NBS PUBLICATIONS

NBSIR 79-1725

Phase II Final Report Computerized Site Security Monitor and Response System

R. T. Moore
R. J. Carpenter
A. W. Holt
A. L. Koenig
R B. J. Warnar

Computer Systems Engineering Division
Institute for Computer Sciences and Technology
National Bureau of Standards
U.S. Department of Commerce
Washington, DC 20234

September 30, 1978

Issued March 1979

Sponsored by
Defense Nuclear Agency
Washington, DC 20305

NBSIR 79-1725

PHASE II FINAL REPORT COMPUTERIZED SITE SECURITY MONITOR AND RESPONSE SYSTEM

R. T. Moore
R. J. Carpenter
A. W. Holt
A. L. Koenig
R. B. J. Warnar

Computer Systems Engineering Division
Institute for Computer Sciences and Technology
National Bureau of Standards
U.S. Department of Commerce
Washington, DC 20234

September 30, 1978

Issued March 1979

Sponsored by
Defense Nuclear Agency
Washington, DC 20305

U.S. DEPARTMENT OF COMMERCE, Juanita M. Kreps, ***Secretary***

Jordan J. Baruch, ***Assistant Secretary for Science and Technology***

NATIONAL BUREAU OF STANDARDS, Ernest Ambler, ***Director***

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

PHASE II FINAL REPORT
COMPUTERIZED SITE SECURITY MONITOR AND RESPONSE SYSTEM

by

R. T. Moore, R. J. Carpenter, A. W. Holt,
A. L. Koenig and R. B. J. Warnar

INTRODUCTION

The Computerized Site Security Monitor and Response System (CSSMRS) was conceived as an integrated, state-of-the-art, computer based system to enhance and improve the overall physical security of storage sites for nuclear weapons and materials. This would result from the interconnection of all site security systems including intrusion detection equipment, duress alarms, guard radio and telephone systems, guard activity sensors, access control equipments, meteorological and environmental sensors and deterrent systems to a distributed processing network of computers. These would be expected to provide timely, accurate and unambiguous information about the site security status or the progress of an attack or intrusion attempt. To the extent that is feasible, appropriate response initiatives would be preprogrammed into the system. Changes in site security status and the resulting response actions would be automatically reported upchannel to higher command levels and backup and reserve forces would be automatically called out in the event of certain identifiable threat situations, particularly those in which continued survival of local guard forces might be doubtful.

Work on the CSSMRS project is being conducted in three phases. In Phase I, research was conducted to determine the applicability and feasibility of certain candidate concepts, to develop the broad outlines of the system design, and to identify specific areas where further research and development effort would be required. During that phase it was determined that the CSSMRS would incorporate a distributed network of processors and telecommunications with heavy emphasis on reliability and graceful degradation in the face of malfunction, either naturally occurring or induced by an adversary. The characteristics of the evolving Forced Entry Deterrent Systems (FEDS) were considered and recommendations were made in support of the development of taggants and trace material detection systems to facilitate the detection and apprehension of an adversary who might have been exposed to a FEDS. The desirability of monitoring environmental sensors in order to more effectively identify nuisance alarms was reaffirmed and research and development of the correlation techniques to effectively utilize this environmental data was recommended. Interfaces with intrusion alarm systems and with alarm assessment systems were studied and technical alternatives for their integration in a CSSMRS were identified. These and other relevant findings are reported in NBSIR 77-1262. (See list of references.)

In Phase II, the various technical alternatives were evaluated, and the physical and functional attributes of the various subsystems and components were identified. Laboratory tests and experiments were conducted as required to support the selection of communications media and protocols, processor characteristics and configurations, response times, and the aspects of reliability and survivability. Processes and techniques were invoked to minimize the influence of site dependent factors and to permit orderly recovery from processor or communications failures. These and other related activities resulted in a system definition that is reflected in the formal CSSMRS Prototype Specifications and in this report.

In Phase III, one or more prototype CSSMRS systems will be procured and installed at appropriate sites for field test and evaluation.

DEFINITIONS

The following definitions are used in this report:

AUGMENTATION FORCE: Troops stationed outside the SITE. The Augmentation Force can be expected to arrive at the EXCLUSION AREA within 4 hours of the time that the summons is sent.

CENTRAL UNIT (CU): The computer complex which is housed within the SSCC, together with its associated communications components.

ELECTRONIC LOCK: A method used for opening the door to a Storage Area. It is activated by an electronic key carried by one of the persons authorized to enter the Storage Area.

EXCLUSION AREA: Any designated area immediately surrounding one or more nuclear weapons/systems. Normally, the boundaries of the area are the walls, floor and ceiling of a structure or are delineated by a permanent or temporary barrier.

FORCED ENTRY DETERRENT SYSTEMS (FEDS): This acronym is defined by the Defense Nuclear Agency (DNA) as a family of deterrent systems that, when activated, will have a measurable impact on one or (preferably) more of the five human senses (sensory capabilities) of either the security personnel or the adversary (preferably both). The desired impact on an adversary is to impair his acuity or his will or ability to continue an attack. The desired impact on security personnel is to enhance their capability of detecting, recognizing, and deterring the adversary objectives. In this report, the principal concern is with FEDS that impact the senses of the adversary.

GUARD CONTROL STATION: All the equipment necessary for a guard to interface with CSSMRS. This includes Digital Display Units, Geographical Display Units, television assessment controls, television assessment monitors, and communication controls.

HIGHER HEADQUARTERS: The remote command unit that is authorized to dispatch the Augmentation Force. It requires the communications facilities over which security status information about the site is conveyed.

PERIMETER STATION: A secure housing, near a perimeter fence, which contains a Remote Unit. It interfaces with the sensors, alarm assessment equipment, and Forced Entry Deterrent Systems that are associated with one or more perimeter segments.

REMOTE UNIT (RU): All of the electronic CSSMRS components which are associated with either a single magazine or a single Perimeter Station. This includes a Remote Computer, Forced Entry Deterrent System(s), Safe/Arm Switches,sensors, sensor interfaces, Electronic Lock, Manual Override, digital communications components, television camera with controls, lighting, and TV interfaces, power supplies, emergency batteries and battery chargers.

RESPONSE FORCE: A group of guards located outside of the Exclusion Area but inside the SITE. The Response Force can be expected to arrive within 5 minutes of the time that the summons is sent.

SAFE/ARM SWITCHES: A combination of electrically and mechanically operated switches which allow or prevent the firing of the FEDS. These are supported by their own independent standby emergency power source. The Safe/Arm Switches are primarily for the protection of authorized personnel.

SITE: The general large area which includes all components except the Augmentation Force.

SITE SECURITY CONTROL CENTER (SSCC): A facility from which control of site sentry and response forces is exercised. This facility includes the Central Unit (CU) and one or more Guard Control Stations.

STORAGE AREA: The area within the boundary fence (or outer boundary fence where two are installed) where nuclear weapons may be retained for use elsewhere.

GENERAL SYSTEM DESCRIPTION

Background

Although the protection of certain areas against unauthorized intruders has long been a recognized duty of base commanders, recent events have made the execution of this duty a problem. There are several powerful reasons for this. First, the material to be protected (nuclear weapons, for example) has grown greatly in value to possible adversaries. Secondly, this decade has seen an enormous increase in the number of fanatical terrorist organizations. Thirdly, the technical expertise of possible adversaries has grown to a point where it can easily defeat many of the security measures employed in the past. Fourthly, many installations are in locations outside the U.S.

It is necessary at this point to explain that CSSMRS is not designed to protect an area against overwhelming force. For good reasons, however, an exact definition of "overwhelming force" is not specified. In general, the type of attack CSSMRS is designed to defeat are those attacks for which advance warning may not have been given by intelligence gathering agencies. (See DoD 5210.41M "Nuclear Weapons Security Manual" for more information.)

In the past, protection of areas against surprise attacks by "small" forces has been accomplished by the use of strongly constructed buildings, fences, and most importantly, guard patrols. Human guards, although excellent in terms of flexibility, are notoriously poor when operating as sensors in a dull, routine environment. Because of this, electronic sensors have been replacing human sensors in many locations during the past decade. Because of sophisticated adversary knowledge, these sensors have had to be upgraded often, with different types of sensors being used in combination to protect against the obvious methods of defeating the individual sensors. Because of the proliferation of sensors and sensor types and be- cause of non-standardization of interfaces, many systems today lack integrated alarm reporting and display methods.

There are many other activities that must be carried out at such a secure area besides monitoring the sensors. Among them are the testing of the sensors (which should be done frequently), use of television for assessment purposes, assignment of guards to patrols and to alarm monitoring, regular reporting to Higher Headquarters, maintenance of disciplined response to various emergency situations, and maintenance of disciplined controls on authorized access. The recent introduction of Forced Entry Deterrent Systems (FEDS) adds another dimension of complexity to overall base control, since the FEDS are powerful chemical and physical methods which can be automatically unleashed against intruders who actually succeed in penetrating a secure area.

The rapidly decreasing cost of computer hardware and digital communications has made it possible to design an affordable system in which many of the above activities are carried out automatically. This report is intended to provide a definitive description of such a system, which, when supported by specifications, can serve as a basis for the procurement of a prototype for field test and evaluation.

Description

Figure 1 shows the block diagram of a generalized CSSMRS. It incorporates a number of Remote Units (RU) and a Site Security Control Center (SSCC) containing a Central Unit (CU) and two Guard Control Stations (GCS). It interacts with a Response Force and an Augmentation Force.

The RUs are physically located within magazines or within Perimeter Stations. The Response Force is usually composed of off-duty guards, while the Augmentation Force is usually located considerably farther away.

In general, each RU contains a Remote Computer which accepts signals from a group of sensors and communicates the status of those sensors to the CU. Each RU also has provision for testing its sensors, upon command from the CU. Each RU also has control of one or more Closed Circuit Television Camera(s) (CCTV) and these cameras may be activated by the CU or from a Guard Control Station, and their output may be viewed at either Guard Control Station. Cameras for assessing perimeter alarms will normally be mounted in pairs on towers, with fixed orientation and field of view. Cameras at magazine sites will normally be mounted within the magazines and may be equipped with pan, tilt, zoom, focus and iris controls as appropriate to the individual installation. RUs will have control over (and testing responsibility for) a group of Forced Entry Deterrent Systems (FEDS) situated within their area. The CU can order testing, arming, and firing of the FEDS over digital communication lines. If communication is interrupted, an RU may arm and fire its own FEDS in response to local alarms.

The SSCC contains the Central Unit, plus two Guard Control Stations. Following the "two-man rule", all displays and controls must be duplicated in such a way that two guards, physically separated from each other, can independently operate and control the CSSMRS. It is absolutely necessary that all guards have a high degree of faith in the reliability of the central computer complex and that they automatically follow its orders To establish this confidence, it is required that the Mean Time Between Failure (MTBF) of the central computer be long enough so that it is extremely rare for any guard to remember a failure. It is specified that this high MTBF be accomplished by using triply redundant computers together with majority logic. These triply redundant computers are operated in synchronism or "lock step" from a common clock. If all three outputs fail to agree on any clock cycle, the computer whose output differs from the other two is ignored and directed into a resynchronizing routine. However, it is not declared faulty unless this routine is unsuccessful.

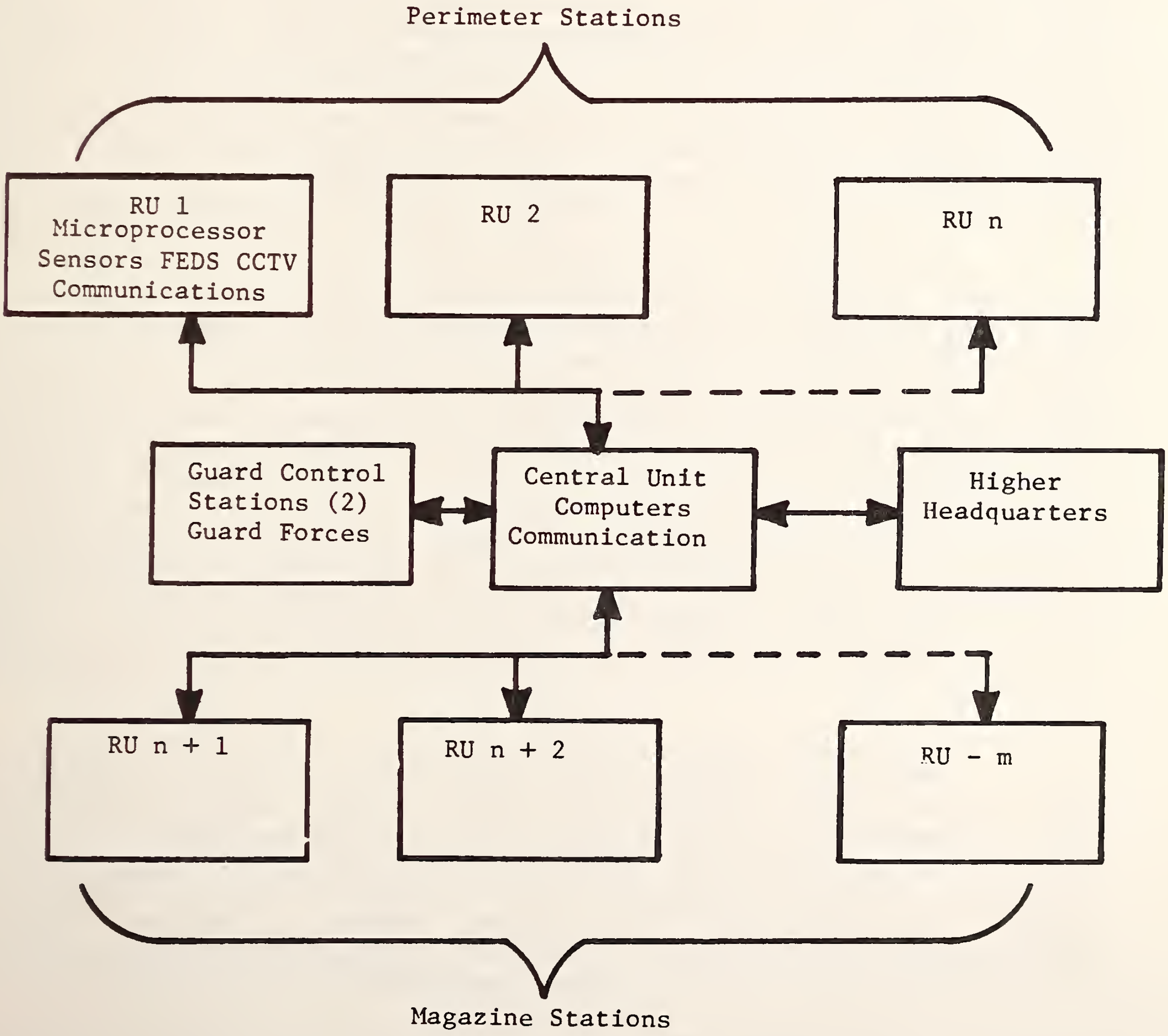


Figure 1 General CSSMRS Arrangement

Communications between the CU and the RUs is by fiber optic digital data links operating at a signalling rate of 56,000 bits per second. The CU is equipped with one or more communications microprocessor "front ends", each of which handles a maximum of 24 RUs, polling each in sequence, and reporting any changes in status to the CU. Advanced Digital Communications Control Procedures (ADCCP), ANSI X3.66, are used as link control protocol. The 56,000 bps signalling rate, together with the limitation of a maximum of 24 stations to a given loop, usually permits an alarm response time of 0.1 second or less. Multiple loops are provided, each operating under control of its individual communications microprocessor, when more than 24 RU's are utilized on a given site. The fiber optic data links are arranged in a dual loop Crossfire arrangement which permits continued operation in spite of a cut cable or the insertion of a jamming signal at any single location. The detection of the occurrence of a cut or jam and the identification of the loop leg where it is located can be accomplished in less than a second.

In the event that communication between the CU and one or more RUs is lost (as evidenced by the failure of a RU to receive a polling message during a time interval of 0.3 second), the affected RU(s) enter an autonomous mode of operation in which they will automatically actuate appropriate FEDS in the event a critical group of intrusion detectors are alarmed. Recovery from the autonomous mode of operation can be made by restoration of regular communications with the CU. When access to the area protected by the autonomous RU is necessary in order for maintenance actions to be accomplished to effect this recovery, it is possible to employ a mechanical override system to inhibit the automatic actuation of FEDS. This system is manually operated and is capable of inhibiting the FEDS only after the generation of a high-powered audible alarm and the passage of a predetermined minimum period of time.

The CSSMRS also provides improved control of access to secure magazines through the use of an electronic key system. This involves the matching of a random number generated by the CU and transmitted to the appropriate storage magazine by the data link to the associated RU with that same number as loaded into a portable electronic device that is issued to the authorized personnel. In both cases the random number is erased after a predetermined period of time, and any attempt to open an electronic lock with an invalid key generates an alarm condition.

To the extent feasible, CCTV is used to assess alarm conditions. Pyroelectric vidicons are preferred for use in CCTV assessment cameras at perimeter stations since they are sensitive to the infrared radiation from living bodies and do not have to depend on the use of artificial lighting. Where appropriate, magazine assessment cameras can be equipped with pan, tilt, zoom, focus, and iris controls that are motor driven and actuated from guard commands transmitted over the digital data communications system. Video signals from cameras are modulated on standard TV carrier frequencies permitting the use of commercial Community Antenna Television (CATV) hardware. The occurrence of an alarm will cause the automatic selection of the appropriate TV channel(s) to select the proper camera(s) to connect to the monitors at the guard control centers. Four monitors are provided so that up to four camera outputs can be displayed simultaneously.

Other guard control center facilities include a geographical display unit that provides an overall indication of site security conditions by means of colored lights on a scaled map of the site, an alphanumeric display terminal that provides detailed information about site security status and preprogrammed guidance regarding selected response actions, a logging printer and a set of functional system command keys and controls. Certain guard activities are monitored -- e.g., alarm acknowledgement -- and failure of the guard forces to comply with established procedures will cause automatic backup measures to be invoked.

Certain naturally occurring environmental disturbances are monitored by special sensors associated with the CU. To the extent that it is possible to do so without reducing the probability of detecting an adversary, the data from these environmental background sensors is correlated with signals from intrusion alarms so as to positively identify and inhibit the reporting of nuisance alarms.

Devices that automatically authenticate claimed identity of authorized personnel by means of fingerprints, voiceprints, handwriting, or other personal attributes may also be interconnected to the CSSMRS to log and control the entrance and egress of personnel in the storage area.

DETAILED SYSTEM DESCRIPTION

Digital Data Communications System

The selection of the digital data communications system for use in the CSSMRS has emerged only after consideration of a large number of factors that are significant to the performance of the overall system. These have included response times, error characteristics, freedom from interference, security and integrity, reliability and maintainability and cost. The parameters that influence these performance factors include the network topology (star, multi-drop, ring, etc.), transmission medium (twisted pair, coaxial cable, optical fiber, etc.), modulation system, coding, signalling rate, and communications control protocol as a minimum. Any choice is likely to have both advantages and disadvantages and the final selection is thus a compromise that is hopefully optimal in some overall sense.

Network topologies that were considered included the star, multi-drop, ring and a novel configuration named "Crossfire". The star arrangement provides an individual communications path from the central station to each remote station; thus, breaking any path will isolate only a single station . Its disadvantages are the large amount of "cable" that are required and the need for either a port per circuit or else complex circuit switching facilities (either virtual or real) at the central station. Multiple drop arrangements where all of the remote stations are bridged across a single communications circuit are much more economical in the use of "cable", but a single cut can fragment the network, and a single jam or "lockup" at a station can disable all network communications. Loop configurations, where messages are received and regenerated at each remote station are even more likely to be fragmented, as a failure at any of the regenerative repeaters will disrupt the further flow of traffic.

The CROSSFIRE configuration (see Figure 2) is a double loop in which traffic flows in two independent but parallel rings. On one of these two rings, data flows in a clockwise (CW) direction; on the other ring the same data flows in a counterclockwise (CCW) direction. This data is identical in timing and content at the transmitting station which may be either the CU or an RU. Data received at the CU is not repeated. Data received at each RU is repeated after a minimal delay of less than a microsecond. This method of repeating data without significant delay takes advantage of the excellent signal to noise characteristics and freedom from external interference that fiber optic data links possess.

When a frame is received at the addressed RU, it arrives over the CW and the CCW loops at slightly different times. Upon arrival via each (or either) loop, the frame check sequence (FCS) is computed, and if correct, the frame is accepted. In addition, frames from both the CW and CCW loops are stored for a period of no more than the differential propagation and repeater delay and are then compared, bit for bit. The RU reacts to the frame in a manner that depends upon the results of the FCS and the comparison of the frame contents. If the FCS of both is correct and the comparisons agree, the addressed RU must send a normal reply to the frame and perform any command contained in the frame. If only one FCS is correct (comparison will always disagree when this occurs), the RU must report the loop on which it did not receive a frame or on which the FCS was incorrect and must perform any command contained in the frame with the correct FCS. If the FCS is incorrect in the frames received over both loops, the RU must respond with a "frame reject" message and ignore the contents of both frames. If both frames are received with correct FCS's but their contents do not agree, this is an indication of a sophisticated attempt at spoofing. Here the RU must also respond with a "frame reject" message and ignore the contents of both frames and if this condition is repeated for three successive polling cycles, the RU enters the autonomous mode.

Since each RU is polled every 0.1 second, the CU can use the above information to quickly determine the location of an attack or malfunction. Any cutting, jamming or spoofing attack at a single location can be detected automatically while still maintaining communication with all RUs.

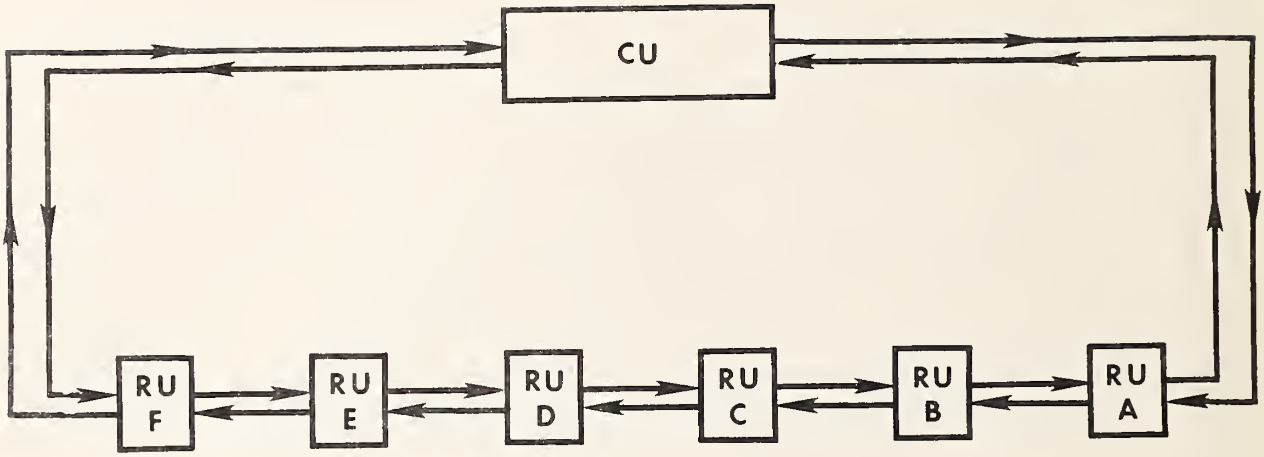


Figure 2 Dual Loop Crossfire Configuration

At least three different communications media could be used to to implement a dual "Crossfire" loop; twisted pair, coaxial cable or fiber optics. The twisted pair and coaxial cable both represent mature technologies with readily available supporting hardware such as connectors and fittings. Both, however, are susceptible to electromagnetic interference resulting from thunderstorms or man-made disturbances, and both can be readily tapped and surreptitiously monitored. Cryptographic techniques could be employed to protect the integrity of the data on the network but these techniques incur a cost penalty and, depending upon the method of implementation, may add overhead bits to the transmitted data stream. Fiber optics, on the other hand, is an emerging technology. New components, such as connectors, power splitters, etc., are being regularly announced. Both the "cable" and the supporting hardware is more costly than the metallic counterparts, but it has demonstrated a clear superiority in several test projects constructed by telephone companies. It is virtually immune to influence from electromagnetic interference or environmental factors such as moisture and temperature. It does not radiate energy that can be surreptitiously picked up, and the difficulty of tapping the very small fiber to extract data or inject false signals is very great. So much so, in fact, that it is considered that the use of cryptography to protect the integrity of transmissions on the cable that are totally within the storage area does not appear to be necessary.

One of the authors of this report has had extensive experience with coaxial cable telecommunications. In addition, two types of fiber optic systems have been procured and have been tested and analyzed on an experimental basis. As a result of his experience, and after careful consideration of all available data, fiber optics has been chosen for use in implementing the dual CROSSFIRE loop configuration within the storage area. Its use was considerd for transmission of video information from the CCTV alarm assessment system, but here the ready availability of cable TV components coupled with the less stringent demands for data integrity and noise immunity favor the use of the coaxial cable. Further, the availability of CATV frequency division multiplex equipment in 24 channel increments tends to establish a convenient upper limit to the number of RUs on a "Crossfire" loop. It should be emphasised that this size of 24 stations per loop is really much more a convenience than an absolute limit.

The selection of fiber optic cable as the transmission medium for the digital data communications network almost automatically limits the choice of modulation to amplitude shift keying (ASK) where the presence of an optical signal represents one condition, and the absence another. Further, since the available bandwidth of the optical fiber is much greater than is likely to be needed, the choice of coding (NRZ, NRZI, Manchester or other) can be based on convenience rather than conservation.

Control Procedures

With respect to communications control protocol, Advanced Digital Communications Control Procedures (ADCCP), ANSI X3.66, is a logical choice for a number of reasons. It is compact, efficient, code independent and incorporates powerful error control procedures. It is expected to be very widely used as it is a super-set of the protocol which has been introduced by some of the leading computer manufacturers, and with only minor variations has been adopted as an international standard. Using this protocol a Primary Station has primary link control capability and issues command frames to, and receives response frames from, Secondary Stations on the link. In the CSSMRS implementation of ADCCP there will be a communications microprocessor located at the CU that is associated with each "Crossfire" loop that functions as the Primary Station, while each of the RUs on that loop will function as Secondary Stations. A frame is a transmission that takes the following form:

F A C (Info) FCS F

Where:

F is a flag octet of the form 01111110

A is an octet depicting the address of a secondary station.

C is a control field octet

(Info) is an optional information field of any length

FCS is a 16 bit frame check sequence providing error control

F is the final closing flag of the frame

In addition to their use as bit synchronizing characters and beginning and end of frame delimiters, the flag characters can be used as "idle-fill" characters. This usage is not contemplated in the CSSMRS network since continuous polling and communications sequences will be maintained between the CU and the RUs in order to insure the immediate detection of any interruption or attempt to insert spurious data in the network.

Protection against the unintended interpretation of data as a flag character in a frame is provided by the insertion or "stuffing" of a zero bit immediately following any five contiguous ones that occur anywhere between the opening flag and the closing flag of a frame. The insertion of the zero bit thus applies to the contents of the Address, Control, Info and FCS fields (including the last five bits of the FCS). The receiver continuously monitors the received bit stream; upon receiving a zero bit followed by five contiguous one bits, the receiver inspects the following bit: If a zero, the five one bits are passed as data and the zero bit is deleted. If the sixth bit is a one, the receiver inspects the seventh bit; if it is a zero, a flag sequence has been received; if it is a one, an abort has been received. Although this may all sound complicated, single-chip, large-scale integrated circuit implementations of the necessary logic to perform this and other ADCCP functions are now readily available.

The Address field is one eight-bit byte that designates a secondary station address. The address that is used in a command frame issued by the primary station is that of the secondary station to which the frame is directed. The address in a response is the address of the responding secondary.

ADCCP provides an extensive repertory of commands and responses that go well beyond the rather modest requirements of the CSSMRS network. These can be satisfied with a subset of only four unnumbered commands and three un-numbered responses. Their bit patterns and the mnemonics by which they are referenced are as follows:

Commands:

Bit Pattern	Mnemonic	Function
11001000	UI	This command indicates that the associated frame has an information field containing instructions that must be executed by the remote station that is the addressee. This information field will contain either one or two eight bit bytes and convey the meanings shown in Table I. The immediate response to this frame will be a UA frame followed on later polling sequences by UI frames reporting any status changes that have resulted from the execution of the received instructions.
11001100	UP	This command is an unconditional request for an immediate full report of the status of the addressed secondary. The frame does not contain an information field. The response is a UI frame with an information field that contains a full status report in the form shown in Table II.
11011000	PN	This is one of the non-reserved command bit patterns that is permitted by X3.66 for use in unique, application dependent circumstances. Here, it has been assigned the meaning of a conditional poll command. The addressed secondary is to respond with a UI frame with an information field reporting any change of status since the last report if any such change has occurred. If there has been no status change, the response is a UA frame.
11011001	APN	This is also a non-reserved command that may be assigned an application dependent meaning. It is used to acknowledge the receipt of a UI response to a PN command occurring on the preceding poll cycle and it conveys the additional meaning of a regular PN command.

Responses:

Bit Pattern	Mnemonic	Function
11001110	UA	This is a response that acknowledges the correct receipt of the immediately preceding command frame. If that immediately preceding command frame was a PN command,

		the UA also indicates that there has been no change in the status at the station such as intrusion or tamper alarm, alarm recovery, loss of power, etc. There is no information field in a UA frame.
11001000	UI	The UI response designates a frame containing an information field. The information field will have the format shown in Table II.
11101001	FRMR	This is a frame reject response and is issued by the addressed secondary when an error is detected in the immediately preceding received frame. An error is indicated by the receipt of a frame that is less than 48 bits long, or one in which the FCS does not compute correctly.

