ESD-TR-75-86

MTR-3022, Vol. 1

JOBSTREAM SEPARATOR SYSTEM DESIGN

SEPTEMBER 1975

Prepared for

DEPUTY FOR COMMAND AND MANAGEMENT SYSTEMS
ELECTRONIC SYSTEMS DIVISION
AIR FORCE SYSTEMS COMMAND
UNITED STATES AIR FORCE
Hanscom Air Force Base, Bedford, Massachusetts

Project No. 522D
Prepared by
THE MITRE CORPORATION
Bedford, Massachusetts
Contract No. F19628-75-C-0001

Approved for public release;
distribution unlimited.

When U.S. Government drawings, specifications, or other data are used for any purpose other than a definitely related government procurement operation, the government thereby incurs no responsibility nor any obligation whatsoever; and the fact that the government may have formulated, furnished, or in any way supplied the said drawings, specifications, or other data is not to be regarded by implication or otherwise, as in any manner licensing the holder or any other person or corporation, or conveying any rights or permission to manufacture, use, or sell any patented invention that may in any way be related thereto.

Do not return this copy. Retain or destroy.

REVIEW AND APPROVAL

This technical report has been reviewed and is approved for publication.

Chester G. Clark

CHESTER G. CLARK, Lt Col, USAF
Project Monitor

Roger R. Schell

ROGER R. SCHELL, Major, USAF
Project Engineer

FOR THE COMMANDER

Frank J. Emma

FRANK J. EMMA, Colonel, USAF
Director, Information Systems
Technology Applications Office
Deputy for Command and Management Systems

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE *(When Data Entered)*

REPORT DOCUMENTATION PAGE

READ INSTRUCTIONS BEFORE COMPLETING FORM

1. REPORT NUMBER ESD-TR-75-86	2. GOVT ACCESSION NO.	3. RECIPIENT'S CATALOG NUMBER

4. TITLE *(and Subtitle)*

JOBSTREAM SEPARATOR SYSTEM DESIGN

5. TYPE OF REPORT & PERIOD COVERED

6. PERFORMING ORG. REPORT NUMBER
MTR-3022, Vol. 1

7. AUTHOR(s)

J. M. Schacht

8. CONTRACT OR GRANT NUMBER(s)

F19628-75-C-0001

9. PERFORMING ORGANIZATION NAME AND ADDRESS

The MITRE Corporation
Box 208
Bedford, MA 01730

10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS

Project No. 522D

11. CONTROLLING OFFICE NAME AND ADDRESS

Deputy for Command and Management Systems
Electronic Systems Division, AFSC
Hanscom Air Force Base, Bedford, MA 01731

12. REPORT OATE
SEPTEMBER 1975

13. NUMBER OF PAGES
51

14. MONITORING AGENCY NAME & AODRESS*(if different from Controlling Office)*

15. SECURITY CLASS. *(of this report)*

UNCLASSIFIED

15a. DECLASSIFICATION/OOWNGRADING SCHEDULE

16. OISTRIBUTION STATEMENT *(of this Report)*

Approved for public release; distribution unlimited.

17. OISTRIBUTION STATEMENT *(of the abstract entered in Block 20, if different from Report)*

18. SUPPLEMENTARY NOTES

19. KEY WOROS *(Continue on reverse side if necessary and identify by block number)*

AFWWMCCS
COLOR CHANGE
COMPUTER SECURITY
PERIODS PROCESSING
REQUIREMENTS ANALYSIS
SECURITY KERNEL

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

The Jobstream Separator (JSS) has been proposed to automate the costly, inefficient, and inconvenient manual process utilized to "change colors" (security levels) at AF WWMCCS sites. The JSS would provide complete isolation among WWMCCS users and data at differing levels by introducing a secure, centralized, certifiably correct, minicomputer system to control electronic switching of peripheral devices during the system reconfiguration phase of the color change. The system would eliminate extensive operator intervention, reduce the delays incurred in the physical removal of storage media, and enable the operator to change security states while maintaining overall security. This report presents a technical and economic assessment of the JSS and recommends development of a prototype system.

TABLE OF CONTENTS

TABLE OF CONTENTS (Concluded)

LIST OF ILLUSTRATIONS

LIST OF TABLES

GLOSSARY

ADP	Automatic Data Processing
color	The specific operational security mode of a computer system consisting of the security classification(s) and/or special access rules that apply to the information accessible by the system, and the clearance and special access class of the users that can access the system.
color change	The complete process of transition of a system from operation at one color to operation at a different color.
GCOS	General Comprehensive Operating System - the operating system used on Honeywell 600 and 6000 series computers.
IOM	Input/Output Multiplexor
JSS	Jobstream Separator System
MPC	Microprogrammable Peripheral Controller
NCALL	A GCOS system command entered at system console by ADP operator to prevent new interactive users from logging on to Honeywell system.
TCALL	A GCOS system command entered at system console by ADP operator to terminate interactive processing by users currently on system.
WWMCCS	World Wide Military Command and Control System - in the context of this report, the term refers to WWMCCS ADP systems which are Honeywell 6000 series computers.

SECTION I

INTRODUCTION

PURPOSE OF THIS REPORT

Volume I of this two part report presents a technical and economic assessment of the Jobstream Separator (JSS). It may be viewed as a combination high-level design and feasibility study, since alternative design approaches, problem areas, and tradeoffs are discussed. The report includes a design overview, functional specification, economic analysis, and recommendation for future implementation of a prototype JSS. This volume references Volume II, which comprises a series of appendices that contain supportive information. Volume II summarizes data collection techniques and results, provides alternative engineering designs, and details the economic analysis offered in Volume I.

BACKGROUND

Air Force WWMCCS sites are currently required to process data of different classification levels for user communities having various clearance levels. There would be no problem in simultaneously processing jobs of different classification levels if a computer system existed that was deemed "secure" and provided the necessary access control mechanisms to insure complete separation and protection of jobs executing at different security levels. However, present WWMCCS hardware and software (Honeywell 6000 series machines operating under the GCOS operating system) are incapable of preventing access by users to any information that the WWMCCS processor can address. Thus, information that is to be made inaccessible to a user, or class of users, must be isolated from the machine.

The lack of hardware/software security mechanisms has played a significant role in shaping the security and operational policies employed at WWMCCS sites, and has spurred the development of procedures that enforce complete separation of environments at different security levels. These procedures, which are necessary from a security point of view, dictate that WWMCCS processing (system usage) be a function of security level. Only one level may be active at a time and each level constitutes a "period". Although necessary, the separation of input jobstreams by security level is costly, inefficient, and inconvenient, especially since the procedures require time-consuming operator intervention when security levels must change.

Period processing is the time-scheduled sharing of dedicated systems. The system is cleared and configured for a homogeneous set of authorized users who process their own data. Upon termination of the allocated period, the system is cleared and reconfigured for the next group of authorized users. Manual procedures are currently used to effect the transition between processing periods (i.e., security levels) -- clearing processors and memory of sensitive data, removing or replacing demountable storage media, physically clearing the facility of all sensitive material, and rebooting the system with a new copy of the operating system.

Although the major benefit of period processing is the secure sharing of computer resources, the process decreases system efficiency due to lengthy transition procedures and thereby restricts and decreases availability of the system to its users. In addition, period processing introduces increased overhead costs in maintaining redundant although differently classified versions of software and data files.

SECTION II

AIR FORCE WWMCCS SECURITY REQUIREMENTS

The purpose of this section is twofold. First it offers a brief summary of operational requirements for Air Force WWMCCS ADP security. The summary focuses on requirements to perform WWMCCS mission and function and not technical requirements necessary to ensure security. Second, this section offers a description of the color-change process currently employed at several WWMCCS sites. A more detailed analysis of the color-change process is presented in Appendix I in Volume II.

OVERVIEW AND SUMMARY OF WWMCCS SECURITY REQUIREMENTS

Resource sharing is a primary factor in determining operational requirements for ADP security. While the existence of sensitive information on every WWMCCS computer creates the basic need for security, it is the need to share data and physical resources in a controlled manner among numerous people, programs, devices and entire systems that shapes security requirements (7).

A summary of some specific requirements for WWMCCS ADP security drawn principally from the SDC report, "Operational Requirements for WWMCCS ADP Security" (8), follows. The requirements enumerated below should be viewed in terms of the question, "What does WWMCCS ADP require in order to perform its mission?", and not in terms of "What are the requirements for a secure system?".

1. Security -- The system must provide security in accordance with regulations set forth in DoD 5200.1-R, "Information Security Program Regulations".

2. Availability -- Use of any WWMCCS system resources (e.g., communication media, languages, access modes, etc.) should be given to any user who has valid need.

3. Concurrency -- Concurrent production (non-programmer) and development (programmer users) work must be supported by the WWMCCS ADP.

4. Variety of User Needs -- The WWMCCS computer systems must accommodate a variety of user access needs. H6000 security developments should not hinder the development of functional mission-related programs.

5. Flexibility -- The system must be flexible and adaptable to changing external circumstances. In addition, security should not constrain the growth and performance of the system when new applications and users are incorporated into the WWMCCS mission.

