NUREG/CR-4298
PNL-5490

Design and Installation of Computer Systems to Meet the Requirements of 10 CFR 73.55

Prepared by J. R. Lewis, K. R. Byers, J. D. Fluckiger, K. C. McBride, S. C. Vickroy

Pacific Northwest Laboratory
Operated by
Battelle Memorial Institute

Prepared for
U.S. Nuclear Regulatory Commission

NOTICE

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, or any of their employees, makes any warranty, expressed or implied, or assumes any legal liability of responsibility for any third party's use, or the results of such use, of any information, apparatus, product or process disclosed in this report, or represents that its use by such third party would not infringe privately owned rights.

NOTICE

Availability of Reference Materials Cited in NRC Publications

Most documents cited in NRC publications will be available from one of the following sources:

1. The NRC Public Document Room, 1717 H Street, N.W.
   Washington, DC 20555
2. The Superintendent of Documents, U.S. Government Printing Office, Post Office Box 37082,
   Washington, DC 20013-7082
3. The National Technical Information Service, Springfield, VA 22161

Although the listing that follows represents the majority of documents cited in NRC publications, it is not intended to be exhaustive.

Referenced documents available for inspection and copying for a fee from the NRC Public Document Room include NRC correspondence and internal NRC memoranda; NRC Office of Inspection and Enforcement bulletins, circulars, information notices, inspection and investigation notices; Licensee Event Reports; vendor reports and correspondence; Commission papers; and applicant and licensee documents and correspondence.

The following documents in the NUREG series are available for purchase from the NRC/GPO Sales Program: formal NRC staff and contractor reports, NRC-sponsored conference proceedings, and NRC booklets and brochures. Also available are Regulatory Guides, NRC regulations in the *Code of Federal Regulations*, and *Nuclear Regulatory Commission Issuances*.

Documents available from the National Technical Information Service include NUREG series reports and technical reports prepared by other federal agencies and reports prepared by the Atomic Energy Commission, forerunner agency to the Nuclear Regulatory Commission.

Documents available from public and special technical libraries include all open literature items, such as books, journal and periodical articles, and transactions. *Federal Register* notices, federal and state legislation, and congressional reports can usually be obtained from these libraries.

Documents such as theses, dissertations, foreign reports and translations, and non-NRC conference proceedings are available for purchase from the organization sponsoring the publication cited.

Single copies of NRC draft reports are available free, to the extent of supply, upon written request to the Division of Technical Information and Document Control, U.S. Nuclear Regulatory Commission, Washington, DC 20555.

Copies of industry codes and standards used in a substantive manner in the NRC regulatory process are maintained at the NRC Library, 7920 Norfolk Avenue, Bethesda, Maryland, and are available there for reference use by the public. Codes and standards are usually copyrighted and may be purchased from the originating organization or, if they are American National Standards, from the American National Standards Institute, 1430 Broadway, New York, NY 10018.

NUREG/CR-4298
PNL-5490
RS, 1S

Design and Installation of Computer Systems to Meet the Requirements of 10 CFR 73.55

Manuscript Completed: May 1985
Date Published: July 1985

J. R. Lewis, K. R. Byers, J. D. Fluckiger, K. C. McBride, S. C. Vickroy

Pacific Northwest Laboratory
Richland, WA 99352

Prepared for
Division of Risk Analysis and Operations
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555
NRC FIN B2877

ABSTRACT

The Pacific Northwest Laboratory has studied the design and installation of computer-managed systems that can help nuclear power plant licensees to meet the physical security requirements of 10 CFR 73.55 (for access control, alarm monitoring, and alarm recording.) Two objectives were to study the power plant security functions that could be aided by a computer-managed physical security system and to evaluate the safety and security considerations of such a system. A further objective was to develop guidance on system design, selection, and installation. The design guidance includes safety and security requirements, design alternatives, computer security, workspace design, and user interface design. Guidance is also provided on writing a system specification for procurement, bid review procedures, and site preparation.

SUMMARY

The Pacific Northwest Laboratory (PNL) has developed guidance for the design and installation of computer-managed physical access security systems at commercial nuclear power plants (NPPs). The purpose of this work was to provide information for licensees who are planning to use or upgrade such a computerized system in meeting the security requirements of 10 CFR 73.55 (access control, alarm monitoring, and alarm recording) and 10 CFR 73.70 (reporting and logging). The information can also be used to assist NRC license reviewers and inspectors in their evaluation of a licensee's computer-managed system. The guidance expressly considers the safety impacts of the failure or manipulation of a computerized security system.

Information was gathered from literature reviews, visits to power plant sites, and discussions with vendors of computer-managed systems. Safeguards and computer science experts at PNL evaluated this data to

- study the power plant security functions that could be aided by a computer-managed system
- evaluate the potential conflicts between safety and security in a computer-managed system
- develop guidance for system design, selection, and installation.

A comprehensive physical security system at an NPP must perform six functions to protect against radiological sabotage:

- deterrence
- detection
- delay
- assessment
- communication
- response.

Each function requires a combination of inherent plant features, security system hardware, and procedures to address all postulated events.

SECURITY FUNCTIONS THAT CAN BE HELPED BY A COMPUTER-MANAGED SYSTEM

The security functions that could be managed by computer are: access control, alarm monitoring, alarm display, and record keeping.

Access control systems are well-suited for computer management. In addition to providing access to areas for authorized individuals, the system can detect entry attempts by unauthorized individuals, or by authorized individuals who have neglected to log out of another controlled access area.

Signals from alarm annunciating devices and access control equipment can be processed by computer and displayed at a central location to indicate the alarm type and location, time and date, special conditions, and any instructions that should be followed. A computer-managed, closed-circuit television (CCTV) system can aid rapid assessment of an alarm condition. The computer can automatically switch the CCTV scene associated with an alarm to an assessment monitor for viewing by an operator at the alarm monitoring station.

A computer-managed security system can maintain records of security alarms and access control information of employees, vendors, and visitors. Information for accountability of site personnel could be available during simulated or actual plant emergencies. Records can also be maintained for alarms and computer systems that malfunction.

CONFLICTS BETWEEN SAFETY AND SECURITY

The primary area of potential conflicts between safety and a computer-managed security system is access control. Access control is both a detection and a delaying function of the security system. However, when access control causes delays to authorized plant personnel responding to an urgent or emergency situation, then a conflict with safety may occur.

The impacts of security on safety can be minimized by following guidelines for a generic system that is designed to reduce the likelihood of such impacts. Some suggested guidelines are--

- Implement highly reliable equipment to improve system reliability.
- Upgrade existing systems or include intelligent front-end multiplexers in the design of new computer systems so that
  1) central computer failure will not thwart vital area access control
  2) front-end multiplexer failure will affect only a part of vital area access control.
- Develop and routinely use walk-through exercises to train employees in efficient procedures for entering and exiting plant vital areas.

SYSTEM DESIGN

For the computer-managed physical security system to meet its functional requirements and minimize safety/security conflicts, the system design must consider system performance criteria in five areas:

- level of protection (how much security desired?)
- system capacity (how large a system?)
- system response (how fast?)
- system reliability (how dependable?)
- user interface (how operated by people?).

After determination of performance criteria, different design alternatives can be considered for implementing the system. Most of the systems now in use at NPPs are centralized systems that monitor alarms, assess alarms, and control access through a minicomputer that receives and processes input from the sensors in the plant. To increase system reliability, most of these systems have a redundant central processing unit and, in some cases, redundant storage of data. An increase in performance and reliability could be achieved by using a distributed system as a design alternative. In a distributed system, a minicomputer interfaces with intelligent multiplexers that oversee sensors in the plant. The intelligent multiplexers check the sensors for alarm or access control signals and can store a limited amount of data. The central minicomputer then communicates with the multiplexers to obtain the alarm or access control data for processing.

The design of computer-managed security systems must take into account the security of the computer system. The special needs for computer system security include:

- prevention of outsider access to the computer system
- compartmentalization of sensitive programs and data files in such a way that insider usage is limited to those whose responsibility requires access
- administrative controls such as system management, risk assessment, and separation of duties
- development of a necessary emergency and/or disaster plan.

The needs can be met by implementing security measures in five areas: 1) facility design, 2) access control, 3) administrative restrictions, 4) specifications in the procurement process, and 5) catastrophe planning.

To fully and efficiently meet the objectives of a physical security system, the system's human factors design must serve the needs of the operating personnel. The human factors associated with a computer-managed physical security system can be organized into three categories: 1) equipment layout and displays, 2) system space needs, and 3) workstation environment. Human factors design principles should be applied to each category to make the hardware compatible with the human operators.

Good design of the physical workspace is not sufficient to ensure effective and reliable job performance by the alarm station operators. Of equal importance is the way information is displayed to the operator at the terminal and the way in which the operator enters commands and data to the system. Human factors guidelines can be applied during the system design stage to ensure usability of the system when it is implemented.

SYSTEM SELECTION AND INSTALLATION

Once the design of the system has been completed, the next step is the development of the system specifications for the purchase of hardware and software. Most utilities will need to write system specifications and select a vendor to provide and install the system. Guidance is provided to aid in the writing of a system specification that will ensure that the vendors bid a system that meets the utilities' needs.

System selection methodology as presented in this report focuses on current vendor information and bid review procedures. Typical vendors of computer-managed security systems are listed. Four general approaches to bid review are outlined: low bid, fixed price selection, evaluation of intangibles, and analytic hierarchic process. The advantages and disadvantages of each approach are discussed.

The final topic of this report is system installation. Improper installation will adversely affect the reliability, availability, and usability of the system. Although installation requirements will vary at different sites, this report gives some general guidance about installation and discusses items that should be considered before system installation. The topics include: site selection, site planning, supply storage, acoustics, environmental specifications, and electrical considerations.

GUIDANCE FOR IMPLEMENTING A COMPUTER-MANAGED SECURITY SYSTEM

The guidance provided in this report covers the stages of system development from conceptual design to system installation. A subsequent phase of this project will provide guidance on verification and validation of the system, system operation, and system maintenance.

ACKNOWLEDGMENTS

This report could not have been completed without the cooperation and assistance of many people in numerous organizations. The authors wish to extend their appreciation to the personnel at utility headquarters and power plants who so willingly assisted us in this endeavor. We extend our gratitude to Battelle colleagues who helped us in technical analysis. In particular, we are grateful to Steve Matsumoto for editing and manuscript preparation. All these contributions make this document a better product than it otherwise would have been. However, the authors take full responsibility for the content of this report.