The Frame Check Sequence, FCS, is a 16 bit cyclic redundancy check sequence that is developed using the CCITT V.41 Polynomial X**16 + X**12 + X**5 + 1 as specified in ANSI X3.66. This provides a very high level of error control; in frames of the size that will be employed in the CSSMRS, it has been estimated that only about 15 to 20 frames per million frames having errors will be accepted as correct frames. If the detected frame error rate is one in 10**5, then an undetected frame error rate of less than one in 10**9 would be anticipated.

In all cases, responsibility for error recovery rests with the primary station. The only initiative that the secondary will exercise is to enter the autonomous mode if it has not received a correct frame of any type within 0.3 seconds.

It will return from the autonomous mode to the normal mode of operation upon the resumption of communications with the CU, or primary.

TABLE I

INFORMATION FIELD FORMAT FOR COMMAND FROM CU TO RU

The information field is of variable length and may contain one or more single byte or two-byte commands. Single byte commands are identified by a zero in bit positions one and two.

FORMAT

BITS								FUNCTION
1	2	3	4	5	6	7	8	
0	0	0	0	0	0	0	1	Pan Camera to the right
0	0	0	0	0	0	1	0	Pan Camera to the left
0	0	0	0	0	0	1	1	Tilt Up
0	0	0	0	0	1	0	0	Tilt Down
0	0	0	0	0	1	0	1	Zoom In
0	0	0	0	0	1	1	0	Zoom Out
0	0	0	0	0	1	1	1	Iris Open
0	0	0	0	1	0	0	0	Iris Closed
0	0	0	0	1	0	0	1	Focus In
0	0	0	0	1	0	1	0	Focus Out
0	0	0	0	1	0	1	1	Lights On
0	0	0	0	1	1	0	0	Lights Off
0	0	0	0	1	1	0	1	Camera On
0	0	0	0	1	1	1	0	Camera Off
0	0	0	0	1	1	1	1	"SAFE" (Disable) FEDS
0	0	0	1	0	0	0	1	through 0 0 0 1 1 1 1 0 Same as above except for + location (next higher perimeter segment number).
0	0	0	1	1	1	1	1	"ARM" (Enable) FEDS
0	0	1	0	n	n	n	n	Test FEDS Identified by Binary Value of n n n n
0	1	0	0	n	n	n	n	Fire FEDS Identified by Binary Value of n n n n provided byte two is identical to this byte.
1	0	x	x	0	x	x	x	Spare Two Byte Commands
1	0	0	0	1	0	0	0	Test Sensor Identified by Binary Value of Byte Two
1	1	0	0	0	0	0	0	Load Electronic Lock With Random Number in Byte Two
1	1	1	x	x	x	x	x	Spare Two Byte Commands

Note that a second byte is required whenever the binary value of bits one and two in byte one exceeds zero.

TABLE II

Format for the information field of frames transferred from the RU to the CU reporting full status or change of status:

Bit	State Zero	State One
1	No change this frame	Flag - Change this frame
2	FEDS electrically "SAFE"	FEDS electrically "ARMED"
3	FEDS manually "ARMED"	FEDS manually "SAFE"
4	Power OK	On backup batteries
5	Lights off	Lights on
6	Lights + off	Lights + on
7	CCTV off	CCTV on
8	CCTV + off	CCTV + on

Then, if this is a response to a command for a full status report, there will follow one byte for each connected sensor and FEDS. This byte will have the following format:

Bit	State Zero	State One
1	Secure condition	Alarm condition
2	No test in process	Test in process

3 through 8 represent binary identity of the sensor or FEDS

In the case of FEDS, the alarm condition (bit one in state one) corresponds to a fired or missing squib.

When bit one of byte one is set to the one state and the frame is a response to a PN command, then only those bytes are transmitted that are required to identify the change in status that has occurred. For example, if a single sensor alarmed, the information field would only contain two bytes; byte one from Table II above, and a second byte denoting the change in status and identity of the alarming sensor.

The following are to be used as Peripheral Identification Numbers (PIN) for the various types of sensors and FEDS that may be associated with any CSSMRS RU. Note that each Perimeter Station controls two fence segments. In this table, those perimeter sensors that are not followed by a "+" symbol are for the segment that has the same address as the Perimeter Station; those followed by a "+" have the next highest segment number.

PIN	Type
1	MAID/MILES
2	do +
3	FDS or piezo fence sensor
4	do+
5	Microwave
6	do +
7	E-Field
8	do +
9	Laser or other optic fence
10	do +
11	BLID or other seismic
12	do +
13	Radar target detection unit (water)
14	do +
15	Sonar
16	do +
17	Acoustic interferometer
18	do +
19	other perimeter
20	do +
	Area Sensors of the following types:
21	Microwave doppler
22	Ultrasonic doppler
23	Radio Frequency (SWR or amplitude)
24	Passive ultrasonic
25	Acoustic
26	Infrared
27	Visible
28	Spare
	Point Sensors of the following types:
29	Capacitance
30	Magnetic
31	Seismic
32	Thermal
33	Vibration
34	Breakwire
35	Foil on glass

36	Magnetic switch
37	do.
38	do.
39	Successful opening of electronic lock
40	Tamper alarm on electronic lock
41	Tamper alarm on any installed sensor
42	Tamper alarm on Remote Computer Cabinet
43	Tamper alarm on CCTV
44	do. +
45	Poll received on clockwise loop only
46	Poll received on counterclockwise loop only
47 - 56	Spares

Forced Entry Deterrent Systems of the following types:

57	Relocker on magazine door
58	Relocker on magazine door
59	Vapor type FEDS in magazine
60	Liquid type FEDS in magazine
61	do. +
62	spare
63	spare
64	spare

By providing this list of identification numbers that can be used for any member of a generic class of sensors, it should be possible for a given site to employ whatever type(s) of sensors are most appropriate to it's environment and circumstances without having to resort to the preparation of site specific software for the CSSMRS. That is, a PIN 9 is always an optical perimeter sensor and a PIN 33 is always a vibration sensor at any RU of any site. Spare PINs have been provided for allocation to possible new sensor types that may be developed in the future.

With the message formats shown in Tables I and II, the RU is required to provide buffer space for six bytes each for the clockwise and counterclockwise message loops at the CROSSFIRE controller, however, only a maximum of four bytes of accepted incoming messages would be passed to the microprocessor: the address and control bytes, and where present, the information field of incoming messages. On the other hand, the communications processor(s) and the CU at the primary station must be prepared to accept information fields of variable length in the messages that they receive in responses from the RUs. In the majority of instances, however, frames exchanged between the CU and the RUs are not expected to contain information fields since under normal, secure conditions there will be a PN command frame going out from the CU and a UA response returning from the addressed RU as each RU on the loop is polled in a continuing sequence without pause or interruption.

A nominal response time target for the CSSMRS has been arbitrarily established as 0.1 second. The only justification for this arbitrary selection is that 0.1 second is comparable to typical minimum human reaction times.

With an operating bit rate of 56,000 bits per second, a primary station can transmit a PN frame and a secondary can transmit a UA frame, each 48 bits long, in 1.72 ms. Allowing 80 microseconds for propagation delay and microprocessor response times, these types of frames could be exchanged with a different RU each 1.8 ms. and a loop of 24 RUs could be polled every 43.2 ms. Looking at it from a different viewpoint, in 0.1 second, with the same operating bit rate, propagation delay and microprocessor response times, there would be time enough for the CU to send a command with a one byte information field and receive a response with a 15 byte information field from each of 24 RUs on a loop. From these calculations we conclude that the 56,000 bit per second signalling rate is adequate to support the target response time in all but the most unusual circumstances. In fact it is difficult to imagine a set of circumstances that would generate data at even this rate. These calculations also justify the position that the RU should expect to receive polling frames at intervals of about 0.1 second, and that if a frame has not been received for 0.3 second it should assume that it has become isolated and should enter the autonomous mode.

CROSSFIRE Operations

Under normal circumstances the communications microprocessor assigned to each loop is continuously polling each Remote Unit in its loop, (see Fig. 3). These polling messages are sent on both the clockwise and the counter-clockwise channel. These messages are repeated, bit by bit with less than a microsecond delay, at each Remote Unit, and they should arrive back at the transmitting CU microprocessor with very little differential delay.

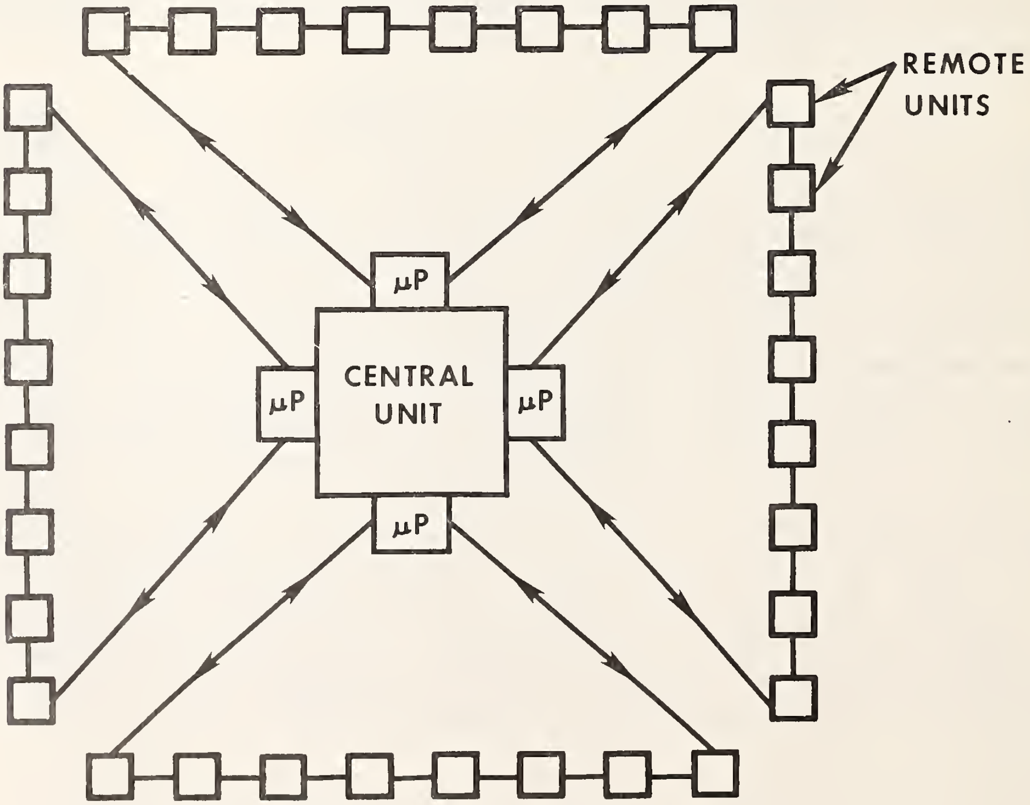


Figure 3 Digital Data Network

Figure 4, "Digital Communications Controller" shows the Remote Unit controls for a CROSSFIRE loop. Note that each loop has an optical receiver, an electronic amplifier and an optical transmitter. Each incoming pulse of light is detected, amplified and retransmitted without delay as a reconstituted bit. Each loop also has a circuit to calculate and confirm the validity of the Frame Check Sequence (FCS), and a buffer register. There is a common comparator to establish whether message contents are identical for each channel. The switches are in the "Receive" position as shown except when the RU is transmitting in response to a poll.

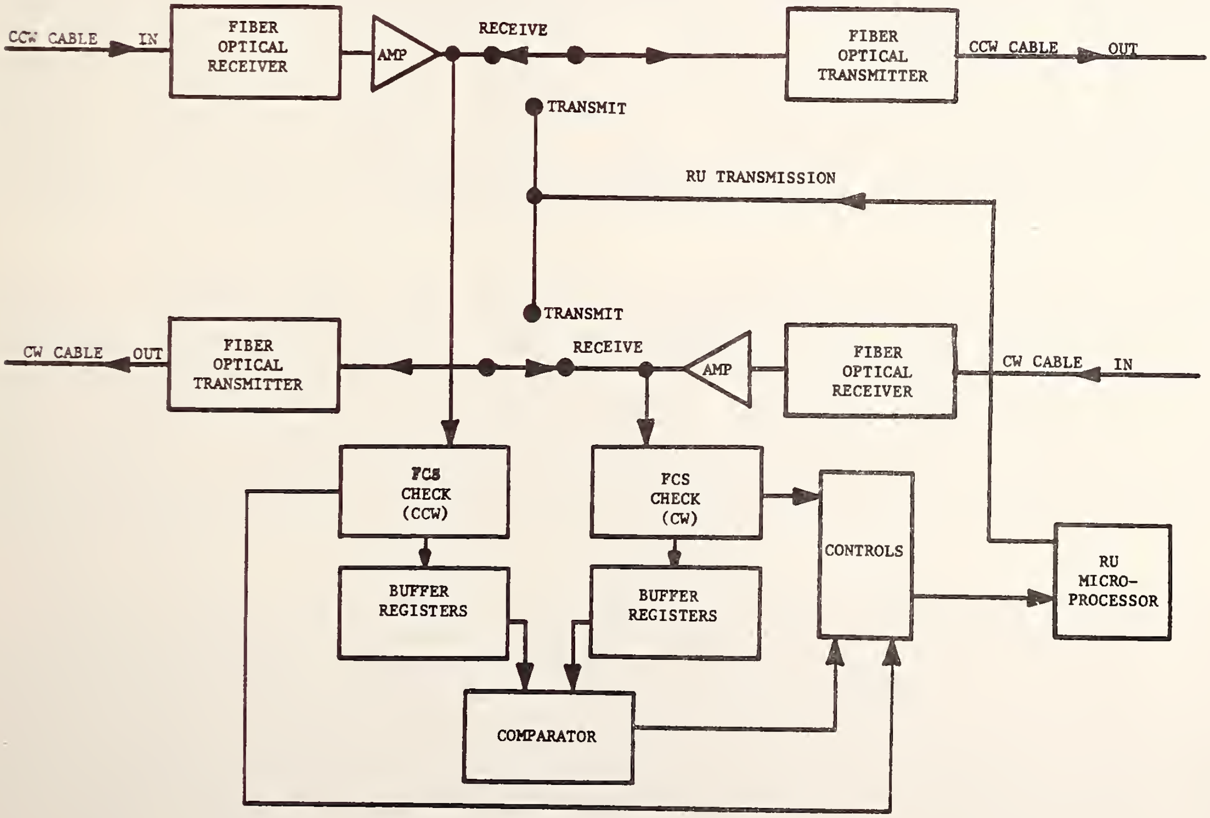


Figure 4 Digital Communications Controller

Assume that each RU is within one microsecond of the two adjacent RU's, on the average, including propagation and retransmission delays. For the maximum population of 24 RUs per loop, a frame received on the CW and on the CCW loop will arrive at any RU within 24 microsecond of each other. This delay is caused by the differing distances from the CU to the RU on the CW and CCW loops. Both the CW and the CCW messages are stored and the FCSs are checked. If the messages are identical and the FCSs correct, the addressed Remote Unit transmits its answer to the polling message. The delay between the poll and the answer must be less than the period required to transmit a minimum length frame; this requirement makes it impossible to spoof the network, as will be discussed in a later paragraph. The answer from the RU to the CU is transmitted simultaneously over both the CW and the CCW channels.

In the event of a cable cutting attack between the CU and RU-A, see Fig. 5, all RUs will receive their polling messages via the CCW channel only. Each RU reports this fact in turn to the CU, which already knows that it is not receiving its own "echo" on the CCW channel. Transmission is initiated by each RU on both channels, but only the CW channel arrives at the CU. The CU, knowing that all of the RUs are replying, but only by way of the CW channel, correctly decides that the cutting attack is between the CU and RU-A. The CU then issues an order to a guard patrol to investigate the path in question, while, at the same time, patching in the closest assessment television camera.

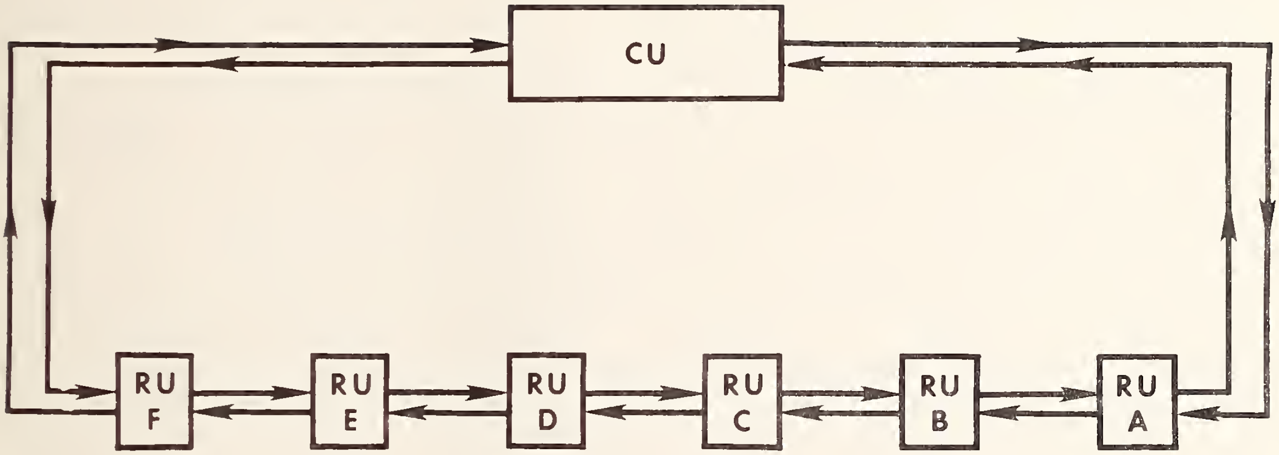


Figure 5 Crossfire Loop

If the fiber optics cable is cut between two RUs, for example between RU-D and RU-E, the location of the attack point is equally straightforward . The CU observes the fact that RU-A,B,C, and D replied to their polls only on the CCW channel, while RU-E and F replied only on the CW channel. The break is therefore in the trench between RU-D and RU-E. Establishing this fact takes only one polling cycle, which is 0.1 seconds or less. Note that this method isolates malfunctioning components as well as adversary attacks.

In the event that a trench is dug up by an adversary and a jamming attack is made, with the jam applied in both directions on both channels, communications is still maintained between all units, and the location of the attack is determined within one polling cycle. Assume the attack was made between RU-D and RU-E. The jamming signal on the CW channel propagates through RU-E and RU-F, but does not affect units D,C,B,or A. The jamming signal on the CCW channel propagates through units D,C,B, and A, but does not affect units E and F. Thus, all messages to units E and F on the CW channel are destroyed, but messages to E and F are correctly received via the CCW channel. Similarly, messages to units A,B,C, and D are destroyed on the CCW channel, but are correctly received on the CW Channel. In order to locate the position of the attack, the Central Unit needs only to recognize that polls from units A,B,C,and D were answered on only the CCW channel, while units E and F answered on the CW channel only.

Note that only messages with a valid FCS are acted upon.

Although cutting of a fiber optics cable is relatively simple (once the trench has been dug up undetected), the insertion of an efficient jamming signal requires more elaborate equipment. The most sophisticated attack is an attempt to insert a false message into the system which is interpreted as originating with a friendly source ("spoofing"). The CROSSFIRE net protects against this by a traffic protocol (previously mentioned) which requires that at no time is there a silent period in the loop which is long enough for an adversary to insert a legal message with a correct CRC. Thus, all spoofs inserted into a fiber without cutting will collide with legitimate messages and cause CRC errors. If a channel is first cut, a very sophisticated spoof may arrive at a down-channel RU successfully, with a correct CRC. If the message did not contain exactly the same message as the one received by the same RU on the other channel, the RU is permitted only to report this occurrence, but is not permitted to follow any commands contained in either message. This results in the addressed station going into one of the autonomous states. The location of such a spoofing attack is determined by the Central Unit in a fashion similar to that used for locating the source of a jam; this is accomplished in one loop polling period. Guards are automatically dispatched to the location.

In the prototype CSSMRS system the defense against bugging relies on the difficulty of conducting surreptitious reading of the fiber optics channels without alerting guard forces. Since the fiber signals cannot be detected remotely, the channel can only be read by excavating a portion of the trench, removing several protective coatings from the fiber,introducing a method of removing a portion of the light energy without interrupting the normal flow of traffic, recording the light pulses, and decoding the complex format.

CSSMRS is also designed so that information obtained by bugging a fiber optics loop is not particularly valuable to an adversary. The most valuable information is the occasional burst of electronic key data, and that data is changed for every access.

Secure Digital Data Link

The CSSMRS requires a secure digital data link between the CU and higher headquarters. Transmissions should be encrypted and should be sent by two different and independent landline paths. This will provide a measure of resistance against adversary attack against a single cable. The communications control protocol should be ADCCP as in the fiber optic digital data network within the storage area, but the operating bit rate should be reduced to 2,400 bits per second so as to be compatible with the transmission capabilities of leased telecommunications circuits that are readily and economically available.

Radio surface or satellite links are not recommended for either of the alternative paths for this secure data link if a landline facility can possibly be employed.

The secure data link is used to keep higher headquarters advised as to the security status of the site, and in certain emergency conditions, to automatically summon Augmentation Forces. It is thus quite important that the operational status of this link be continuously monitored. This can be accomplished by the regular exchange of messages between the CU and the higher headquarters station using both manual and automatic exchange routines that are independent of messages that report site status. The automatic routine begins when the CU selects one of the two redundant paths and sends a test frame to the higher headquarters station. This frame has an information field containing four eight bit bytes. The first byte contains any randomly selected bit pattern except eight zeros and the next three bytes are a three digit ASCII sequence number. Upon receipt at the higher headquarters station, the first byte of the information field is tested for "ones". If all bits are zero, it is not a circuit test frame and the rest of the bytes represent a message conveying information; if one or more bits in the first byte are "ones" the remaining bytes are a sequence number to be used to confirm operational status of the link. This sequence number is accepted, incremented by one, modulo-999, and placed in the information field of a four byte return frame whose first byte also contains a random, non-zero, binary value. This frame is returned via the same communications path on which it was received. On the next exchange, the other path is employed and the process is repeated. These exchanges can be accomplished in about 75 ms., so they should be automatically initiated at the same time as the RU polling cycle (every 100 ms.) and three unsuccessful attempts to exchange frames on either path is considered as an adequate basis for declaring an outage on that path.

The use of the random field in byte one of the messages that are exchanged to monitor the integrity of the redundant path secure data link is to make it more difficult to attack the cryptographic system. This variable together with the changing sequence number in the other three bytes of the information field permits an average of 128,000 different messages to be transferred before one is repeated. It should be noted, however, that an adversary could record one of the monitoring messages and then attempt to substitute this recording for an information bearing message from the site to higher headquarters. There would be one chance in a thousand that the recording would have the expected sequence number. The random field in byte one helps protect the crypotgraphic system but does not influence the continuity of sequence numbers.

At intervals of approximately 30 minutes, selected so as to occur at times of low activity, the CU will instruct the guard that is on duty at the guard control station to initiate an exchange message with higher headquarters. His response will cause a message exchange sequence as described above. Successful exchange on both paths will result in the display of an appropriate message to the guard and cause this message to be entered in the log. The automatically initiated exchange messages are not displayed or logged so long as the exchange is successful; failures will, however, result in the display and logging of a failure message so that service restoration action can be initiated in the event of a single path failure, or emergency procedures invoked if both paths fail.

Response Forces Call-up Link

A signalling circuit is provided from the CU to the barracks or ready-room from which on-site Response Forces can be called in an emergency. This circuit is used to activate a local alarm such as a horn, bell or siren as a signal for the Response Forces to turn out immediately and proceed in accordance with the prepared plans to reinforce the guards in the storage area. Redundancy in this alarm signal is provided by a high intensity civil defense air raid type alarm signal located within the storage area that is activated concurrently with the local alarms and which would be capable of alerting the Response Forces even if their normal call-up link had been cut.

Video Data Transmission System

Closed Circuit Television (CCTV) will be employed in the CSSMRS to the maximum extent practical for the assessment of alarms. Standard 525 line video equipment is selected on the basis of cost, availability and maintainability. Cameras will normally be operated with the vidicon heaters continuously powered so that video output is immediately available without a warm up delay. This is controlled using command frames over the digital data network as described in the preceding sections. Where remote control of other camera features such as pan, tilt, zoom, etc., are required the appropriate drive motors will be energized by the RU microprocessor through the interpretation of the applicable digital commands. Each of the motor drive commands will cause application of power pulses to the selected stepping motor to continue for 0.1 second, thus a series of identical drive commands on successive poll cycles will result in essentially continuous drive motion. The displacement from "home position" caused by any drive command is remembered by the RU and when the camera is turned off and released from assessment the command sequences are recalled and are reversed so as to return the camera to a preset, optimized initial condition. It is anticipated that not all cameras may require such adjustment features and when they are not so equipped, that fact will be annunciated at the viewing monitor in the guard control stations.

For transmission of the video from the CCTV cameras back to the CU and the guard control stations, consideration was given to three alternatives: individual optical fibers, individual coaxial cables and frequency division multiplexing a limited number of camera output signals on a single coaxial cable.

Optical fibers are available with adequate bandwidth for video use, but the electrooptical transducers (lasers and photodetectors) with the required response times are very expensive; typically hundreds of dollars each as contrasted to the few dollars each for transducers capable of supporting the 56,000 bit per second digital data network. While these costs will probably decline with future use of fiber optic components in telephone trunking applications, it was not believed that they could be currently justified for alarm assessment applications.

Individual video coaxial cable per camera circuits have been used in many alarm assessment installations. Their advantage is that the failure of a single cable disables only a single camera; their disadvantages include the large amounts of cable required, the likelihood that many equalizing amplifiers may be required and the lack of routing redundancy. The construction work that accidentally cuts through a cable trench will probably disable many cameras rather than a single camera.

The third alternative, frequency multiplexing a limited number of cameras on a single coaxial cable, capitalizes on the techniques and hardware that have been developed for the cable television industry. Commercial hardware is readily available to accept video from a camera and modulate one of up to 24 of the standard television carrier frequencies. Twenty four cameras can then be bridged on a single cable that covers one loop segment of the digital data network and shares the same cable trenches. Broad band repeater amplifiers are installed as required along the length of the cable at appropriate RUs. Each camera has a separate channel and the common repeaters amplify all channels. By installing a second cable running in the reverse direction as shown in Fig. 6, a loop arrangement is formed so that there are two alternative paths from each camera location to the CU. This provides a desirable degree of redundancy and resistance to attack. At perimeter locations, where two fixed cameras are mounted on each tower and aligned to cover one perimeter segment, one camera will be connected to one cable and the other camera will be connected to the other cable. At magazine locations, where only a single, possibly controllable, camera is installed, it will be connected to both cables. All cameras are synchronized to prevent picture roll-over when switching monitors from one camera to another or when switching a camera to automatic recording devices. Sync pulses are sent out over the cables used for incoming signals using base band signalling and appropriate low pass filters. Monitors are high resolution television receivers and any monitor can be connected to any camera by simply switching in the proper cable and proper frequency on that cable.

The exact positioning of perimeter assessment CCTV cameras is, of necessity, site specific, but some general guidelines are suggested in Figure 7. Here, two cameras are mounted on a common pole and trained on the same 100 meter perimeter segment. One of the cameras is equipped with a 75 mm lens that will provide 0.75% horizontal field of view resolution over a 25 meter wide region at the remote end of the 100 meter perimeter segment, and coverage over an increasingly narrow region back to the near end of the segment. The second camera is equipped with a 50 mm lens and provides an enlarged wedge of coverage over the near 50 meter portion of the segment. The cameras are mounted in a housing that is resistant to fire from small arms and that is shaped so that ropes cannot be readily suspended from it but will slide off. The housing is elevated about 5 meters and is swung outside of the inner fence so that the outside of the inner fence is within the field of view of both cameras. The pole or tower supporting the cameras is located about 50 meters away from the segment that they will assess.