6. User Impact -- Security features should have little impact on the way a user uses the system.

COLOR CHANGE PROCESS

The color-change process may be viewed as a series of steps performed by WWMCCS ADPE personnel whenever a change in security levels within the Honeywell 6000 system must occur.

The procedures are predominantly security oriented and prescribe the sequence of steps to be taken when changing colors during daily (normal) or crisis situations. The minor variation in procedure noted from site to site can be attributed to factors such as system configuration, workload, or the nature of mission requirements.

Operation

The color-change can be logically divided into three distinct phases (See Figure 1):

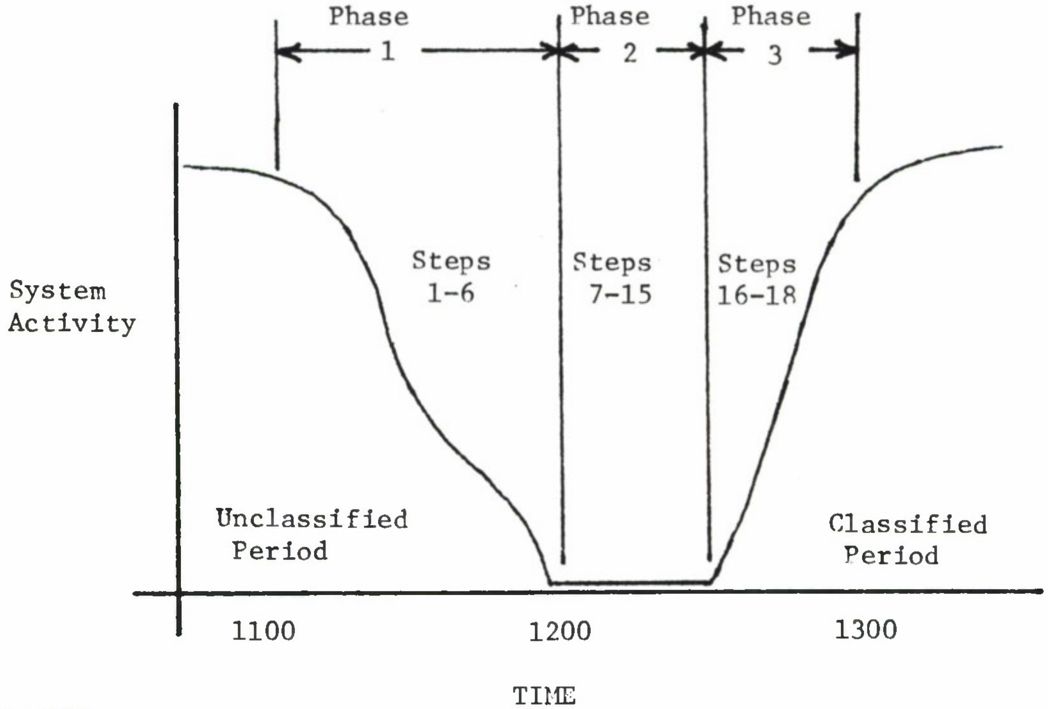
Phase 1 - (pre-change) -- quiesce the Honeywell system in an orderly fashion, so that the processor shutdown can be done without job loss.

Phase 2 - (trans-change)

a. annihilate all traces of the "current" security level by clearing memories, processors, and peripheral devices, and physically removing all storage media.

b. create a "new" security level by introducing a new set of storage media, bootloading a fresh copy of the operating system, and reconfiguring peripheral devices.

Phase 3 - (post-change) -- restart the Honeywell system at the "new level".



LEGEND:

Slowdown Phase

1. No new jobs accepted
2. Warning message to interactive users
3. NCALL issued
4. TCALL issued
5. Wait for Spoolout to finish
6. Perform file backup (optional)

Changeover Phase

7. Remove cards, tapes
8. Clear CRTs, DN-355
9. Clear Core/Dump Core
10. Initialize controllers
11. Change ribbons
12. Reconfigure system
13. Mount new packs
14. Reboot controllers
15. Reboot DN-355

Restart Phase

16. Start Honeywell systems
17. Inform users system is up
18. Accept new logons

Figure 1. Chronicle of 3-Phase Color-Change Activity

Phase 1 -- The Slowdown Period

The primary function of Phase 1 is to ready the WWMCCS system for an upcoming scheduled color-change. This phase is used to drain the system of all active jobs, finish printing activity, perform backup file save procedures and terminate most, if not all, system activity. The duration and start of the slowdown phase is site-specific and is a function of system workload, WWMCCS mission, and system configuration. Usually, this phase begins 45 to 60 minutes prior to the scheduled changeover. Thus, when one speaks of the "start" of the color-change process, a distinction must be made as to what "start" means -- the beginning of preliminary procedures to ready the system for the change in security levels, or the beginning of the color-change activities, proper (see description of Phase 2).

Phase 1 Functions

The major functions performed during Phase 1 activity are designed to:

1. Limit job entry into the system -- Process selected jobs awaiting execution in the input queue, prevent execution of "large" jobs already in the input queue, and save the unexecuted portion of that queue for later processing.

2. Process printout data in the spoolout file (SYSOUT) and/or save the unprinted portion for later processing.

3. Gracefully terminate interactive user activity by providing enough time for users to save files and logoff (20 to 30 minutes prior to scheduled color-change).

4. Back-up (save) system and user files.

5. In the event of emergency processing requirements, terminate the session in the most expedient manner, while still meeting some portion of the above requirements.

Phase 2 -- The Changeover Period

This phase of the color-change process begins immediately following the conclusion of Phase 1 activity. The Honeywell system is in a relatively dormant state at the start of Phase 2 operations -- no user tasks are currently in execution, the time-sharing subsystem has been suspended, all telecommunication facilities shut down, any unprocessed jobs saved, and system and user files backed up. The main purpose of Phase 2 activity is to perform the actual change in colors or security levels. This goal is met by first systematically annihilating all traces of the current system and then creating a new system environment to take the old one's place.

Phase 2 Functions

The functions in Phase 2 activity are to:

1. annihilate current system environment (security level)

   a. dismount all removable storage media (tapes, disks, paper, ribbons, cards)
   b. clear main memory (including GCOS operating system)
   c. clear all buffers and memory in peripheral devices (DATANET 355 Communication Controller, Microprogrammed Peripheral Controller (MPC), Input/Output Multiplexor (IOM), System Controller Units)
   d. perform security check

2. create new system environment (new security level)

   a. mount new storage media
   b. load new version of GCOS operating system
   c. re-initialize all peripheral devices (MPC's, IOM's, disks, tapes, System Controller Units, DATANET 355's)
   d. perform security check-and-double-check procedures

Phase 3 -- The Post Color-Change Period

This phase begins after the conclusion of Phase 2 color-change procedures. A fresh copy of the operating system is ready to be loaded, memory has been cleared, and all devices have been readied.

Phase 3 Functions

The major functions performed during this phase, which is actually the beginning of the "new" processing period, are to:

1. reinitiate the GCOS operating system,
2. make available all user options,
3. reconstruct any suspended spoolout activity,
4. resubmit any pending jobs not previously executed.

The spoolout and pending jobs referred to in steps 3 and 4 are remnants from a previous session at the current level.

SUMMARY OF COLOR CHANGE PROCESS

The color change is not a "bounded, finite period", that can be analyzed and quantified to the nearest minute, but is an "open-ended" process functionally dependent on the WWMCCS site's mission, workload, and configuration. However, once the system has been quiesced and is ready to undergo clearing, reconfiguration and re-initiation, the steps performed on the quiescent system during the change-over period become quite standard and can be analyzed in detail. The periods prior to and immediately following a color-change are variable in duration and flexible in nature. The "effective duration" of a color-change is close to 60 minutes, rather than 30 minutes, which constitutes only Phase 2 activity. Thus, when one talks about a color-change process, it must be made clear which phase is under consideration.

Effectiveness of Color Change

The extent to which current AF WWMCCS color-change procedures meet the WWMCCS Security Requirements enumerated earlier may now be examined.

1. Security: system security is maintained according to DoD standards by securing physical perimeters and by allowing only one classification level to be active at any time.

2. Availability: the availability of WWMCCS system resources is reduced to the extent that color-change procedures occupy potentially productive machine time. In addition, the single-level nature of the processing prevents the system from being available to all users on a timely basis. High-priority processing of a level different from the current one must be delayed until a color-change can be performed, and the work in progress must be discarded.

3. Concurrency: color-changing does not permit true concurrency of production and development work at different security levels.

4. Variety of User Needs: user access requirements can be met only to the extent that they are single-level in nature and able to tolerate the delays inherent in the color-change process.

5. Flexibility: color-change procedures are reasonably flexible, since they are essentially manual. They may, however, limit the growth and performance of the system. The mandatory prior scheduling of infrequent color-changes is inherently an inflexible and cumbersome procedure.