CONTENTS

ABSTRACT iii

SUMMARY v

ACKNOWLEDGMENTS ix

1.0 INTRODUCTION 1.1

1.1 BACKGROUND AND STUDY OBJECTIVES 1.1

1.2 APPROACH TO STUDYING COMPUTER-MANAGED SECURITY SYSTEMS 1.2

1.3 REPORT ORGANIZATION 1.3

2.0 CURRENT INDUSTRY PRACTICES 2.1

3.0 PHYSICAL SECURITY AT NUCLEAR POWER PLANTS 3.1

3.1 DESCRIPTION OF SECURITY REQUIREMENTS 3.1

3.2 FUNCTIONS OF PHYSICAL SECURITY 3.2

3.2.1 Deterrence 3.4

3.2.2 Detection 3.4

3.2.3 Delay 3.5

3.2.4 Assessment 3.6

3.2.5 Communication 3.6

3.2.6 Response 3.7

3.3 SECURITY AND THE EMPLOYEE 3.7

3.4 COMPUTERIZED SECURITY FUNCTIONS 3.8

3.4.1 Alarm and Access Control 3.8

3.4.2 Security Records 3.11

3.4.3 Other Functions 3.12

3.5 CONFLICTS BETWEEN SECURITY AND SAFETY 3.13

4.0 DESIGN OF COMPUTER-MANAGED SECURITY SYSTEMS 4.1

4.1 SAFETY AND SECURITY REQUIREMENTS 4.1
4.1.1 System Failures 4.2
4.1.2 Site Access Control 4.4
4.1.3 Vital Area Access Control 4.4
4.1.4 Compliance with ALARA 4.7
4.1.5 Operations and Security Coordination 4.7
4.2 DESIGN REQUIREMENTS 4.8
4.2.1 Level of Protection 4.8
4.2.2 System Capacity 4.9
4.2.3 System Response 4.10
4.2.4 System Reliability 4.11
4.2.5 User Interface 4.11
4.3 DESIGN ALTERNATIVES 4.12
4.3.1 Dedicated Computer Systems 4.12
4.3.2 Centralized Systems 4.13
4.3.3 Distributed Systems 4.15
4.3.4 Systems Reliability 4.17
4.3.5 Fault-Tolerant Systems 4.18
4.4 USE OF NEW TECHNOLOGY 4.20
4.5 COMPUTER SECURITY 4.21
4.5.1 Facility Design for Computer Security 4.21
4.5.2 Control of Access to the Computer 4.23
4.5.3 Administrative Measures for Computer Security 4.25
4.5.4 Specifications for Procurement 4.27
4.6 WORKSPACE DESIGN 4.27

4.6.1 Equipment Layout and Displays to Meet Task Requirements 4.27

4.6.2 System Space Needs 4.32

4.6.3 Work Station Environment 4.35

4.7 USER INTERFACE DESIGN 4.36

4.7.1 Data Entry 4.36

4.7.2 Sequence Control 4.38

4.7.3 Data Display 4.41

4.8 OTHER DESIGN CONSIDERATIONS 4.43

4.8.1 Economic Analysis 4.43

4.8.2 System Integration 4.44

4.8.3 Software Design 4.44

4.8.4 Software Development Tracking 4.45

5.0 SYSTEM SELECTION AND INSTALLATION 5.1

5.1 SYSTEM SPECIFICATION DESIGN 5.1

5.2 SELECTION OF SYSTEMS 5.3

5.2.1 Current Vendor Information 5.4

5.2.2 Bid Review Procedures 5.5

5.3 SYSTEM INSTALLATION 5.14

5.3.1 Selecting a Site 5.14

5.3.2 Site Planning 5.15

5.3.3 Supply Storage 5.17

5.3.4 Acoustics 5.17

5.3.5 Environmental Specifications 5.18

5.3.6 Electrical Considerations 5.18

6.0 REFERENCES 6.1

APPENDIX A - TYPICAL SYSTEM SPECIFICATION A.1

APPENDIX B - EXAMPLE OF THE ANALYTIC HIERARCHIC PROCESS B.1

FIGURES

3.1 A Typical Commercial Nuclear Power Plant Showing the Protected Area and Vital Areas 3.3

3.2 Functional Diagram of a Physical Security Computer System 3.9

4.1 Centralized Security Computer System 4.14

4.2 Distributed System 4.16

5.1 System Selection Hierarchy Example 5.12

5.2 Pairwise Comparison Matrix for Rating the Relative Importance of Criteria 5.13

B.1 System Selection Hierarchy Example B.2

B.2 Pairwise Comparisons of Evaluation Criteria for System Selected B.4

B.3 Computation of Normalized Weights B.4

B.4 Pairwise Comparisons of Criterion Dimensions for Delivery, Experience, and Quality B.5

B.5 Pairwise Comparison of Vendors A, B, C B.6

B.6 Hierarchial Composition of Weights for the System-Selected Decision B.8

TABLES

4.1 Barrier Penetration Times 4.10

5.1 Major Computer-Managed Security System Vendors 5.6

B.1 Scale for Coding Responses B.3

1.0 INTRODUCTION

Commercial nuclear power plant (NPP) licensees tend to rely on computer-managed systems to help meet the physical security requirements of 10 CFR 73.55 (for access control, alarm monitoring, and alarm recording) and the reporting and logging requirements of 10 CFR 73.70 (Energy Regulations 1981). The failure (or manipulation) of these computer-managed access control systems has a potential impact on safety. Recognizing this impact, the Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, has contracted with the Pacific Northwest Laboratory (PNL) to develop guidance for designing, operating, and maintaining computer-managed systems for physical security at NPPs. This report provides guidance on computer system design and installation. A subsequent report will provide guidance on computer system operation, evaluation, and maintenance.

1.1 BACKGROUND AND STUDY OBJECTIVES

The requirements for physical protection of nuclear power reactors against radiological sabotage are defined in 10 CFR 73.55 (Energy Regulations 1981). The regulation covers 1) general performance objectives and requirements, 2) physical security organization, 3) physical barriers, 4) access requirements, 5) detection aids, 6) communication requirements, 7) testing and maintenance, and 8) response requirements. The last five topics are of particular interest for this study because these are the areas where a computer-managed security system might benefit the licensee. For example, a computer-managed system can control access to a plant and to specific locations within the plant. The system can be linked to detection devices that can provide alarms at a central location and thereby aid in directing the alarm response.

As computer technology advances, many licensees may consider upgrading the hardware or software of their current systems, or expanding the functions performed by their system, or installing a system for the first time. To meet the requirements of 10 CFR 73.55, the computerized systems must be reliable, secure, and efficient, and must not jeopardize the safety of plant personnel. These goals are not mutually exclusive, and tradeoffs must be made by the licensee during the designing or upgrading of a system.

This is a two-phase study to provide guidance on 1) the computer system design and installation and 2) on computer systems operation, evaluation, and maintenance. The objectives of the first phase of the study are to

- study the security functions at an NPP that could be aided by a computer-managed physical security system
- evaluate safety and security considerations for a computer-managed system
- develop system design, implementation, selection, and installation guidance.

This report presents the findings obtained while meeting these objectives. It is intended to be used by the licensee as a source of information on the topics that are associated with a computer-managed security system. It can also be used as a source of information to assist NRC license reviewers and inspectors in evaluating a licensee's computerized security system.

1.2 APPROACH TO STUDYING COMPUTER-MANAGED SECURITY SYSTEMS

Information for this report was gathered from literature reviews, site visits, and discussions with vendors. The safeguards and computer science expertise of PNL staff members was combined with this data to meet the study objectives.

The literature review was performed to obtain information on several key topics:

- previous NRC and Department of Energy (DOE) studies and reports on safeguards and physical access security systems
- computer security
- computer hardware and software design
- human-machine interfaces
- computer system installation.

The reference section of this report lists sources for obtaining more knowledge on many of these topics.

After an initial literature review, several criteria were established for selecting sites for site visits. The group of visited power plants was to include:

- a representative system from each of the major vendors of computer-managed security systems
- a plant that currently had no computer system or was making a major upgrade to its existing system
- plants with varying numbers of years of operating experience
- plants with varying numbers of years of experience with computer-managed security systems
- plants with varying numbers of vital areas and categories of employees.

Based on these criteria, eight sites were selected for visits. The visits to NPPs were used to gain insight into the security functions performed at a plant, the computer-managed systems currently used by the licensees, and the benefits gained and problems encountered by the utilities in using these systems. Plant personnel from the security organizations and the personnel responsible for operating and maintaining the computer systems were interviewed. The specific sites are not identified, but the information obtained from each visit is used to support the findings presented in this report.

1.3 REPORT ORGANIZATION

The following section (Section 2) briefly reviews current industry practices, defining some basic terms and summarizing the functions now supported by computer-managed security systems at the plants that were visited.

Section 3 describes the general security requirements at NPPs, details the functions that can be aided by a computer-managed system, and discusses the safety/security conflicts that may arise from a computer-managed system.

Section 4 discusses the design considerations of computer-managed security systems. Included are:

- the interaction of safety and security requirements when a computer-managed security system is used (4.1)
- controlling elements that must be considered in system design (4.2)
- alternative structures for implementing computerized systems (4.3)
- new security technology that should be considered (4.4)
- special security requirements of the computer system itself (4.5)
- design of the workspace (4.6)
- design of the user interface and data displays (4.7)
- other considerations for implementing the system design and software. (4.8)

The final section (Section 5) discusses preparation of a formal system specification, describes methods of selecting a system in response to bid proposals, and offers guidance on system installation. Appendices include an outline of a typical system specification and an example of using one selection method--the analytic hierarchic process.

2.0 CURRENT INDUSTRY PRACTICES

The industry uses a variety of computer-managed systems, but all of them perform the same basic functions. The systems detect perimeter access violations, assess alarm situations, alert the security guard force, control access into zones within the plant perimeter, log accesses to and from zones, log access violations, and provide accountability reports on personnel locations. This information is displayed to operators in the central alarm station (CAS) and the secondary alarm station (SAS).

To detect perimeter access violations, various intrusion detection systems (such as microwave or E-field systems) are installed on the plant perimeters. All of the sites visited also had closed-circuit television (CCTV) cameras that covered the perimeter areas, access gates, and some doors. Some of these cameras are monitored continuously, while others are monitored automatically when an alarm is triggered in the zone that the camera is covering. Some plants automatically record the camera image when an alarm is received. There are a few remotely controlled pan/tilt/zoom cameras at some plants.