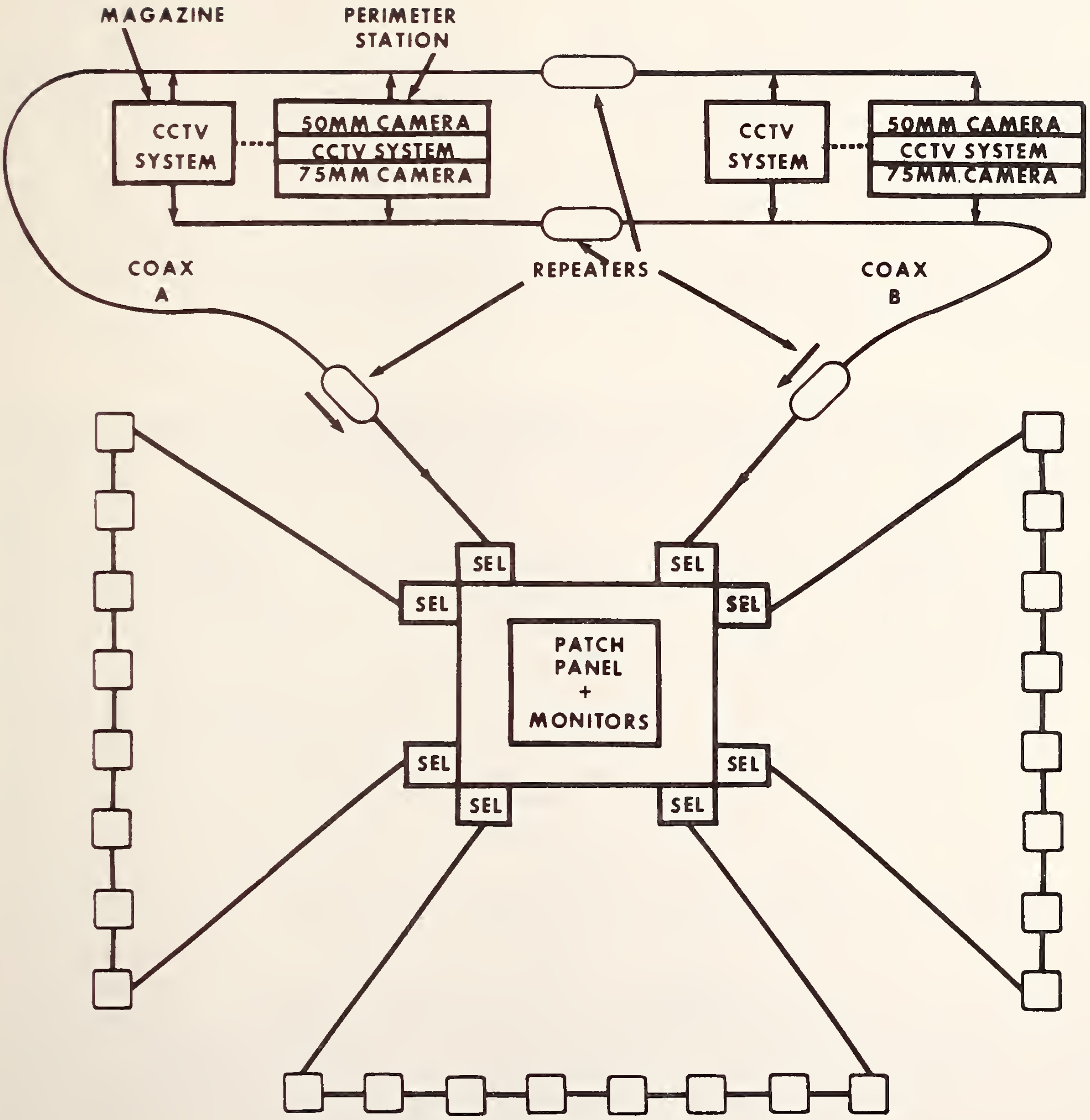


Figure 6 Proposed Video Network

This CATV approach is advocated for any CSSMRS installation where more than four CCTV assessment cameras are employed because of its flexibility, economy and redundancy. Where four or fewer CCTV cameras are used for assessment, individual cables interconnecting the video signals from each camera to its own monitor are the preferred arrangement.

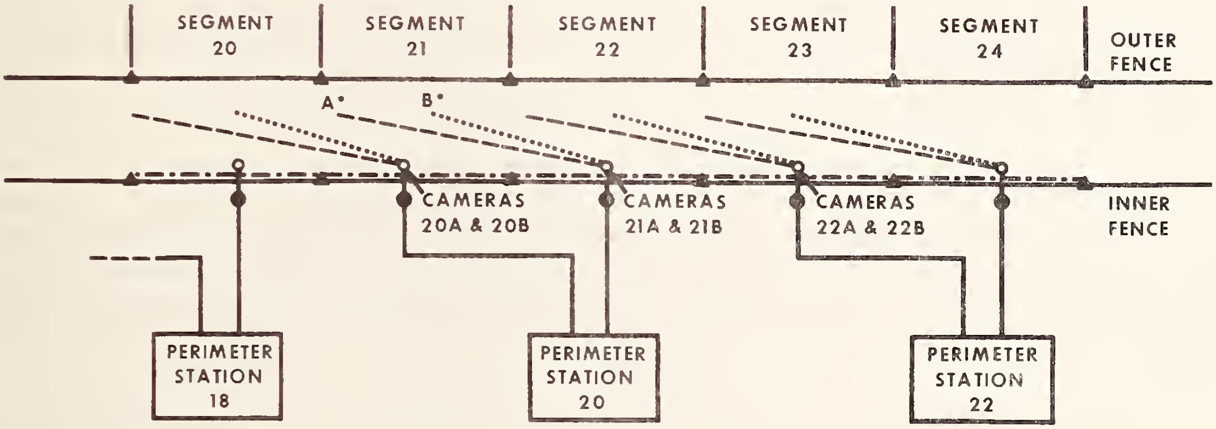
Voice Communications Facilities

Telephone communications will be required between the Guard Control Stations and each guard patrol station, magazine entrance and RU. In addition, radio communications will be required between the Guard Control Stations and each mobile and ambulatory patrol, and a public address system is required to warn would-be intruders. It is assumed that these facilities will already be on-site and that their adaptation to the CSSMRS will involve only minor extensions to the existing network and the addition of voice activated recording facilities.

Remote Unit

A Remote Unit, RU is a generic term that has been coined to describe that assemblage of CSSMRS components that are collocated at either a single magazine or a single perimeter station. In the case of a magazine, it includes a microprocessor, FEDS, Safe/Arm switches (electronic and manual), an electronic lock with its manual emergency override mechanism, digital communications components, an appropriate selection of sensors and testing components, CCTV (with camera controls if required), video communications components, lighting and controls, all of the interface components necessary to integrate these elements and, finally, main and backup power supplies for their operation. These will all be installed within the magazine. In the case of a perimeter station, similar components are involved; however, a single microprocessor will be associated with the sensors, FEDS, CCTV, etc., required for two perimeter segments (zones) each having a nominal length of 100 meters. For a perimeter RU, the microprocessor, Safe/Arm switches, power supplies, communications and interface components are installed in a small, walk-in, reinforced concrete shelter with a steel door that is secured with an electronic lock and security padlock and having a manual electronic lock override mechanism. The shelter should be equipped with intrusion alarms and FEDS and should be generally similar to a squared off and greatly miniaturized magazine without earth cover. It should generally be located about 25 meters inside the inner perimeter fence of the exclusion area at the junction of the two perimeter segments under its control and in a position to minimize the lengths of the trenches containing the interconnecting cables for sensors, FEDS, CCTV, etc., and to minimize the cover that might be afforded an adversary attempting to penetrate the perimeter. Fig. 7 illustrates the general arrangement. This arrangement is meant to be suggestive rather than exact, and CCTV camera locations, in particular, will have to be carefully arranged to suit the requirements of any particular site.

Alternative arrangements, including semi-buried caskets, were considered for housing the components of the perimeter stations. These appeared to have potential problems such as those associated with drainage and water control or lack of accessability for maintenance or vulnerability to damage or disablement from small arms fire. It was judged that these disadvantages could be best countered by the construction of a perimeter station of the type described above.



NOTE:
* CAMERA A = 75 MILLIMETER LENS
* CAMERA B = 50 MILLIMETER LENS

Figure 7 Relative Location of Perimeter Stations and CCTV Cameras

It is vital that the microprocessor and its associated components be provided with a very high degree of physical security. Compromise of the microprocessor could adversely impact the security of the perimeter segments or magazine with which it is associated. It is for this reason that it must be installed within the magazine or within a similarly protected shelter structure. There they can contribute to the maintenance of their own security in two ways. The first is in connection with the handling of the random number that is used to open the electronic lock on the door of the magazine or shelter structure. The second contribution to the maintenance of self security comes about from the entry of the microprocessor into an autonomous mode of operation when communications with the CU is lost. In this mode, the alarming of a prescribed group of sensors is assumed to represent positive evidence of an unauthorized access attempt, and the automatic response is activation of appropriate

FEDS. This response must be inhibited when loss of communications with the CU is a result of system malfunction and access must be made to perform maintenance actions, and the implementation of this inhibiting function must occur in a way that does not provide an inviting avenue of attack by an adversary. It is accomplished using a manually operated, mechanical override to the electronic lock that automatically generates an audible alarm and that permits access only after the expiration of a preset minimum period of time.

Electronic Lock

At least one of the currently operational procedures for accessing a special weapons storage magazine requires that operations personnel and security personnel, in the required numbers, proceed to the designated magazine where they telephone the security center to request that the intrusion alarms be placed in the access mode. The security center has, of course, been alerted to expect a request for authorized access. Each of the two groups at the magazine has obtained its own key to one of the two security padlocks on the magazine door and when telephone communication has been established with the security center, they each unlock one of the padlocks and open the door.

This procedure provides a very high degree of protection but it is conceivable that it might be subverted by some combination of defection, deceit and collusion. With the CSSMRS, additional protection is provided through the use of an electronic lock that could either be added to the present arrangement, or could possibly replace one of the presently employed security padlocks.

The electronic lock would be released by the matching of two numbers. The matching must occur within a limited time of the access authorization, and only a single trial match would be permitted. When access to a magazine is authorized, the CSSMRS central processor generates a random number that is loaded into CU memory and stored for later transmission to the remote microprocessor associated with the designated magazine or shelter housing. When authorized personnel arrive at the RU and telephone the Guard Control Center and advise that they are ready to access the protected area, then the stored number is transmitted to the RU. Upon receipt, this number is transferred to the buffers of the electronic lock which is located inside the structure and the lock is enabled for a one minute period of time. Only a single comparison may be made within the time interval, and if a match with the random number occurs, an electrical latch on the magazine door is released and its release reported. If a trial is made and the match does not occur the enable period is terminated and an alarm condition is reported to the CSSMRS central processor. An alarm condition is also reported if a match is attempted when the acceptance time is not enabled.

The same random number that is stored for transmission to the electronic lock is also loaded into a portable, battery operated key at the alarm central station. An interval timer in the key is also started, and at the expiration of this interval the number is erased from the key memory. This electronic key, together with the appropriate padlock key(s) are then taken by the authorized personnel to the designated magazine. After telephoning the Guard Control Center,the electronic key is plugged into an appropriate receptacle on the exterior of the magazine and the resulting match of the random numbers in the key and the lock within the acceptance time interval releases the latch.

There are two types of keys; single use keys and master keys. When a single use key is used to open an electronic lock, the random number which it contained is erased. Master keys retain the random number with which they have been loaded and can be used to open any number of locks that have been loaded with the corresponding number; they are erased only at the expiration of the time period with which they were loaded.

Successful matching of the random numbers in the lock with those carried in the key causes an electrically powered solenoid to withdraw a bolt from its strike in the door sill, releasing the door. This solenoid is interlocked with the manual Safe/Arm switch located inside the structure. Power to the solenoid is interrupted when the Safe/Arm switch is placed in the "Safe" position by authorized personnel immediately upon their entry. This interruption of power will permit the bolt to drop into a position that will prevent the door from being reclosed until the manual Safe/Arm switch has been placed in the "Armed" position. (A three minute timer is also started when the lock is opened, and its rundown will also release the bolt even if the Safe/Arm switch is not actuated.). This should be the last action of authorized personnel prior to their exit of the area, and it shall cause the solenoid to again be powered for 30 seconds, lifting the bolt and permitting the door to be closed. At the expiration of the 30 second delay period power is removed from the solenoid, dropping the bolt into its strike and locking the now closed door.

The random number that is generated by the CU and used to open the electronic lock is an eight bit byte. This is a convenient size to handle with a microprocessor and lock comparator electronics. Larger sizes of random numbers would require the use of more electronics components for storing the number and comparing it with the number contained in the key, and this larger component count would result in reduced reliability and shorter MTBF. Eight bits is considered adequate from the security standpoint since any attempt to use a key outside the acceptance time window will cause an immediate tamper alarm (Table II, PIN No. 40). An adversary is given no opportunity to try to pick the lock by trying all bit combinations , and any wrong bit pattern that is applied within the acceptance time gate will give an alarm. In addition, such a bogus attempt will cause the contents of the lock storage register to be cleared and the acceptance time interval to be terminated. Also, correct matching of the key and lock numbers in connection with an authorized access will also clear the registers in the lock and in a single use (as contrasted to master) key and terminate the key acceptance gate periods of both.

The foregoing description assumes a legitimate access attempt under circumstances when all components of the CSSMRS are functioning in a normal manner. This may not always be the case as malfunctions will occasionally occur in communications, microprocessor or other system components and it will then be necessary to access the microprocessor shelter housing or the magazine to perform corrective maintenance actions. This is accomplished using the manual override mechanism.

Override Mechanism for Electronic Lock

Access to a magazine under circumstances when a malfunction has occurred in the data link, the microprocessor or the electronic lock itself, requires that there be an override procedure which can be invoked. This procedure must permit safe access to the magazine by authorized personnel but with minimum compromise to the security of the magazine against an unauthorized adversary.

It is believed that these objectives can best be attained through the use of non-electronic facilities that would: a) require a special tool to operate, and b) would sound a high intensity audible alarm when actuation was started, and c) would insure that actuation could not be completed before the expiration of a predetermined time interval, and d) at the end of this time interval would physically withdraw the bolt of the electronic lock from its strike, and e) would force the electronic Safe/Arm device to the "Safe" position to prevent the inadvertent actuation of FEDS.

A conceptual arrangement which could be used to accomplish these functions could be mounted on the interior of the magazine door. It would be actuated by means of a crank that would be inserted through a sleeve in the door so as to engage a shaft enclosed by the sleeve and rotate this shaft. Rotational speed would be limited by a centrifugal governor arrangement that would disengage the shaft from the mechanism that it drives if the crank were to be rotated too rapidly. The shaft, when rotated at a suitably low speed, would drive a set of reduction gears that would further reduce the speed. These would, in turn, drive a lead screw that would move a yoke arrangement that would pull the bolt of the electronic lock using a flexible metal cable. Pulling this cable would also actuate the valve on a compressed nitrogen cylinder that was connected to an air operated horn to sound an audible alarm long before the bolt is withdrawn.

A sketch showing one way that such a mechanism might be implemented is shown in Fig. 8. This sketch is intended only to illustrate a concept; it is not a complete engineering design.

Item A is a casting that serves as the major frame of the device, supporting the bearings (not detailed on the sketch) and other major components. It is mounted on the inside of the magazine door (mounting arrangements not shown) and fitted with a protective cover (not shown) with the drive shaft, B,,projecting into a metal sleeve through the door. A crank may be inserted into the sleeve through the door from the outside and will have holes that will mate with the unsymmetrically located studs on the end of B. The studs on shaft B are intended to make it difficult to rotate the shaft with any thing other than the appropriate crank which should be kept in a secure area when it is not in use.

A deep socket wrench, F, is normally forced to engage the hexagonal section, G, as a result of pressure from spring E. This socket wrench is free to slide on the square section of B above the spring, E. It is linked to three governor weights, D, (only one is shown in the lower view of the sketch) which are securely attached to the shaft by collar, C. The size of these governor weights, D, and the rate of spring, E, are set to cause disengagement between F and G to occur at any rotational velocity greater than about one revolution per second.

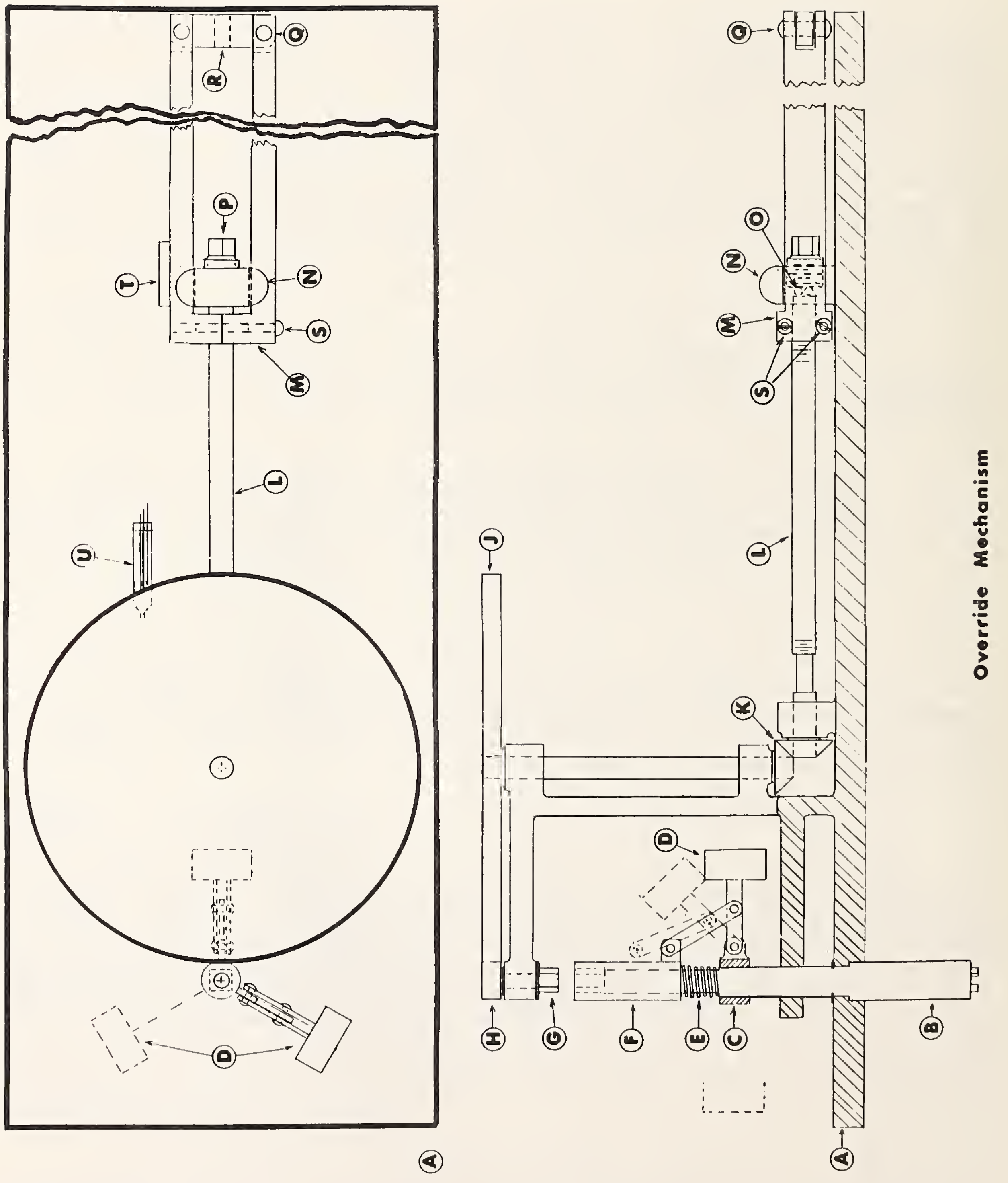


Figure 8 Override Mechanism

Rotation of shaft, B, at an acceptably low speed, drives spur gear, H, which engages another spur gear, J, further reducing the rotational velocity by a factor of about ten. This rotation is translated through a right angle by bevel gears, K, to drive a threaded shaft, L. A split yoke, M, is attached to the threaded shaft, and is slowly moved from the position shown in the sketch up toward the bevel gears. The threads on L are undercut at the end nearest to K so that excessive cranking cannot drive yoke, M, into the bearing support adjacent to K but rather drops M off of the threaded section of L when the undercut is reached. The yoke is kept roughly aligned with shaft, L, during its travel by machined slots in the side of bearing block, N, which also seats the right hand end of shaft, L, which is supported by the thrust bearings, O, that are, in turn, contained by plug, P.

A flexible cable is attached to the yoke at R. This cable actuates the valve on a cylinder of dry nitrogen during the initial part of the movement of the yoke, releasing the gas to blow an air horn. The cylinder valve is pulled by a branch cable that is spliced into the main cable. There is a spring in series with this branch cable that permits motion of the main cable to be readily continued after the limit of travel of the nitrogen cylinder valve has been reached. The main cable is attached to the bolt of the (normally electrically actuated) solenoid lock and its length is such that the bolt will be pulled clear of the strike just before the magnet, T, on the side of the yoke, M, reaches and actuates the sealed reed relay, U. When reed relay, U, is actuated, this forces the electrical Safe/Arm switch to the safe position disabling the FEDS and also provides a signal to the authorized personnel seeking access that the override procedure has been successfully completed.

Reset of the override mechanism is facilitated by the fact that yoke, M, is split. The screws, S, can be loosened and the pivot at point, Q, permits the halves of the yoke to be separated, freeing them from the threads on L and letting the yoke be returned to its normal position adjacent to N. Then the two halves of the yoke are refitted on the threads and the screws retightened. The nitrogen cylinder must also be replaced with a full cylinder to complete the reset process.

In addition to the features described above, the override mechanism should be equipped with a mechanical flag or similar signal that would provide non-electrically powered indication to authorized personnel when the operation had been completed, and a tamper alarm should be incorporated together with a pressure operated alarm to signal low gas pressure in the storage tank.

Fig. 9 shows an artists conception of the installation of an override mechanism on a magazine door.

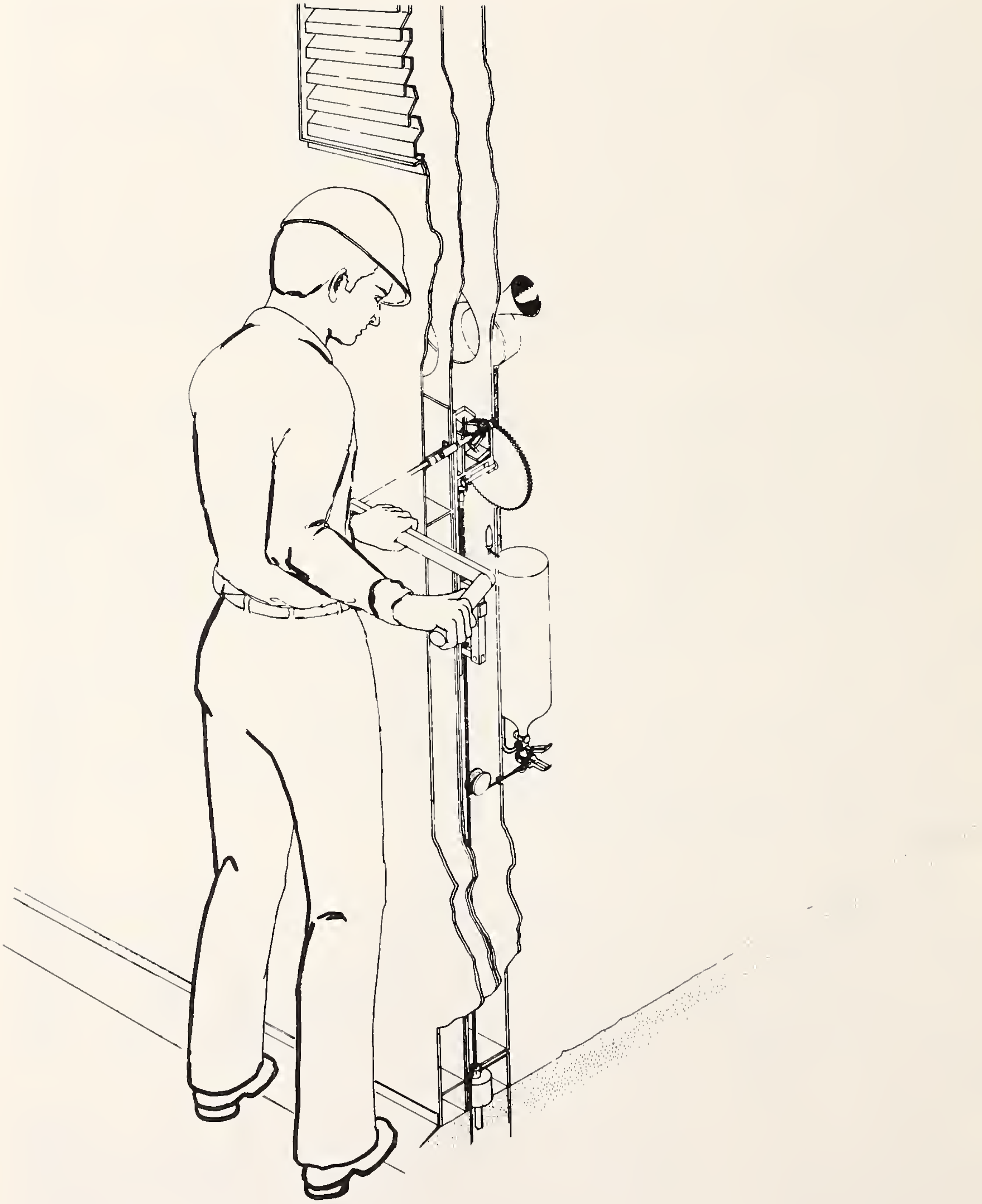


Figure 9 Artists Conception of Override Mechanism

Since it will be necessary to use the override mechanism when there has been a failure in either the communications or microprocessor capabilities at a RU, the normal procedures for establishing an access will not be available. As a consequence, the moment that service is restored by the repair crew, sensor alarms will be reported to the CU and displayed at the Guard Control Stations. Local operational procedures must accommodate this. For example, the location of the RU where the override action is planned is known in advance to the guard forces and the appropriate alarm indicators can be marked using a grease pencil or liquid chalk or other easily removable marking method. In addition, the repair crew might be given an electronic key loaded with a random number having a long life time so as to be likely to be still valid after the passage of the time needed to make repairs. Then, when service had been restored, the maintenance personnel could telephone the Guard Control Station and go through the normal access procedure converting the alarm status to an access status on the appropriate displays and indicators at the Guard Control Station. This would provide the additional benefit of testing the electronic lock.

Safe/Arm Provisions for FEDS

The FEDS must be configured in a RU in such a way that they can be quickly and reliably actuated when they might be needed in an emergency, but protected against accidental or unintended firing. It should be nearly impossible for FEDS to be actuated as a consequence of activities conducted in the course of authorized accesses to a protected area, or as a result of deliberate harassment efforts on the part of an adversary. There should also be a very high probability that they will be actuated if an adversary succeeds in penetrating the protected area, whether or not the RU affected has been cut off and cannot communicate with the CU. Fig. 10 is a simplified block diagram showing the Safe/Arm arrangements and other features that have been incorportated in the configuration of the RU to support these objectives.

Power to fire the squib that actuates a FED passes through an electrically controlled Safe/Arm switch first, then through a manually controlled Safe/Arm switch, and then through individual computer controlled firing switches, one for each FED. Both of the Safe/Arm switches must be in the "Arm" position, and the appropriate fire control switch must be actuated in order for the squib of the selected FED to be fired. The squibs are low impedance devices, typically about one ohm, and are reliably initiated by a current pulse of several amperes magnitude.

Normally, when a magazine is in a secure state, the electrical Safe/Arm switch is in the "Safe" position and the manually controlled Safe/ Arm switch is in the "Armed" position. If a sensor alarm occurs, the RU reports it to the CU in response to the next poll. It is then reported and displayed at the Guard Control Station where it is acknowledged and assessed. If, as a result of the assessment, the guard determines that there is a valid threat, he may elect to actuate the FEDS. He does this by first commanding that the FEDS be armed. This is done by means of a message from the CU to the RU that switches the electrically controlled Safe/Arm switch to the "Armed" position. The guard then actuates function keys that direct the firing of the FEDS and the resulting message from the CU to the RU actuates the proper fire control switches.

The foregoing assumes that assessment is a prerequisite to actuation of a FED because only a single alarm has been triggered and this could have been caused by malfunction or some nuisance event rather than by an adversary. This uncertainty would not exist, however, if several different types of sensors protecting the area were to be alarmed in the proper sequence. For example, if the magnetic switch on the door of a magazine were to become alarmed, followed immediately by an alarm from a sensor of visible light located inside the magazine, followed in turn by an alarm from a motion sensor located inside the magazine, there would be a high order of certainty that the door of that magazine had been opened, admitting both light and someone who was moving around inside. Under these circumstances, the CU would be programmed to arm and fire FEDS without waiting for guard assessment and action. Further, in the event communication between the CU and the RU had been cut off, the RU would be programmed to take the same actions autonomously and fire the FEDS on the basis of the alarms from this special sensor group.

When authorized access to an RU occurs, the random numbers transmitted to the electronic lock and loaded into the electronic key match when the key is plugged into the lock receptacle. This actuates the solenoid that opens the bolt of the lock. Normally the personnel making the authorized access would now open the door, enter the magazine and proceed to the manually operated Safe/Arm switch to throw it to the "Safe" position as their first act after entry. If however, communications between the RU and the CU should fail between the time that they had entered the magazine and the time that the manually operated switch had been placed in the "Safe" position, the special sensor group described above would be alarmed and the RU would autonomously fire the FEDS unless prevented from doing so by other means. Such a means is invoked for the safety of authorized personnel. The fact that the electronic lock has been operated as a result of a match in the random numbers is logically combined with the RU computer's attempt to arm the electrically controlled Safe/Arm switch to start a timer which will delay the arming command for 30 seconds and will sound a warning horn for this period. This delayed firing sequence can be stopped by either of two actions. The manually operated Safe/Arm switch can be placed in the "Safe" position (which releases the solenoid actuated bolt) or the personnel can retreat, closing the magazine door and removing the alarm causing conditions. If the latter course of action occurs, the matching signal from the electronic lock is reset automatically by the rundown of a timer that was started at the time that the lock was opened.

In instances when access is made after using the mechanical override to the electronic lock (required in the event of failure of certain RU components), the electrical Safe/Arm switch is positively forced to the "Safe" position and any computer commands to the contrary are inhibited. The "Safe" condition of the electrical Safe/Arm switch is annunciated when the override mechanism has been actuated to the end of it's cycle.