6. User Impact: operation at a single security level places fundamental limitations on a user's capabilities. Additionally, some users are adversely affected by color-change procedures. The requirements that interactive users log-off well before scheduled color-changes, and that job lengths be tailored to the color-change schedule, for fear of delay or loss, may be taken as examples.

SECTION III

JSS FUNCTION

INTRODUCTION

This section focuses on the design criteria used to formulate and synthesize the Jobstream Separator system concept. The first subsection enumerates the full set of JSS requirements. Next, a high-level description of the JSS and its operation during a color-change is offered. Once this operational foundation has been laid, a discussion is presented that addresses secure multilevel processing and certification of the JSS. Ensuing subsections describe the functional elements which comprise the JSS and examine JSS effectiveness in meeting WWMCCS security requirements.

JSS OPERATIONAL REQUIREMENTS

Based on WWMCCS security requirements, the inadequacies of the current procedures noted previously, and data obtained from the JSS requirements analysis survey of the AF WWMCCS complement (see Volume II, Appendix VII), several JSS requirements may be specified. Some JSS operational requirements are:

- Shorten Phase 1 activity. A fast process must be developed to terminate all system and user activity in order to prepare for scheduled color-change.

- Shorten Phase 2 activity by eliminating or reducing manual operations.

- Provide a quick means of restarting the Honeywell system where it left off at a previous level rather than with a freshly initialized operating system.

- Provide the system with complete report generation, log entry, and journalization of the color-change process.

- Provide self-checking hardware components that can detect failures that might compromise security during the color-change.

- Provide the operator with the ability to override all hardware and software facilities. The operator must be able to return to current manual procedures if so desired.

- Display instant, accurate summary data so that the operator can keep abreast of the automated color-change.

- The system must serve as stop-gap, short-term solution.

- The system must permit tailoring to specific sites.

- Must provide easy to use interface with operator.

- Automate the clearing of peripheral and system equipment.

- The JSS software must be small and certifiably correct.

- The JSS must not require major or numerous changes to existing GCOS.

- Must serve as add-on security control facility.

SYSTEM DESCRIPTION

The Jobstream Separator is an automated, centralized, certifiably correct, minicomputer system that controls electronic switches connected to various peripheral devices for purposes of dynamic reconfiguration (4). The proposed system is based on a secure minicomputer connected to both the main processor (H6000 series single or dual processor) and to an array of hardware switches that are, in turn, connected to various I/O devices. The minicomputer changes the security level of the WWMCCS computer system while maintaining overall security.

The crux of the proposed system is to provide complete isolation among users and data at differing security levels, with emphasis placed on implementing the isolation by use of electronic switches controlling reconfiguration rather than physical removal of media. A generalized system configuration implementing the concept is shown in Figure 2.

The basic function of the JSS can be explained in terms of Figure 3, a pictorialization of JSS functional requirements.

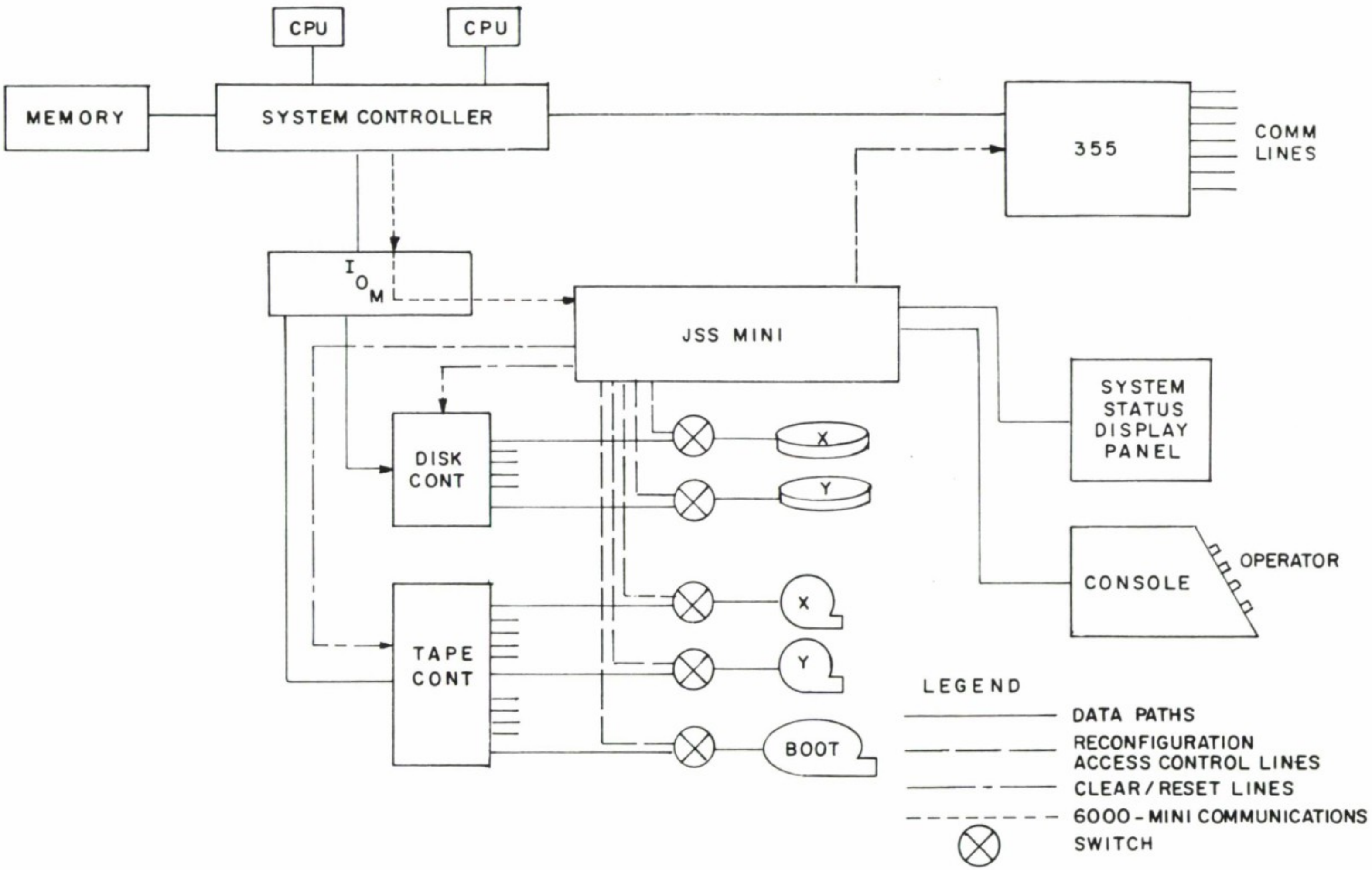
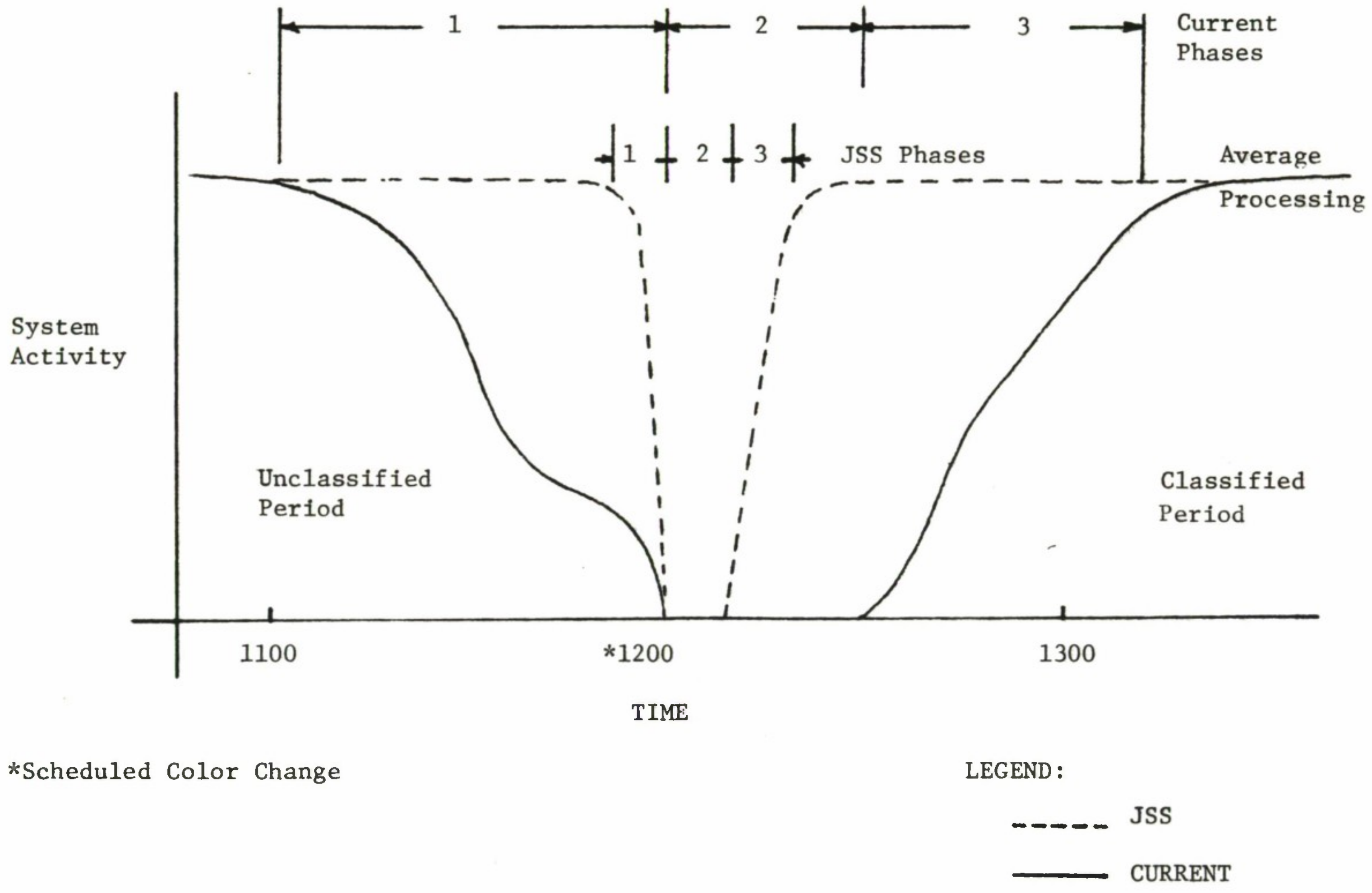