Of those plants that had a computer-managed security system, all use card readers at the doors to control access into areas. Most of the sites also had card readers for personnel to use whenever they exited an area (exit card readers). The system response when someone failed to insert an identification card at an exit card reader varied from plant to plant. One of several types of response might occur when the individual attempted entry at the next door:

- The access violation is logged and displayed, but the individual is granted immediate access to the next area.
- The access violation is logged and displayed, but the individual could gain access to the next area by inserting the identification card in the reader a second time.
- The access violation is logged and displayed, and the individual is denied access to the next area until cleared by the CAS operator.
- The access violation is logged and not displayed, and access to the next area is completely unrestricted.

In addition to equipment for detecting intrusions at primary access doors and the perimeter, the sites all had tamper-indicating alarms on emergency exit doors, manhole covers, card readers, and other critical security detection devices.

Alarms and CCTV images were displayed on monitors in the CAS and SAS. The operators in the CAS and SAS respond to the alarms and eventually clear them from the system after the alarms have been checked out and reset. Alarms were logged on a hard-copy device. At the sites visited, the alarm displays were

alphanumeric displays and the operator responded by entering a command. At one plant, the CAS or SAS operator could call up a back-lit slide projection display of the alarm location.

Most of the systems were dedicated to security. However, one plant had a system that also performed radiation exposure monitoring (REM). The security function had priority over the REM function if a conflict occurred in the allocation of system resources.

3.0 PHYSICAL SECURITY AT NUCLEAR POWER PLANTS

The general strategy for physical security against overt attack at NPPs is to detect the attempt early and to delay the attack enough that the adversary can be confronted by a security response force sufficient to prevent radiological sabotage. The physical security functions addressed in this chapter must be accomplished in a manner that

- assures that intrusion is detected
- allows rapid assessment of the threat and determination of the appropriate response
- minimizes the false alarm rate to avoid overloading the system's (or the operators') capacities
- provides adequate delay until response forces arrive.

Protection against covert operations by either outside or inside adversaries is provided by protected area and vital area access subsystems that

- prevent unauthorized access to protected areas
- record personnel movements within the plant
- prevent unauthorized access to vital equipment.

The initial parts of this section address general physical security at NPPs: requirements, functions, and employee responsibilities. Readers familiar with the terms and concepts presented might wish to scan these and turn to subsequent discussions that deal specifically with applying a computer-managed system: the security functions that could be managed by a computer, the potential conflicts that can arise between security and safety when security functions are implemented, and ways to resolve these conflicts.

3.1 DESCRIPTION OF SECURITY REQUIREMENTS

The Atomic Energy Act of 1954 and the Energy Reorganization Act of 1974 directed the NRC to regulate the physical security provided by its NPP licensees. The NRC physical security objective for NPPs is to develop and require implementation of measures designed to prevent, deter, and respond to acts of radiological sabotage. Radiological sabotage is defined as a deliberate act of destruction, damage, or manipulation of vital equipment which could result in the release, beyond the plant boundary, of sufficient radioactive materials to endanger public health and safety by exposure to radiation. Physical security systems are, therefore, primarily designed to prevent sabotage of vital equipment. Physical security is important because it is another measure, in addition to backup safety systems, that assures the safe operation of an NPP.

A physical security system is intended to prevent deliberate acts that could cause a release of radiation and endanger public health and safety. Therefore, the NRC and the licensees must assure that adequate physical security systems are installed at all operating NPPs because an act of radiological sabotage could have the same effect as a major accident.

The regulations governing physical security at NPPs require that all licensees have a physical security organization, physical barriers, access control measures, detection aids, communications equipment, response equipment, and enough tests to assure that these measures are working properly.

To combat radiological sabotage at an NPP, a typical protection system is designed to prevent access of unauthorized persons to areas where they could cause a serious release of radiation. Such areas are designated "vital areas" and are protected by at least two barriers and access controls. The first barrier is at the "protected area" perimeter, and the second barrier surrounds the "vital area" itself. Individuals entering an NPP at the protected area entry point are searched for contraband (weapons, explosives, etc.). The protected area is usually monitored by CCTV, posted security officers, or patrolling officers to detect attempts at entry through other than designated entry points. The protected area barrier is usually a chain-link fence topped with barbed wire and equipped with electronic intrusion alarms. A typical NPP layout including the protected area and vital areas is shown in Figure 3.1.

Within the protected area are specific areas that are vital to radiological security. Disabling equipment or systems in these vital areas could either directly cause a radiological release or prevent mitigation of a threatened release caused by damage elsewhere. Typical vital equipment includes the reactor containment, the main reactor controls, and the pumps, piping, and valves essential for reactor cooling.

Vital areas are enclosed with physical barriers such as concrete walls and metal doors. To enter a vital area, an individual must first have authorization from plant management. Entry into a vital area is through controlled access points typically equipped with electronic card readers for verifying access authorization. Vital areas are locked and equipped with alarms that are monitored by two independent alarm stations manned by security personnel.

3.2 FUNCTIONS OF PHYSICAL SECURITY

This section discusses the physical security functions at an NPP. Understanding the purpose of each function will help identify functions that are well-suited for computer management. The computer-managed security functions are further discussed in Section 3.4.

There are six functions that a comprehensive physical security system at an NPP must perform to provide protection against acts of radiological sabotage.

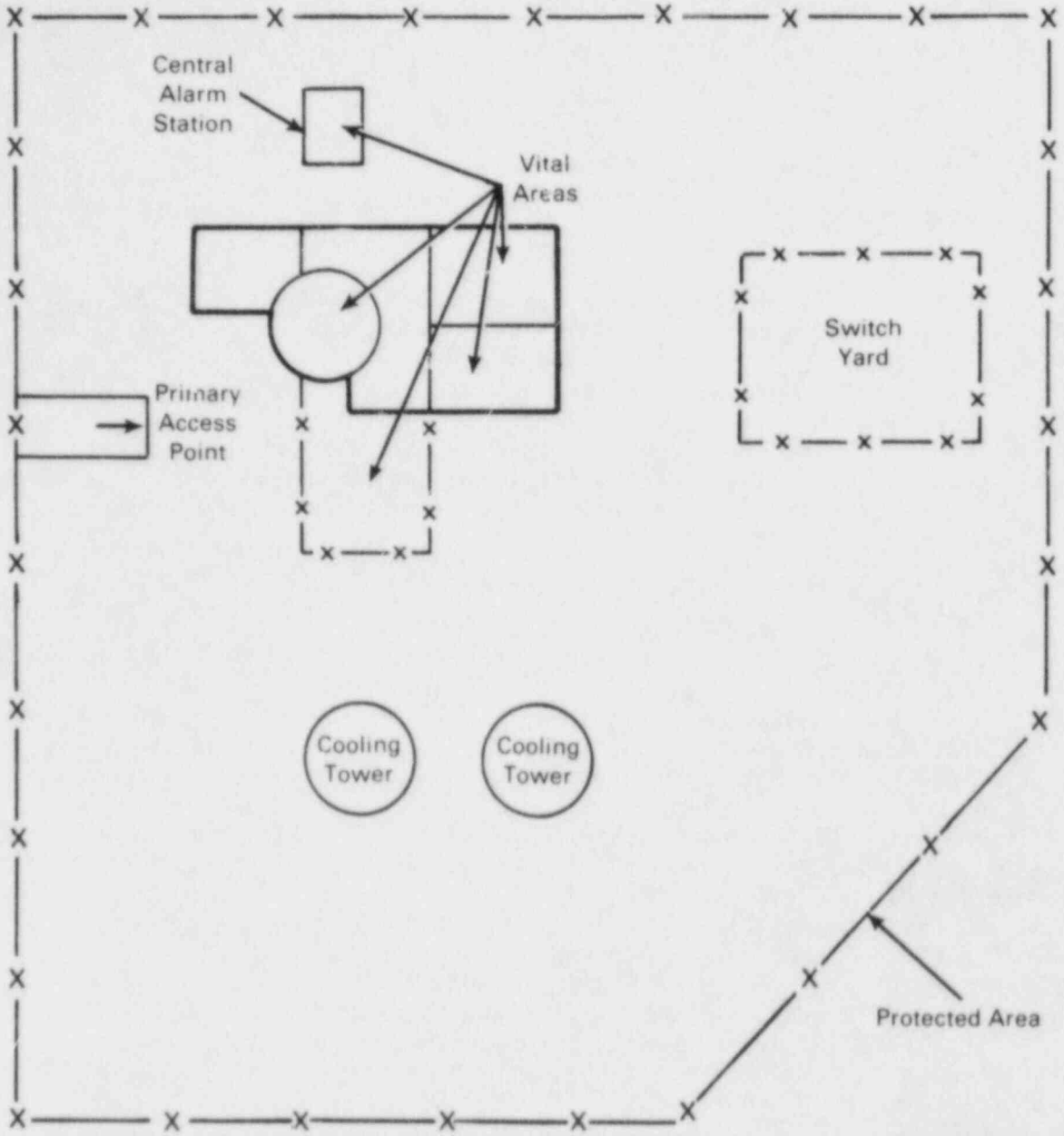

FIGURE 3.1. A Typical Commercial Nuclear Power Plant Showing the Protected Area and Vital Areas

These functions are:

- deterrence
- detection
- delay
- assessment
- communication
- response.

Each function requires a combination of inherent plant features, security system hardware, and procedures developed to address all postulated adversary scenarios and event contingencies. Depending on the internal organizational and administrative structure of a facility, these indicative, responsive, and preventive functions can be initiated quickly enough to meet the objectives of 10 CFR 73.55. To understand the total picture of physical security at a nuclear power plant, it is first important to understand each protective function and the interrelationships between functions.

3.2.1 Deterrence

Deterrence is the ability of a plant's protection system to reduce an adversary's probability of success to a point where the disadvantages of an attack on the plant outweigh advantages. For our purposes, the adversary is a rational potential saboteur who may be operating alone or with a group and who may be an employee of the utility or its contractors.

The ability of the security system to identify unauthorized acts and the quickness of the identification are important factors in determining the effectiveness of the deterrence. Therefore, training and cooperation between operational entities are very important elements of the protection system. Abnormal situations must be recognized and communicated to the proper facility organizations for them to respond effectively and quickly. If the organizational structure does not support a common understanding among employees and stimulate feelings of trust among employees of different organizations, then communication lines break down, destroying the ability to identify and respond to situations that may be a direct result of sabotage.

Any deterioration of the security system, either organizationally or in the effectiveness of equipment or manpower, will change an adversary's perception of sabotage success. If any element of the system becomes weak, then compensatory measures must be immediately implemented to maintain deterrence. A protection system is always performing at its best when it is deterring rather than when it is preventing.

3.2.2 Detection

Detection is a determination that an event or unauthorized action may have occurred. Assessment of the detected event is addressed separately in

Section 3.2.4. The possibility that the detection is false must be considered, and the extent of that possibility will depend on the method of detection and the equipment used for detection.