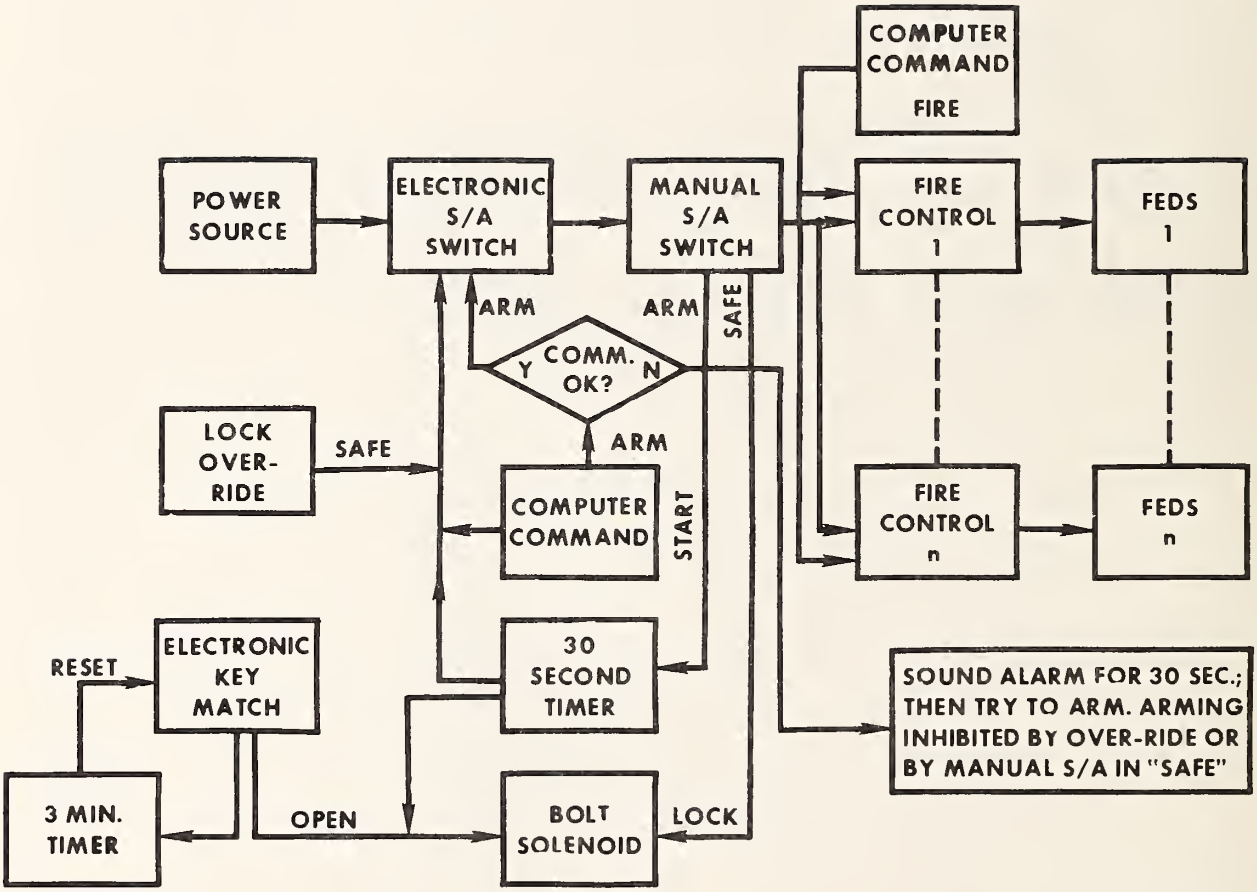


Figure 10 Safe/Arm Switch Arrangement

Just as the first act on entering a protected area is to place the manually operated Safe/Arm switch to "Safe", the last act before leaving is to switch it back to "Armed". This action starts a 30 second timer. The timer actuates the solenoid of the locking bolt, permitting the door to be closed, and inhibits any command from the computer to arm the electronic Safe/Arm switch. This provides personnel the same protection against the loss of communication during exit that they received during entry. The warning horn is again sounded if communication loss should occur prior to rundown of the timer and exit of the personnel.

Three voltage sensing points are provided in the arrangements and these can be used with appropriate computer commands to test the power source used for firing FEDS, to test the continuity of each of the FEDS squibs and to ascertain the position of each of the two Safe/ Arm switches. Additional details reqarding the circuitry of the Safe/ Arm system may be found in the Appendix.

Microprocessor

The microprocessor that is a part of each RU must be selected to be reliable and to be tolerant of environmental variations, particularly temperature extremes. It should be economical in power requirements and should function properly in spite of modest variations in supply voltage. Complementary metal oxide semiconductor (CMOS) fabrication techniques yield devices that meet these requirements and are recommended for this application. All programs should be stored in read only memory (ROM) while static random access memory (RAM) is provided for variable data.

The Remote Unit computer can assume any one of nine possible states. These are:

Initial State

Secure State Normal

Alarm State Normal

Arm FEDS State Normal

Fire FEDS State Normal

Secure State Autonomous

Alarm State Autonomous

Arm FEDS State Autonomous

Fire FEDS State Autonomous

Autonomous states are entered if no communication exists between the RU and the CU.

The program occupies only one "state" at a time, although many activities may be carried on while in each state. Programs are modular in form to facilitate both documentation and possible future modification.

The operating system and all of the program modules are based on cyclic polling of inputs rather than being interrupt driven. The programs shall contain at least the following modules:

Initialization. This shall consist of those functions that are necessary to bring the microprocessor at the RU up from the power-off condition to the Secure State Normal.

Polling Sensors and Electronic Lock. The status of each sensor and the electronic lock shall be polled in a cycle which is never to exceed 80 ms and which is to be started immediately following a response to a poll command from the CU. When an alarm condition is detected from any sensor, a special area in RAM (called the Status Report) is updated with the sensor identity number; a Status Change flag is set to control the type of response made to the next poll by the CU; the State is changed from Secure State Normal to Alarm State Normal. An incorrect attempt to operate the electronic lock is considered an alarm condition.

Responding to Commands from the CU. The microprocessor at the RU begins to monitor a poll time window 80 milliseconds after the last poll was received, and continues to monitor this window until the next poll is received or until 220 ms additional time passes, whichever occurs first. If the poll is received within the poll time window, the frame is accepted, if correct, and acted upon. A UI command is acknowledged and the instructions in the information field are executed. A UP command causes a UI response with the Status Report contained in the information field. A PN command causes a UA response if the status change flag has not been set and a UI response with the change information if it has been set. An APN or UI frame must be received as the next command following this response. If the poll is not received within the poll window (0.3 second since the last poll) the Autonomous Mode Normal State is entered. In the Autonomous Mode, the sensors are polled on a 0.3 second cycle which is completed within the first 80 ms while the balance of the cycle time is spent monitoring the poll time window to insure immediate recognition of service restoration. One of the possible commands that the RU may receive is to initiate tests on selected sensors or FEDS. Upon initiation of each test, the RU microprocessor will resume other activities until the tests are complete and the results stored in the Status Report area for transmission to the CU follwing the next poll.

Transferring Key Codes to the Electronic Lock. The processor is to recognize a key code transfer message from the CU and load the lock register with the random eight bit byte that is received and enable the key acceptance time gate for one minute.

Monitoring Communications Continuity. This program module is to reset a timer each time a valid poll or other message is received from the CU and cause the RU to enter the Autonomous Mode if communications are lost for a period of 0.3 second or more. When communications are restored, the Normal mode is reentered and any changes to status are reported to the CU. The receipt of traffic on both the CW and CCW loops is also monitored and any deviations from normal are reported even though valid communications still exists on one loop.

Arming and Firing FEDS. In the Normal Mode, arming and firing FEDS occurs only in response to specific commands from the CU; however, in the Autonomous Mode the FEDS can be armed and fired as a result of the alarming of a Special Sensor Group and without specific commands from the CU. This program module is arranged to perform these functions.

Sensors, sensor testing devices and FEDS are all assigned addresses on the microprocessor I/O bus and treated as simulated peripherals. In general, interface adaptors will be required to accommodate the different signals representing secure or alarm conditions that are output by the different types of sensors.

Power Supplies

The primary source of power for all RU components is 115 volt nominal, 50-60 Hz, single phase. This is converted to dc as required for the operation of sensors, microprocessor, FEDS and other components. Backup rechargeable batteries shall be provided for all components except the CCTV and lights. The batteries shall have the capacity required to maintain four hours of operation after the failure af the primary power, and shall be automatically fully recharged within 24 hours after the restoration of primary power. Transition from primary to battery power or vice versa shall not cause interruption on normal operation; however, such a transition shall be monitored and reflect a change in status that will be reported back to the CU.

Central Computer Complex

The Central Computer Complex is to consist of the following elements:

Central Computer (triply redundant)

Communications Microprocessors
(one per CROSSFIRE loop)

Reliability Considerations

An exceptionally high degree of reliability in the Central Computer is essential to an acceptable level of performance of the CSSMRS. If an RU fails, a guard can be posted at the protected area until service can be restored. Failure of a communications microprocessor poses more of a problem, but even this sort of failure temporarily disables only a small portion of the physical security system at a site. Failure of a Guard Control Station causes inconvenience, but the second Guard Control Station is available to maintain the continuity of security surveillance. Total failure of the Central Computer, however, would have a major impact on the site security posture, and every effort must be made to minimize the possibility that this could occur.

This sort of reliability requirement is neither new nor unique. It exists in many computerized applications that range from airline reservation systems through on-line process control systems such as are used with nuclear power generating plants to manned space flight systems. The general solution to the problem involves the use of redundant computer systems with the techniques for the application of the redundancy and the associated trade-offs between hardware and software complexity often being application dependent. For example, one approach (selected for CSSMRS) involves the simultaneous processing of the same data by multiple computers and the periodic intercomparison of results to ascertain that agreement exists. Another technique that is sometimes employed where a slight delay is tolerable, is for the backup processor to reconstruct the current status working from a backup data base that is as current as feasible. The first arrangement is used in the manned space shuttle flight control computer. Redundant processors work in parallel and their results are compared several hundred times per second. Because of slight differences in processing rates strict software precautions must be invoked to insure that each of the computers is operating on identical input data. If one computer received as input, data that had just been modified by the processing of another of the computers, their outputs could not agree. Frequent pauses are necessary to ensure that each processor has caught up with the others. Problems of this type are aggravated by electromechanical computer components such as rotating memory units. Indeed, these electromechanical devices are themselves far more susceptible to failure than are solid state memory components.

Failures in computer systems can result from either hardware or software malfunction. The current state-of-the-art does not provide a method of positively assuring that a complex software package is completely free of any hidden flaw. The probability that software flaws will be detected and can be corrected in the course of testing is enhanced if the software is modular in form and avoids the use of interrupts to the greatest extent possible. These desiderata have been reflected in the conceptual design of the CSSMRS software. In a similar fashion, the probability of hardware malfunction can be minimized through conservative design, protection against environmental and electrical transients and the maximum utilization of solid state components together with the minimum use of moving-part components. These features are further reinforced with the proposed redundancy implementation involving the synchronous operation of three processors in "lockstep" and the continuous comparison of outputs and the selection and use of only those that are valid.

Central Computer

A block diagram of the Central Computer is shown in Figure 11. The major elements are three computers, Computer A, Computer B and Computer C. These computers are to be driven by a common clock and are to have identical programs. At some time during each clock period there is to be a time when the information on all high speed buses is identical. This identity is to be checked by a set of comparators once per clock period. These comparators are to have output means which identify a computer whose buses are not identical to at least one other computer. In Figure 11 these output means are shown as three wires "A" BAD, "B" BAD, and "C" BAD. A Resynch Controller (not shown in Figure 11) provides certain necessary control signals during a resynchronizing operation.

All information passing from the three computers to output ports is to pass through gating such that only information from the two "OK" computers is passed to the output ports. These gates provide the capability of continuing to output the information generated by the two computers which are in agreement, even though the third computer is in non-agreement. This gating is to be of such a form that if any one gate fails it can affect only one of the high speed buses. In Figure 11, this latter function is performed by the Majority Voting Logic.

All incoming information from input ports is to be coupled through an Input Port Multiplexer. The addresses for the Input Port Multiplexer are to be supplied by a set of gates similar to those used to drive the output ports. The output of the Multiplexer is to be connected to the three high speed buses by buffers.

The computers selected for the Central Computer function are to be of the best commercial quality.

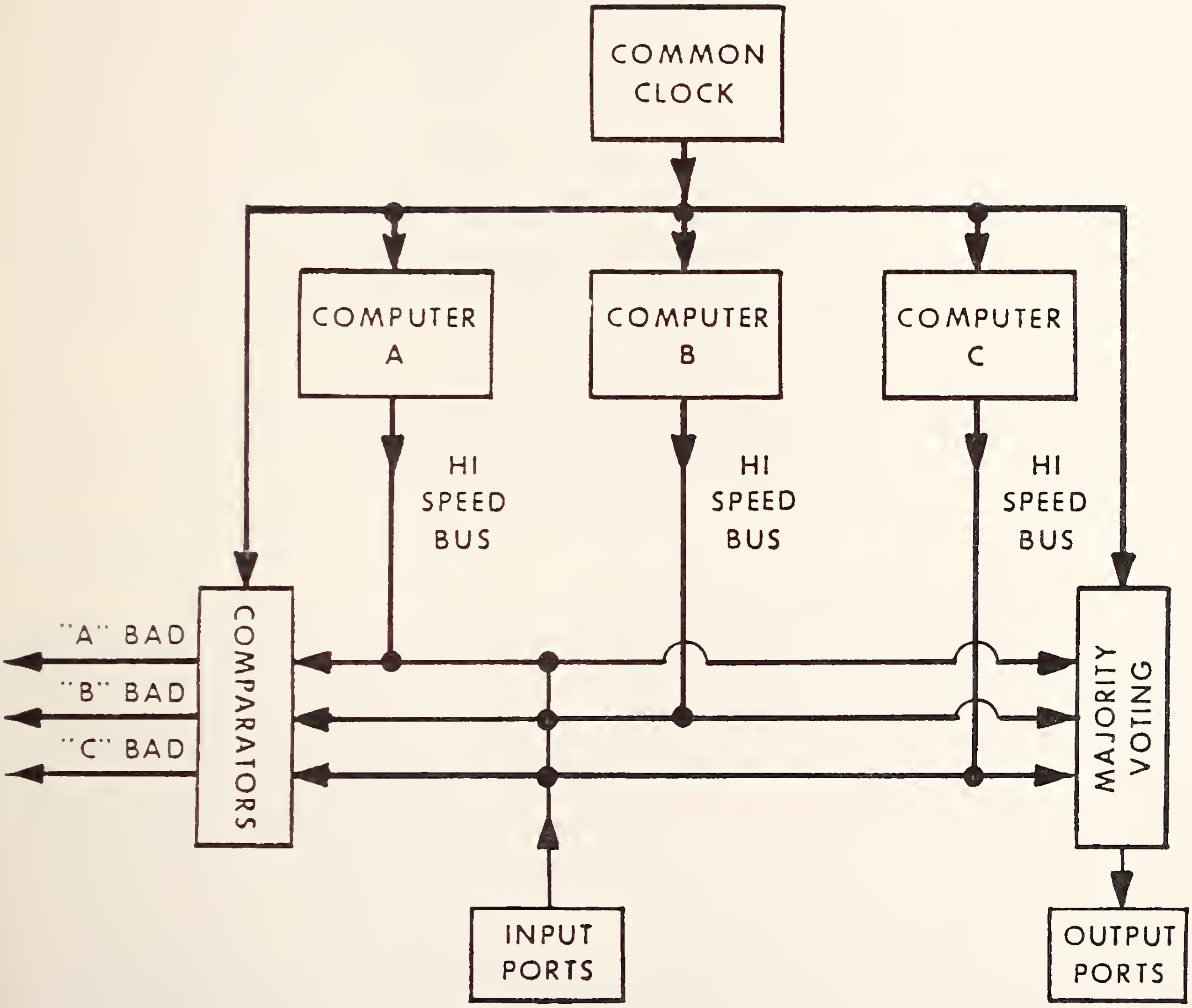


Figure 11 Triply Redundant Central Computer

Program Modules of the Central Computer

The Central Computer Program is to consist of an Operating System and the following Program Modules:

Initialization
Resynchronization
RU Status Update
Status Change Dissemination
Geographical Display Unit Driver
Guard Operating Panel Indicators Driver
Digital Display Unit Driver
Logging Printer Driver
Guard Control Station Monitoring
Independent Reaction
Assessment Patching
Guard Login/Logout
Random Guard Assignment
Access Control
Sensor Testing
FEDS Testing
Environmental Correlation
Communication Monitoring
Self Testing
Response Forces Alerting Driver
Augmentation Forces Communications Driver

Initialization Module

Each of the three redundant computers is to have its own independent power supply and backup power supply. At time of power-up, a central power control is to recognize that all three supplies are up; when this has occurred a signal is to be sent to all three computers which enables them to proceed, in lockstep, with the initialization orders. The Initialization Module clears and presets all memory and registers to their appropriate values.

Resynchronization Module

The purpose of the Resynchronization Module is to provide the capability for recovering from a transient event (such as may be produced by a lightning stroke) without losing information stored in memory and without seriously impacting the performance of the Remote Units. If, after three tries at resynchronization, the system still has one computer in disagreement with the other computers, a hardware failure is assumed, and notification is given to the Guard Force that a repairman is to be called. The system then continues with two computers.

The Operating System is to provide at approximately one second intervals an opportunity to enter the Resynchronization Module. This time is called the All OK Check Time. If, at this check time , one of the Computer OK lines is down (indicating that there has been some computer disagreement since the last Check Time) the operating system is to enter the Resynchronization Module. If no Computer OK lines are down, the Operating System skips the Resynchronization Module.

Upon entering the Resynchronization Module, control is passed to the Resynch Controller, which is central to all three computers. The first step is to mask all possible interrupts from outside sources. Assume that Computer A has had a disagreement with Computers B and C. The Resynch Controller sets B and C to a WAIT condition. The next step is for Computer A to take control of Computer B's high speed buses. Computer A is to then copy the contents of all of the RAM located in Computer B. Upon completion of this task Computer A notifies the Resynch Controller and goes into a WAIT state. the Resynch Controller then removes the WAIT condition from all three computers and vectors them to the synchronized exit from the Resynchronization Module.

If Computer B is the nonconforming unit, then Computer B copies RAM from Computer C. If Computer C is the nonconforming unit, Computer C is to copy RAM from Computer A.

RU Status Update Module

This module is to receive status information about each Remote Unit and to update the RU Status Memory if status has changed.

During normal communication load conditions, the module shall poll each of the Communications Microprocessors (CM) at a rate such that all CMs are read within an 80 millisecond period. Since the CMs are to act as information buffers, each polling will result in the Central Computer receiving a complete report on all the changes occurring in any reportable items at all the Remote Units reporting to that Communications Microprocessor. Following a poll in which no RUs reported changes, a Communications Microprocessor Summary Report will state that each RU has been contacted and that the status of no RU has changed. Under such conditions, this program module does not change the data in the RU Status Memory.

Included in the report from the CM to the Central computer is a CROSSFIRE Communication Loss Word (CCLW). One of these words is associated with each RU and indicates the number of polls that that particular RU has missed since the last good response from that RU to the CM. This word is to consist of two bits as follows:

00	- No polls missed
01	- One poll missed
10	- Two polls missed
11	- More than two polls missed

In keeping with the general principle of reporting changes only, this CROSSFIRE Communication Loss Word needs to be included in the summary message from CM to Central Computer only for those specific RUs for whom the CCLW has changed. This occurs whenever one or more polls have been lost.

The CROSSFIRE Communication Loss Word is to be used in the Communications Monitoring Module.

The RU Status Memory is to consist of two bytes for each Remote Unit in the CSSMRS. The format for information within those bytes are as follows:

Byte 1	Bit 1	Communication Loss Word
"	Bit 2	" " "
"	Bit 3	Secure/Alarm
"	Bit 4	No Access/Access
"	Bit 5	Safe/Arm
"	Bit 6	Number of FEDS sets fired
"	Bit 7	" " " " "
"	Bit 8	" " " " "
Byte 2	Bit 1	Normal power/Backup power
"	Bit 2	All sensors OK/not OK
"	Bit 3	All FEDS OK/not OK
"	Bits 4 through 8 available as spares.	

The messages transmitted from the Communications Microprocessors to the Central Computer are to be sent via dedicated First-In-First-Out buffers (FIFO) to act as load levelers. Each message from a CM to the Central Computer is to consist of a summary of the entire last polling cycle of the loop of RUs which it is responsible for. This summary is to be organized by Sensor type; under each Sensor type which had a change, the specific RU number having such an alarm is listed.

Each of these messages will have as a part of it a Poll Period Word (PPW).The PPW is to consist of two bits; if the last poll conducted by the Communications Microprocessor was completed within the normal poll cycle time, the time word is 00. The complete code for time words is as follows:

00 - Completed between 0.0 and 0.1 sec.
01 - Completed between 0.1 and 0.2 sec.
10 - Completed between 0.2 and 0.3 sec.
11 - Completed in more than 0.3 sec.

The PPW is to be used as additional input information to the Environmental Correlation Module.

The Communication Microprocessor's firmware is to be designed in such a way that, during times of abnormally high levels of communication, the loop polling cycles may increase beyond 100 milliseconds. An abnormally high level of communication is defined as being more than 100 alarms being reported per CROSSFIRE loop per polling cycle.

Similarly, the firmware for the RU Status Update Module is also to be designed in such a way that, during times of abnormally high levels of communication between the Central Computer and the Communication Microprocessors, the polling cycle of the CMs by the Central Computer shall be allowed to lengthen.

When any reportable status change is posted to the RU Status Memory, the number of that RU is also stored in a portion of memory called the Change File.

Status Change Dissemination Module

The purpose of the Status Change Dissemination Module is to output any alarms or other reportable changes in RU Status to the Guard Control Stations, via the appropriate driver modules.

The Status Change Dissemination Module is to first investigate the Change File. If the Change File shows that an RU has had any change in status since the last time this Module was called, the Module reads the Status of that RU from the RU Status Memory. The Module firmware is to then make a decision, based on the type of status change, and on the output of the Environmental Correlation Module, as to whether the information is to be sent to the Geographical Display Unit, the DDU,the Guard Operating Panel Indicators (GOPI), the Logging printer, or all four.

Geographical Display Unit Driver Module

The purpose of the Geographical Display Unit Driver Module is to accept data from the Status Change Dissemination Module and illuminate appropriate indicators on the Geographical Display Unit. The Geographical Display Unit Driver Module is to reside in a microprocessor dedicated to this task. The Geographical Display Unit Microprocessor drives hardware lamp drivers.

See Section on Geographical Display Unit for details.

The Geographical Display Unit Driver Module is to be able to accept up to 512 indicator changes per second. For changes which require a guard acknowledgement, these indicators are to flash under Driver control until such acknowledgement is made.

Two indicators per RU are to be serviced. One of the indicators is to be yellow, indicating that an authorized access is in process. The other indicator is to be red, indicating that the RU has at least one alarm condition.

Guard Operating Panel Indicator Driver Module

This module accepts inputs from the Status Change Dissemination Module, and it outputs steady or flashing commands to specific hardware lamp drivers.

Digital Display Unit Driver Module

The purpose of this module is to provide the coupling between modules of the program and the Digital Display Unit.

Under normal operating conditions this module accepts inputs only from the following Modules:

Status Change Dissemination
Independent Reaction
Assessment Patching
Random Guard Assignment
Access Control
Sensor Testing
FEDS Testing
Environmental
Communication Monitoring
Self-Testing

At certain times the system will be under control of a computer programmer or repairman, who is to be called the Analyst. This module is to be capable of receiving inputs from every module and the Operating System when the Central Computer is under control of the Analyst.

The output of this module is sent to the Digital Display Units located within the Guard Control Stations.

This module shall have the capability of converting information coded in various digital formats into strings of ASCII characters which form easily understood English phrases and sentences. ROM capacity for 1000 phrases averaging 64 characters per phrase shall be provided.

Physically, the character information is to be sent to the Digital Display Unit at a speed of at least 2400 bits per second.

Logging Printer Module

With the exception of test data, this module is to accept all the information generated by the Digital Display Unit Driver Module, convert it into a format suitable for printing on a hard copy printer, and deliver this information at a rate of at least 2400 bits per second to the printers located within the Guard Control Stations.

With respect to test data on Sensors and FEDS, only those tests which show changes in the operational condition shall be logged.

The log is to contain all information about any changes in state of the CSSMRS, including all messages sent to guards and all orders given by guards which are not purely verbal.

Guard Control Station Monitoring Module

This module is to accept all information generated by the Guard Control Stations and disseminate this information to the appropriate program module or peripheral device.

Function Switches to be monitored within the GCSs are to be the following:

Ten Digit Keypad
Acknowledge
Location Select
Two Digit Code Lifetime
Code Key
Code Master Key
Access
Master Access
Secure
Arm FEDS
Safe FEDS
Fire FEDS
Confirm
Cancel
TV On/Off

Lights On/Off
TV Bad/OK
Pan, Tilt & Zoom Controls
Test Sensors
Test FEDS
Test HQ Links
Guard Login
Guard Logout
Summon Response
Summon Augmentation

The Ten Digit Function Switch Pad output is to be distributed to the Location Selected Register and to the Login/Logout Module.

The Acknowledge Function Switch information is to be made available to the Status Change Dissemination Module, which, in turn delivers the information to the driver modules for the Geographical Display Unit, the GOPI, the DDU, and the Logging Printer. It is also to be made available to the Independent Reaction Module

Information from the Location Select Function Switch and the Function Switch Pad is to be stored in the Location Selected Register. This information is used to govern the Remote Unit to which many of the guard commands are directed.

The Two Digit Code Lifetime switch is used to indicate the period of time during which a random number that is assigned to an electronic key will be valid. The time is expressed in increments of 10 minutes each and the maximum lifetime that is allowable for any single random number key code is 640 minutes (10 hours and 40 minutes).

The Code Key Function Switch together with the Ten Digit Keypad and the Location Select Function Switch is used to load a random number into a single-use electronic key and to store that same number for subsequent transmission to the designated RU. This number is erased from memory after it has been successfully received by the RU.

The Code Master Key Function Switch is used in a manner analogous to the Code Key Function Switch except that it is used to load the key into a master electronic lock key, and the random number is not erased from memory after transmission to a single RU; it can be transmitted to multiple RUs up to the limit of its lifetime.

The Access Function Switch, together with the Location Selected Register provides information to the Status Change Dissemination Module. It is used with a one-time-use electronic key for making an access to a single designated RU.

The Master Access Function Switch is similar in operation to the Access switch, but is used with a master electronic key.

Information from the Secure Function Switch, together with the Location Selected Register, is to be provided to the Status Change Dissemination Module for the purpose of informing the CU that access to a particular RU is terminated; or that an alarm condition is to be terminated; or logging the return of a Remote Unit from ACCESS to SECURE.

Information from the Arm FEDS Function Switch, together with the Location Selected Register, is to be provided to the appropriate Communication Microprocessor for transmission to the addressed RU. The module is to reject the command if the particular RU is not in the Alarm State.

Information from the Safe FEDS Function Switch, together with the Location Selected Register, is to be provided to the appropriate Communication Microprocessor for transmission to the addressed RU .

Information from the Fire FEDS Function Switch, together with the Location Selected Register, is to be provided to the appropriate Communication Microprocessor for transmission to the addressed RU if this command is confirmed. The module is to reject this command if the particular RU is not in the Alarm State.

Information from the Confirm Function Switch is to be used within the GCS Monitoring Module to force the guard to make an extra confirming function switch stroke before certain critical commands are transmitted.

The Cancel Function Switch is used to terminate commands that are not confirmed.

Information from the TV On and TV Off Function Switches is to be used, in conjunction with the Location Selected Register to turn the camera(s) at that RU on or off. The "Camera On " command also serves to turn on the assessment lights (if any) at the selected RU and creates an entry on the Digital Display Unit recording this condition. The "Camera Off" command removes the "Camera On" entry from the Digital Display Unit but does not turn off the lights or affect the entry about them on the Digital Display Unit.

The information is also to be sent to the Assessment Patching Module, which assigns the monitor(s) selected by the Monitor Pointing Switch to the new camera. The module must also communicate with the RU Status Memory; if a Storage Area is being legitimately accessed the module is to refuse a request for TV assessment at that Storage Area.

The TV Bad/OK Function Switch is a momentary action, spring-return, center-off, switch that is used to log changes in the operational status of CCTV equipments at designated locations.

Information from the Lights On/Off Function Switchs is to be used, in conjunction with the Location Selected Register, to turn the assessment lights on and off at the selected RU. The Digital Display Unit shows the identification of any RUs where lights are on. The entry is removed when the lights are turned off.

Information from the Pan, Tilt & Zoom Controls is to be used, in conjunction with the Location Selected Register, to effect pan, tilt, and zoom of the CCTV camera at the selected RU when the camera at that RU is so equipped.

The Test Sensors and Test FEDS Function Switches are used with The Ten Digit Keypad and the Location Select Function Switch to test the Sensors and FEDS respectively at the designated RU.

The Test HQ Links Function Switch causes an automatically generated test transmission exchange on each of the alternate links to the Augmentation Force Headquarters, and for the results of this test to be recorded on the logging printer.

Information from the Login and Logout Function Switches and the 10-digit keypad is to be distributed to the Login/Logout Module.

Information from the Summon Response Force Function Switch is to is used to actuate audible alarms locally and at the Response Force Headquarters.

Information from the Summon Augmentation Force Function Switch is to be output to the Secure Digital Link for transmission to the Augmentation Force Heaquarters.

Independent Reaction Module

This module is to receive information from the Status Change Dissemination Module and from the Guard Control Station Monitoring Module and is to initiate action independently of guards in the following circumstances:

INPUT	REACTION
Special Sensor Group Alarm	Arm & Fire FEDS immediately

No Acknowledgement at GCS	Alert Resonse Force and Augmentation Force
RU Miss 3 Consecutive Cycles	Instruct Guard at SSCC to Post Guard(s) and Alert Maintenance Personnel

Assessment Patching Module

This module accepts information from the RU Status Update Module and outputs information to a Communications Microprocessor to turn on assessment camera(s) following an alarm. The module also is to select assessment monitor(s) on a rotating basis and is to activate an appropriate set of video switches to accomplish this. The module also accepts information from the GCS Monitoring Module and selects and activates switches to provide monitor(s) to view a guard selected location. The module also outputs information to a set of Camera Identity Indicators mounted on the monitors in the Guard Control Stations. Indicators are also to display to the guard what camera controls are available at that particular RU.

