobs on individual computers.

The capabilities of the interactive programming system include a detailed configuration accounting scheme which assigns numbers to compilations and program modifications. This will also be true within the data base management system where, if desired, constant data base change records exist which include time and source of update. All interactions, whether program or data base, will be via the mass storage system which requires the detailed record and designation of master program files. Identical configuration identification procedures will apply to the classified tape areas where tape headers identify the necessary classification designation and certification associated with configuration control.

One of the outgrowths of the structured programming discipline is detailed listing annotation which includes designation of changes. The overall operational executive system will monitor and record error responses in both hardware and software, including a dump of configuration system data to help identify the software versions or components associated with a malfunction. All of these special capabilities will provide sophisticated configuration management within AFGWC.

2.4.4 Real-Time Computer Operations (F4400)

Computer operations in the AFGWC architecture have been centralized for both the special access perimeter and the normal access perimeter. These two central console areas will perform all normal operator functions associated with the operations of the AFGWC computer system. Since these operations consoles interface with various processors scheduled at various security levels, the design has been provided for the separation of input and output parameters to and from the console. Dedicated computer operations support processors exist for the input to the console and for the output to the console. This guarantees security separation and prevents the possibility of sending classified information back through an unclassified line to an unclassified processor.

The software for the operations consoles will be designed in a manner that will key all inputs to code words or code symbols which indicate the originating processor of a message, allowing the operator to effect proper routing. Since the output support processor for each of the operation centers is a one-way communication device, it also serves as a focal point for information that is destined for the downgrade consoles. In essence, this means that the output support processors associated with both the special access and normal access perimeter operation centers exist in a mixed mode environment. However, no device throughput is possible; the information either is sent to a printer where it can be observed visually by an operator and downgraded or maintained at a security level or on a CRT associated with the console with no throughput capability.

All main processors will be connected to the central operation centers via direct input/output channels. Each half of a main processor will have dedicated both an input/output channel for an output channel to the central operations console and also from the central operations console. In the event of failure of one or both of the central operations consoles, all main processors will have the capability of being controlled from the main processor maintenance console. This provides a backup to the centralized operations centers. The system software for each of the main processors will be designed such that all communications to and from the centralized console will be tagged with the related priority. This priority will differentiate between items destined for the central operations console that pertain to normal operator messages and higher priority types of messages that have to deal with either equipment failures or the requirement for contingency action by the operator.

In the normal operating environment of AFGWC, network control will assume the task of systems scheduling, thereby relieving the operations center of the requirement to maintain cognizance of current systems scheduling and loading. This function will be performed by the network controller, thus reducing the load on the centralized operations console. Additionally, in the enhanced AFGWC architecture, the response to various program parameters executing in the main processors will be provided by the systems support consoles; i.e., special operations consoles, forecaster consoles, and program consoles.

2.4.5 Continuity of Operations (F4500)

In this functional area, AFGWC will be expected to provide backup support as necessary to the following agencies:

a. ETAC (Environmental Technical Applications Center)

b. Carswell ADWS

c. NWS (National Weather Service)

d. FNWC (Fleet Numerical Weather Central)

2.4.5.1 ETAC (F4510)

By 1982, AFGWC will provide the capability to assume, on a degraded basis, the operational functions of the USAF Environmental Technical Applications Center (ETAC) whenever the ETAC facility becomes inoperative for longer than a twelve-hour period. For periods of ETAC outage of more than twelve hours, AFGWC will maintain a 6-12 hour ETAC data base and will accumulate and store five consecutive days of this data base throughout the period of ETAC outage. In addition, AFGWC shall be capable of providing a 90-day archive of processed historical weather data to ETAC in the event that the ETAC outage is of a duration which prevents ETAC from reconstructing the data required to produce a 3-month weather history report.

To meet the ETAC backup requirement as defined, the following scenario has been recommended:

a. AFGWC will provide continuous storage of the ETAC climatological data base.

b. A dedicated communication link will be established between ETAC and AFGWC.

c. ETAC, when operational, will update the AFGWC stored ETAC data base via a dedicated communications link.

d. ETAC will provide to AFGWC the operational computer programs required by AFGWC to maintain and update the ETAC data base during those periods of contingency support.

e. AFGWC will provide a backup capability to ETAC on the following basis:

   1) No support will be provided for periods of outage of 12 hours or less.

   2) For periods of outage of more than 12 hours, AFGWC will maintain a 6-12 hour old data base and will accumulate and store historical weather data for the preceding five days. The accumulation and storage of five-day historical data will be initiated 12 hours after ETAC has been inoperative.

3) AFGWC will provide a 90-day archive of weather data for backup of the ETAC system.