Figure 2. Generalized JSS System Configuration
Emphasizing Access Control Lines



*Scheduled Color Change

Figure 3. Functional Requirements for Proposed System

One can see from Figure 3 that the JSS allows the onset of Phase 1 to occur much later in the normal processing period. That is, Phase 1 slowdown activity occurs approximately 5 minutes rather than an hour before the change. Also, the duration of Phase 2 activity has been lessened, and Phase 3 activity, the restart period, has a steeper rise-time, and therefore, reaches "average" processing throughput much sooner than does the existing system.

Description of JSS-Controlled Color-Change

Table I summarizes the steps or system events that would occur when a JSS minicomputer is in control of the color-change process. Figure 4 gives a picture of timing considerations of the new process.

The color-change begins with the initiation of a special task that saves pertinent system state information and quiesces the operating system. The correctness of the save operation is important to the reliable resumption of processing, but has no security implications. Once the system has been quiesced (no jobs are in execution, and memory and all device buffers have been saved), the GCOS system notifies the minicomputer that quiescing is completed. The GCOS operating system may now be annihilated and cleared for security purposes.

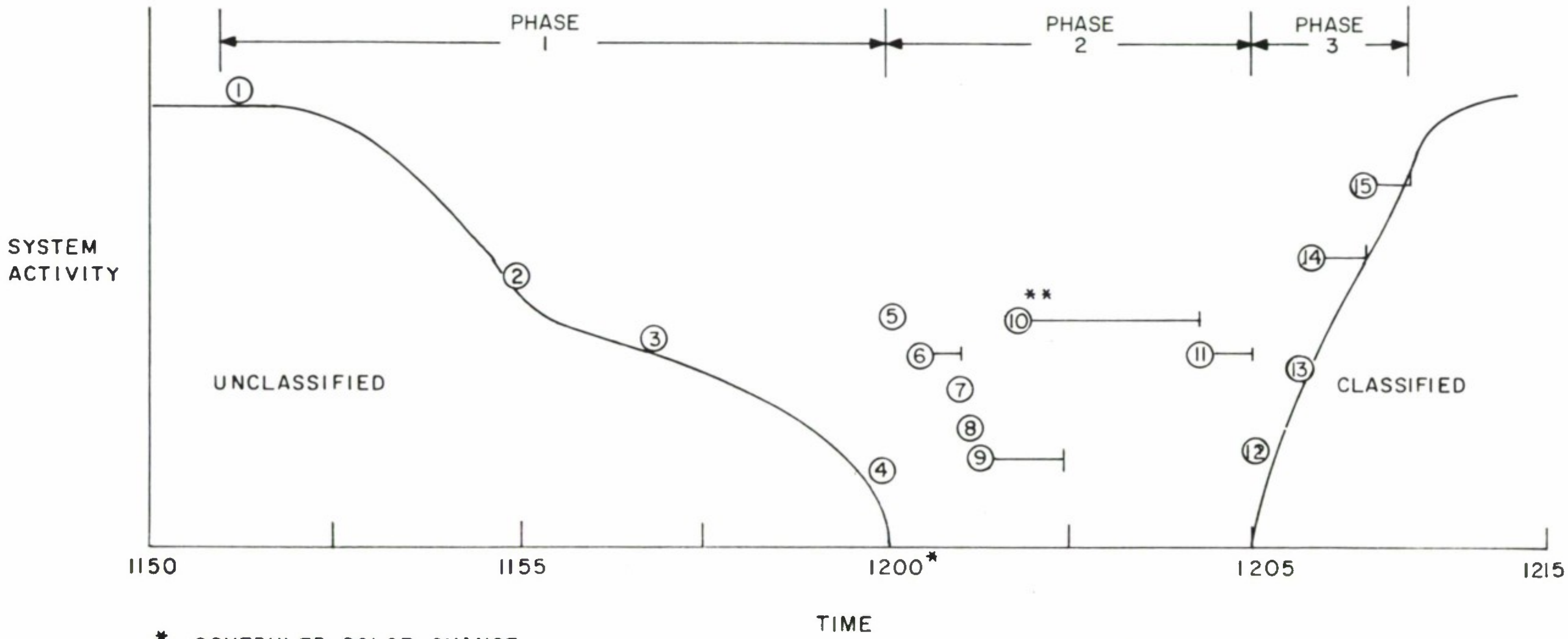
Assume for the moment that a color-change from security level X to security level Y is in progress and that, as today, different types of information are segregated on separate storage devices (marked X and Y in Figure 2). In operation at sensitivity X, the minicomputer closes the switches to the disk and tape drives of level X and opens switches to all other drives. This configuration prevents the forwarding of level X communication that might compromise that information's security. When a color-change is to occur the minicomputer opens all switches to level X drives. It then attaches (connects) a read-only "Clear" boot-load tape ("BOOT" tape in Figure 2) to the tape controller and sends a signal to the processor's boot-load control line. The clear program, a stand-alone program that exists in some form at every WWMCCS site, is the only security-related main processor program and serves to initialize the main processor, memory, and various system controllers.

When the clear program terminates, the system is ready for reconfiguration, during which time the level X drives (including those in the level X operating system) will remain disabled, and level Y drives (level Y operating system) will be enabled.

Table I

JSS Controlled Color-Change Checklist

Step	Event
0.	Baseline Activity.
1.	Phase-1 begins. Interactive users warned 10 minutes prior to scheduled color-change. Users given 5 minutes to finish up. NCALL system command issued to prohibit new logons.
2.	Interactive users logoff; operator issues TCALL command.
3.	QUIESCE GCOS. Operator/mini initiates special GCOS task that interrupts active system and user tasks.
4.	GCOS quiesced. No user or system job activity-end of Phase-1.
5.	Phase-2 begins. JSS electronically disconnects all devices of current level, including system save disk pack.
6.	Purge Program loaded and executed.
7.	Main memory, processor registers, system controller registers, IOM buffers and registers, and microprogrammed peripheral controllers are all cleared.
8.	JSS disconnects drive containing clear program.
9.	Operators remove cards, listings of old level from machine room. Ribbons on printers and console are dismounted.
10.	Disk drive reconfiguration begins. If not enough drives are available for new level, operators remove some current level packs to free the needed number of drives. If enough are free, no dismount/mount operations are performed.
11.	JSS electronically enables (connects) drives of new level, Phase-2 ends.
12.	Phase-3 begins - new level activated.
13.	All devices are reinitialized.
14.	If a new level is to be a continuation of a level that was previously active (a level that was interrupted for a color-change), then disks, tapes and printers are repositioned to where they were when interruption by checkpoint process occurred.
15.	I/O operations at new level are restarted, if any. Phase-3 ends.



* SCHEDULED COLOR CHANGE

** VARIABLE DURATION (0 TO 5 MINUTES DEPENDING ON # OF DRIVES)

NOTE:
SEE TABLE I FOR
DESCRIPTION OF
ENCIRCLED NUMBERS

Figure 4. Chronicle of JSS-Controlled Color Change Activity

The minicomputer opens the switch to the "clear" tape, closes switches to level Y drives and initiates another boot-load, this time from a drive containing a previously saved level Y system state. If no previous level Y system state exists, processing starts anew.

SECURITY OF THE JOBSTREAM SEPARATOR

Introduction

The Computer Security Technology Planning Study panel, (1) sponsored during 1972 by the Air Force Electronic Systems Division, was convened to define a coherent approach to the problem of "multi-level" computer security -- the problem of sharing computer services and information in a controlled way among users of varying clearances. The panel recognized the futility of correcting the flaws in current operating systems and recommended instead that developers of secure systems "start with ... a model ... refine and move (the model) through various levels of design into the mechanisms that implement the model system" (1).