Each Guard Control Station is to have four assessment monitors that are arranged as two pairs. One pair is located on either side of the Digital Display Unit. When a perimeter segment is selected for assessment, the output of the camera equipped with the 75 mm lens viewing that segment is displayed on the upper monitor of the designated pair of monitors. The output of the camera that is equipped with the 50 mm lens viewing that segment is displayed on the lower monitor of the designated pair. If the location that is selected for assessment is a magazine, then only the lower monitor of a designated pair is activated; the upper monitor displays a blank screen. There is only a single set of camera controls. A two position Monitor Pointing Switch in front of the guard selects which of the monitors is connected to the camera that will respond to this set of controls (and other function switch controls).

The procedure during a sequence of alarms is to be as follows. Assume that initially Guard A is viewing RU 71 (a perimeter segment) on the Left Monitor Pair, with no alarm present. When an alarm is reported to the Assessment Patching Module from RU 80, (a magazine) the module is to automatically turn on the lights and camera at RU 80, patch that camera through to the Lower Right Monitor, and send camera identity and control information to the indicators associated with the Right Monitor. Guard A at this time is to acknowledge the alarm. As soon as he has completed his viewing of the Left Monitor, Guard A may push his Monitor Pointing Switch to the right, which action is then to connect his camera controls to operate the controls of the camera at RU 80. Unless other changes are made, all commands to an RU are then directed towards RU 80. These commands may include arming and firing the FEDS, as well as the secure command.

The guard at Guard Control Station B may choose identical action or different.

Automatic monitor patching is to be done to that monitor pair which is not , repeat - NOT, selected by the two position Monitor Pointing Switch. Thus, if another alarm occurs following the above sequence, the camera at the new alarmed RU is turned on and its video patched into the Left Monitor Pair. Camera controls remain associated with the camera at RU 80, however, until the Monitor Pointing Switch is manually thrown to the left position. Subsequent alarms are to be queued until a monitor pair is available.

When multiple alarms occur in a short period of time, each must be acknowledged within less than forty seconds to avoid the automatic call-out of Response Forces. The acknowledgement function can be accomplished by either actuating the Monitor Pointing Switch or the Acknowledge Function Switch. When the latter is used, it has no affect on the assessment patching so long as there are other uncleared alarms in the queue.

All alarms are to stay in the Alarm Queue until one guard or the other has actuated a Secure Function Switch addressed to that RU at which the alarm originated, or alternatively, until the sensor has been determined to be malfunctioning.

The Alarm Queue is to be a closed, end-around loop or circular buffer,i.e., when the newest alarm in the queue is displayed, the next one to be displayed is the oldest alarm which has not yet been secured.

As far as assessment patching, the two Guard Control Stations are to be completely independent. Each station has its own Alarm Queue, and at either Guard Control Station sequential selections from that queue can be made automatically by flipping the Monitor Pointing Switch. Acknowledgements , and Securing may be accomplished from either GCS.

Actuation of the Monitor Pointing Switch causes the "oldest" picture to be replaced by the next oldest picture in the queue. Thus, if the third alarm RU was on the Left Monitor Pair, the fourth alarm RU on the Right Monitor Pair, the fifth alarm is to replace the third alarm when the Monitor Pointing Switch is thrown from Left to Right.

Guard Login/Logout Module

This module accepts information from the Keypad, the Guard Login Function Switch, and the Guard Logout Function Switch. It also accepts information from the real time clock. The purpose of this module is to keep a log of which guards are on duty, and at what time they came on duty and went off duty.

Random Guard Assignment Module

The purpose of this module is to assign the on-duty guards to various posts within the Secure Area. It receives information from the Login/Logout Module and from the real time clock. It outputs information to the Status Change Dissemination Module, which in turn is to display it on the DDU and print it on the printer.

This module is to generate new random assignments for guards at random intervals between two and four hours. Guard jobs to be switched include the two GCSs, mobile vehicles,guards posted outside Remote Units, and guards assigned to aid in accessing Storage Areas.

This module is also to randomly select, from a pre-printed table of routes, pseudo-random paths for patrol vehicles to follow when there are no alarms to investigate. The route number is to be sent to the vehicle via the DDU and the guard manning the primary Guard Control Station.

Access Control Module

The purpose of this module is to control the personnel entering the Storage Areas and the Perimeter Stations. It is also to control the issuance of Electronic Keys. It receives data from the Keypad, the Access Function Switch, the Guard Login/Logout Module, the RU Status Memory, and other modules as necessary. It is to output data to the Geographical Display Unit, the DDU, the Logging Printer, and to the Electronic Lock Loading Port. It also sends a copy of the electronic key code to the RU , via the Communications Microprocessor.

There are three different types of "keys" to be controlled. These are the Electonic Keys, the Mechanical Keys, and the override mechanism crank. It is not the responsibility of the Central Computer to control the login/logout of each of these keys; this is to be the responsibility of the Guard Duty Officer. At certain installations "Master Electronic Keys" will be required. These are to be keys with an allowed multi-use provision. The Access Control Module will send identical key codes to the Remote Units to be thus accessed. This portion of the module is to be activated only by a special procedure which will be specified at a later date.

When an Access is to be made to an RU which is in the Secure State Normal or the Alarm State Normal, an Electronic Key and a Mechanical Key are to be issued. If the RU is in any other state, a Mechanical Key, an Electronic Key and a Crank Key are to be issued. The number of any RU to be accessed is to be entered into the Central Computer by means of the Keypad and the Access Function Key. When this occurs the proper key code will be transmitted to the RU where it will be valid for one minute.

At the time that the electronic key code is transmitted to a RU, the Access Control Module will cause the yellow light on the Geographical Display Unit to flash for the RU that is about to be accessed. When the RU is actually accessed, alarms will be transmitted that will cause the yellow light to become steady.

Guard instructions shall be for one member of the access team to telephone the GCS from the outside of the RU before attempting an access.

Sensor Testing Module

The purpose of this module is to initiate the routine testing of sensors at the Remote Units. It accepts information from the RU Status Memory and outputs information to the Remote Unit under test, the Digital Display Unit, the Guard Operating Panel indicators, and the Logging Printer.

A guard may also initiate testing of the sensors at a RU by means of the Keypad and the Location Select and Test Sensors Function Switches. This will cause the CU to generate a series of messages to the RU that will sequentially test each of the sensors at the selected location.

This module is to have a low priority in terms of Central Unit time demands. It is to be designed so that each sensor in the CSSMRS is tested once per 24 hour period on an automatic basis.

The results of this testing are to be reported by summary only to the DDU,and the Logging Printer as long as tests remain positive. Any tests failed are to be reported on the DDU and the Logging Printer in detail at once.

FEDS Testing Module

This module is to be similar to the Sensor Testing Module except that the electrical continuity of the firing squibs are tested instead of sensors.

Environmental Correlation Module

The purpose of this module (which may be implemented in a separate computer at the option of the contractor) is to compute the probability of natural occurrences having triggered nuisance alarms, and to inhibit the distribution of alarms to the DDU and the Geographical Display Unit if there is a high degree of certainty that the alarms were caused by natural occurrences. It is widely known and accepted that many types of environmental background disturbances can stimulate intrusion detection sensors and produce nuisance alarms. These are nuisance alarms rather than false alarms because the sensor is responding to the stimulus that it was designed to respond to; it is just that the source of that stimulus is from a naturally occurring event rather than an intruder. For example, seismic sensors that respond to the slight earth motions produced by the passage of an intruder will respond equally well to motion induced in the earth by the roots of a wind blown tree, or to disturbances produced by a distant earthquake. Thunder, sonic booms or the passage of heavy vehicular traffic such as a train can also induce earth motions. There are, however, enough distinguishing features about many of these disturbances that it should be possible to identify them through the application of digital correlation techniques utilizing data from other sensors. For example, thunder, sonic booms and passing trains all produce acoustic disturbances as well as earth motions, and this fact might be used to assist in the identification of the source of the disturbance. The limited amount of research that has been conducted in applying these sorts of correlation techniques has shown much promise, but much more work will have to be done before the full potential that is believed to exist can be applied to the CSSMRS.

The inputs to this module are from sensors specialized to detecting natural phenomena (such as thunderstorms, earth tremors, etc.) and the reports of the sensors located at the Remote Units. The environmental sensors will be located at or near the SSCC and will provide direct inputs to the correlation processor.

Other inputs to this module that are also not yet fully defined are signals from detectors that are capable of recognizing trace materials that may be incorporated in FEDS. These could provide indication of the activations of FEDS by an RU operating in the Autonomous mode.

Communications Monitoring Module

The purpose of this module is to monitor the communication cycles between the Communication Microprocessors and the RUs in each of their CROSSFIRE Loops. The input to this module is from the RU Status Memory, and the output is to the Geographical

Display Unit, the DDU, the Guard Operating Panel indicators, and the Logging Printer.

If any RU misses more than 3 polls sequentially, on either the CW Loop or the CCW Loop, the module is to compute the most probable point that an attack or an equipment failure has occurred. A guard patrol is to be immediately dispatched to the suspected location. TV Assessment is also to be used; note that communication still exists if only one of the redundant loops is down. If assessment and direct observation by a guard patrol do not discover the cause of the failure, the on-duty repairman is to be dispatched.

If both redundant loops fail, a guard must be posted at any Remote Units that are not in communication with the CU, in addition to the other actions denoted in the previous paragraph.

Self-Test Module

The purpose of this module is to provide certain automatic checks to see if the Central Computer is operating. These checks are to include an arithmetic check, a sum of the numeric equivalent of all the orders in ROM, and several testing dialogues between the computer and the guards manning the GCSs.

These tests are to have a low priority, but a complete set of the tests are to be performed within each four hour period, or whenever required by a guard.

Response Forces Alerting Driver Module

This module is to alert the nearby response forces in the event of emergency conditions. It is activated either by manual action on the part of on-duty guard forces, or by the failure of the on-duty guards to acknowledge an alarm within the alloted time interval. Its output is energizing an audible alarm at the barracks, ready room or other designated location of response forces, and simultaneously energizing a high intensity alarm located within the exclusion area, but audible to the response forces.

Augmentation Forces Driver Module

The purpose of this module is to provide a method of alerting the Augmentation Force in case a situation arises that the guard forces on duty cannot handle. The method of communication itself is to be two way digital links, using encryption , from the SSCC to the headquarters of the Augmentation Forces.

The driver module is also to provide a testing program for the links. The test program is to be one of the low priority modules and provides for the exchange of pseudorandom sequence numbers between the CU and the higher headquarters controlling the Augmentation Forces alternately on each of the dual redundant links. The procedure has been described in the section on the secure digital data links.

Operating System for the Central Computer

In order to reduce the number of undiscovered errors in programs, and in order to reduce the period needed to debug programs, the Operating System (OS) and all the program modules are to be based upon cyclic polling of inputs instead of being interrupt driven. The only exceptions to this philosophy are to be the Initialization Module and the Resynchronization Module. Any further exceptions to this philosophy will be justified in writing by the contractor.

All commands of the Operating System and the Program Modules are to be stored in Read Only Memory (ROM).

The Cycle Period for the Operating System is to be 0.1 second. During periods of low activity, e.g., few or no alarms, the program is to be padded up to 0.1 second by using low priority modules, as will be explained in succeeding paragraphs.

All inputs which desire servicing shall be serviced sequentially in each Cycle Period of the Operating System. During times when alarms are occurring, the low priority padding modules are to be skipped as necessary in order to keep the Cycle Period at 0.1 second. As the alarm rate increases beyond the point at which the OS can maintain the 0.1 second period, even with all low priority modules cut out, the Cycle Period is to be increased as necessary in order to service all input requests.

Figure 12 shows a flow chart of the Operating System of the Central Computer.

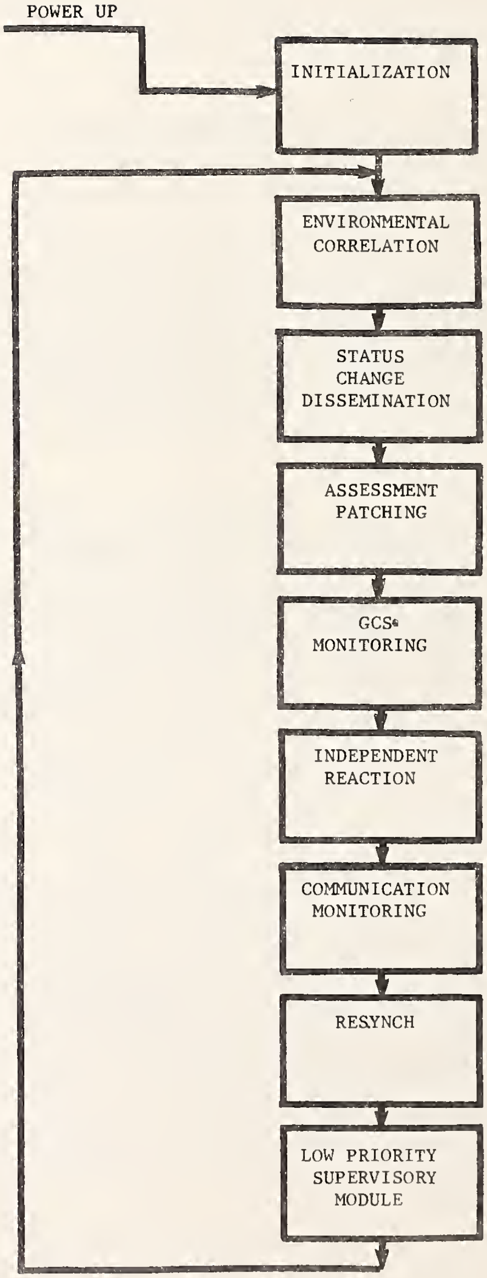


Figure 12 Flow Chart of Operating System for the Central Computer

Following Powerup, the Initialization Module is to be entered.

The poll of the Environmental Correllation Module is the first event of the Cycle Period.

Next, the pointer registers for the Status Change Dissemination Module are to be checked. If changes have occurred, outputs are to be sent to the Driver Modules for the Geographical Display Unit, the DDU, the GOPI, and the Logging Printer.

Following this, the Assessment Patching Module is to be entered if there has been a new alarm.

Next, the Guard Control Station Monitoring Module is entered. This Module checks the flags for each one of the Function Keys. For each function key there is a Sub-Module.

Next, the Independent Reaction Module is entered.

When each of the Function Switches has been serviced the Communication Monitoring Module is to be entered.

Following this, the flags for resynchronization are to be checked. If an error flag has existed for a period of a second, and if three resynchronization tries have not already been made, the Resynchronization Module is called in. If three tries have already been made a request for the repairman is to be sent to appropriate output modules.

The execution of the Resynchronization Module is always to be followed by returning to the Environmental Correlation Module.

If the Resynch Module is not executed, the Cycle Clock is interrogated. If there is still time within one Cycle Period to excecute one or more of the low priority modules, these are to be executed.Following their execution , the OS is to call in the Environmental Correlation Module for the beginning of a new Cycle Period.

Low Priority Supervisory Module

The purpose of this module is to order the execution of certain low priority tasks in a cyclic manner so as to use up the remaining time in each Major Cycle Period. This Supervisory Module is to be entered following the Resynchronization Module, but no time will be spent performing low priority tasks if resynchronization was actually performed, since that activity is expected to require several tenths of seconds.

A hardware chip, called the Cycle Clock, is to keep track of the length of time since the beginning of the Major Cycle Period.

At the beginning of this supervisory module the Cycle Clock is to be interrogated. The module is to choose one or more tasks to perform on the basis of how much time remains in the Major Cycle Period and how recently each task has previously been performed.

These low priority tasks are driven by the following modules:

Random Guard Assignment
(Not to be entered if any assessments are
in progress)
Computer Initiated Sensor Test
Computer Initiated FEDS Test
Computer Self-Test
Headquarters Link Test

Communications Microprocessors at the Central Unit

Communications between the Remote Units and the Central Unit are to be controlled by a group of small computers called the Communications Microprocessors (CMs). Each of these is assigned to poll a number of Remote Units (up to 24 RUs) in a CROSSFIRE loop.

In order to allow the CMs to send information to the Central Computers without interrupting the Central Computer's program, a First-In-First-Out (FIFO) buffer is to be used.

Program Modules for the Communications Microprocessor

The modules are to consist of the following:

Initialization
Polling of the Remote Units
Communication Loss Word Generator
Poll Period Word Generator
Summary Report Preparation
Self-Test

Initialization Module

The purpose of this module is to recognize that power is properly up and then preset all memory and registers to their appropriate values.

Polling of the RUs Module

The polling of the remote units is to be done on a cyclic basis such that each RU is normally polled during a time window between 80 milliseconds and 100 milliseconds from the last poll. If , during periods of relative inactivity, or because of having very few RUs to poll, excess time is available to the CM, the CM is to go into a "Pause" state to pad out the extra time.

Under conditions of heavy activity the CM may not be able to maintain this cycle, and , under such circumstances, the polling cycle is to be extended as necessary.

The control procedures and message formats have been previously described in the descriptive sections on digital communications.

Communication Loss Word Generator Module

The purpose of this module is to keep track of the recent answering of polls by each RU, so that proper action can be taken if communication is lost. The input to this module is from the polls, and the output is to the Summary Report Generator Module.

Each CU is to have a Communication Loss Word (CLW) associated with it in the memory of the CM. The word is to consist of two bits with meanings as follows:

00	- No polls missed
01	- One poll missed
10	- Two polls missed
11	- More than two polls missed

The CLW is to be reported to the CU (via the Summary Report) each time the CLW has changed.

Poll Period Word Generator Module

The purpose of this module is to keep track of how long the last polling cycle took to complete. The input to the module is information from the polls and information from an interval timer hardware chip. The output is to the Summary Report

Generator Module.

The Poll Period Word (PPW) is to consist of two bits with meanings as follows:

00 - Completed between 0.0 and 0.1 sec.
01 - Completed between 0.1 and 0.2 sec.
10 - Completed between 0.2 and 0.3 sec.
11 - Completed in more than 0.3 sec.

The eventual destination of the PPW is the Correlation Module in the Central Computer program.

Summary Report Generator Module

The purpose of this module is to reorganize the data which must flow from the CM to the Central Computer in such a way that the Central Computer program is optimized with respect to speed, especially the RU Status Update Module and the Environmental Correlation Module.

Inputs to this module are from the Polling of the Remote Units Module, the Communications Loss Word Generator Module, and the Poll Period Word Generator Module. Output from this module is to the First-In-First-Out (FIFO) buffer which provides information from the CM to the Central Computer.

The Summary Report is to be organized by Peripheral Identification Number. Each Sentence of the report is to consist of a flag byte, one byte carrying the PIN of a peripheral type, one byte containing the total number of this type which have gone into an abnormal status during the last poll period, two bytes for each RU at which a change has occurred. This last RU byte contains the identification of the RU and also contains information about the new state of that peripheral at that RU.

Power for the Central Computer Complex

In keeping with the overall requirement for extremely high reliability in the Central Computer Complex, each of the three computers in the triply redundant configuration should operate from its own independent power supply. Thus, failure of a single power supply could only affect one of the three computers. Each of the power supplies must have floating backup batteries with capacity to continue uninterrupted operation for at least fifteen minutes following the loss of primary power. It is anticipated that normally the sites emergency generator units could be powered up and assume the essential loads in less than one minute. As a third level of protection against even the failure of site emergency generator units, the Central Computer Complex should be equipped with liquified gas fueled internal combustion engine generator units that could be used to maintain the charge of the backup battery systems. Fuel required to support the CU total power requirements for at least 24 hours must be maintained at all times. This auxiliary generator must be suitably isolated from the normal (commercial) and the site emergency source of primary power so that load transfer would not involve synchronization of frequency or phase and would not introduce switching transients. Start up of the liquified gas fueled generator should be automatically initiated within five minutes after loss of normal or emergency primary power. Liquified gas is preferred to gasoline for this engine generator system because of its more reliable starting characteristics.

The comparators and the selection logic used for input to or output from the A, B an C Bus of the redundant computer system are to be powered from the three backup battery systems using diode coupling so that failure of all three batteries and their associated power supplies would be required to disable this circuitry.

The backup batteries should be capable of being fully recharged within four hours after having furnished the complete power requirements of the CU for a period of fifteen minutes.

Location of the Central Computer Complex

It is anticipated that the location of the Central Computer Complex will be site specific. In all instances, however, the selected location should be secure and well protected and subject to the two man rule, i.e., no single individual, be it guard or repairman, should have access to the complex alone. A magazine located close to the SSCC should be considered as a likely candidate if there is not a suitable vault or strong room within the SSCC itself. Insofar as practical, the backup battery power supply and the liquified gas powered engine generator should also be located in a protected area where they would not be subject to easy disablement by man-portable weapons.

Guard Control Stations

There are two Guard Control Stations in the CSSMRS that provide the principal interface between the system and security personnel. One of the Guard Control Stations within the Site Security Control Center will be designated as the primary, while the other station, typically located in a surveillance tower, is designated a secondary station and serves as a backup to the primary station. All controls, indicators and displays are duplicated in the two Guard Control Stations and the guard at each location has the same capability to interact with the system.

Only one station and one operator is actually needed to operate and control the CSSMRS. The second station has been added to raise the reliability of the system, to provide an extra monitor of operations, extend the two-man rule to station activities, to increase the capability and effectiveness during times of unusually high activity by permitting task overflow to this second station, and to reduce vulnerability in the event of an attack and loss of a Guard Control Station.

CSSMRS components that are available to the guards at each station include a Digital Display Unit (CRT display of alphanumeric data), two CCTV monitors, a group of Function Switches, a key pad and thumbswitches for data entry and system control, status indicator lamps, audible alarms, a port for loading the electronic key, appropriate display labels, a digital date-time clock, a logging printer, television controls , an audio tape recording and playback system, a keyboard/display terminal and a map-like Geographical Display Unit. Their general arrangement is shown in Figures 13 and 14. These components are mostly peripherals that are attached to the input/output bus of a microprocessor that is in communication with the CU via a fiber optic digital data link and using the same speed and control procedures that are employed with the data links to the RUs. Here, however, a star configuration is employed between the CU and the two Guard Control Stations rather than the CROSSFIRE dual loop arrangement used with the RUs. Each station has its own power supplies and backup batteries with capacity to continue all operations for at least fifteen minutes after loss of primary power and with hook-up to the emergency gas powered generator system that supplies the CU as backup in the event that the standby site power is unable to restore service within five minutes after loss of power.

Each Guard Control Station is equipped with an operating console that houses the various displays and controls that the guards use to interact with the system, and a voice intercommunications facility is provided between the two stations to facilitate cooperative actions under emergency or peak load circumstances and to resolve any problems involving contention since neither station has preemptive rights over system controls.

Identical graphic display information and audible warning signals provide additional feedback and guidance to the two operating security personnel.

A duress alarm system is provided at each Guard Control Station and arranged so that if it is activated a silent signal will appear at the other Guard Control Station in the form of a message on the Digital Display Unit directing the guard to take action appropriate to that specific site. The method of activating this duress alarm is optional and may be any suitable form of concealed switch. In the case of personnel being placed under duress in the course of accessing a magazine, it is anticipated that this would be signalled by the use of cue-words in the telephone exchanges that they would make with the SSCC.

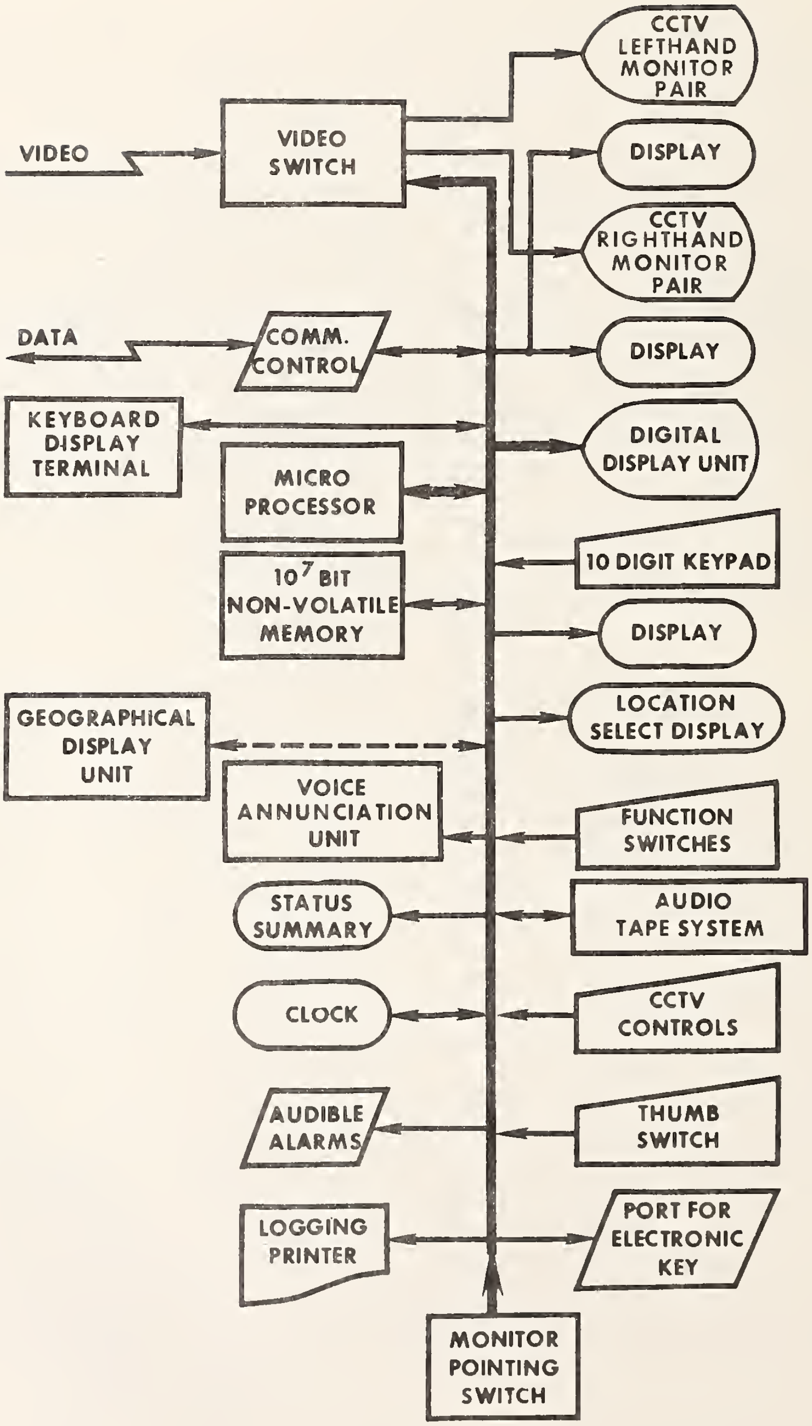


Figure 13 Block Diagram of Guard Control Station Configuration

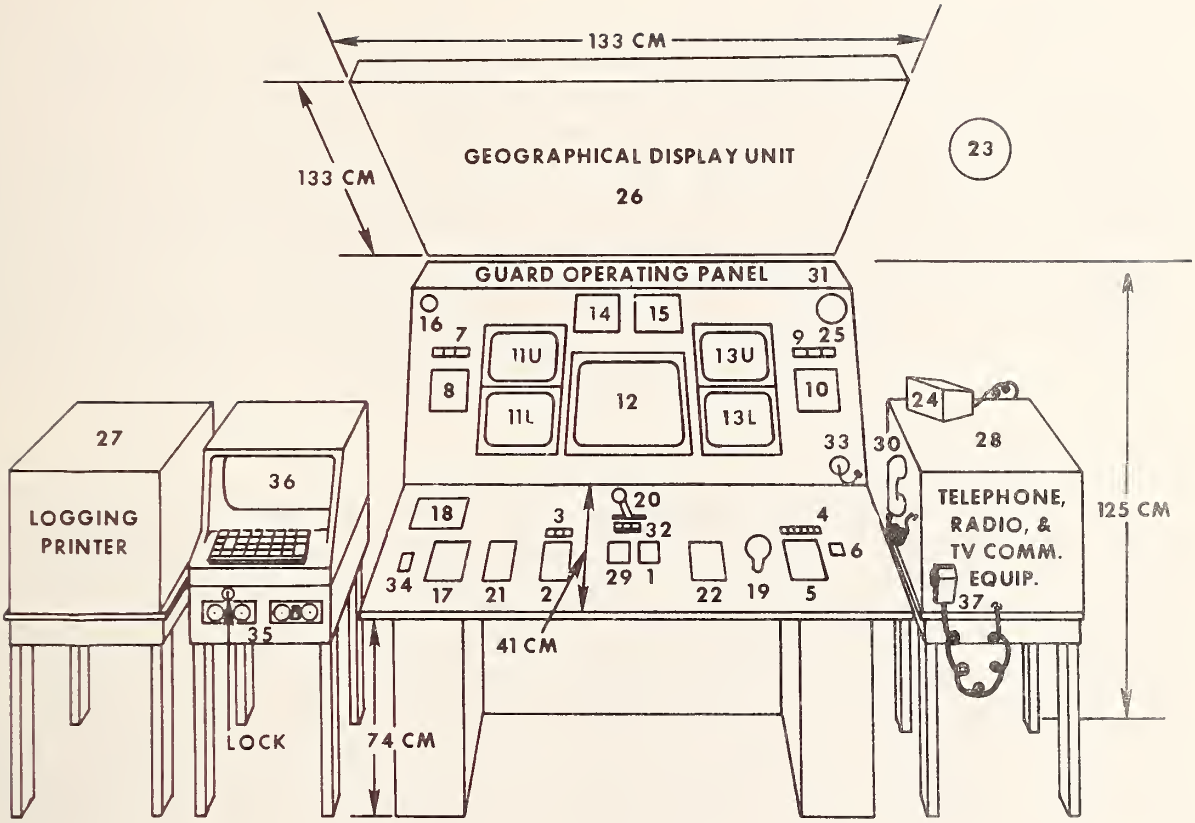


Figure 14 General Arrangement of Guard Control Station Components

In Fig. 14, the numbers associated with various components of the station are referenced in the descriptions that follow.