To meet the ETAC continuity of Operations backup requirement, then, AFGWC will be required to perform the following activities whenever the ETAC facility is inoperative for more than 12 hours:

a. Maintain a 6 to 12-hour-old data base whose contact is equivalent to the ETAC climatological data base.

b. Initiate procedures for accumulating and storing historical weather data for five consecutive days commencing 12 hours after ETAC has become inoperative. This activity is to allow ETAC to reconstruct their data base when they become operational.

c. Initiate the procedures for processing and storing, on magnetic tape, data for a 90-day archive of weather history. This activity is to assure the availability of data for a 90-day ETAC weather report in the event the ETAC facility is inoperative for five days or more. It will require AFGWC to operate on its computers, programs equivalent to the current ETAC SPECTRA 70/45 and IBM 360-44 programs. If the ETAC facility is inoperative for a full 90-day period, AFGWC must provide a tape storage capacity for $1,336.5 \times 10^6$ 36-bit words.

d. Provide data as follows:

   1) Summarized data for JOPS
   2) Climo wind input to SIOP
   3) Worldwide airfield summaries
   4) Clear line-of-sight/cloud-free line-of-sight probabilities
   5) Worldwide cloud cover statistics
   6) Moonrise/Moonset - illumination
   7) Sunrise/Sunset - daylight/darkness calculations
   8) Solar geophysical historical information
   9) Diffusion information
   10) Comfort/human stress factors
   11) Tide, wave, storm (oceanic) summaries

e. Provide historical daily weather summaries

2.4.5.2 Carswell (F4520)

Capability to back up Carswell should be available at AFGWC by 1982. Functions will include:

a. Data acquisition from overseas ADWS facilities.

b. Maintaining interfaces with other communication systems.

c. Support to MBWS automated functions--to include data collection, dissemination and display.

d. To provide a total backup capability for Carswell, all input data communication sources to Carswell will be switchcable to AFGWC.

e. Carswell data decoding and data processing computer programs will be available at AFGWC for operation on AFGWC computers.

The missions of the Automated Weather Network (AWN) are: (1) to acquire and transport Sino Soviet weather data to AFGWC and (2) to acquire, process and distribute weather data to various DoD agencies. Carswell AFB is the present site for collecting, processing and distributing AWN data and products. Current AWN data supplied to AFGWC by Carswell represents 26% of the daily data output of Carswell. The other 74% is supplied to various Dod customers.

In the event of a loss of the Carswell facility, overseas AWN data cannot be supplied to AFGWC because (1) there is no direct communication links between AFGWC and the overseas data sources and (2) AFGWC does not have the decoder programs to process data directly from the overseas facilities. These capabilities must be available to AFGWC in order to fully back up Carswell.

2.4.5.3 NWS (F4530)

If operations are disrupted at the NMC, AFGWC will transmit a number of teletype messages and FAX charts. These backup transmissions will include a wide variety of weather summaries, with emphasis on severe local storm forecasts and aviation wind forecasts.

This backup would have negligible impact on data base computation (most of the related computations are already done by AFGWC), a minimal impact on the input functional area, and greater impact on the support area, especially those outputs dealing with facsimile products and teletype messages.

When NMC is completely down, charts will be transmitted on the NAFAX and NAMFAX networks. Teletype bulletins will be transmitted to Carswell for further routing. When communication lines to NMC are operable, GWC will send digital aviation wind forecasts to NWC via high-speed data link through Carswell. However, when AFOS becomes operational, AFGWC will probably be configured as a node on the National Distribution Circuit.

The year 1978 is the assumed date of implementation. There are three parts to the backup requirement:

a. Aviation Winds - These will be supported in the same manner as current operations. Bulletin data will be extracted from the Global Data Base.

b. FAX Circuit - These will not be routinely produced and currently require an extensive manual effort. As many as 59 separate FAX transmissions may be made in a 24-hour period.

c. Severe Weather Function - This partially-manual function may be via a link with AFOS. It will include various watches and warnings. In general, all current formats will be used. Four TTY bulletins and one FAX chart are prepared each 24-hour period to service this function.

2.4.5.4 FNWC (F4540)

The Navy is interested in primary and secondary sensor information from DMSP so that it can perform its missions satisfactorily. The Navy has been able to make plans for linkup with communications satellites to receive this data in the post-1978 time period. Thus, AFGWC's support to FNWC for DMSP will only be from 77-78.

At the present time, small amounts of UNIVAC 1110 time are used to process special sensor data from DMSP and transmit this to FNWC. This information is currently stripped out and sent to the Navy under RTOS control on a dedicated 4800 baud circuit.

Based on extrapolation of current computer times used for processing data, Navy estimates indicate that over 5 hours of 1110 time per day would be required each day for the smooth and fine DMSP data, or over 10 hours of 1110 time for all of DMSP imagery data. This is basically a worst-case assumption, and assumes that the entire global surface would be transmitted. This obviously is an undesirable situation, especially considering the limited capabilities of the 4800 baud circuit.

The Navy has suggested that some crude preliminary filtering be accomplished at System V or its equivalent prior to transmitting the imagery data to the Navy. For example, computer time can be cut in half simply by deleting information on the southern hemisphere, which is assumedly relatively unimportant to the Navy. In addition, all land masses can be blocked out, again by some crude geographical filtering. Together, these two approaches to the filtering would cut down the amount of data that must be transmitted to a little more than 2 hours of 1110 time for the fine and smooth data.

To accommodate the transmission of the large amounts of data that would still remain, the Navy has suggested that some sort of direct high speed line (50 Kilobits) direct from System V or its equivalent should be employed (50 Kilobits is the approximate maximum CTMCs can handle).

2.4.6 Data Base Construction and Maintenance (F4600)

(This topic is treated directly in section 1.9.4.5, Software Development.)

As noted in Section 1.0, SDC is compiling an extensive list of related working papers that were generated as part of the system design effort. Appendices containing these documents will be issued under separate cover.