The panel recommended that the model represent an abstract reference monitor that controls the access of subjects (active system elements) to objects (items of information) within the computer system. Figure 5 presents a schematic diagram of the relation among subjects, objects, reference monitor, and reference monitor data base. The figure gives examples of typical subjects, objects, and data base items.

In operation, an implementation of a reference monitor allows or forbids access by subjects to objects, making its decisions on the basis of subject identity, object identity, and security information. The implementation of the reference monitor both mechanizes access rules and ensures that they are enforced within the computer.

The security technology panel stated that a reference monitor implementation must meet the following three requirements:

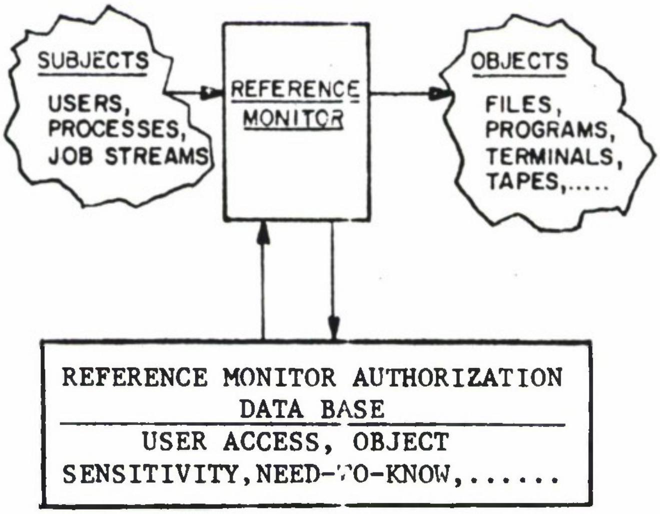


Figure 5. Reference Monitor

1. Completeness -- The implementation must be invoked on every access by a subject to an object.

2. Isolation -- The implementation and its data base must be protected from unauthorized alteration.

3. Certifiability -- The implementation must be small, simple, and understandable so that it can be verified to perform properly.

The requirement for completeness demands that the implementation of the reference monitor include both hardware and software to avoid the complexity and overhead that would result from software validation of every access. The requirement for certifiability makes the same demand because certain hardware architectures preclude the implementation of a small, simple reference monitor.

The requirement for certifiability requires in turn a criterion for certification -- a definition of the correct operation of a reference monitor. Such a definition has been developed by MITRE with ESD sponsorship (3). The definition takes the form of a very general finite-state mathematical model of a secure information system. The model characterizes an information system in terms of its subjects and objects, their classifications and compartments, and the current (instantaneous) and allowed (potential) accesses of subjects to objects.

In addition to describing the state of a secure information system, the model includes functions that can cause the system to make transitions from one secure state to another. These functions express such operations as the creating and deleting of objects by subjects and the gaining and releasing of read or write access to objects by subjects. In each case, the function identifies conditions on the state of the system that determine whether the state change is allowed and specifies the new state if the change is allowed.

The finite-state security model has been used to guide the design of a reference monitor implementation using the DEC PDP-11/45 minicomputer (6). The software portion of this reference monitor implementation is referred to as the security kernel. The kernel software and PDP-11/45 create a virtual environment for processes that will execute uncertified programs. The environment is similar to that in a real PDP-11 in that it has the general purpose registers and instruction set of the PDP-11. The virtual environment has, however, a much different memory structure -- a non-random access segmented virtual memory that is selectively shared with other processes. The kernel provides the process with functions for operating on the virtual memory, and for communicating and synchronizing with other processes. Programs executing in the process can execute any unprivileged PDP-11/45 machine instruction or invoke any kernel function, although in either case the desired operation can be aborted (by the segmentation unit or the kernel) to prevent a security compromise from occurring.

The reference monitor design implements the subjects of the model as processes and the objects as segments, input/output devices, and interprocess communication channels. The kernel program includes an entry point corresponding to each function of the model. In addition, two other classes of functions are required to fit the reference monitor implementation into an environment of finite hardware with limited functions. The first added class of function provides for altering the representation of the current security state -- for example, by multiplexing one processor among many processes. The second added class provides interpretive access to those objects like interprocess communication channels whose direct reading and writing cannot be adequately restricted by the PDP-11/45 hardware.

The technical verification that an implemented reference monitor is a true representation of the security model requires a formal proof. The proof approach that has been developed (2) requires the description of the reference monitor by a formal specification. Such a specification can be proven to be both internally consistent and in direct correspondence with the rules and states of the security model. The specification, in turn, imposes requirements for the proof or testing of the reference monitor software and hardware.

Security of the Jobstream Separator

The discussion above has defined the reference monitor concept and indicated, in a very general way, the approach to certifying a reference monitor's security. The security of the Jobstream Separator configuration is based on the recognition that a Jobstream Separator can implement a reference monitor. While the Jobstream Separator design concept was first devised in 1970, there was no fundamental basis for certifying it as secure at that time. It was not until 1972 that the reference monitor concept was defined.

A subsequent "rediscovery" of the Jobstream Separator concept in late 1973 was followed by the realization that the reference monitor concept provided a basis for certifying a Jobstream Separator as secure. For the certification of the Jobstream Separator to be carried out, it is necessary to identify subjects and objects in the system, and to assure that the three requirements for a reference monitor implementation are met.

The active elements in a system including a Jobstream Separator are entire jobstreams of uniform sensitivity. Thus these are the subjects whose operations are controlled. The objects that the subjects access are the peripheral and storage devices controlled by the device access switches. With this identification, it can be seen that every access by a subject to an object is mediated by the switches of the reference monitor. Similarly it is clear that the Jobstream Separator minicomputer and switches are isolated from access by the jobstreams.

The requirement for certifiability of the reference monitor mechanism must be met in the context of the computer security model described above. The design proposed below is only one of several that might be proven equivalent to the model. Its virtue is that it is reasonably understandable and makes maximum use of existing certification results.

The basic design strategy for certification of a Jobstream Separator is to use a security kernel in the Jobstream Separator minicomputer. The kernel can have the same organization as an existing kernel but must support a special class of processes, and a special class of objects. The special processes are "surrogates" for the various jobstreams that may be active in the controlled WWMCCS computer. The special objects are similarly surrogates for the individual disk and tape drives that are controlled by the minicomputer.

In operation, the augmented security kernel may allow only one surrogate process, corresponding to the active WWMCCS processor jobstream, to be active at a time. The surrogate need not control the minicomputer's processor while it is active, but must relinquish its active status explicitly before another surrogate can become active. When the kernel "multiprograms" surrogate processes, it must disconnect the device switches of the old process level, clear the WWMCCS processor's main memory, registers and control units, and connect the switches of the new level. The operations described are entirely analogous to those that the kernel performs when it unloads and reloads the machine registers and memory map while multiprogramming ordinary processes.

While color-changing on the WWMCCS processor corresponds to multiprogramming of surrogate processes, reconfiguration of drives from level to level corresponds to creation and deletion of objects. If a disk drive is to be changed (say) from unclassified to secret, an unclassified process must first destroy the object corresponding to that drive. This destroy operation will have the effect of denying the unclassified surrogate process access to the drive -- or turning the control switch off. Then a secret process may create an object corresponding to the drive, and a secret surrogate process may then get access to the drive -- turning the switch on. The distinction between "processes" and surrogate processes in this paragraph assumes that non-surrogate processes are used to interact with the operator's control panel and to establish the environment in which surrogate processes (and hence the WWMCCS processor) run. This approach enhances the system's flexibility since these non-surrogate processes can multiprogram on an arbitrary basis, unlike the surrogate processes which cause a color change by becoming active.

The use of surrogate objects to represent controlled drives allows the Jobstream Separator to support the reading of lower level media by higher level jobstreams. The PDP-11/45 security kernel supports such a "read-down" option for all objects. For the option to be useful in the Jobstream Separator, the switches and drive interfaces must be configured to support pure read-only access by the WWMCCS processor. If the configuration does not support such access, the kernel can simply disallow it.

While the destroy and create operations control the internals of the access to drives, they do not insure that an operator has dismounted unclassified media and mounted secret. Some operator interaction must be associated with the change of media, and must be guaranteed by the Jobstream Separator. The best approach to obtaining this guarantee is probably to augment the kernel further with mechanisms to insure that the drive is turned off when an object is deleted, and that an operator has taken some action when an object is created.

The general design approach outlined above can be translated into formal specifications in a reasonably straightforward way. The existing formal specification for the PDP-11/45 security kernel need only be modified by the addition of special objects and surrogate processes. The specifications for handling both surrogate process and special objects parallel those for ordinary processes and objects, so little innovation is required. Only the semantics of some operations will be changed to reflect the characteristics of the new subjects and objects. Similarly, the proof effort being expended on the security kernel for the PDP-11/45 will guide the Jobstream Separator proofs, and major elements of the proof can be used intact.