Guard Operating Panel (31)

The Guard Operating Panel (GOP) has been laid out with emphasis on Human Factors Engineering. Controls and indicators have been arranged in groups that conform with the natural sequence of operation to facilitate error-free operation by the guards. All surfaces are slanted to some extent and controls and indicators are sealed and recessed for protection against spilled liquids, harmful particles, accidental operation or inadvertent operator inflicted damage. All components should be selected for reliability, long life, ease of operation and physical sturdiness together with a minimum of moving mechanical parts.

Digital Display Unit (12)

The Digital Display Unit is central to the operator's console. It displays two types of information: dynamic, action events such as alarms and recommended response actions, and quasi-static status information such as equipment malfunctions, accesses in process, sites where CCTV and/or lights are on or locations where backup battery power is maintaining operation. The latter information is displayed continuously during normal, no-alarm conditions on a 30.5 cm (12 in.) diagonal screen cathode ray tube capable of displaying a 24- line by 80-character format. When an alarm occurs, this display is stored and is replaced by the alarm information displayed in large characters in a 16-line by 32-character format. The occurrence of an alarm is also signalled by a short audible tone which is followed, after acknowledgement of the alarm, by vocalization of the alarm information using a voice annunciation system. If the alarm has not been acknowledged within 15 seconds, another distinctive tone signal is emitted and the voice announcement is repeated. If another 15 seconds passes without acknowledgement, a high intensity alarm is sounded for 10 seconds and then the Response Forces are summoned and higher headquarters is alerted.

Alarm information remains on the Digital Display Unit until cleared. Clearing can occur as a result of assessment that discloses that the alarm resulted from some innocuous nuisance event followed by actuation of the "Secure" function switch, or clearing can follow from a guard patrol coping with an intruder and eventual restoration of secure conditions. Finally, clearing can also result from failure of the alarming sensor to pass a sensor test. The malfunctioning sensor is then listed on the quasi-active status file where it remains until it successfully passes a sensor test following maintenance action. This file is displayed continuously except when uncleared alarms are present.

Full information about only a single alarm at a time is presented on the display. When there is more than one alarm outstanding, data about the additional alarms is placed in an circular buffer, closed loop queue, and these data, together with the voice annunciation of the second and subsequent alarms, is presented to the guard(s) as they may be called up sequentially and independently at either of the two Guard Control Stations. Whenever there is more than one alarm outstanding, the display will carry the legend, "MORE ALARMS", and their location(s), in addition to the information about the alarm that is being displayed. Alarms may be called up in the sequence in which they were acknowledged by using the Monitor Pointing Switch, or may be called up in any sequence using the ten-digit key pad and Location Select function switch. The information to be presented about each alarm includes location, type of sensor, time of alarm onset, whether the alarm was momentary or is persisting and, where appropriate, suggested response actions.

Information that is presented in the status display (when there are no uncleared alarm conditions) includes the identification number of the guard(s) that are logged in, identification of any CSSMRS components that are judged to be malfunctioning as a result of failing self-test, identification of any CCTV cameras or camera lights that are on, or that have been determined to be malfunctioning, identification of any components that are operating on backup battery power, identification of electronic keys which have been issued for authorized access actions and the time remaining during which their use is valid, RUs that are in the access state, and finally, any unacknowledged routine instructions to security personnel such as patrol routing, sensor test request, etc.

CCTV Monitors (11,13)

On either side of the Digital Display Unit, a pair of CCTV monitors are mounted. These are 20 cm. (8 inch) nominal diagonal, black and white display tubes, and either monitor can be connected to any assessment camera on the site. Associated with each monitor there is an alphanumeric display that automatically indicates to which camera the monitor is connected and indicates what types of controls (pan, tilt, etc.), if any, are available at that camera. The camera location is identified by the identity or zone number of the RU associated with the camera, and the available controls are identified by display of appropriate label information.

Monitor Pointing Switch (20)

A Monitor Pointing Switch is provided on the console to facilitate the rapid switching of both camera controls and function switch controls from the location displayed by one monitor to that displayed by the other. This switch is arranged so as to provide unambiguous indication of the location and monitor to which the controls are attached. The principal use of this switch is to facilitate the rapid assessment of multiple alarms that may occur within a relatively short time interval. For example, assume that the site is secure, that the function switches have been disassociated with any RU by selecting the non-existent or null location designated "000", and that the Monitor Pointing Switch is directed toward the left-hand monitor, but that both monitors are dark. Then, an alarm occurs. The CCTV camera at the alarming RU is immediately selected. It and the lights are turned on and the scene is displayed on the right-hand monitor. If the RU is associated with a perimeter station both monitors in the right hand pair are activated and the scene from both of the perimeter segment cameras appears on the right hand monitor pair. If the alarm is from a magazine, only the lower monitor of the right hand pair is activated. An audible signal alerts the security personnel at the guard control stations. The site status information is removed from the Digital Display Units and replaced by summary alarm information ((location and type(s) of sensor)) together with a request for guard acknowledgement. Acknowledgement is accomplished by throwing the Monitor Pointing Switch to the right-hand monitor. This also attaches the control capabilities of the location dependent function switches to the RU at which the alarm has occurred and displays the identity of that RU on the Location Select Display, silences the audible alarm, enables the voice annunciation system to verbally annunciate the alarm at that Guard Control Station only, and releases any supplementary response instructions for display on the Digital Display Unit and removes the acknowledgement request from that display. At the secondary Guard Control Station, the CCTV scene from the alarming RU would appear on the unselected monitor pair and the summary alarm information would appear on the Digital Display Unit. Cessation of the audible alarm and removal of the acknowledgement request from the digital display would provide evidence that the alarm had been acknowledged at the primary station. The guard at the secondary station could optionally acknowledge also, and in this event, he would also receive the voice annunciation of the alarm and the supplementary digital response instructions on his display unit.

If, while assessment of this first alarm is in process at the primary station, a second alarm occurs, then the audible alarm is again started, the legend, "MORE ALARMS - ACKNOWLEDGE", and their location(s), appears on the Digital Display Unit, the light in the "Acknowledge" function switch begins to flash and the left-hand monitor displays the scene from the CCTV camera(s) at the location of this new alarm. The primary station guard now has optional courses of action. He can actuate the "Acknowledge" function switch immediately; this will silence the audible alarm and delete the "ACKNOWLEDGE" portion of the legend on the digital display and queue the alarm information for subsequent attention. This leaves his function switches and camera controls still connected to the site of the first alarm where that assessment may be continued. Alternatively, he can actuate his Monitor Pointing Switch to the left to acknowledge this new alarm as well as to release his controls and function switches from the right-hand monitor location and attach them to the location of this new alarm. If he felt that he could complete his assessment of the first alarm and clear it in a few more seconds after the second alarm sounded, he could elect to defer any acknowledgement actions on the expectation that the secondary guard station would acknowledge within the allowable time interval between 15 and 30 seconds after initiation. As a final option, he could use the voice intercommunications facilities to request that the secondary station guard handle the second alarm.

Audio Tape System (35)

A dual, cassette type audio tape system is provided to record all audible events including radio, telephone, intercom and guards comments that occur during alarm conditions. The tape recorder is to be turned on automatically when an alarm is acknowledged by the guard, and is to be turned off automatically after all alarms have been cleared and the time of day annunciation has been made. There are to be two cassette receptacles on the recorder. One is protected by a locked cover so that only the shift supervisor can install and remove cassettes. The other is accessible to the guard. Both receptacles are equipped with sensors that are arranged so that the insertion and removal of all cassettes is recorded on the logging printer. The same information is to be recorded on both tapes.

A separate audio playback unit is located conveniently to the keyboard/display terminal and is used by the guard to play back the tape that is accessible to him when he is preparing messages on the terminal regarding the disposition of alarms. During these intervals, the guard would install an alternate cassette in the recorder so as to be available in the event another alarm occurred.

Location Select Display (32)

This is a three-digit display that identifies the RU or zone to which the attachable function switches or controls are associated. Its value will be the same as the value shown on the three-digit display associated with the CCTV monitor that has been selected by the Monitor Pointing Switch.

Ten-Digit Key Pad (5)

The Ten-Digit Key Pad is used to enter numerical sequences into the CSSMRS. These sequences will always be associated with the use of one of the function switches and will represent either the identity number of guards logging on or off duty or else the identification number of a RU that is to be accessed or to which CCTV controls or addressable function switches are to be attached. A ten-digit display will always indicate the last number that has been entered into the system using the key pad. A CLEAR key will be provided on the key pad to facilitate the correction of erroneous entries.

Function Switches (1, 2, 6, 18, 21, 22, 29, 34)

There are 24 function switches on the Guard Control Station console. Eight of these might be considered global or not associable with a specific RU; two are selective and are only used with a limited subset of the other function switches; the rest are attachable, that is, the results of their actuation are directed to one specific RU at any given time.

Global Functions

The global function switches are:

ACKNOWLEDGE Used to acknowledge an alarm and place it in a queue. If no other alarms are outstanding, this will also attach function keys and CCTV controls to the alarming RU.

LOCATION SELECT Used with the Ten-Digit Key Pad to select an RU to which other function keys or CCTV controls are attached.

GUARD LOGIN Records the time and identity of a guard logging on duty.

GUARD LOGOUT Records the time and identity of a guard logging off duty.

TEST HQ LINKS Performs a test on the secure data links to higher headquarters.

TEST LAMPS Illuminates all indicator lamps to insure their operability.

SUMMON RESPONSES As indicated.

SUMMON AUGMENT Summons Augmentation Forces from higher headquarters upon actuation of the CONFIRM function switch.

Selective Function Switches

The selective function switches are:

CONFIRM
CANCEL — Both of these controls are used only in conjunction with the function switches used to fire FEDS or to summon Response or Augmentation Forces. Contention between Guard Control Stations in connection with the use of these controls is prohibited by system design.

Attachable Function Switches and Controls

The following are function switches that direct operations taking place at one or more specific RUs:

ACCESS — Used in conjunction with the Ten-Digit Key Pad to transmit the random number to a designated RU that has previously been loaded into a one-time use electronic key assigned for authorized access to that RU.

CODE KEY — Used to load an electronic key with a random code that is good for the time interval shown by the two-digit thumbswitches and is assigned to the RU designated by the number entered on the Ten-Digit Key Pad.

CODE MASTER KEY — Used to load a master electronic key with a random number that is valid for the time interval shown on the two-digit thumbswitches and that may be used at any RU to which this code is transmitted using the MASTER ACCESS function switch.

MASTER ACCESS — Used in conjunction with the Ten-Digit Key Pad to transmit a master electronic key code to a designated RU.

SECURE — Used in conjunction with the Ten-Digit Key Pad to terminate an access or to clear an alarm at a designated RU.

SAFE FEDS — Sets the designated electronic Safe/Arm switch to the "Safe" position.

ARM FEDS — Sets the designated electronic Safe/

Arm switch to the "Armed" or enabled position.

FIRE FEDS — Fires designated FEDS upon actuation of the CONFIRM function switch.

TV ON/OFF — The "On" function turns on both the CCTV camera and the lights (if these are required by the camera) at the designated location. The "Off" function turns off only the camera.

TV BAD/OK — Logs changes in the operational status of the designated CCTV on the Digital Display Unit and on the Logging Printer.

LIGHTS ON/OFF — Turns the lights on or off at the designated location.

TEST SENSORS — Initiates an automatic test of the sensors at the designated location.

TEST FEDS — Initiates an automatic test of the FEDS at the designated location.

SPARE — Undefined.

CCTV Controls (17, 19)

A multifunction joystick is provided in a convenient location for right-hand operation to facilitate issuance of pan, tilt and zoom control orders to a selected camera that is equipped with these features. Another control group for camera lens iris adjustment and focus are arranged for left-hand operation. Camera controls are attached to a specific camera by using the Monitor Pointing Switch, either alone (when acknowledging an alarm or cycling through a queue of uncleared alarms), or in conjunction with the key pad and "Location Select" function switch which provides complete freedom of choice.

Two-Digit Thumb Switch (3)

The Two-Digit Thumbswitch is used to set the time interval, in ten minute increments, during which an electronic key is valid. The display shows three digits, with the least significant digit permanently set to zero, so that the displayed value can be read directly in minutes. This value is loaded into the electronic key along with the random number key code and when the indicated time has expired the key code is erased.

Audible Alarms (16, 23)

Onset of an alarm condition is accompanied by an audible alarm signal that persists for 30 seconds or until the alarm condition is acknowledged, whichever occurs first. The audible alarm is to have an intensity of at least 60 dBA as measured from a position that is within two feet of the normal ear position of the security personnel that would man the Guard Control Station consoles. Fifteen seconds after initiation, there shall be a distinctive change in the nature of this alarm signal. Thirty seconds after its initiation, this signal is followed by a bell or horn producing a sound level of at least 90 dBA as measured anywhere within the Guard Control Stations and which persists for ten seconds unless terminated first by alarm acknowledgement. At the end of the ten second final warning period Response Forces are automatically summoned.

Voice Annunciation Unit (25)

Each Guard Control Station is equipped with a Voice Annunciation Unit that is used to verbally annunciate alarm messages and appropriate response recommendations. It is implemented in the CSSMRS to supplement the transfer of information from the DDU to the guards reducing their requirements for reading skills and training. The Voice Annunciation Unit is activated each time an uncleared alarm is selected using either the Monitor Pointing Switch to advance the alarms in an outstanding queue, or whenever the key pad and "Location Select" function switch are used to bring up a selected alarm. The Voice Annunciation Unit will be designed around a ten million bit, non-volatile memory that contains a digitized vocabulary of approximately 150 words in each of two languages, or five million bits if only a single language is required. This will provide for 100 seconds of speech at 50,000 bits-per- second. The digital representations of the words used to assemble an alarm message would be recalled from this memory and stored in a buffer from whence they would be used to drive a digital-to-analog converter to produce the verbal alarm annunciation. The speech would be output at a rate of approximately 90 words per minute which is a rate that is natural yet deliberate and easy to understand. Further, the speaker used to record the vocabulary that is digitized can be selected on the basis of articulation and understandability and could be a newscaster or other professional communicator.

In addition to vocalizing alarm information, the Voice Annunciation Unit will articulate the time-of-day immediately after any alarm condition is cleared. This will permit a time tag to be attached to each sequence of audible events that are recorded on the tape recorder during alarm conditions so as to facilitate their association with the proper alarm.

Status Summary Display (15)

This display is a group of five colored indicators' that provide a concise summary of overall site status. A green indicator is illuminated only when all RUs or zones are secure. A red indicator shows whenever there are any uncleared alarm conditions. A yellow indicator designates that some authorized access is in process on the site. A white indicator is illuminated when any CSSMRS component is functioning on backup battery power and an amber indicator is illuminated if a contention condition occurs in connection with system commands that might be issued by the personnel at the two Guard Control Stations. Such contention might occur, for instance, if both guards were to select the same CCTV camera and one were to try to pan right as the other tried to pan left. This sort of innocuous contention is resolved through verbal exchanges using the voice intercommunication facilities between the two stations. Contention is non-damaging through system design in connection with the use of the "Confirm" and "Cancel" function switches.

Clock (14)

The clock is a digital, 24-hour, time-of-day clock that provides the same time information that is recorded on the logging printer to a resolution of one minute.

Logging Printer (27)

The Logging Printer is used to provide a permanent record of all site security status changes. It records, together with the time, all of the data elements that appear on the Digital Display Unit except that recommended response messages may be referenced by their identity number rather than printing the full prerecorded text. The printer shall be capable of accepting and continuously printing input data at a speed of at least 2400 bits per second and shall produce a single copy record using a non-impact printing process. Identical entries are made on the logging printer at each of the Guard Control Stations so that two copies of the log are available; one of these would normally be reserved for the use of the supervisor. A non-impact printer is recommended for this application because of the increased reliability that is associated with mechanisms having fewer moving parts.

Port For Electronic Key (33)

This is simply a connector into which the electronic keys, either single-use or master keys, are inserted. It permits loading the random number key code and the time period for which this code is valid into the key.

Geographical Display Unit (26)

A Geographical Display Unit is provided at both the primary and secondary Guard Control Stations. It is a scaled, map-like representation of the site. It shows and identifies each RU and each perimeter segment, and each of these are provided with two colored indicators. There is a red indicator which flashes when any alarm condition is reported from that zone, and which changes to steady red when the alarm is acknowledged and is extinguished when the alarm is cleared. There is also a yellow indicator that is illuminated whenever an authorized access is in process. This display panel is normally mounted above the operators console.

Keyboard/Display Terminal (36)

A keyboard/display terminal shall be provided for the guard to use in an off-line mode to compose a message identifying the disposition of each alarm. The terminal shall be equipped with editing capabilities which will readily permit a guard that has only "hunt and peck" typing ability to compose, edit, change or correct text until he is satisfied with it. Then, using a suitable function key on the terminal, he will cause the text to be transferred to the logging printer where it will be permanently recorded. The terminal shall be arranged to provide appropriate cues to aid the guard in this task by asking for the disposition of alarms that are identified by their time of occurrence. These requests will appear on the display one at a time, and each will remain until such a time as the guard has an opportunity to respond.

In addition, this terminal shall be capable of being converted to an on-line mode of operation for use by system analysts or maintenance personnel. This conversion shall be under the control of a key-locked switch.

SYSTEM OPERATION

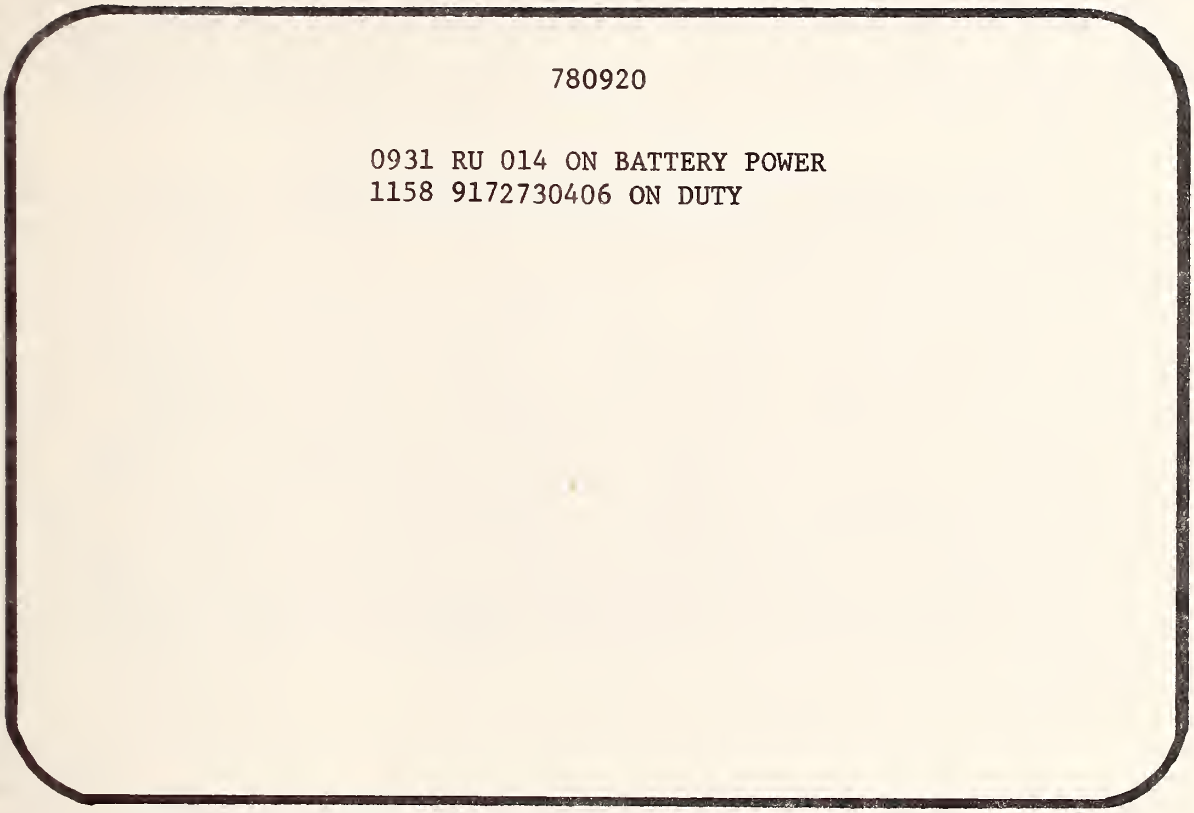
The detailed descriptions of the various CSSMRS subsystems and components that have been presented in the preceding sections of this report have, in general, also included a substantial amount of material that is descriptive of the system operation. In this section, that descriptive material will be expanded and amplified with particular emphasis on those aspects of the operation that are perceived by the guards or security personnel that must interface with the system.

Login/Logout

A guard is admitted to, say, the primary guard control station at a site for his scheduled tour of duty. He would typically greet the guard that he was relieving and would exchange verbal comments about the current site status and any unusual event that might have occurred during the shift that was ending. Assuming that no uncleared alarms exist, the Digital Display Unit would show the personal identity number of the guard that was about to be relieved together with the time that he logged on duty. By using a digital personal identity number rather than a name, the preparation of another module of site specific software can be avoided. The display unit also lists any malfunctioning sensors, FEDS, CCTVs, RUs or digital data links and the time at which their failure was discovered. Also listed are any system components that are operating under backup power, and CCTV cameras and associated lights that are on, and any RUs that are in an access condition. These same items have also been permanently recorded by the logging printer as they occurred.

The guard that is going on duty enters his personal identity number using the Ten-Digit Key Pad. He verifies that he has done so correctly by examining the ten-digit display that shows the last number entered. If it is not correct, he clears the entry and its display using a "Clear" key on the pad, and reenters the correct number. When he is satisfied that it is correct, he pushes the momentary action "Login" Function Switch. The time, his personal identity number and the words "ON DUTY" appear on the Digital Display Unit and are recorded by the logging printer.

In a similar manner, the guard that is being relieved enters his personal identity number and actuates the "Logout" Function Switch. His "ON DUTY", time and identity number are erased from the screen of the Digital Display Unit and his logout is recorded by the logging printer. Assuming that one RU was on battery power, the information on the Digital Display Unit is now as shown in Figure 15.



```
               780920

     0931 RU 014 ON BATTERY POWER
     1158 9172730406 ON DUTY
```

Figure 15 Digital Display After Login

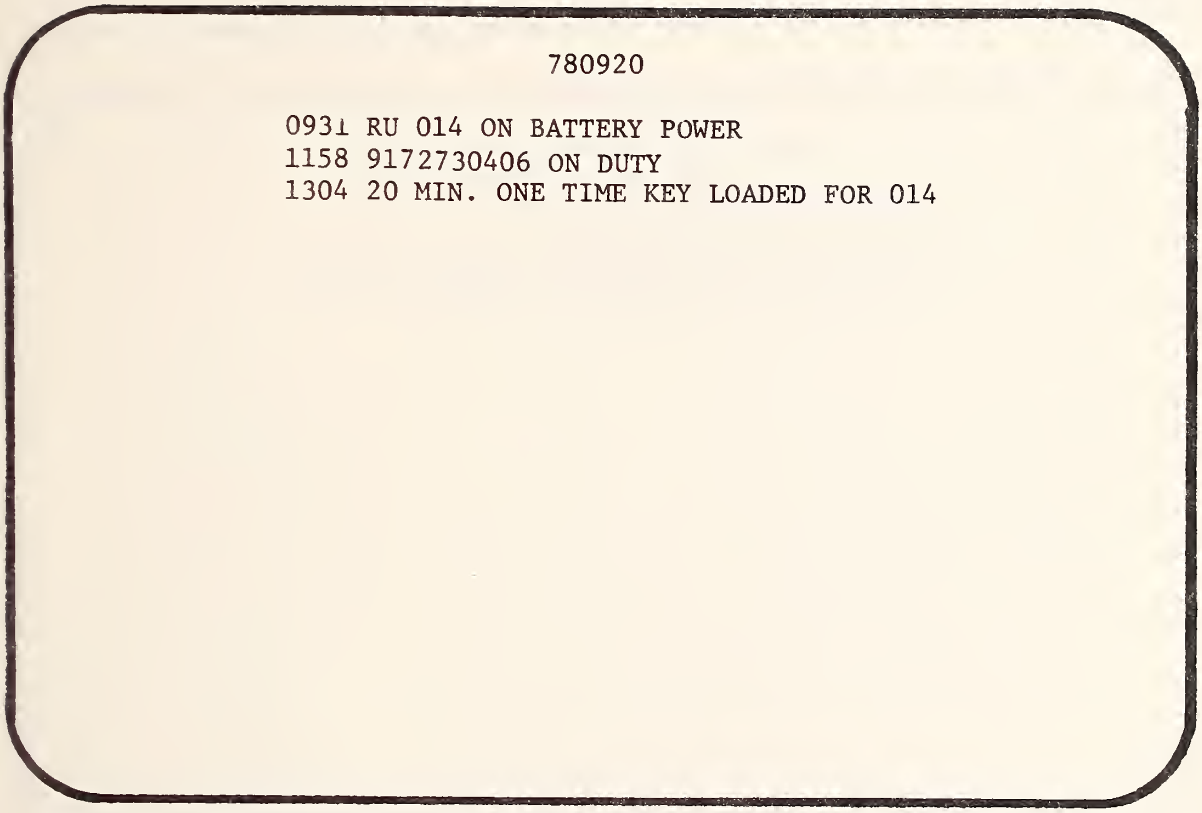
In this display, 780920 represents two digits each for year, month, and day, respectively. 0931 is the time that RU 014 reported that it had gone on battery power and 1158 is the time that the guard having personal identity number 9172730406 logged on duty. (For clarity, the identity of the second guard is not shown in this illustration.)

Access

One of the listings on the Digital Display Unit at the "changing of the guard" described above is the indication that RU 014 is functioning on backup battery power. In the verbal exchange between the guards, it was noted that maintenance action had been requested immediately after the condition had been automatically reported by the CSSMRS and acknowledged by the guard. There are green and white lights on in the Summary Status Display.

Now the maintenance personnel arrive and present themselves to the Security Officer who issues them an electronic key and authorizes the guard on duty to load it for access to RU 014 with a valid time window of 20 minutes. A key to the mechanical security padlock on the door at RU 014 is issued to the guard patrol that will accompany the maintenance personnel to their destination.

The guard on duty at the primary guard control station inserts the electronic key in the key port. He sets the Two Digit Code Lifetime Thumbswitches to 02. (A third digit is fixed at zero, so the actual reading of the switches is 020, the desired value in minutes). He enters the value 014 on the Ten-Digit Key Pad and confirms that it was correctly entered by examining the ten-digit display of the last value entered. Satisfied that it has been correctly entered, he actuates the Code Key Function Switch. The central computer generates a random eight bit number that is loaded into the electronic key and is also stored in a register for later transmission to RU 014. Successful loading of the electronic key is signaled by the illumination of an indicator on the key that will stay on for 20 minutes (the code lifetime) or until the key is used, whichever occurs first. A new entry appears on the Digital Display Unit as shown in Figure 16.



```
                    780920

        0931 RU 014 ON BATTERY POWER
        1158 9172730406 ON DUTY
        1304 20 MIN. ONE TIME KEY LOADED FOR 014
```

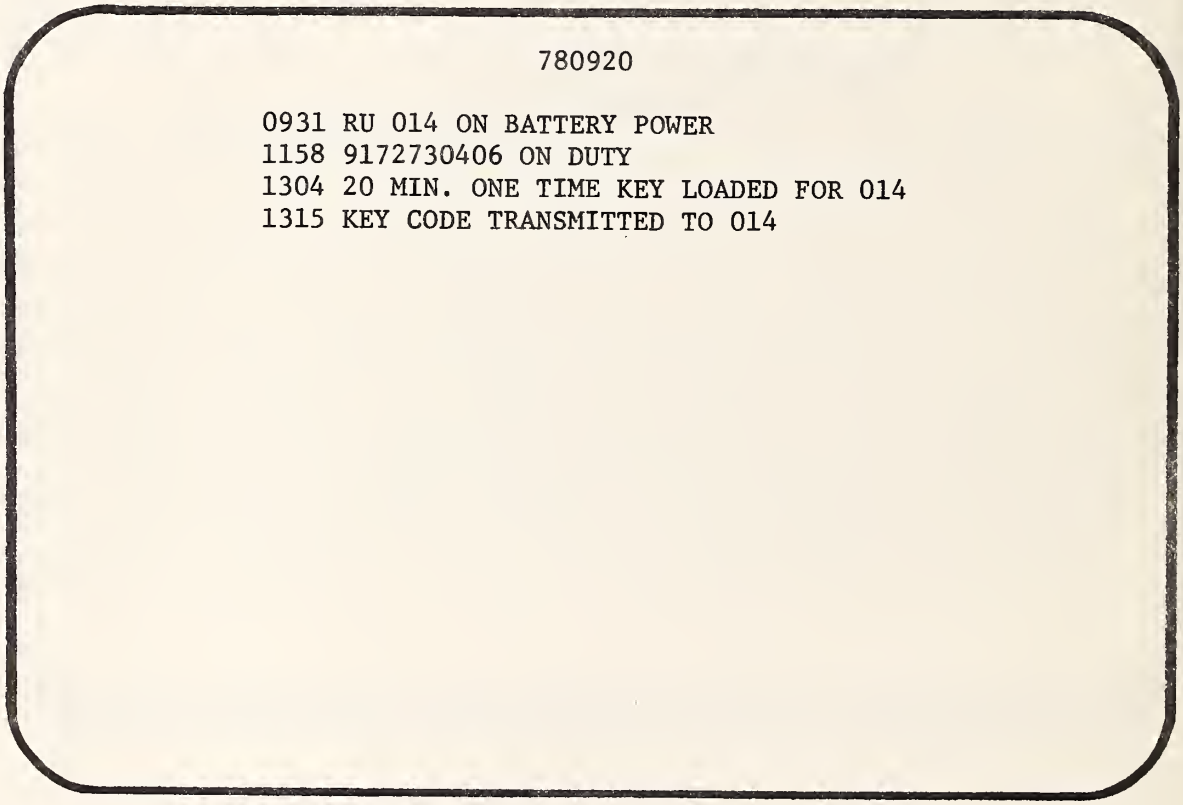
Figure 16 Digital Display Loading Key

The 1304 entry also appears on the logging printer.