All detection systems have a potential for false alarms, and one function of the physical security system is to minimize the probability of false alarms to maintain a credible and efficient system. Each alarm generated by the system must be treated as a valid alarm, and appropriate actions must be taken in response. Once the system is degraded by a high rate of false alarms, the response may change because the security personnel are aware of the unreliability of the detection equipment. Before this occurs, compensatory measures must be taken to replace defective equipment, change any adverse characteristics of the detection environment, or implement alternative detection procedures.

In most cases detection results from some type of sensor indicating that some event has occurred. However, detection can also occur by visual surveillance. The "two-person rule" is an example of surveillance used as a detection tool. Each person entering a vital area critical to the radiological safety of the plant is accompanied by another person, and the two people maintain constant visual surveillance of each other's activities. This procedure is effective if the two people are not in a conspiracy and if each would recognize unauthorized actions performed by the other. Visual surveillance would be used in vital areas where a single, unauthorized act could lead to the release of radioactive material into the environment.

Surveillance by plant personnel during normal duties, including roving security patrols and alarm station operators watching CCTV monitors, is a detection tool routinely used. Although false alarm rates are usually low for this kind of surveillance, unfortunately so is the detection probability. For high-risk areas where sabotage consequences are great, surveillance of the area should be used only as a back-up to supplement a more reliable detection system.

The important role of security-minded personnel in the detection of unauthorized activities is discussed in Section 3.3.

3.2.3 Delay

The purpose of the delay function is to slow the progress of an adversary until the threat can be assessed by responding forces, and the adversary can be apprehended. Delaying features can take many forms. The most obvious form is a physical barrier that simply increases the time required by an adversary to complete the sabotage.

Another delaying feature is the use of detailed or multiple procedures that must be followed before a saboteur can complete the sabotage. The delay is effective if the time necessary to follow the procedures is longer than the time between the alarm and the response. Another form of delay could be

interposing security personnel between the adversary and the adversary's physical goal. Although this may not be desirable in all cases, it is an alternative.

When delaying features are designed into a facility, it is important to consider what the threats might be, what delaying techniques are not obtrusive to normal plant operations, and what the response times should be: these considerations determine how much delay is necessary. An effective security system incorporates multiple delaying features into the design with some delay near the points of detection to facilitate accurate assessment of the situation.

3.2.4 Assessment

The security function of assessment includes determining the cause of an alarm and characterizing the situation if the alarm is genuine. Response to an alarm condition is initiated by the operators of the alarm monitoring stations. The station operator observes any CCTV coverage of the alarmed area or surrounding areas and checks the alarm status for other areas. A security officer is dispatched to check for abnormal conditions and assure that the alarm can be reset by the alarm station operator. If the alarm is triggered by wind, animals, or nearby authorized activities, the alarm is categorized as a nuisance alarm. An alarm is valid if the system functioned as intended and if an indication is found to substantiate the alarm condition, for example, a door propped open. The most difficult alarms to assess are those that have no probable cause. These alarms are categorized as "false alarms."

If an alarm occurs in an area monitored by CCTV, rapid assessment by the alarm monitoring station operator may be possible. However, in most cases a security officer will be required to locate the cause of the alarm by actually going to the detector location. CCTV is also effective as an assessment tool for nuisance alarms where animals trigger the alarms and can be seen on the monitor before they move out of the area.

3.2.5 Communication

The communication function begins when an alarm signal is received at an alarm monitoring station. The alarm station operator notifies a responding security officer who then assesses the alarm condition. After this initial assessment, further notifications may be necessary, and the communications system must provide the means to rapidly contact additional security personnel, offsite local law enforcement agencies, plant management, and plant personnel (if a local emergency is declared).

The communication function must be capable of working under routine and adverse conditions, including severe weather, plant operational emergencies, and a single adversary act of sabotage. Communications must be rapid enough that an adequate response force can respond in time to prevent successful

perpetration of an unauthorized act of radiological sabotage. The facility security plan must address methods and procedures for notifying the right people at the right time.

3.2.6 Response

If there are indications that an abnormal activity or condition exists, then the alarm station operator initiates an appropriate response by plant security officers and local law enforcement agencies. The goal of this phase of the response is to locate and contain the possible adversary and prevent any further unauthorized activities. The onsite security force is the first line of defense. The responding officers must be able to successfully engage any adversary specified in the general performance objectives of 10 CFR 73.5-5(a), and, as a minimum, delay the adversary until additional assistance arrives. Response procedures should be prepared and maintained for all postulated adversary scenarios of unauthorized activities leading to radiological sabotage. Periodic testing of response capabilities will indicate the response forces' effectiveness and provide the training necessary for response forces to maintain their skills.

3.3 SECURITY AND THE EMPLOYEE

Security at any NPP is the responsibility of all employees, not just of the security force personnel. Employees must cooperate with security to assure that the overall security at the plant is as good as it can be. This means following routine security procedures for plant access. Security equipment cannot be expected to perform as intended if employees abuse the equipment and procedures. Because ineffective security could lead to a plant shutdown, which could mean lost jobs, it is in the best interest of all employees to maintain good security.

Employees who are aware of good security practices are in an excellent position to detect unauthorized activities. Security personnel cannot observe all of the employees working and probably would not be able to distinguish some unauthorized activities from normal duties. The detection function must be a part of each employee's everyday routine. The presence of knowledgeable personnel willing to help the security force provides not only detection with immediate assessment of the situation but also deterrence to the potential adversary. The result is an effective expansion of the security force to include all plant employees. Unauthorized activities become more difficult to conceal.

Cooperation between the security organization and plant employees can only be achieved when security is trusted and accepted by employees. The attitudes of security personnel in performing routine duties where contact with other plant employees is part of the job will affect this relationship. It is important for plant management to verify that communication lines between the operations shift supervisor and the security watch commander are open. The security watch commander should have an up-to-date schedule of plant activities that

might affect security procedures and personnel. The operations shift supervisor should be informed of special security activities, such as training exercises, or of problem areas with security equipment.

3.4 COMPUTERIZED SECURITY FUNCTIONS

The computer is a potential tool for aiding the utility and security staff as they perform their security functions. As shown in Figure 3.2, the security functions that could be managed by computer are: alarm monitoring, access control, alarm display, and record keeping. Additional functions such as maintenance of security training records and radiation exposure monitoring might be considered as part of the system if adequate computer resources are available. These functions are detailed in the following sections.

3.4.1 Alarm and Access Control

Two of the main security functions that can be computer-managed are detection and assessment. Signals from alarm annunciating devices and access control equipment can be processed by computer and displayed at a central location to indicate the alarm type and location, time and date, and any special conditions that may exist or any instructions that should be followed. Certain areas that may require a rapid assessment of the alarm condition where security officers are not normally present will benefit from a computer-managed CCTV system. The computer can automatically switch the CCTV scene associated with an alarm to an assessment monitor for viewing by the operator at the alarm monitoring station. The detection and assessment functions work together in a computer-managed security system to provide a fast, accurate indication of the plant security status under alarm conditions.

There are several different types of perimeter intrusion alarm systems. These include but are not limited to microwave, E-field fence, and fence disturbance systems. These systems are all partitioned into alarm zones with each zone sending a signal to an alarm distribution center. Each system type has a characteristic false alarm rate dependent on the environmental conditions at the detector location. The false alarm rate should be monitored for significant changes, and compensatory measures should be implemented if the rate falls outside acceptable limits. A computer system is helpful in maintaining records of specific alarm rates and can be used to analyze data in real-time.

Intrusion sensors in vital areas may be systems composed of door switches or area motion detectors. Although these systems also have a false alarm rate, it should be much lower than perimeter intrusion detection systems because the environment is usually controlled. Several alarm sensors associated with one vital area are usually connected to the same alarm distribution center. More information about specific sensor locations will be available if the alarm distribution centers can identify the exact alarm sensor that is activated. A computer-managed system can keep records of each individual alarm sensor or distribution center, which will assist in scheduling maintenance to prevent undetected equipment failures that would degrade the security system.

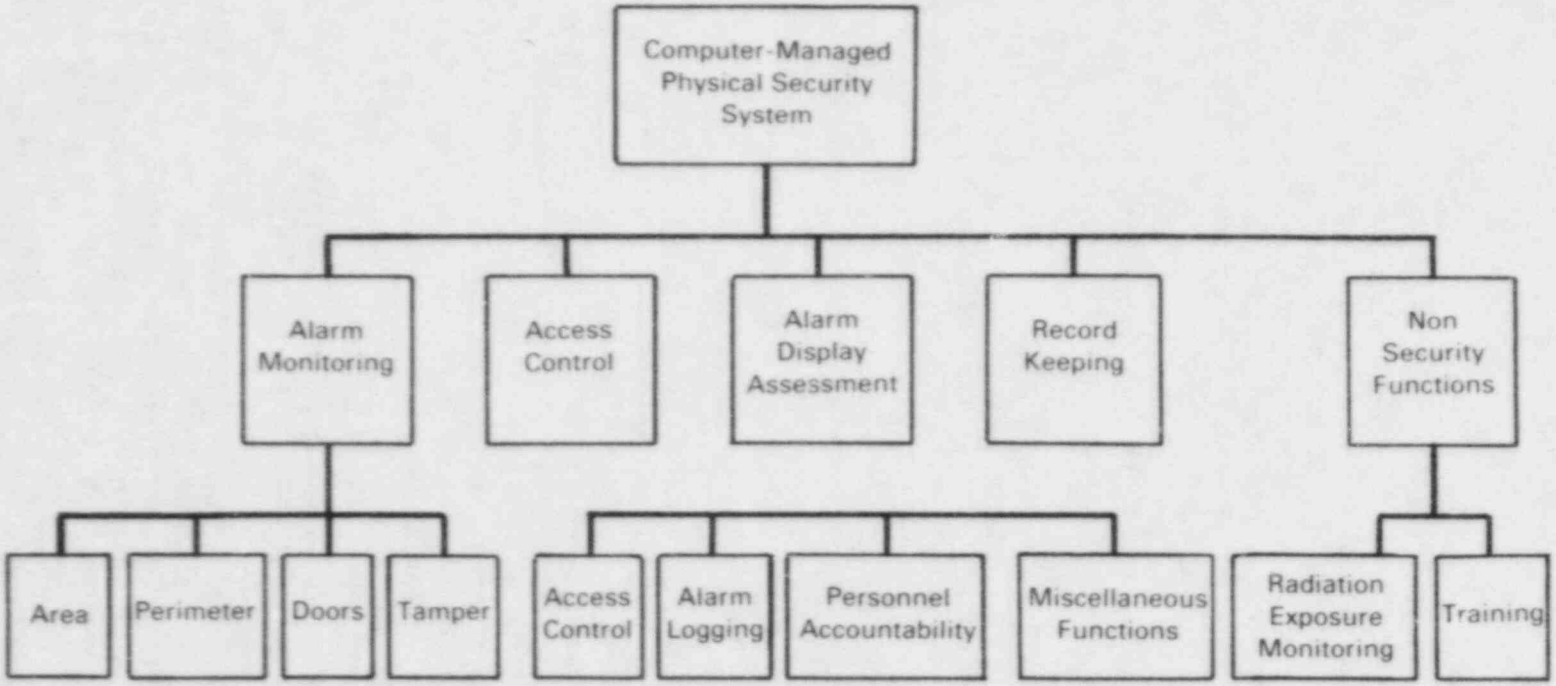

FIGURE 3.2. Functional Diagram of a Physical Security Computer System

Access control systems are well-suited for computer management. In addition to providing access to areas for authorized individuals, the system can detect entry attempts by unauthorized individuals or ascertain whether an authorized individual who is attempting to enter an area is already logged into another controlled access area. This last feature is known as "antipassback."