Minicomputer Requirements

The discussion above has described an approach to assuring the security of the Jobstream Separator. As this approach is based on the use of a security kernel in the separator minicomputer, it is appropriate to discuss the hardware requirements of a security kernel.

The key attributes of the PDP-11/45 that are used by the security kernel are its memory management (segmentation) unit and its possession of two domains of privilege.* While the PDP-11/45 is relatively fast and costly, slower, cheaper minicomputers such as the PDP-11/35 also possess the required hardware attributes. Other manufacturers' computers (Data General, Varian, etc.) also possess the required characteristics, but would require the development of security kernels from scratch.

The remainder of this paper assumes the use of a PDP-11/35 minicomputer with a security kernel based on the one that has been developed for the PDP-11/45. Other alternatives may be considered preferable** if and when a Jobstream Separator is implemented, but the PDP-11/35 and kernel provide a basis for planning.

JSS FUNCTIONAL ELEMENTS

Minicomputer Functions

This subsection offers an overview of the functions performed by the JSS minicomputer during normal (non-color change) and color-change periods. The points enumerated below are addressed in more detail in ensuing discussions. The minicomputer must:

* In fact, the PDP-11/45 supports three domains, but only two are required for a relatively simple application like the Jobstream Separator.

** For example, ESD has contracted with Honeywell for a study of secure minicomputer architectures which might ultimately result in additional secure minicomputers and kernels.

- interact with the operator.
- perform status checking of access control switches.
- control the system status display panel.
- monitor mounting and dismounting of removable storage media.
- reconfigure tape and disk drives.
- clear and reset system devices in the final stages of color-change.
- collect statistics.
- produce a summary report and log of color-change actions.
- provide an automated checklist.
- provide the operator with override capability.
- communicate with the H6000.

The minicomputer-operator interface allows the operator to enter commands or queries. Commands direct the minicomputer to perform a desired service (e.g., reclassify the security level of a drive, disable a malfunctioning access control switch, override a software task, update a system table). Operator queries request that the minicomputer produce reports on the minicomputer's console or printer, if one is available, (e.g., device availability, device security level, system status, current phase of the color-change, system statistics, etc.). Another facet of operator-minicomputer interaction enables the operator to enter a detailed description of the WWMCCS system environment. Typical specifications include number of disk and tape drives, access control switch connection mappings, number and type of security levels to be processed, etc. The description, which is usually a "one-shot" process performed when the minicomputer is made operational for the first time, can also be used if an existing configuration is modified (e.g., a disk drive is added) in any way.

The minicomputer serves as a system monitor during "normal" operating periods. By awakening a special status checking routine on a periodic basis, the minicomputer insures that the actual status of an access control switch is equal to the expected status contained in the minicomputer's internal table.

As an added security feature, the minicomputer monitors all mount and dismount operations performed by operators. Although one of the basic requirements of the JSS is that it reduces the number of mount and dismount operations performed during a color-change, some may be required due to a lack of available disk drives. When such an occasion arises, the minicomputer insures that a disk pack or tape reel of the proper security level is mounted on the appropriate disk or tape drive, by matching data obtained from bar-code labels attached to the drive and storage media with expected data stored internally.

Table II summarizes the system functions performed by the minicomputer during the course of daily operations. In most instances, there is a distinct minicomputer system task that performs the function outlined in the table.

Table II

Summary of System Functions Performed by JSS-Minicomputer

Phase 1. Pre-Color Change (monitoring system during normal operation)

a. Status checking of peripheral devices.
b. Operator intervention -- commands to initiate color change.
c. Error-condition identification.
d. Report generation.
e. Control of display devices/panels.

Phase 2. During-Color Change

a. GCOS Communication.
    (1) Send signal to H6000 to begin clear process.
    (2) Receive signal from H6000 indicating end of clear process.
b. Reconfiguration Activities.
    (1) Connection/disconnection of devices.
    (2) Creation and maintenance of Internal Control tables.
    (3) Allocation of devices (tapes/disks) by mini per operator/GCOS requests.
    (4) Control of display panels.
    (5) On-line security checking during mounts and dismounts (machine readable labels).
    (6) Reporting on status of entire system to operator's console.
c. Clear/Reset Phase - minicomputer program clears and resets buffers in various devices.
    (1) Input/Output Multiplexors.
    (2) Microprogrammed Peripheral Controllers.
    (3) DATANET Communication Processor.
    (4) System Controllers.

Phase 3. Post-Color Change (prior to restart of GCOS system at new level)

a. Statistics collection/summary report.
b. Restart of processing.
c. Checklist of actions performed and remaining.

System Checkpoint/Restart

In order to minimize lost time during Phases 1 and 3 of the JSS controlled color change, the system checkpoint/restart facility must meet the following requirements:

1. Processing and I/O activity must be terminated rapidly and in a state capable of being restarted without error;

2. The detailed state of all system components, that are connected at the current security level and will be connected at a new level, must be stored on a medium which will be isolated from the system at other levels;

3. After the level switch has occurred, the detailed state of all system components that are connected at the new security level must be correctly established, to that which existed at the end of the previous period at this level. Those components which have been connected at another level must have their states restored from saved information. Components which have been disconnected since the previous period at the new level may retain their previous state.

System security is not dependent on the correct operation of the checkpoint/restart facility, so that several alternatives are available for its implementation. Briefly, the requirements may be met by a GCOS-independent program which depends entirely on the capabilities of the H6000 hardware; by the addition of a routine to the GCOS Hard Core Monitor; or by the alteration of a GCOS privileged slave module. An examination of these alternatives is provided in Appendix II, Volume II of this report.

Electronic Switching of Peripheral Devices

The concept of electronic switching of peripheral devices (i.e., tapes or disks) presupposes that a physical switch can be connected from the JSS control minicomputer to various devices. The connection of the switch to the minicomputer raises very few implementation problems. Switches or gates of all types are commonly connected to a variety of minicomputers via a general purpose interface board. Software in the minicomputer is used to send specific digital signals or set voltages on control lines.

The feasibility of providing externally controlled, fail-safe, switches of the sort shown in Figure 2 for disk, tape, and other auxiliary storage devices has already been determined. Each disk or tape drive contains lines whose functions are "reservation control" and "write inhibit". The former line electronically inhibits any access to the drive, while the latter prevents the execution of write operations directed to the drive. If the control minicomputer is given access to these lines, it can deny the WWMCCS processor access to the drive.

A technical problem associated with the control of disk and tape drives is one of providing the necessary access lines and connectors; the circuits within the drive are already present. The provision of reservation control and write inhibit at the drive itself allows the control of access to be independent of the disk or tape control units. Thus, providing the minicomputer with the ability to control access to disk and tape drives appears to require only straightforward engineering. The design of the electronic switch is discussed in detail in Appendix III, Volume II.

Label Reading Mechanism (Optional)

Since the JSS may allow dynamic reconfiguration of peripheral devices (i.e., disk and tape drives), a device could, during the course of daily operation, contain storage media of various security levels. Although the JSS assures that peripheral devices are connected to the computer at the proper time and at the proper security level, it cannot assure that the proper tape or disk is mounted on the correct drive at the correct time.

In order to reduce the possibility of operator error in the mount and dismount process, both during normal processing periods and during the color change reconfiguration phase, a facility based on machine readable label technology may optionally be incorporated into the JSS system. This facility would serve as a means of monitoring the security level of all storage media handled by the WWMCCS computer, and would provide extensive control and verification. Machine readable identification labels would be attached to each tape and disk drive and to each tape reel and disk pack. The operator would be required to input the identification data to the Jobstream Separator at mount time, by stroking a wand across the machine readable data. The JSS minicomputer would compare the security level of the storage medium with the current classification of the drive. If a match occurred the mount operation was successful; if not, an error condition would be signalled to the operator at the JSS console, and the display panel modified to reflect the error and a tone sounded at the wand outlet.

A detailed description of the label reading facility is offered in Appendix V of Volume II.

EFFECTIVENESS OF JSS

The effectiveness of the JSS in meeting the list of WWMCCS Security Requirements is examined in the following paragraphs.

1. Security: system security is maintained by physically securing the system perimeter (as is currently done), by isolating security levels to avoid compromise and by providing a reference monitor, which is physically secure and certified correct, external to the main system.

2. Availability: the availability of WWMCCS system resources is maximized by the rapid security level changes allowed by the JSS. Processing by the system remains single-level in nature, but high-priority processing of a different level from the current one may be quickly accommodated with no loss of the pre-empted work.

3. Concurrency: the JSS does not support simultaneous production and development work at different security levels. The ability to rapidly change security levels does allow production and development processing to be interspersed at frequent intervals throughout the day.

4. Variety of User Needs: the JSS supports only single-level processing. It drastically reduces the delays induced by the color-change process, by allowing both rapid and frequent security level changes to meet immediate user requirements.

5. Flexibility: the modular, expandable nature of the JSS allows it to be tailored to a system's requirements, and to be altered when they change. Relatively frequent and flexible occurrences of security level change are allowed by the JSS.