In the event that the key loaded indicator had not come on (signaling that the key had been loaded), it would have been necessary to obtain a replacement key from the Security Officer and to repeat the loading process. This would have resulted in the generation of a new random number that would replace the one previously stored in the key register for later transmission to RU 014.

The maintenance personnel with their guard patrol escort proceed to RU 014 and upon arrival telephone back to the control station and notify the guard there that they are ready to enter. The guard then enters 014 on the Ten-Digit Key Pad, confirms that it is correct using the ten-digit display, and actuates the Location Select Function Switch followed by the Access Function Switch, and tells the maintenance personnel to go on in. The Location Select Display shows the number 014 and a yellow indicator at the position of RU 014 begins flashing on the Geographical

Display Unit, and the Digital Display Unit appears as shown in Figure 17.



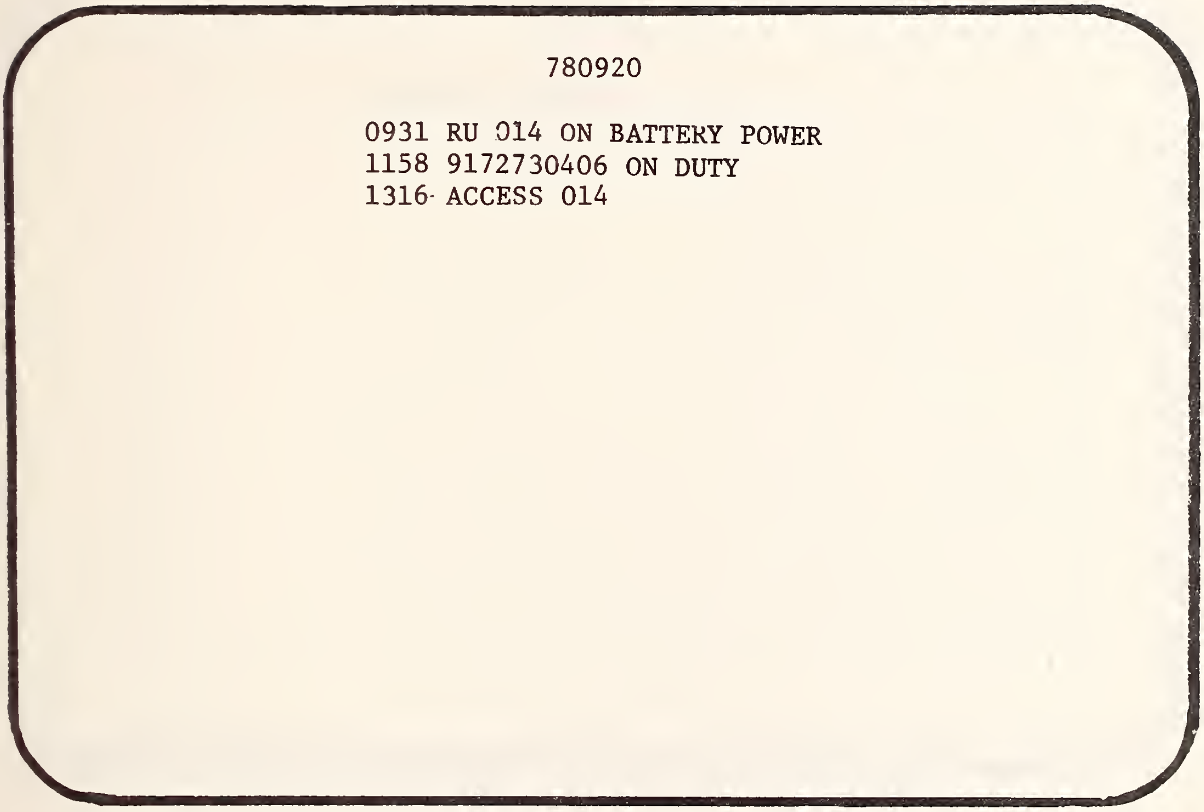
```
                    780920

       0931 RU 014 ON BATTERY POWER
       1158 9172730406 ON DUTY
       1304 20 MIN. ONE TIME KEY LOADED FOR 014
       1315 KEY CODE TRANSMITTED TO 014
```

Figure 17 Digital Display After Transmission of Key

The 1315 entry is also recorded on the logging printer.

A few seconds later, the maintenance personnel plug the electronic key into it's port at RU 014, the codes match and the solenoid operated bolt is withdrawn from its strike and the door can be opened. Back at the primary guard control station, the flashing light on the Geographical Display Panel goes to a steady state of illumination. The yellow access indicator in the Status Summary Display Group goes on and the green indicator goes off. (This, as well as the information on the digital displays, appears at both guard control stations). The Digital Display Unit appears as shown in Figure 18 and the 1316 entry is recorded on the logging printer.

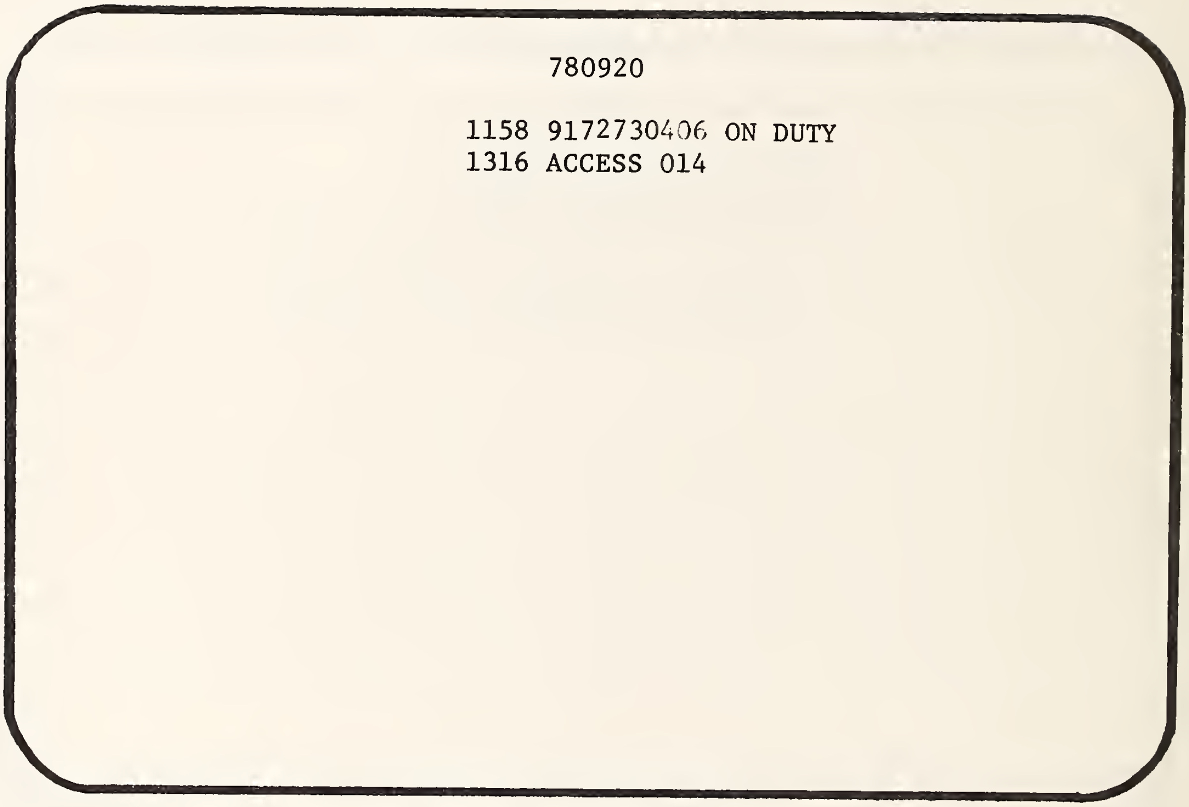


```
                    780920

0931 RU 014 ON BATTERY POWER
1158 9172730406 ON DUTY
1316 ACCESS 014
```

Figure 18 Digital Display After Access

After a half hour or so of work, the maintenance personnel correct the equipment malfunction at RU 014. At this time the white light in the Summary Status Display is extinguished and the Digital Display Unit appears as in Figure 19. The entry, "1350 POWER RESTORED RU 014", is recorded on the logging printer.

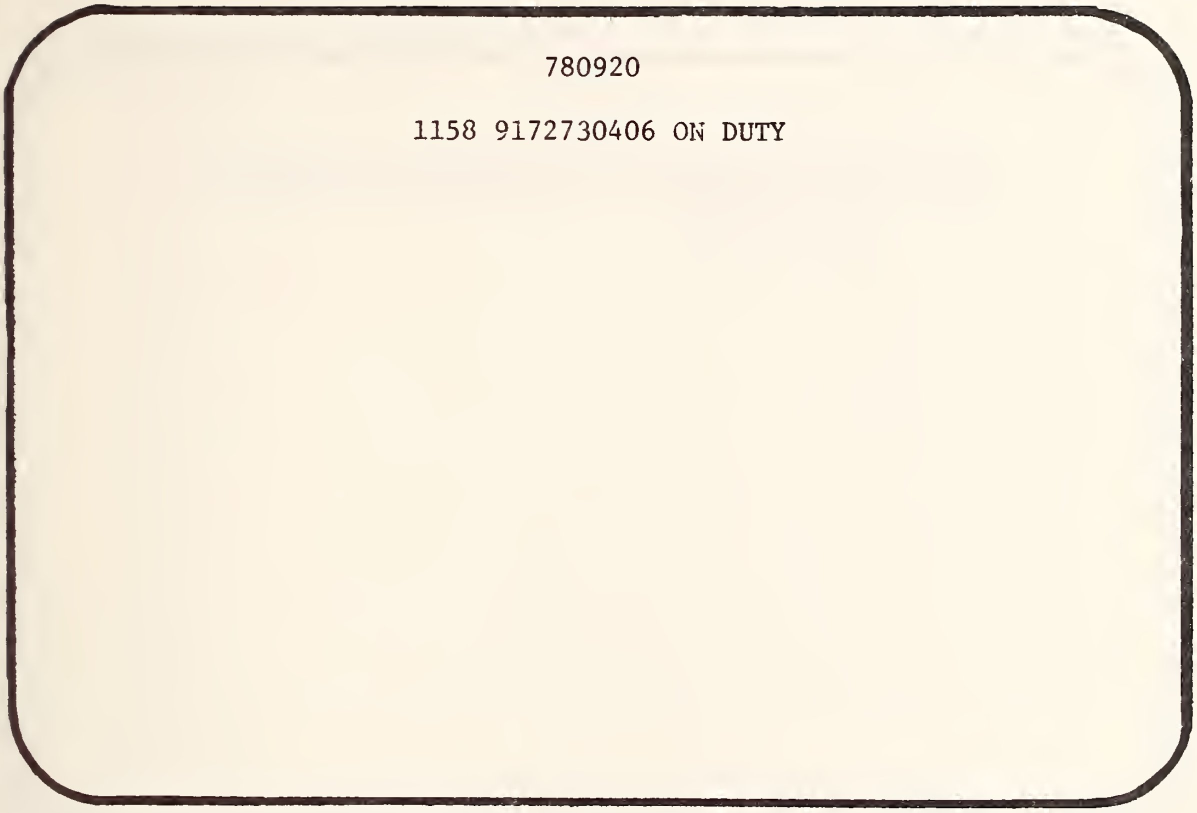


```
                780920

           1158 9172730406 ON DUTY
           1316 ACCESS 014
```

Figure 19 Digital Display After Power Restored

The maintenance personnel and their escort now exit RU 014, closing and locking the door, and telephoning the guard to advise him that RU 014 can now be secured. The guard confirms that 014 still appears in the Location Select Display (if it did not, he would enter it using the Ten-Digit Key Pad and the Location Select function switch) and actuates the Secure function switch. The yellow indicator on the Geographical Display Panel is extinguished and the yellow indicator on the Status Summary Display is replaced by green. The entry, "1358 SITE SECURE", is recorded on the logging printer and the digital display shown in Figure 20 appears.



780920

1158 9172730406 ON DUTY

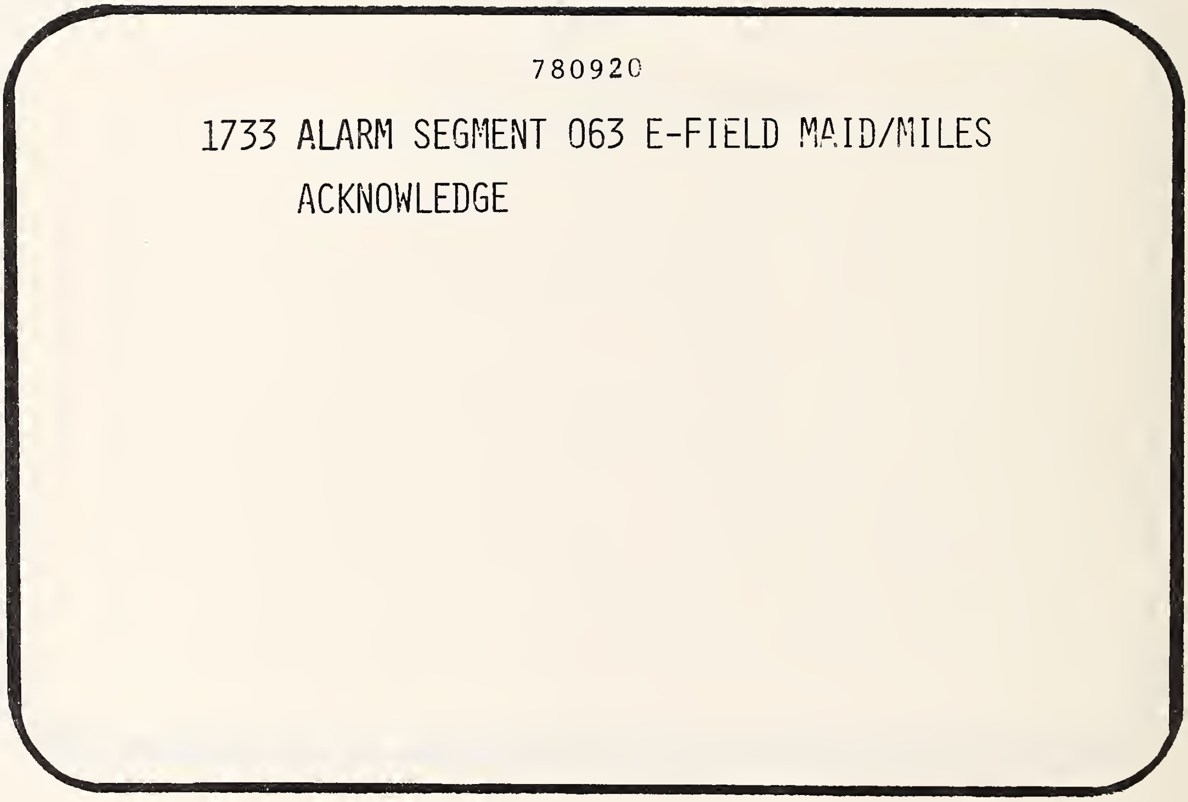
Figure 20 Digital Display, Site Secure, Fully Operational

Alarms

At 1733 on the same date as the preceding description, a deer jumps over the outer perimeter fence of RU (segment) 063 and almost immediately produces alarms in E-Field and MAID/MILES sensors protecting that segment.

At the primary Guard Control Station, a flashing red light appears on the Geographical Display Panel at the position corresponding to segment 063.

At both stations, an audible alarm comes on, the Status Summary Display indicator changes from green to red, the outputs from the CCTV cameras covering perimeter segment 063 appear on the screens of the monitor pair that have not been selected by the Monitor Pointing Switch, and the digital display is as shown in Figure 21. The same entry is recorded on the logging printer. The Acknowledge Function Switch lamp is flashing on and off.



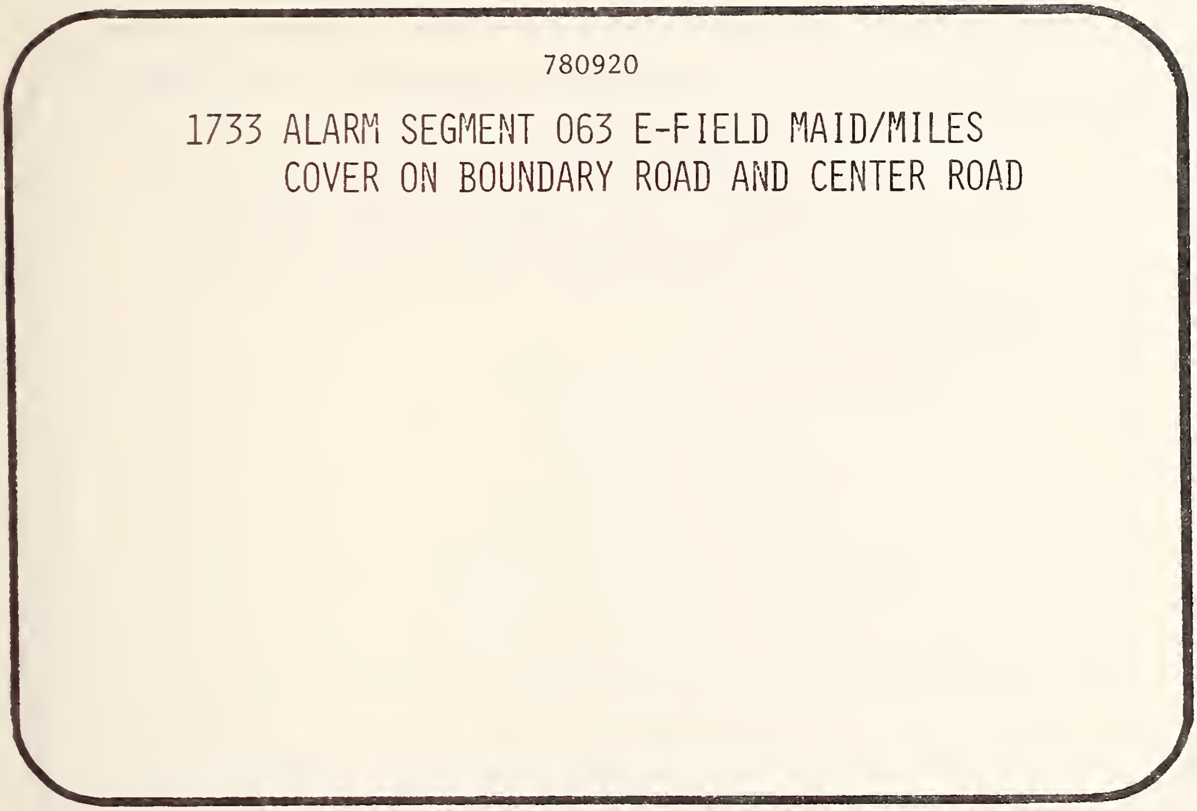
780920

1733 ALARM SEGMENT 063 E-FIELD MAID/MILES

ACKNOWLEDGE

Figure 21 Digital Display When Alarm Occurs

The guard at the primary station operates his Monitor Pointing Switch to select the monitor pair that is displaying the segment 063 scenes. The audible alarm is silenced and the flashing light in the Acknowledge switch is extinguished. The indicator associated with the selected monitor pair displays "063" and "NO CONTROLS". The digital display changes to that shown in Figure 22 and the voice annunciating system announces, "Alarm, segment zero six three, E-Field, MAID/MILES, cover on Boundary Road and Center Road". The flashing red lamp on the Geographical Display Panel is now on steady at segment 063. No new entries are recorded by the logging printer.



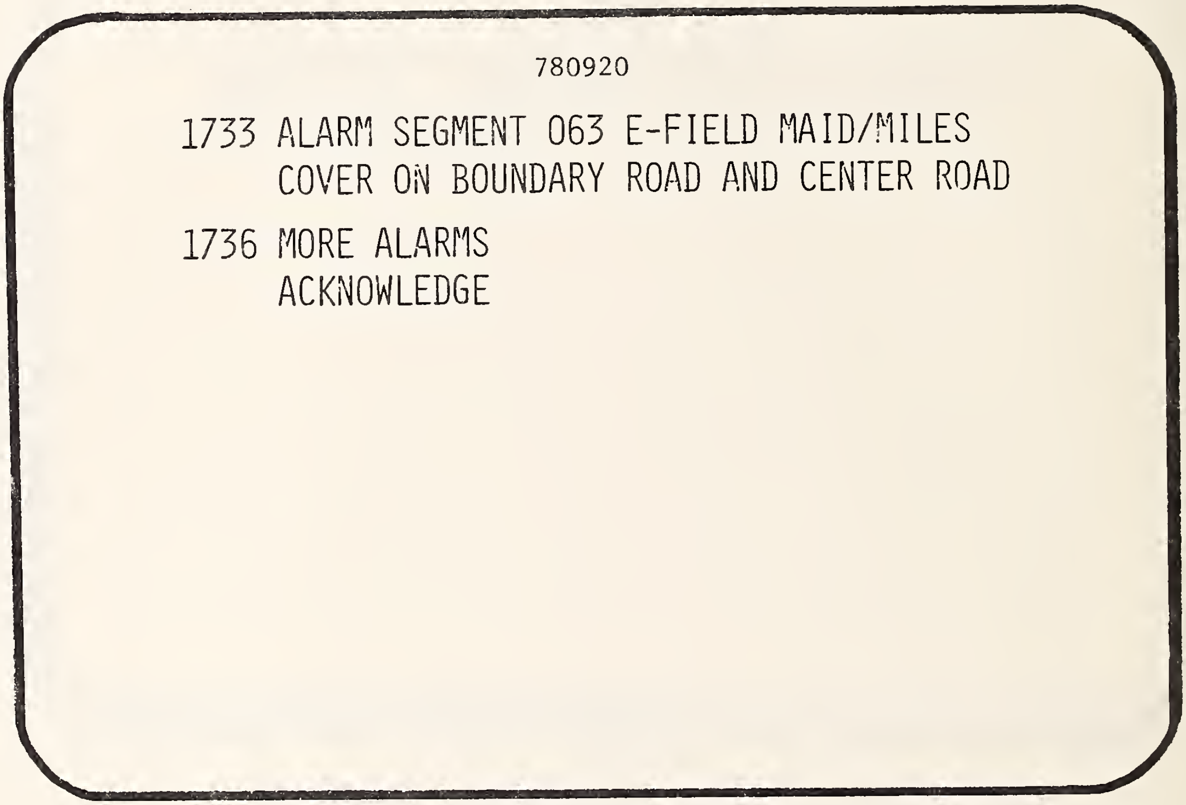
```
                    780920
   1733 ALARM SEGMENT 063 E-FIELD MAID/MILES
        COVER ON BOUNDARY ROAD AND CENTER ROAD
```

Figure 22 Digital Display After Alarm Acknowledgement

When the alarm condition occurred and the CCTV assessment cameras were automatically patched in to the monitors at the Guard Control Stations, the deer that caused the alarm was immediately seen and identified. The guard at the primary station then advised two of his roving patrols by radio that there was a deer in segment 063 and directed one of them to approach the segment via Center Road and the other to approach via Boundary Road and see if they could drive it back over the fence and out of the site. As they converged on the target sector, the deer moved into sector 064 alarming the E-Field Sensor there before finally jumping the outer fence and leaving.

When the E-Field sensor at segment 064 was alarmed, the audible warning signal and flashing "Acknowledge" switch indicator lamp was reactivated at both Guard Control Stations, and a flashing red indicator was illuminated at sector 064 on the Geographical Display Panel at the primary station. The Digital Display Unit carried the messages shown in Figure 23. The logging printer recorded the following entry, "1736 ALARM SEGMENT

064 E-FIELD".

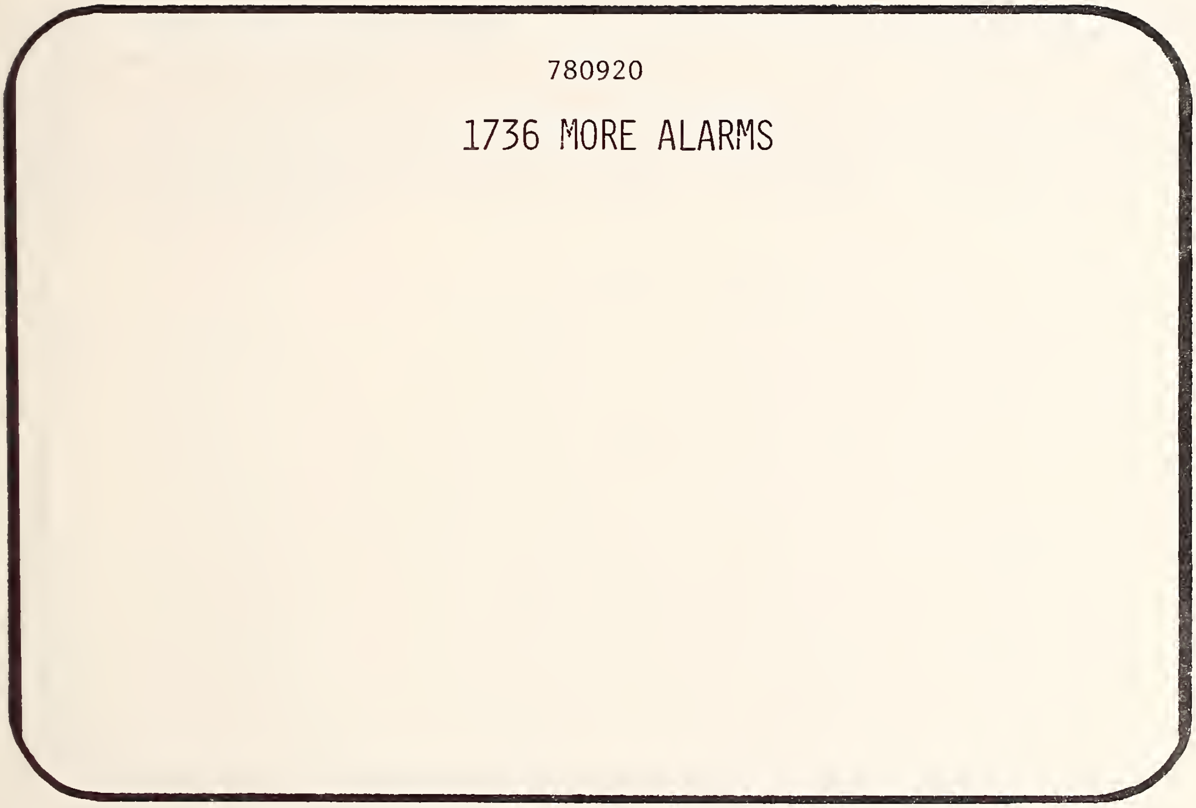


```
                    780920
1733 ALARM SEGMENT 063 E-FIELD MAID/MILES
     COVER ON BOUNDARY ROAD AND CENTER ROAD
1736 MORE ALARMS
     ACKNOWLEDGE
```

Figure 23 Digital Display After Second Alarm

This time, since the guard at the primary station had seen the deer moving toward segment 064, and it was again visible in the other monitor pair which was enabled when the alarm occurred, acknowledgement was made by actuating the Acknowledge Function Switch. This silences the audible alarm and changes the flashing light at segment 064 on the Geographical Display Unit to steady red and removes the "ACKNOWLEDGE" entry from the screen of the Digital Display Unit.

When the guard observes the deer finally jump over the fence, he actuates the Secure and TV OFF Function Switches. Since his controls are attached to RU 063 by the Monitor Pointing Switch, and since the alarm causing conditions now no longer exist in that segment, the red light on the Geographical Display Panel that is associated with segment 063 is extinguished by the "Secure" command and the CCTV cameras at 063 are turned off. The logging printer record the following entry, "1737 SEGMENT 063 SECURE", and the digital display shows the entry "1736 MORE ALARMS". The Digital Display Unit appears as shown in Figure 24.