Antipassback has the advantage of a more positive control of vital area access. However, under urgent plant conditions it may not always be feasible to log out of an area when responding to a potentially serious situation. If vital area access cannot subsequently be granted, then a conflict between safety and security occurs (safety/security conflicts are discussed in Section 3.5). As a result of the study performed by the Haynes committee to review power reactor safeguards requirements (NUREG-0992), the NRC has reversed its initial position and recommended that the antipassback feature of card access control systems be removed for reasons of plant safety. Some utilities have chosen to retain this feature, recording all "passback" attempts but still granting access, while other utilities have eliminated the feature for key operations and emergency response personnel but retained it for all other site personnel.

Another feature that can be included in a computer-managed access control system is a duress access code. Vital areas where unauthorized access and a single adversary act could result in a radiological release to the environment can be positively controlled by the use of an access code in conjunction with a key card. A variation of the authorized code can be used to indicate to the security system that entry into the vital area was made under duress. This detection function should have the highest alarm priority, which would result in immediate response by the security force to control the situation before sabotage can be performed.

Closed-circuit television (CCTV) for assessment of alarm conditions and for general site surveillance should be managed by computer for it to be an effective tool for security. Perimeter intrusion alarms can be effectively assessed using CCTV, provided the system can respond quickly enough to activate the appropriate camera(s) and display the scene on a video monitor before an adversary who triggered the alarm can exit the viewing area of the camera. Alarm sensors should have established priorities for alarm monitoring. The computer-managed system should be able to evaluate multiple alarms and establish CCTV camera viewing priority. Multiple monitors can be available for viewing different areas simultaneously. Under normal no-alarm conditions the computer should cycle the CCTV camera scenes through the multiple monitors to assure that each camera is functioning properly and to assure that the monitors do not "burn in" one scene onto the monitor's screen.

General site surveillance and alarm assessment is enhanced by the use of CCTV cameras with pan/tilt/zoom capability. However, if the cameras are designated to look at specific alarm zones, the cameras must be moved back to that specific viewing angle after each use by the alarm monitoring station operator. Otherwise that alarm zone might not be under surveillance when an alarm is

received by the computer system. The camera can be controlled by the computer to automatically return to a predefined position after the operator has released control.

The computer-managed system can also activate remote video recording devices when an alarm is received. Recorded alarm scenes may help operators review an alarmed area for possible reassessment, and the scenes will be a record of alarms received for subsequent audit and assessment of the operator's performance at the alarm monitoring station.

3.4.2 Security Records

The NRC requires that licensees subject to the provisions of 10 CFR 73.55 keep security records of alarm annunications and access control information of employees, vendors, and visitors [10 CFR 73.70]. A computer-managed security system can easily maintain records of security alarms and access control information. Typical records of an alarm received by the alarm monitoring system include

- type of alarm
- location
- alarm circuit
- date and time
- operator acknowledgment of the alarm
- response details, including reason for the alarm.

Records should also be maintained for alarm and computer systems that malfunction. The same information as listed for each alarm should be recorded, including the length of time out-of-service and the compensatory measures employed during that time.

Access control information can also be logged using a computer-managed security system if some form of identification, such as a key card, is used to monitor personnel movements throughout the site. Upon becoming a site employee or an authorized vendor or visitor, an individual would be issued a specially coded key card.

The security system can maintain the following individual records:

- names and addresses of all authorized employees
- names and addresses of all individuals authorized access to vital areas and the vital areas to which authorization is granted
- register of all visitors and vendors
- log of all vital area accesses, including names and times of entry and exit.

A special function of a computer-managed access control system is the security "watchtour." A specially-coded key card that does not allow access to any controlled access area is assigned to a roving security officer. As the officer makes the required security checks, a record of the "tour" is made in the computer each time the key card is inserted into any card reader. A watchtour should never be performed in the same order as the previous watchtour, and a predetermined time should be established for movement between card readers. If card readers are equipped with key code input capability, the duress function can be utilized.

A side benefit of a computer-managed access control system is that the information is readily available for accountability of site personnel during simulated or actual plant emergencies. During an emergency involving site evacuation, personnel are instructed to proceed to assembly points for accountability and subsequent evacuation. At the assembly points, the personnel use their key cards to log out of the plant. Personnel not accounted for can be quickly identified by the computer, which can supply the names, badge numbers, last known location, and the time the last card entry was made. This information will aid emergency teams in locating and evacuating all nonessential operating personnel.

3.4.3 Other Functions

The computer-managed physical security system may have the capacity to support related functions that use the data that is already available from the system. Examples of these special functions are:

- employee training records
- security officer training records
- special radiation work procedures (RWPs)
- radiation exposure monitoring.

Functions that are related to the personnel access control information can be used to identify special conditions for vital area access. Records of the periodic training of employees and security officers can be used in conjunction with plant access to notify individuals of their need for retraining or requalification. These functions should not be used as a basis for denying access to any area, but notifications to the employee or supervisor could be made to insure that training requirements are met.

Monitoring or control of vital area access should be considered to protect the health and safety of the employee when special RWPs are required or when an employee has nearly approached the maximum radiation exposure allowed for that period. The computer system could warn the operators or even deny access, for example, when an employee who is approaching the exposure limit tries to gain access to a radiation area. Exemptions could be made for critical personnel on a case-by-case basis, and provisions in the security procedures could allow access under emergency or urgent situations.

The extent of these special functions, which may intrude upon the normal security functions performed by the computer, must depend on the data storage space available and the system response time. In no way should any of the special functions degrade the security of the facility or permit obtrusive conditions to be imposed on normal plant operations by the security system. Possible design characteristics of security systems incorporating special safety functions are addressed in Section 4.

3.5 CONFLICTS BETWEEN SECURITY AND SAFETY

In October 1982, the NRC Executive Director for Operations appointed a five-member committee to evaluate the impacts of NRC security requirements on operational safety at commercial nuclear power plants. The findings of the committee indicated that the security requirements might conflict with safety to varying degrees among the licensees, and that these conflicts might result in a serious compromise of safety in an emergency situation (NUREG-0992). One of the generic findings in NUREG-0992 was that licensee reviews of safeguards and security plans, contingency plans, and related implementing procedures did not evaluate the potential impacts of these plans on plant and personnel safety. The recommendation made by the committee was to include specific examination of the safety/safeguards interface in the NRC Regulatory Effectiveness Reviews.

This section addresses the generic conflicts between safety and security and discusses those issues related to computer-managed security systems. Section 4.1 identifies the safety and security requirements associated with the design of computer-managed systems that address these conflicts.

The primary contributor to safety/security conflicts is access control. Access control is both a detection and a delaying function of the security system. However, when access control causes delays to authorized plant personnel responding to an urgent or emergency situation, then a conflict occurs. Delay of employees or contractor personnel can create a variety of safety problems; for example,

- delay of access for time-critical repairs
- delay of access for time-critical operations
- delay of the response force in accessing a vital area to prevent sabotage
- delay of employee evacuations.

When critical equipment fails or is sabotaged, there is some critical time within which a failed component or system must be detected and repaired if an accident is to be avoided (Richardson 1982). If access controls designed to

protect vital areas might delay operational or security personnel from reaching an area to prevent or repair the damage of critical equipment, then there is a conflict between security and safety goals.

Another aspect of access control is the degree of internal compartmentalization required for security. Having all vital equipment in one vital area provides little in the way of safeguards because it would not provide defense in depth, but extreme compartmentalization could delay access to vital equipment enough to create safety problems. The number of vital areas varies significantly among licensed plants, and adding additional controls for operational, health physics, or administrative concerns compounds the potential safety problems caused by delay. When establishing vital areas and equipment, the licensee with assistance from NRC should review the plant design to optimize safeguards and minimize the obtrusiveness to safe plant operation. The licensee review should be a coordinated effort of all the organizations that would normally require access, such as operations, health physics, security, and maintenance.

Compartmentalization notwithstanding, several other factors can account for delay caused by the access control function. For a remote access control system these include:

- electrical power failure
- computer failure
- card reader failure
- misread or ignored card
- antipassback
- no access authorization - invalid card
- system delays.

These factors are related to the computer-managed security system and are discussed in Section 4.

4.0 DESIGN OF COMPUTER-MANAGED SECURITY SYSTEMS

For the computer-managed physical security system to minimize safety/security conflicts and perform the functions described in Section 3, the system design must be carefully considered. Although NPP installations are similar in many respects, the plants also have unique requirements for computer-managed security systems, making it impossible to discuss a specific system design. Therefore, this section of the report will discuss the design issues and provide guidance on ways the specific design requirements may be established at individual plants.

The specific topics are:

1. Safety and Security Requirements
2. Design Requirements
3. Design Alternatives
4. Use of New Technology
5. Computer Security
6. Workspace Design
7. User Interface Design
8. Other Considerations (System Integration, Economic Analysis, and Software Management).

4.1 SAFETY AND SECURITY REQUIREMENTS

The function of a computer-managed security system is efficient and effective control of a network of security hardware. The result must be positive control of access to protected areas and vital areas that are limited to only authorized individuals. Unauthorized access attempts, whether by tactics of force, stealth, or deceit, must be detected and response actions taken, using a system of security hardware and administrative procedures, before acts of radiological sabotage occur. While doing this, the system must also be able to minimize the impacts of security on the safe operation of the plant and the safety of plant personnel. Safety and security are not always compatible, which necessitates compromises when designing a system. This section identifies the areas where safety and security must be addressed together to produce an acceptable computer-managed security system.