6. User Impact: the limitations due to operation at a single security level are still present with the JSS. The adverse impact of changes in security level is minimized by the rapidity of the JSS-controlled change and by the preservation of work in progress prior to initiation of the change.

SECTION IV

ECONOMIC ANALYSIS

INTRODUCTION

This section of the report presents the economic aspects of the Jobstream Separator (JSS). It presents the costs to acquire, test and evaluate a prototype JSS at a WWMCCS site, and the costs to implement a phased program of providing this added capability at five additional WWMCCS sites. Furthermore, this section presents an implementation schedule that forms the basis for the phased funding required for the JSS program. The final portion of this section presents an evaluation of the costs and the benefits to be derived from the implementation of the JSS program.

METHODOLOGY

The method used in this economic analysis was first, to estimate the cost of a prototype JSS at a single WWMCCS site, including the installation, test, and evaluation of its operational capability. These costs are considered RDT&E costs and are of a non-recurring nature. In addition, the investment costs to equip five additional sites were estimated, as were the annual operation and maintenance costs for all six sites. The total non-recurring RDT&E costs were apportioned among the six JSS sites in order to determine the average cost of a JSS site.

The costs for a JSS site were then compared with the benefits that the added capability provides. Some of the benefits are qualitative in nature; the emphasis here is on quantitative aspects, such as annual loss of computer time and the dollar value of such a loss, and a cost comparison between the JSS total cost and the dollar value of the lost computer time.

Costing Ground Rules and Assumptions

For costing purposes, the following ground rules and assumptions were made. The ground rules define the methodology used in developing and presenting the costs; the assumptions define those cost sensitive areas that have not been completely coordinated with higher headquarters, which were made on a tentative basis in order to proceed with the analysis.

Ground Rules

- The economic analysis was performed according to the guidelines provided in Department of Defense Instructions No. 7041.3, October 1972.
- The costs included in the estimates are those applicable cost elements listed and defined in MIL-STD-881.
- The costs for the JSS program were phased by fiscal year on the basis of the assumed implementation schedule.

Assumptions

- System design, engineering, integration and technical direction will be performed by the Air Force using in-house resources.
- The cost of additional peripheral storage devices that might be incorporated in a JSS configuration is not reflected in these estimates. Such devices are not an inherent part of the JSS system.
- No additional personnel will be required to operate and maintain the JSS.
- The JSS will remain in operation until 1980 at which time its function will be replaced by a secure multi-level processing capability.
- The JSS will be installed at a total of six AF WWMCCS sites (including the prototype site). Four of the six systems are MAC, SAC, NORAD/CONAD, and AFDSC. These are large systems that process multi-level data, and with the exception of AFDSC (which operates in a controlled sharing "high-water mark" environment), perform color changes on a regular basis. The two remaining target systems for a JSS represent an arbitrary number of smaller sites that do not currently perform color changes or perform them infrequently; applications growth at these sites is expected to result in security requirements where none currently exist.

Implementation Schedule

The implementation schedule assumed for the JSS program is presented in Figure 6. Though the schedule is technically feasible, other constraints such as time required for program approval, availability of funds, budget cycle, have not been considered at this time. Certain comments pertaining to the schedule are warranted, as follows:

- The operational date for the five non-prototype JSS sites is based on a plan of concurrent procurement, installation and check out at all sites. Overseas JSS sites may require additional time. Nine months are allotted between program approval and issuance of a contract. This is an optimistic schedule, since most of the system design and performance specifications will have been completed by the time the program is approved. This period is used to generate Requests for Proposal (RFP).

COST ESTIMATES

Summary

A summary of the total costs estimated for the JSS is presented in Table III. The costs include recurring and non-recurring costs and are aggregated into RDT&E, Initial Investment, and Annual Operations and Maintenance.

The minimum cost estimated for the single prototype JSS site (later to be an operational site) is $765K, of which $685K is non-recurring. The $75K recurring costs cover procurement of the mini-computer and additional hardware, spare components, and transportation. Each additional JSS site will incur $75K of investment costs and approximately $5K per year for its maintenance.

The total cost of a six site JSS program, based on one year of operation with concomitant O&M cost, is $1,165K. The average cost for the six sites is approximately $195K per site through the first year of operation and maintenance. The details of these costs are provided in the following section.

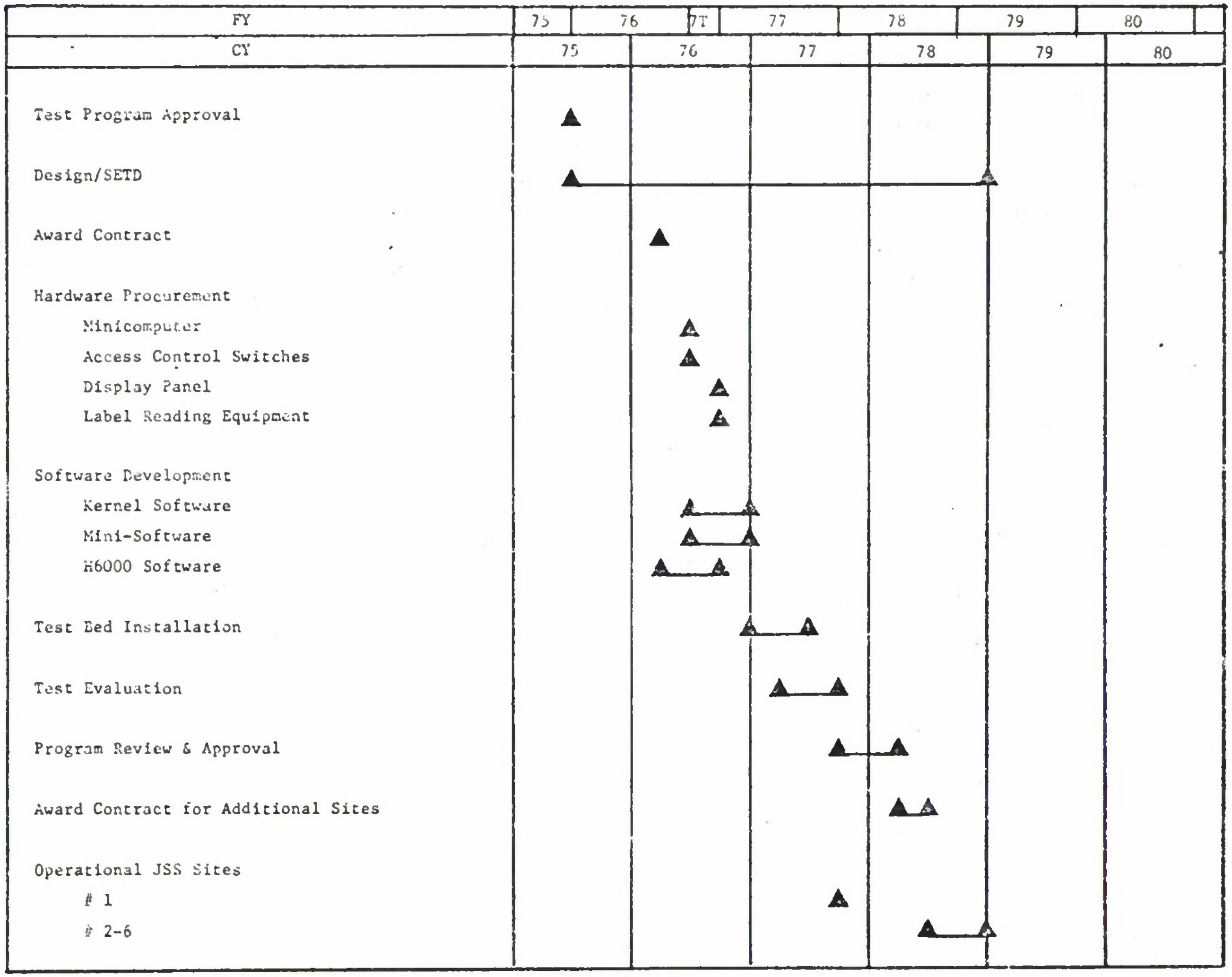


Figure 6. Implementation Schedule by Calendar Year

Table III

JSS Summary Costs
(Thousand Dollars)

	RDT&E		Initial Investment	1 Year O&M	1 Year Total
	Non-Recurring	Recurring			
PROTOTYPE SITE	685	75		5	765
ADDITIONAL COST PER SITES			75	5	80
TOTAL SIX SITE JSS PROGRAM	685	75	375	30	1165

Detailed Costs

The details of how the costs were derived, the rationale used and other supporting data are presented in this section. Table IV presents a further level of detail of the costs to develop, acquire and operate the six JSS sites for one year.

- System Design and Engineering: This element was estimated on the basis of five engineering man-years at $60K per year. On the basis of the implementation schedule (Figure 6), it is determined that 3 engineers will be required to prepare design and performance specifications and prepare a bid package over a 9 month period. A minimum of one engineer will be required to monitor the program from contract award date to operational date of the JSS sites.