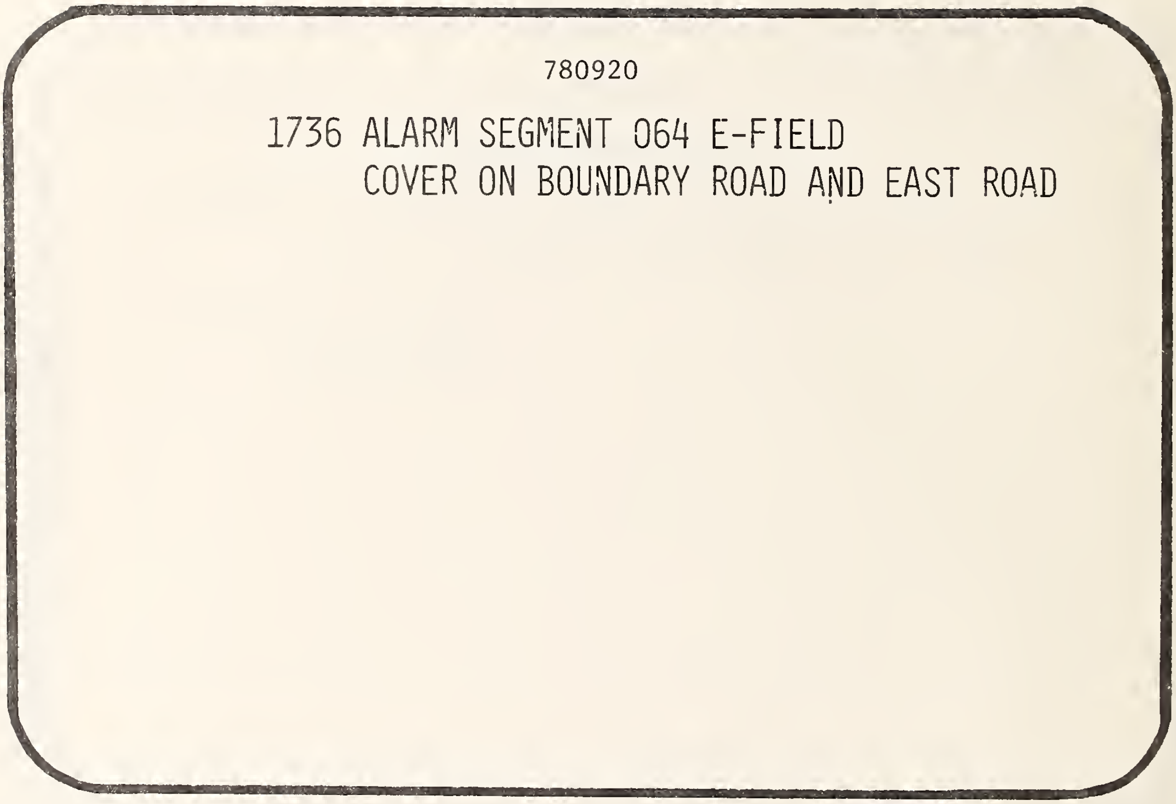


780920

1736 MORE ALARMS

Figure 24 Digital Display With More Alarms

The guard then actuates his Monitor Pointing Switch to the alternate position, attaching his controls to RU 064 and bringing that alarm out of the queue. The number 064 replaces 063 in the Location Select Display. The digital display immediately carries the message shown in Figure 25 and this same message is annunciated by the voice system.



```
                780920
   1736 ALARM SEGMENT 064 E-FIELD
        COVER ON BOUNDARY ROAD AND EAST ROAD
```

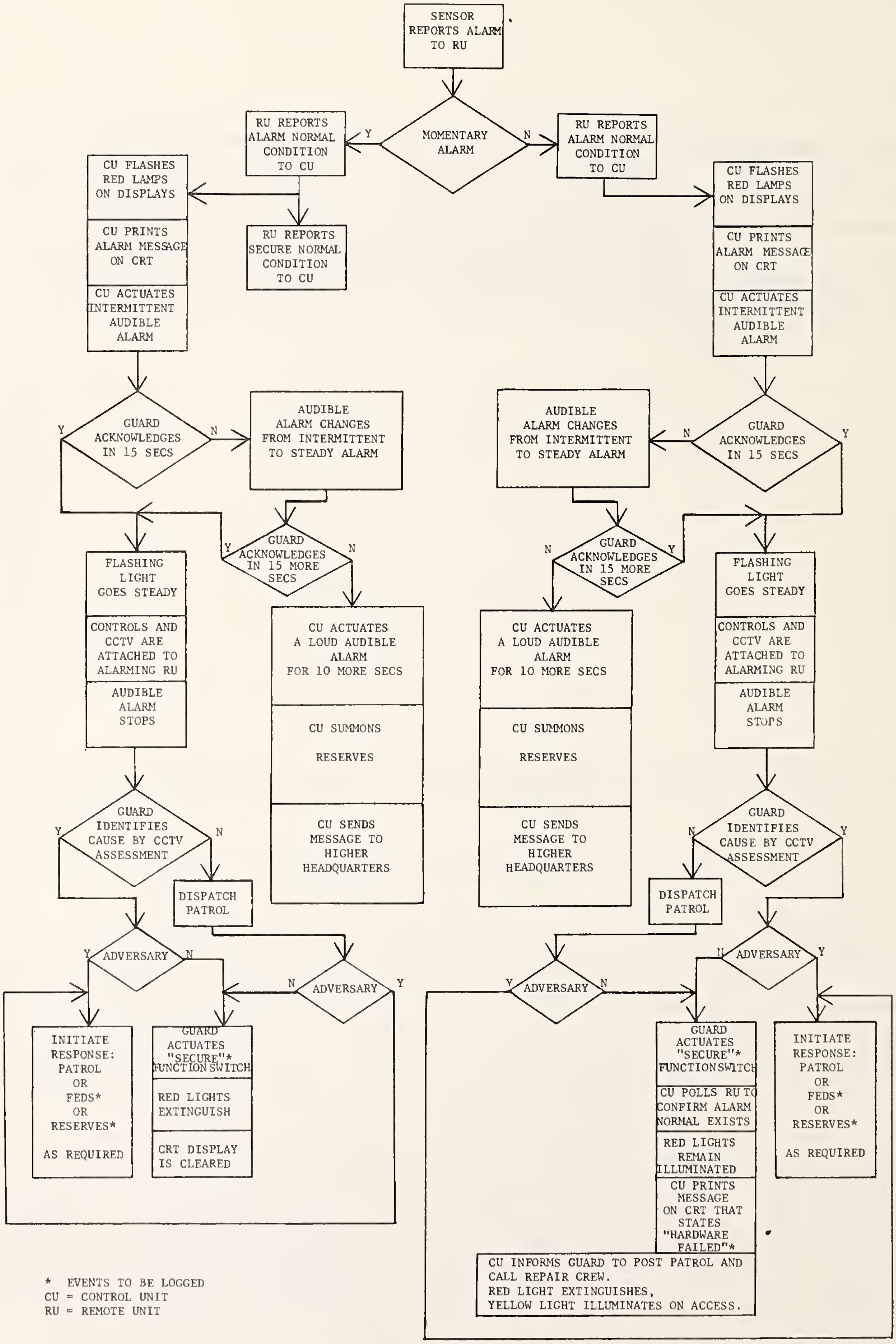
Figure 25 Display of Second Alarm Details

The guard now actuates the Secure Function Switch. The remaining red light on the Geographical Display Panel is extinguished and the red indicator on the Summary Status Indicator is replaced by green. The digital display reverts to that shown in Figure 20 and on the logging printer the entry, "1738 SITE SECURE", is recorded. He actuates the TV OFF Function Switch and the cameras are turned off and the monitor pair goes blank.

There is no way that the disposition of alarms such as the ones described above can be recorded automatically. The off line terminal would be used for the composition of appropriate comments regarding the disposition of alarms. When the guard completes the composition of the required information, he actuates the "Log" function switch on this terminal and the contents of the screen are transferred to the logging printer where they are recorded and the screen is cleared.

As a further illustration of the interactions between the security forces at a site and the CSSMRS, the flow diagrams shown in Figure 26 depicts the principal alternatives in the response to an alarm.

It should be noted that all alarms except those that might have been screened out by the Environmental Correlation Module are accepted by the CU as actual alarms. Momentary alarms are assessed, recorded, resolved and secured with the same diligence that is applied to continuing alarms. The supression of continuing alarms that result from sensor malfunction is accomplished through failure of the sensor to properly respond to the sensor test command.


SENSOR REPORTS ALARM TO RU
MOMENTARY ALARM
Y
N
RU REPORTS ALARM NORMAL CONDITION TO CU
RU REPORTS SECURE NORMAL CONDITION TO CU
RU REPORTS ALARM NORMAL CONDITION TO CU
CU FLASHES RED LAMPS ON DISPLAYS
CU PRINTS ALARM MESSAGE ON CRT
CU ACTUATES INTERMITTENT AUDIBLE ALARM
CU FLASHES RED LAMPS ON DISPLAYS
CU PRINTS ALARM MESSAGE ON CRT
CU ACTUATES INTERMITTENT AUDIBLE ALARM
GUARD ACKNOWLEDGES IN 15 SECS
Y
N
AUDIBLE ALARM CHANGES FROM INTERMITTENT TO STEADY ALARM
AUDIBLE ALARM CHANGES FROM INTERMITTENT TO STEADY ALARM
N
GUARD ACKNOWLEDGES IN 15 SECS
Y
GUARD ACKNOWLEDGES IN 15 MORE SECS
Y
N
N
GUARD ACKNOWLEDGES IN 15 MORE SECS
Y
FLASHING LIGHT GOES STEADY
CONTROLS AND CCTV ARE ATTACHED TO ALARMING RU
AUDIBLE ALARM STOPS
CU ACTUATES A LOUD AUDIBLE ALARM FOR 10 MORE SECS
CU SUMMONS RESERVES
CU SENDS MESSAGE TO HIGHER HEADQUARTERS
CU ACTUATES A LOUD AUDIBLE ALARM FOR 10 MORE SECS
CU SUMMONS RESERVES
CU SENDS MESSAGE TO HIGHER HEADQUARTERS
FLASHING LIGHT GOES STEADY
CONTROLS AND CCTV ARE ATTACHED TO ALARMING RU
AUDIBLE ALARM STOPS
GUARD IDENTIFIES CAUSE BY CCTV ASSESSMENT
Y
N
DISPATCH PATROL
DISPATCH PATROL
N
GUARD IDENTIFIES CAUSE BY CCTV ASSESSMENT
Y
Y
ADVERSARY
N
N
ADVERSARY
Y
Y
ADVERSARY
N
N
ADVERSARY
Y
INITIATE RESPONSE: PATROL OR FEDS* OR RESERVES* AS REQUIRED
GUARD ACTUATES "SECURE"* FUNCTION SWITCH
RED LIGHTS EXTINGUISH
CRT DISPLAY IS CLEARED
GUARD ACTUATES "SECURE"* FUNCTION SWITCH
CU POLLS RU TO CONFIRM ALARM NORMAL EXISTS
RED LIGHTS REMAIN ILLUMINATED
CU PRINTS MESSAGE ON CRT THAT STATES "HARDWARE FAILED"*
CU INFORMS GUARD TO POST PATROL AND CALL REPAIR CREW.
RED LIGHT EXTINGUISHES,
YELLOW LIGHT ILLUMINATES ON ACCESS.
INITIATE RESPONSE: PATROL OR FEDS* OR RESERVES* AS REQUIRED

* EVENTS TO BE LOGGED
CU = CONTROL UNIT
RU = REMOTE UNIT

Figure 26 Flow Diagram of Alarm Response

LIST OF ACRONYMS

ADCCP	Advanced Data Communication Control Procedures
ASCII	American Standard Code for Information Interchange
CATV	Community Antenna Television
CCLW	Crossfire Communications Loss Word
CCTV	Closed Circuit Television
CCW	Counterclockwise
CLW	Communications Loss Word
CM	Communications Microprocessor
CMOS	Complimentary Metal Oxide Semiconductor
CPU	Central Processing Unit
CSSMRS	Computerized Site Security Monitor and Response System
CU	Central Unit
CW	Clockwise
DDU	Digital Display Unit
DMA	Direct Memory Access
DPENA	Data Port Enable
FCS	Frame Check Sequence
FDS	Fence Disturbance Sensor
FEDS	Forced Entry Deterrent Systems
FIFO	First In - First Out
GCS	Guard Control Station
GDU	Geographical Display Unit
GOP	Guard Operating Panel
GOPI	Guard Operating Panel Indicator
HQ	Headquarters
I/O	Input/Output
LSI	Large Scale Integration
MSG	Message
OS	Operating System
PPW	Poll Period Word
RAM	Random Access Memory
RDA	Receiver Data Available
ROM	Read Only Memory
RSA	Receiver Status Available
RU	Remote Unit
TBMT	Transmitter Buffer Empty
TEOM	Transmit End of Message
TSA	Transmitter Status Available
TV	Television
USYNRT	Universal Synchronous Receiver/Transmitter

REFERENCES

Barnoski, M. K., Data Distribution Using Fiber Optics, Applied Optics, Vol.14, No.11, November 1975.

Beaudry, M. D., Performance-Related Reliability Measures for Computer Systems, IEEE Transactions on Computers, Vol. C-27, No.6, June 1978.

Moore, R. T., et al, Computer Site Security Monitor and Response System, NBSIR 77-1262, June 1, 1977.

Rawson, E. G., et al, Fibernet: Multimode Optical Fibers for Local Computer Networks, IEEE Transactions on Communications, Vol. COM-26, No.7, July 1978.

Sheridan, C. T., Space Shuttle Software, Datamation, July 1978

APPENDIX 1

Notes on ADCCP Communications Interfaces

A universal synchronous receiver/transmitter (USYNRT) on one LSI chip has been used to implement a data link between two microprocessors that uses the ADCCP protocol. The chip is a multi-protocol device, capable of handling several popular bit-oriented and byte-oriented protocols. Since the ADCCP protocol has been selected for this application it will be the only one discussed here.

The primary function of the USYNRT is to take parallel data (bytes) from the computer and present it in serial form to the communications line along with beginning and end of frame flags and error check (CRC) code. Conversely, when receiving data from the serial line it must be able to detect frame flags, do error checking and present the message to the computer in byte form.

The chip contains seven 8-bit registers: receiver data, receiver status, transmitter data, transmitter status & control, secondary address, mode control, and data length select. Data transfer between registers and computer is in parallel over a bidirectional bus. Registers are selected by the state of three address lines; another control line determines bus direction.

Other control lines of interest are:

RDA	Receiver Data Available
RSA	Receiver Status Available
TBMT	Transmitter Buffer Empty
TSA	Transmiter Status Available
DPENA	Data Port Enable

DPENA is an input which must be asserted for every data transfer between computer and chip. The other lines listed above are outputs which indicate the status of major registers. RDA is asserted when a character has been received and transferred into the data register. RSA is asserted when the last byte of a message has been received or in the event of receiver error. TBMT is at a high level when either the transmit data buffer or control register is ready to accept new data. TSA is asserted to indicate a transmitter underflow conditon.

When functioning as a transmitter the chip puts the beginning-of-frame flag on the serial line then serializes the address, control, and information bytes as they are transferred from the computer. Transmission is completely transparent, i.e., no code combinations are forbidden. To avoid confusion between data and flags, automatic "bit stuffing" takes place on a byte that has more than five adjacent ones. (A flag is 01111110). The extra zero bits inserted by the bit stuffing are automatically stripped at the receiver end. After the computer has sent the last byte it must set the Transmit End of Message (TEOM) bit in the control register. The chip then sends a 16-bit CRC down the line followed by the end-of-frame flag. After the flag the line goes idle if TEOM is cleared; if not cleared the chip sends continuous flags.

When functioning as a receiver the chip monitors the serial input line and searches for a beginning-of-frame flag. When the first non-flag byte has arrived and is transferred to the data buffer the RDA control line is asserted. The computer must read the contents of the buffer; failure to do so before the next byte arrives results in an overrun condition. An overrun will cause the assertion of RSA. RSA is also asserted after the final flag to indicate end of message. At this time the computer must read the receiver status register to ascertain whether or not the frame was received without error. This fact is indicated by a single bit in the status register; the CRC code itself is not presented to the computer.

The USYNRT may be set to Secondary Address Mode by writing a bit into the mode control register and by writing the station address into the secondary address register. Now the RDA line will not be asserted until a message is received with an address field that matches the station address; all other frames will be ignored.

Interface to a microprocessor

Since the USYNRT contains several registers plus a number of control lines that must be interfaced it is treated not as one device but as 13 devices for programming purposes. However, the microprocessor architecture allows for direct selection of only 7 input and 7 output devices. More devices can be addressed by building a multi-level system in which one I/O intruction selects a device selector, etc. Rather than construct such a complex system all the USYNRT registers and lines were interfaced using memory-mapped I/O, i.e., each register (device) has an address of a non-existent memory location. This was accomplished by connecting memory address lines from the CPU to the register address lines and read/write line of the USYNRT chip. The data bus of the chip is tied directly to the data bus of the CPU and memory read and write signals are used to generate DPENA. Reading and writing is done with load and store instructions instead of normal I/O intructions.

To alleviate some of the speed restriction inherent in programmed I/O, the interface was expanded to permit data transfers via direct memory access (DMA). Only the receive and transmit data buffers are interfaced this way; other functions remain entirely under program control. For DMA transfers the program initializes the appropriate CPU register (R0) for a memory pointer, starts the USYNRT with programmed I/O, then issues a DMA Permit command to the interface. The chip address lines are then forced to the proper state for the transfer and the control handshaking takes place between RDA and TBMT with the DMA state signal from the CPU; thus, bytes are transferred to/from memory without execution of computer instructions once the process has started.

The end-of-frame procedure remains under program control. For receiving, this means the program must look for the assertion of the RSA line, indicating end or error. For transmitting, the software must monitor the contents of R0 in order to determine when to terminate the message. When the last byte has been transferred, the DMA channel must be disabled and end-of-message procedure completed under program control.

Interface to another microprocessor.

The USYNRT interface to the second microprocessor is similar to that of the first in that each register on the chip is treated as a separate I/O device; however, since the second microprocessor is able to directly address 256 devices, the registers are interfaced as conventional I/O ports. The register address lines and the read/write line of the chip are connected to 4 of the CPU address bus lines. This means that read and write operations for a given register have separate port addresses.

The bidirectional data bus of the USYNRT is separated into two busses in this interface in order to mate with the bus structure provided by the boards on which the computer resides.

A unique feature of this interface is that it utilizes the vectored interrupt feature of the second microprocessor. The most-used control outputs of the USYNRT, namely RDA, RSA, TBMT and TSA are connected to the CPU board as interrupt lines. The assertion of any one of these lines causes an interrupt to occur. If the CPU has been conditioned for the vectored interrupt mode, a pointer will be formed using these four lines plus four hard-wired lines. This pointer, together with 8 bits from a CPU register, becomes the 16-bit starting address of an interrupt service program. Thus, the interrupt is vectored to the service routine appropriate for the line or combination of lines asserted. Of course, the interface may be operated in a programmed I/O mode as well.

Details of FEDS Safe/Arm Provisions

Figure A-1 shows schematically the circuitry required to reliably fire the FEDS and at the same time provide protection against unintended firing during the course of authorized access to the protected area.

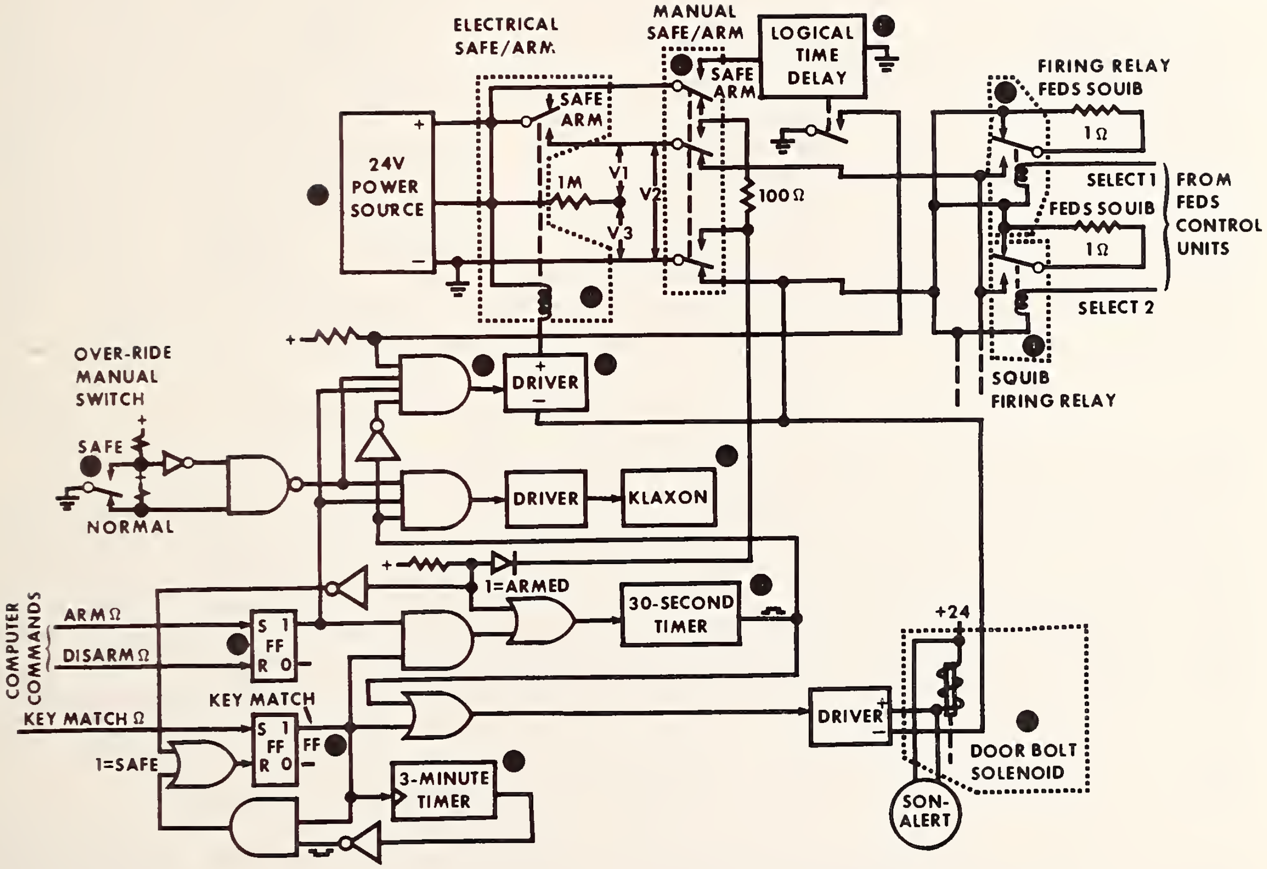


Figure A-1 FEDS Safe/Arm Circuitry

A FED is actuated by a squib, a low impedance device that is fired by a dc current pulse of several amperes magnitude. This current pulse must pass through an electrically controlled Safe/Arm switch, a manually controlled Safe/Arm switch, and then through a computer controlled firing switch that is provided for each individual FED. For reliable firing it is imperative that all switch contacts have low electrical resistance, therefore the switches must be heavy duty devices and be well protected from contamination and corrosion.

The Manual Safe/Arm switch is a three-pole, double-throw switch located in a conspicuous place inside the magazine near the door. Its size must be large, not only for electrical reliability, but also so that its operation is simple and unambiguous.

Two of its three poles carry current to the squibs; the third is used to actuate a time delay relay which will be explained later.

The Electrical Safe/Arm switch is a heavy duty relay with a single set of contacts in series between the positive terminal of the power source and the Manual Safe/Arm switch. It is actuated by a solid-state driver circuit but the common terminal of the driver circuit is wired to ground through the Manual Safe/Arm switch, inhibiting operation while the manual switch is in its Safe position. The driver is preceded by a logical AND gate which demands that the following conditions be met before the relay can move to the Arm position: computer command to arm, 30-second timer not running, time delay relay released, and override switch closed. How these conditions are met or not met can be best explained by going through typical operational sequences:

Normal entry and exit----Electrical Safe/Arm is in Safe position, Manual Safe/ Arm in Arm. The first event for authorized access is the occurrence of a "match" signal from the electronic lock; this signal is used to actuate the lock bolt solenoid, allowing the door to open. The first act of the person entering the magazine is to move the Manual Safe/Arm switch to Safe. This action causes the key match signal to clear and the bolt solenoid to de-energize. The last personnel action before leaving the magazine is to switch Manual Safe/Arm back to Arm. This will start the 30-second timer which in turn actuates the bolt solenoid, permitting the door to be closed. This operation of the bolt serves as a reminder to restore Manual Safe/Arm to Arm; if this step is omitted the door cannot be closed.

Failure during entry----In the above procedure it is assumed that the Electrical Safe/Arm relay remains in the Safe position. It is possible however, that communications between the RU and CU could fail between the time the door was opened and the time that the Manual switch was set to Safe. If this happened, the RU, now in autonomous mode, would likely command FEDS to fire since the select sensor group would most certainly be in an alarm state. It is necessary then to delay the effect of the computer command and warn personnel of the failure. The presence of the key match signal AND the computer command to Arm starts the 30-second timer mentioned above. A signal from this timer is used to inhibit actuation of the Electrical Safe/Arm switch and will cause a klaxon or loud horn to sound. During this 30-second period the person entering may (a) place the Manual Safe/Arm switch to Safe or (b) retreat and close the door, removing the alarm causing conditions. If he chooses (a), the lock bolt will be released and key match signal cleared as described above. For case (b) the expiration of a three-minute timer, started when the lock was opened, will insure that the bolt is eventually released and the lock cleared.

Failure during exit----If the communications failure occurs between the time of Manual Arm and actual exit, a similar personnel hazard exists. Again the 30-second timer will be used to delay Electrical Safe/Arm actuation. In this case the timer is started when Manual Safe/Arm is moved to Arm. Unfortunately, this produces a dangerous "race" condition, i.e., the FEDS firing circuit is complete for an instant before the timer can start its inhibiting action. The remedy for this situation is a time delay relay with delay-on-release action. The operation is as follows: the relay actuates immediately when the Manual Safe/Arm is moved to Safe. From the contacts of this relay another Electrical Safe/Arm inhibit signal is derived. When the Manual switch is returned to Arm this inhibit signal remains until the delay time has expired; thus, the inhibit is continuously present while the switching is taking place. The delay period of the relay could be 30 seconds or less. Again, the klaxon will sound if the RU tries to arm FEDS during this time.

Access by Mechanical Override----A third inhibiting input to the Electrical Safe/Arm relay is derived from the mechanical override switch. This normally closed switch opens when the override mechanism has been actuated to the end of its cycle. The klaxon is also inhibited by this switch since its warning is not necessary for this situation. When the override switch is open and Electrical Safe/Arm is Safe, an LED is illuminated and a mechanical flag appears outside the magazine indicating that it is now safe to enter.

Computer controlled testing of the power source, FEDS squib continuity, and Safe/Armswitch positions can be implemented by voltage sensing at the three test points shown on the diagram, Figure A-1. For these tests it is only necessary to detect the presence or absence of voltage at the specified test point.

SAFE/ARM SWITCHES AND FEDS TEST PROCEDURES

Test	Procedure	Voltage Present	Voltage Absent
Power Source	Measure V3	Source Good	Source Dead
Electrical Safe/Arm Switch Position	Measure V2	Armed	Safe
Manual Safe/Arm Switch Position	Command Electrical Safe/Arm to Safe; Then Measure Vl	Safe	Armed
FEDS Squib Continuity	Manual Safe/Arm Set to Arm; Electrical Safe/Arm Set to Safe; Computer Select FEDS; Measure Vl	Squib Good	Squib Open

NBS-114A (REV. 9-78)

U.S. DEPT. OF COMM.
BIBLIOGRAPHIC DATA SHEET

1. PUBLICATION OR REPORT NO.
NBSIR 79-1725

2. Gov't. Accession No.

3. Recipient's Accession No.

4. TITLE AND SUBTITLE

PHASE II FINAL REPORT
COMPUTERIZED SITE SECURITY AND RESPONSE SYSTEM

5. Publication Date
March 1979

6. Performing Organization Code

7. AUTHOR(S) R. T. Moore, R. J. Carpenter, A. W. Holt,
A. L. Koenig, and R. B. J. Warnar

8. Performing Organ. Report No.
NBSIR

9. PERFORMING ORGANIZATION NAME AND ADDRESS

NATIONAL BUREAU OF STANDARDS
DEPARTMENT OF COMMERCE
WASHINGTON, DC 20234

10. Project/Task/Work Unit No.

11. Contract/Grant No.
IACRO DNA EO 77-805,
78-803, 79-802

12. SPONSORING ORGANIZATION NAME AND COMPLETE ADDRESS (Street, City, State, ZIP)

Defense Nuclear Agency
Washington, D. C. 20305

13. Type of Report & Period Covered
Final

14. Sponsoring Agency Code

15. SUPPLEMENTARY NOTES

□ Document describes a computer program; SF-185, FIPS Software Summary, is attached.

16. ABSTRACT *(A 200-word or less factual summary of most significant information. If document includes a significant bibliography or literature survey, mention it here.)*

The Computerized Site Security Monitor and Response System (CSSMRS) is conceived as an integrated, state-of-the-art, computer-based system to enhance and improve the overall physical security of storage sites for nuclear weapons and materials. This would result from the interconnection of all site security systems, including intrusion detection equipment, duress alarms, guard radio and telephone systems, guard activity sensors, access control equipments, meteorological and environmental sensors, and deterrent systems to a distributed processing network of computers. These would be expected to provide timely, accurate, and unambiguous information about the site security status or the progress of an attack or intrusion attempt. To the extent that is feasible, appropriate response initiatives would be preprogrammed into the system. Changes in site security status and the resulting response actions would be automatically reported up-channel to higher command levels and backup and reserve forces would be automatically called out in the event of certain identifiable threat situations, particularly those in which continued survival of local guard forces might be doubtful.

17. KEY WORDS *(six to twelve entries; alphabetical order; capitalize only the first letter of the first key word unless a proper name; separated by semicolons)*

Central unit; computerized; detection; electronic lock; exclusion area; forced entry deterrent systems; guard control station; higher headquarters; perimeter station; remote unit; response force; triply redundant central computer

18. AVAILABILITY ☒ Unlimited

□ For Official Distribution. Do Not Release to NTIS

□ Order From Sup. of Doc., U.S. Government Printing Office, Washington, DC 20402, SD Stock No. SN003-003-

☒ Order From National Technical Information Service (NTIS), Springfield, VA, 22161

19. SECURITY CLASS (THIS REPORT)
UNCLASSIFIED X

20. SECURITY CLASS (THIS PAGE)
UNCLASSIFIED X

21. NO. OF PRINTED PAGES
117

22. Price
$6.50