Minimization of the impacts of security on safety begins by identifying guidelines for a generic system design. Although no two computer-managed security systems at two different nuclear power plants are alike, they share the common safety/security issues discussed in Section 3.5. The following items are suggested as guidance to reduce the likelihood of a security impact on plant safety:

- Implement highly reliable equipment to improve system reliability. (Fault-tolerant systems are discussed in depth in Section 4.3.5.)
- Upgrade existing systems or include intelligent front-end multiplexers in the design of new computer systems so that:

1) central computer failure will not thwart vital area access control, and

2) front-end multiplexer failure will affect only a part of vital area access control.

- Develop and routinely use walk-through exercises to train employees in efficient procedures for entering and exiting plant vital areas.

These items are addressed in detail later in this section. The areas addressed in the following subsections deal primarily with the interaction between security and plant operations. The focus is on access control because that is the concern of both security and operations personnel.

4.1.1 System Failures

A power failure is a potential cause of security system failure. The security system computer must have an emergency power back-up consisting of an uninterruptible power supply (UPS) and either an independent power line or a standby diesel generator. Loss of power or failure of electric door strikes and card readers can occur unless they also receive power through the UPS system. Indication of loss of power must be immediately transmitted to the CAS/SAS operators for action to avert possible safety problems.

The failure of system components is another potential cause of security system failure. The consequences of power or component failures and the necessity for back-ups are discussed in the following paragraphs.

Computer Failure

The security computer system must have emergency power back-up in case the primary power fails. If the computer loses power, then the subsequent loss of access control information may cause significant access delays and prompt the use of major security compensatory measures.

Computer operation can also be interrupted or lost because of malfunctioning components. To avoid this situation, systems have been designed with back-up components. Duplicate central processing units can be used with either automatic or manual switchover when a failure is detected. Although duplication greatly reduces the chance of a nonoperational system, failures still occur, and the same compensatory measures must be used as when loss of power occurs.

Alarm Station Back-up

In addition to duplicate system components, the NRC requires two independent alarm monitoring stations. All functions of the security system handled by the CAS must also be controllable from the SAS. During an emergency

situation a plant operator must have the ability to communicate with the SAS operator if he is unable to communicate with the CAS operator for any reason.

Failure of Electrical Door Locks

Plant and personnel safety can be affected by the failure of vital area door locks when the electrical power to the door fails or when the security computer system fails. NUREG-0992 specifies that:

> Upon loss of electrical power, interior vital area doors are not specifically required to fail in the locked position. These doors may fail in the open position if procedures are established which provide prompt compensatory measures for the open door (for example, deploying guards to strategic points).

NRC regulations give the utilities the option of having vital area doors fail in the open position during a power or computer failure; this option would prevent potential safety problems. However, a breach of security could result unless compensatory measures for protecting the open doors are instantaneous. The potential security problem exists if the open doors would give vital area access, even for a brief time, to insiders or to intruders who may have advanced beyond the plant perimeter.

Some utilities have elected to require that vital access doors fail in a locked state and to rely on the immediate availability of keys and other compensatory measures to maintain safety. These measures include deploying guards with door keys to maintain accountability for vital area access and providing crash bars on locking door knobs so that personnel could always exit vital areas. These utilities feel that access to these areas requires positive control at all times.

Card Reader Failure

It is possible that an individual card reader could fail and its status not be observed by the computer, depending on the problem; for example, the read heads may be misaligned; water, dirt, or debris may be interfering with the reading of the card; or there may be an electronic problem. When the computer is not aware that a problem exists, the card user must notify the CAS/SAS operator that the equipment is malfunctioning. If an emergency exists and an operator has no other means of accessing a vital area (i.e., hard keys), then a potential safety problem exists.

Near each card reader there should be a telephone or intercom that can be used to notify the CAS/SAS. The security organization should take compensatory measures to permit unimpaired access until the card reader is repaired or replaced.

4.1.2 Site Access Control

Emergency response personnel should be properly identified so that their access to the plant will be unimpeded during an emergency. Security procedures and training must be adequate to permit security personnel to give unimpeded access to properly identified individuals even if the security computer is not functioning.

Area Access Denial

Key plant personnel can be denied entrance to certain areas if the computer system fails to recognize their authorization. Procedures and training must be implemented to provide a means for security personnel to identify the individuals who compose the minimum shift complement so these personnel are not denied access in the case of a computer malfunction.

Key Card Replacement

Plant personnel associated with key safety or security functions should be able to request and obtain a replacement key card any time a key card is broken or repeatedly fails to function properly. While key card replacement is normally performed by day-shift security office personnel, emergency issue cards can be available from the security shift supervisor and assigned the same access authorization that is associated with the defective key card. The effect is minimum delay of plant personnel without incurring any access restrictions.

4.1.3 Vital Area Access Control

The design of a system to control access to vital areas should consider emergency access, the "vital island" concept, antipassback, exit denial, misread access cards, and system delay.

Emergency Access

Security procedures should be provided to expedite the access of operations and health physics personnel to vital areas during urgent or emergency conditions if a key card fails to be read by the computer system. Upon receipt of authorization from the Watch Engineer, the CAS/SAS operator could allow immediate access to the person requesting the vital area access and manually log that person into the computer accountability system. An armed security officer can then be dispatched to verify authorized access.

The capability should exist for the CAS/SAS operator, or alternatively under extreme emergency conditions for the Watch Engineer or Shift Supervisor, to override the computer-managed access control system and allow immediate access to vital areas. This ability should be controlled and monitored by the computer system. If possible, zones should be established so that allowance of unimpeded vital area access is limited to only the zone requiring access. This feature would have less impact on security forces responding to secure the area than overriding the entire system, which would significantly degrade security.

Vital Island Concept

The idea of minimizing the number of card reader interfaces for vital area access should be investigated whenever possible. The vital island concept, or grouping of several vital areas into one larger vital area, provides an opportunity to minimize card readers. Operators encounter fewer card readers, and that enhances accessibility, helps contamination control, and adheres to ALARA principles. The concept may require a tradeoff between the security system's ability to closely account for individuals in the plant and a slight reduction in security associated with vital equipment. If two separate vital systems control the release of radioactive materials and both are within the same vital area, then access for the purpose of radiological sabotage is more attractive than if the systems are in separate vital areas.

Minimizing the number of card readers can also positively affect security. Fewer readers can reduce the system delay in reading cards plant-wide. Maintenance on the readers is reduced, as is the number of responses required by security to verify access during system malfunctions.

Antipassback

Antipassback is a procedural feature available on some computer-managed access control systems. The system uses a logic sequence to determine a valid card access transaction. Antipassback would deny subsequent vital area access to a person who fails to log out of a vital area. Failure to log out may be due to an urgent need to reach a piece of vital equipment and the card was not in the reader long enough. This would be essentially the same as "tailgating," which is following someone through a door after that individual has logged out.

Since the person is still logged into a specific area, according to the computer, access to another area is denied until that person is logged out and the logical sequence is restored. This type of procedure may create serious safety consequences, and its use is not required by the NRC. However, several utilities have opted to retain the antipassback feature for the majority of their employees while exempting persons with critical jobs. Antipassback is an administrative control procedure and an accountability tool for controlling access to vital areas and for assuring that people use the access control system properly.

NRC Information Notice 83.36 strongly encourages licensees to eliminate the antipassback feature from their computer-managed security systems because of the safety concerns. This suggestion was made for all personnel who require plant access, not just emergency response team members (operations, fire brigade, staff health physics, and security personnel). NUREG-0992 states that antipassback features in vital area access control systems may adversely affect safety.

A feature similar to antipassback that should also be eliminated is any requirement for sequential carding, i.e., requiring personnel to card into one area before being allowed access to another area. One example of sequential coding is requiring a person to first card-in at a radiation controlled area

(RCA) access card reader before vital area access is allowed by a security card reader. If the RCA card reader is not functioning properly, vital area access might be difficult.

Exit Denial

Another aspect of vital area access control concerns exiting an area. An individual authorized to be in an area should not be denied exit from that area when the computer system does not previously have the person carded into the area. Failure of a person to be logged into the area may be legitimate (such as a card reader malfunction) or illegitimate (the person "tailgated" into the area, inadvertently or not). However, a person with a valid key card attempting to exit an area is physically in the area, regardless of the means of entrance. Exit should be allowed and the accountability records updated to reflect vital area access. If this situation is recurring, security personnel should contact the person and the person's supervisor for appropriate corrective action.

Misread Access Cards

This problem may be indistinguishable from card reader failure, but the problem may not be due to the card reader. Cards become worn and must be replaced periodically, with the replacement frequency depending on the amount of use and type of reader. If a card is suspected of being defective, then it should be replaced immediately. Interviews with operator personnel at nuclear power plants have shown that cards that misread in one reader may not misread in all readers. Therefore, when security checks the suspect card, it may function normally and the request for a new card may then be denied. Operators, therefore, purposely break the card so that a new one must be issued. If the safety of the plant and personnel must be placed on prompt key card access, then suspect cards should always be replaced immediately. Provisions should be made by security to issue replacement key cards when necessary without waiting until the next available day shift when key card issue personnel are available. Forms can be filled out and logs completed after the fact.

System Delay

As mentioned in Section 3.5.1, system delays may create a safety problem. At those sites visited, access control systems normally enabled entry into a vital area within two seconds. If the access control system is near its maximum capacity of data storage, as could be the case during power outages, then the delays are longer. In addition, procedural delays were noted at two different sites. At one site the system requires that if two or more people are logging into a vital area with the access door held open for convenience, then each person after the first must leave his access card in the reader for five seconds. If the card is not read by the computer and that card holder tries to access another vital area, access will be denied (if antipassback is used) until the card holder has cleared with the CAS using an internal telephone paging system. Another site requires a 20-second delay between persons logging out of certain vital areas when they leave those areas. Separate card readers should be available for entering and exiting vital areas. If only one

reader is used for both, then the system must provide a delay to allow a person enough time to log out. In effect this delay ties up the system, which requires anyone wanting access to wait until the system is cleared. These delays in a critical situation could result in safety problems.

4.1.4 Compliance with ALARA

Access control system equipment associated with vital areas with high radiation fields can present problems with the as low as reasonably achievable (ALARA) principles. As mentioned previously, card reader failure at a vital area where high-radiation fields exist might necessitate the posting of a security officer as a compensatory measure. If the problem appears to be extensive, then alternatives to posting an officer should be considered, for example, temporarily expanding the vital area to a location where the radiation is within acceptable limits. Also, the vital area exit denial problem can be a safety concern for an individual attempting to exit a high-radiation area. Procedures should be implemented to allow immediate exit, causing an alarm, and permit the individual to wait in a safer area until the security response arrives.