Table IV

JSS Detailed Costs

	(Thousand Dollars)	
RDT&E		
System Design, Engineering	300.	
Subsystem Development		
Hardware	20.	
Software	240.	
Data	50.	
Install, Test and Evaluate	75.	
TOTAL RDT&E		685.
INVESTMENT		
Hardware	360.	
Spares	70.	
Transportation	20.	
TOTAL INVESTMENT		450.
ANNUAL O&M		
Maintenance and Spares	30.	
TOTAL JSS PROGRAM		1,165.

- Hardware Development: This is an engineering estimate of $10K to design and develop the display panel and $10K to design and develop the necessary electronic switches.

- Software Development: This is based on an estimate of 49 man-months at $60K per man-year. This includes fifteen man-months to modify and recertify the secure kernel software; sixteen man-months for the minicomputer software and eighteen man-months to modify the H6000 software. See Table V for further details.

- Data: Documentation is based on 20% of the hardware and software development costs of $260K.

- Install, Test and Evaluate: Based on one engineering man-year at $60K and one-half technician man-year at $30K. The installation is estimated to require 30 days per site, while the testing and evaluation is estimated at 60 days per site.

- Hardware Costs: The hardware costs of $360K included under Investment is intended for the following items:

- 6 Minicomputers and peripherals	@ $40K	- 240.
- 6 Panels and sets of switches	@ $10K	- 60.
- 6 Label reading equipments	@ $10K	- 60.

- Spares: This amount represents the spare parts required for the first year of operation and is calculated on the basis of 20% of the initial hardware costs.

- Transportation: The cost to ship the equipment in addition to the spares required for the first year of operation is estimated at 5% of the value of the equipment and the spares.

- Annual Maintenance and Spares: The $30K figure is an engineering estimate based on monthly maintenance figures of comparable commercial equipment.

Table V

Software Development Estimates

SYSTEM	SUBTASK	MAN-MONTHS
JSS Minicomputer	Kernel Modification and Certification	15
	Access Control Switch Software	4
	Display System	4
	Mini-H6000 Communication	4
	Set/Clear of Honeywell Hardware	4
TOTAL		31
Honeywell 6000 Series GCOS Additions and Modifications	Quiescing Program	15
	H6000-Mini Communication	3
SUB-TOTAL		18
TOTAL MAN-MONTHS		49

Phased Funding

The costs for the six site JSS program shown on Table VI ($1,165K for one year of operation and 30K per year for continued operation through FY 1981) lends to a total program funding reequirement of $1,225K. These funds are phased by fiscal year on the basis of the Implementation Schedule shown on Figure 6. The funds are presented by budget appropriation and total funds required for each fiscal year.

Table VI

JSS Program Phased Funding

FY	75	76	7T	77	78	79	80	81	TOTAL
RDT&E (3600)		295	135	120	120	15			685
Equipment Procurement (3080)			60		320	70			450
O&M (3400)						30	30	30	90
TOTAL		295	195	120	440	115	30	30	1225

COST/BENEFIT EVALUATION

This section of the Economic Analysis will address and evaluate the costs to be incurred and benefits to be derived with the implementation of the JSS. The costs of JSS have been shown to average $20K per site over the projected three-year life of the six site system. The benefits to be derived by this expenditure will be presented in this section of the report with supporting data included in Appendix VI of Volume II. Because each WWMCCS site might benefit from the JSS in a different way, due to different equipment configurations and equipment utilization, a single measure, dollars per computer system hour, will be used.

The basic benefit to be derived from the JSS is the reduction in H6000 computer lost time, from the current 45 minutes average for a color change to 10 minutes average. The savings of computer time, developed in Appendix VI, is as follows:

	Computer Time Saved
- Savings per site per year:	639 hours
- Savings per site for program life:	1,917 hours
- Savings for six site program:	11,502 hours

The loss of computer time must impact upon individual sites in at least one of several ways: by introducing additional delays in processing priority, routine, or deferred jobs; by requiring the manning of additional computer operations shifts, or a larger operations staff per shift; or by forcing the procurement of additional equipment, or modification of existing equipment, to increase the site's throughput and/or processing capability. The specific effect has not been defined, because each site would solve the loss of computer time in a different way; however, there is an intrinsic value to computer hours which for the purpose of this report has been set at $429/hour. This is equivalent to $268K per site per year or approximately $4.83 million during the three-year projected life of the six site system. Detailed derivation of these amounts can be found in Appendix VI of Volume II. The total program cost of $1.2 million for the Jobstream Separator System compares favorably with this figure.

Conclusions

The quantitative and qualitative effects described above are not intended to be absolute measures of the JSS' effectiveness. They illustrate the benefits that should accrue, depending upon the WWMCCS sites selected for JSS implementation. The quantifiable benefit is a savings of $4.83 million in H6000 series computer time, in return for an overall program cost of $1.2 million for the six site, three-year program. The non-quantified benefit is the ability to respond more rapidly to crisis requirements, without the degradation of response time presently imposed by security requirements.

SECTION V

RECOMMENDATION AND CONCLUSION

It is intended that the JSS provide the requisite isolation of security levels with a much lower penalty in time and inconvenience than is exacted today. The system is an application of existing security principles to a current security/operations problem. As such, the JSS may be viewed as both an interim and an alternate solution. It is an interim solution because it will aid WWMCCS users until the more general multilevel security solution is available. It is an alternate solution because it provides a means to improve operations for sites which will not be immediately able to upgrade their present equipment when a secure general purpose system becomes available.

The proposed system design is based on known principles of computer security and would not compromise the protection of information. Since precise requirements exist for maintaining a secure environment, the Jobstream Separator can be shown to meet these requirements. The implementation would result in some cost for additional equipment, but it offers the prospect of improved efficiency of main processor usage and improved user service on existing WWMCCS hardware. The existence of a prototype Jobstream Separator would provide system managers with an alternate mode of operation whose costs and benefits would be investigated without fear of compromise of sensitive information.

SUMMARY OF JSS BENEFITS

The advantages of the Jobstream Separator are:

1. Less time spent per color-change.

2. Less system dead-time.

3. Better operational cost effectiveness.

4. More time for productive processing at each level right up to the scheduled color-change time.

5. More colors (security levels) can be active per day -- better mix of security levels means all site operations are being satisfied on a more convenient schedule.

6. Centralized control of WWMCCS system with all security-related aspects of color-change operation under control of certified, secure minicomputer system.

7. Less operator intervention -- speeds up process and reduces likelihood of operator error.

8. Better response-time in the event of crisis situation.

9. No need for procurement of additional processors to provide unilevel, dedicated processing environment.

FUTURE JSS DESIGN TASKS

The JSS is to be "retro-fitted" or incorporated as a component into a large, complex, existing system. Some of the JSS design factors are briefly described in the following paragraphs:

- Minicomputer system -- hardware interfaces, software design, software certification, security kernel, fail-safe mechanism.

- Operator interface to JSS -- human factors analysis of role of operator in JSS-controlled environment, security controls to aid operator (displays, light pens, CRTs, etc.), error recovery procedures.

- Changes in security policies needed if different level storage media are to exist in the same room at the same time. Must ensure that the JSS and procedural controls obviate the need for such stringent regulations.

- Hardware access control switch is needed to connect mini to various devices. Switch must be reliable, economical, and fail-safe; if failure occurs, switch must not permit access to a device and must signal its own failure.

- Access to Honeywell proprietary design specifications will be needed for various system devices and their controllers, in order to establish hardware connection for mini-controlled access switch.

- Modification of portions of the Honeywell system software is required in order to create a checkpoint/restart capability that will quiesce the system in such a manner as to permit restart of all system and user tasks at a later time.

RECOMMENDATION

The Jobstream Separator has been proposed to reduce the inefficiencies and inadequacies of current WWMCCS color-change operations. In view of the benefits to be gained by such a system, it is recommended that a prototype system be built and retrofitted into an existing, fully operational WWMCCS site.

Six AF WWMCCS sites can be equipped with a JSS and be made fully operational by FY78. It is estimated that the savings in H6000 time over a three-year period as a result of JSS operation would have a value of $4.3 million in return for an overall JSS program cost of $1.2 million.

REFERENCES

1. J. P. Anderson, Computer Security Technology Planning Study, ESD-TR-73-51, October 1972.

2. D. E. Bell and E. L. Burke, A Software Validation Technique for Certification: The Methodology, ESD-TR-75-54, April 1975.

3. D. E. Bell and L. J. LaPadula, Secure Computer Systems, ESD-TR-73-278, Volumes 1 and 2, November 1973, Volume 3, April 1974.

4. S. B. Lipner, "A Minicomputer Security Control System", The MITRE Corporation, MTP-151, Bedford, Massachusetts, February 1974.

5. W. L. Schiller, Design of a Security Kernel for the PDP-11/45, ESD-TR-73-294, December 1973.

6. W. L. Schiller, The Design and Specification of a Security Kernel for the PDP-11/45, ESD-TR-75-69, February 1975.

7. System Development Corporation, "A Framework for Computer Security", TM-WD-5733/000/00, 31 March 1974.

8. System Development Corporation, "Operational Requirements for WWMCCS ADP Security", TM-WD-5733/001/00, 31 March 1974.