If an emergency occurred in which plant personnel must be evacuated or moved to the Operation Support Center (OSC) or evacuation staging area because of potential radioactive material releases, it is possible that the CAS and SAS would not be staffed, and therefore security monitoring of the vital and protected areas would not be performed. Security activities would be performed completely by security personnel supporting the declared plant emergency from the OSC or from remote plant access highways. An alternative to this degraded security condition would be to harden the CAS for occupation and use during emergency conditions that could result in a radioactive release. Then security personnel could continue to use the computer system to support the security functions.

4.1.5 Operations and Security Coordination

Interface problems between security and operations can be reduced by increased awareness and through cross-training and indoctrination of the roles, responsibilities, and general practices of both organizations. The operations personnel should be aware of the duties of the security personnel, the importance of those duties, and how operators should interact with security to assure safe, secure operation of the plant. Likewise, security personnel should be aware of the operations functions that affect security. This would entail knowing which areas of the plant are routinely visited by operations personnel, the frequency of those visits, and the normal paths used to get there. An understanding of the importance of a particular operational function and of the frustration that occurs when security procedures interfere with that function would put security/operational interface problems in perspective for the security organization.

These interactions are important for a computer-managed security system because problems normally encountered by plant personnel using the access control system can be controlled when coordinated planning and bi-directional communications exist between security and operations.

No Access Authorization

The security practice for granting authorization for vital area access is usually to allow access if a person's normal duties involve possible work in that particular vital area. Licensees' interpretations of normal duties vary, and so do their security practices. The best practice would be to limit the number of authorized personnel to the few needed to perform the work. However, a safety/security conflict may occur if an unauthorized employee requires access under emergency conditions. Also, if the access authorization list is frequently updated and an authorized employee with a critical job function is not on the updated list, then another conflict occurs. These situations should not occur because authorization verification should be performed by security and operations management at regular intervals. At the other extreme, the worst practice would be to allow access to all vital areas for all plant personnel, which is not acceptable.

4.2 DESIGN REQUIREMENTS

The main functions of the computer-managed physical security protection system are to: 1) detect unauthorized activities, 2) delay adversary actions until an appropriate response can be made, and 3) control access into zones within the plant. The conceptual design of the computer system is the first step to be taken in the development of a system that performs these functions.

To complete a conceptual design of a physical access security system, the performance criteria for the system must be specified. The performance criteria for the computer-managed portion of the system will be a subset of the overall performance criteria. The sources of performance criteria are NRC regulations and the level of protection desired by the utility. These performance criteria will define the basic requirements for the physical protection system. The system performance criteria must address the following:

- level of protection
- system capacity
- system response
- system reliability
- user interface.

4.2.1 Level of Protection

Protection in depth is a design principle that needs to be considered in the conceptual design of the physical protection system. Protection in depth means to protect against a single point of failure by a design that requires an adversary to pass through several detectors and barriers to reach vital equipment or materials. Various levels of protection are obtained by placing

detection and delay components at different locations and/or by increasing the quantity and quality of these components.

The level of protection that the utility desires will have an impact on the computer-managed system in several ways. First the system capacity will be affected by the number of sensors in the plant. System response time may increase or decrease as the number of detection and delay components vary.

The utility needs to clearly define the level of protection that is required very early in the design phase. Factors that affect the level of protection include such considerations as the size of the facility, the location of the facility, and the perceived threat to the facility. Once this has been established, the rest of the performance criteria can be addressed.

4.2.2 System Capacity

Adequate system capacity will vary from plant to plant. System capacity involves central processing unit (CPU) memory size, CPU speed, input/output (I/O) speed, disk storage capacity, and tape storage.

Before the size of the system can be determined, the utility should have a complete facility description. This description should include a layout that shows the site boundary, access points, building locations, and plans for all significant buildings. All doors, gates, hatches, vents, manhole covers, and other openings in structural surfaces should be identified and classified according to the types of access allowed. The types of access would include uncontrolled openings, controlled openings that limit access to authorized individuals, and one-way emergency exits.

In addition to accesses, all locations that require alarm sensors should be identified. These sensors include perimeter intrusion, CCTV cameras, tamper sensors on card readers and manhole covers, and door strikes.

Each access control point must be evaluated to determine whether control and monitoring should be applied to ingress, egress, or both. The amount of traffic through each access control point during the regular shift, off-shift, and outages should be estimated.

System capacity requirements vary with the time span for polling the sensors. For example, the sensors might be polled at 1-second, 30-second, or 1-minute intervals. A careful evaluation must be made to determine the polling interval required for each sensor. The interval must be small enough to ensure that any unauthorized access or tampering will be detected. On the other hand, a sensor should not be polled more often than necessary because that would put too high a demand on system resources.

Disk storage requirements are governed by the number of card keys issued, the number of employees on site, and the number of visitors or temporary badges that are expected to be issued. Disk storage requirements vary with the type and amount of historical data that must be maintained and reported. Disk

storage requirements would be smaller if the system has the capability to store infrequently needed historical data on magnetic tape.

4.2.3 System Response

System response requirements depend upon the functions performed, i.e., barrier penetration detection, tamper alarming, door access, alarm logging, and access control updating. Each of these functions has its own response time requirement.

A 1978 Brookhaven National Laboratory study provided basic data on the times required to forcibly penetrate the types of barriers commonly found in nuclear power plants (Fainberg and Bieber 1978). These times vary from 0.5 seconds to penetrate an 8-foot security gate up to 23 minutes to penetrate a 12-foot reinforced concrete wall. The typical barriers around the perimeter of a power plant and their associated penetration times are shown in Table 4.1.

For a security force to prevent a sabotage attempt when an adversary penetrates a barrier in an unmanned area of the perimeter, it is critical that system alarm detection, system alarm notification, and CCTV activation times fall within these penetration times so that, at the very least, the intruder's path through the perimeter can be tracked by a CCTV display in the CAS or SAS. As can be seen from Table 4.1, the system response time will depend on the type of barrier around the plant.

The most important aspect of tamper detection and alarming is to detect that tampering has occurred and where it occurred. The response time is not as critical as it is for barrier penetration.

The system must detect unauthorized access attempts through doors and immediately notify the CAS and SAS so that appropriate assessment and response can be initiated. Also, an authorized individual's subsequent access through the doors must be handled efficiently.

System response cannot be degraded by non-security functions that may be performed on the same hardware. If the system has the capacity to perform other functions, the security functions must have the highest priority at all times. In an emergency or cases of heavy work load, this may mean that the other functions are shut out completely. This shutout needs to occur automatically if the security workload warrants the action.

TABLE 4.1. Barrier Penetration Times

Barrier	Penetration Time (Seconds)
barbed-tape obstacle	18.0
7-ft chain-link fence	4.3
7-ft chain-link fence w/concertina	8.4
8-ft security gate	0.5

4.2.4 System Reliability

Because of the importance of the detection, alarm, and access control functions, computer-managed physical security systems must be highly reliable. In discussing system reliability, Wensley (1982) has specified that:

> For a system to have high integrity implies not merely an appropriate design, but also a technique for understanding and analyzing the system to be able to provide assurances that the system will perform correctly. High integrity means that the control system will deliver the correct control signals at the correct time, even when a fault has occurred internally in the system.

Computer-managed physical access security systems must maintain a high integrity in addition to meeting reliability requirements.

System reliability is usually defined in terms of system availability. It is difficult to define a specific system availability figure, although with proper design of the system an availability of 95% is feasible. The utility must plan for alternate means, using their security guards, to cover the functions when the system is unavailable unexpectedly or because of planned maintenance. Therefore the availability of alternate security measures will affect the reliability requirements for the system.

The utility must compile information about environmental conditions in various areas of the facility, although these conditions will have a limited effect on the computer system. These conditions affect the safeguards components selected because weather conditions, electromagnetic interference, and interior noise, heat, and humidity may degrade component performance. The range of environmental conditions must be identified for all significant interior and exterior areas.

4.2.5 User Interface

The design of the system displays and the system interaction methods must consider characteristics of the personnel who use the system. The users of the system will typically be members of the plant's security force. These individuals will be very knowledgeable about security functions but may have little or no experience with computer systems.

A training period will be required for each user of the system; at the end of training period each user will be fairly proficient at performing the routine functions. However, there will be some functions that will occur infrequently in the routine course of operations, and this factor must be considered in the design of the user displays and interfaces. User interface design is discussed in more detail in Section 4.7.

The information that the computer-managed system must provide CAS and SAS operators on a routine basis includes

- alarm notification
- access violation notification.

This information may be available on a visual display terminal or a CCTV screen or both. There should be a positive indication of any new alarm or access violations that occur. If the number of alarms that are received exceeds the capacity of the display device, the operator must be made aware of that fact and must be able to retrieve the remainder of the alarms efficiently.

4.3 DESIGN ALTERNATIVES

At the outset of the system design phase, functions and requirements are viewed as those tools which will shape, change, and eventually produce a working system. The earlier sections of this document have introduced and described functions and requirements for a computer-managed security system.

Sometimes requirements other than security functions are incorporated into a new system because of convenience or because of budget limitations. For example, fire alarm monitoring, operations control, safeguards control, and administrative functions may be included in a security computer system. If the utility chooses to implement these functions, then security functions such as access control, alarm monitoring, and intrusion assessment will be required to compete for system resources. This fact must be carefully considered in the design of the system to ensure that security functions receive highest priority and that there are sufficient resources to perform these functions adequately.

Three general design alternatives considered in this report are:

- a disjointed set of dedicated systems
- a centralized system
- a distributed system.

The following sections discuss each of these design alternatives in further detail along with the advantages and disadvantages of each alternative.

4.3.1 Dedicated Computer Systems

Dedicated computer systems are stand-alone systems that perform a specific function or functions and have no communication links with other systems. In the context of computer-managed, physical access security systems an example of a dedicated system used for a specialized function would be a relatively small minicomputer system (or a microcomputer system of comparable computing power) used solely for alarm monitoring. Alarm sensor states might be printed on a line printer, and sensors in a positive alarm state could be displayed on the operator console as well as on an annunciator panel.

Concurrent with the operation of the alarm monitoring system, another dedicated system could be doing access control. This second dedicated system would control electronic door locking/unlocking devices based on input from card readers.

Advantages of Dedicated Systems

- Component failures affect only a specific stand-alone system. For example, if the access control system were not operational, the alarm monitoring functions would not be degraded.
- The limited scope may allow the acquisition of relatively inexpensive hardware, such as microcomputers, to perform the security functions.
- The software for the less complex systems may be easier to maintain, and updates to the system may be easier to implement.
- Each dedicated system can be completely upgraded or replaced without affecting other systems.

Disadvantages of Dedicated Systems

- Operators must be trained for each system and will need to use separate consoles to communicate with each dedicated system.
- Hardware and software maintenance of several different systems would be required.
- Data would be maintained separately for each stand-alone system. In some cases, this would result in a duplication of data storage. The CAS or SAS operators would need to integrate information from separate sources to make an assessment.
- Each dedicated system may require independent system security (i.e., access control).
- Each system would have limited processing capability.

No NPP sites visited had selected stand-alone systems to manage security functions. The disadvantages far outweigh the advantages, and stand-alone systems are not recommended.

4.3.2 Centralized Systems

Most of the NPP sites visited had implemented centralized security systems that performed the alarm monitoring, access control, and assessment functions. These systems are based on a minicomputer that receives input from the sensors in the plant. The minicomputer polls all the sensors (see Figure 4.1).

Advantages of Centralized Systems

- All of the data reside in one system. This avoids duplication of data, minimizes the data updating tasks, and provides information necessary for the system to perform assessment functions.
- Operator training is needed for only one system.

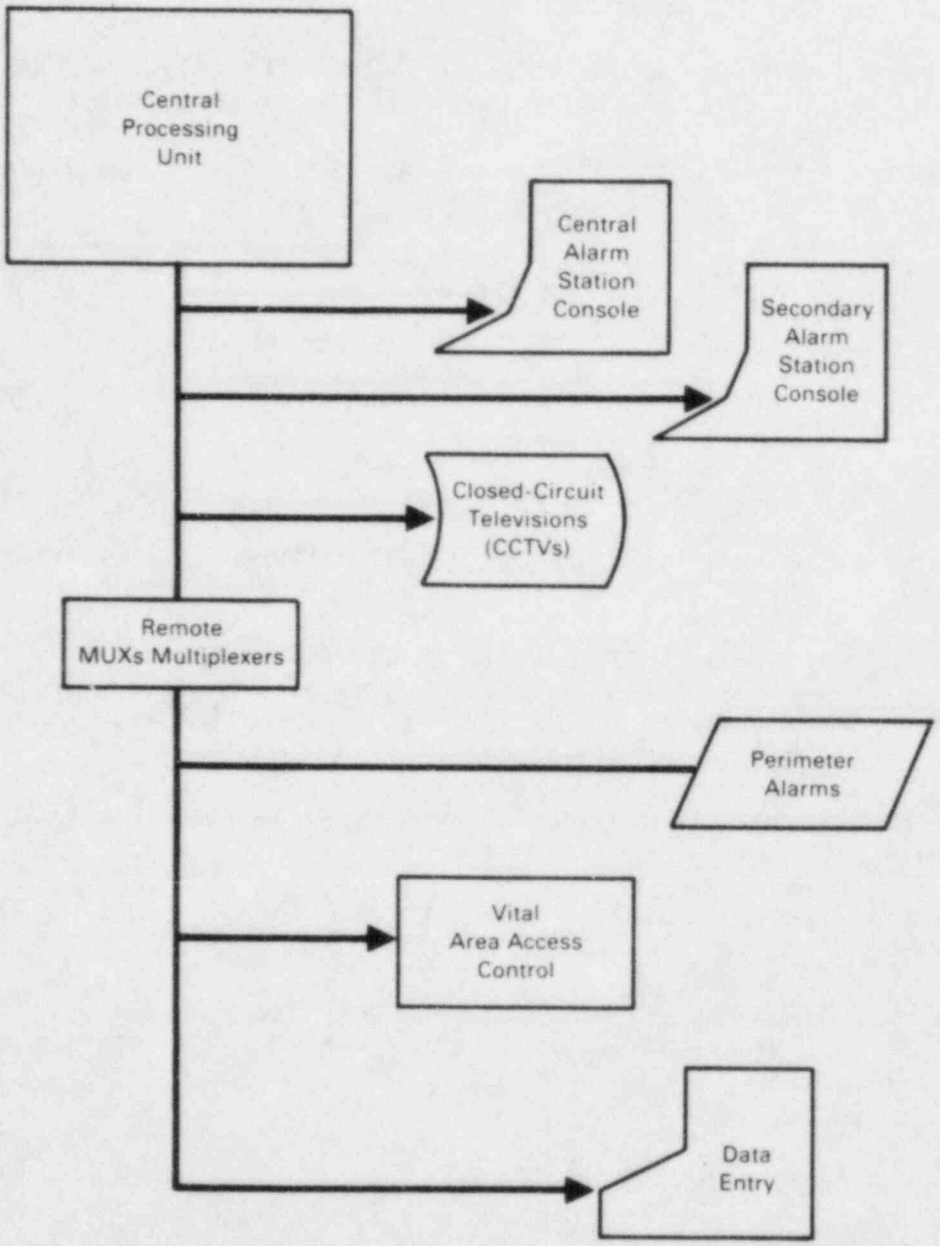

FIGURE 4.1. Centralized Security Computer System

- The CAS/SAS operators have all of their information integrated on a single display, and their communication is limited to a single system.
- Hardware and software maintenance are needed for only one system.
- Computer system user access control is needed for only one system.
- More powerful processing capability is available, which may result in a decrease in system response time.

Disadvantages of Centralized Systems

- Failure of the central system causes a generalized failure of all of the functions.
- Replacement of a major part of the centralized system may require complete system upgrade or replacement.
- Because the centralized system may be more complex than smaller dedicated systems, there may be a greater probability for failure.
- System performance may be degraded by too many functions trying to execute concurrently (i.e., access requests, alarms, assessment, etc.).

The centralized minicomputer system concept seems to be working adequately at the sites visited. The major disadvantage appears to be a degradation of system response time during periods of high traffic volume. This disadvantage can be minimized by the installation of a distributed system described in the next section.

4.3.3 Distributed Systems

Distributed systems in the computer-managed physical access security environment consist of a minicomputer interfaced to intelligent multiplexers that communicate with a set of sensors (see Figure 4.2). The intelligent multiplexers do the sensor polling and have the capability to store a limited amount of data in local memory. The central minicomputer then communicates with the multiplexers to obtain alarm signals or access control requests.

Advantages of Distributed Systems

- The intelligent front-end multiplexers can perform a wide variety of duties, thereby reducing the load on the CPU and avoiding degradation of CPU processing. This will result in better system response time.

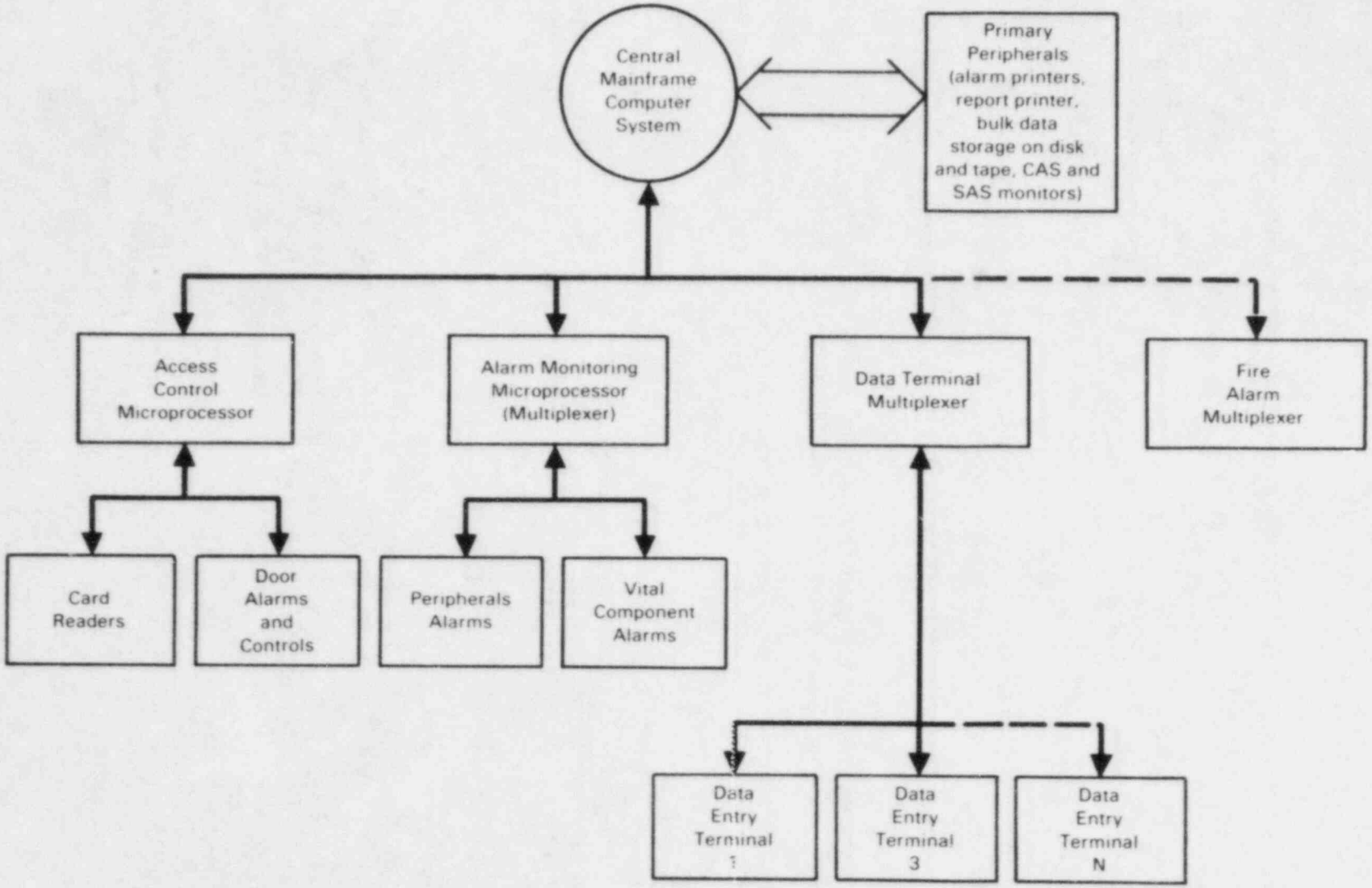

FIGURE 4.2. Distributed System (Network)

- The failure of part of the system (i.e., central processor or front end multiplexer) will not result in a generalized failure. For example, if the central minicomputer fails, the intelligent front end processors can still perform access control functions, thus providing individuals access to locations within the plant.

- The modular design simplifies hardware and software maintenance.

Disadvantages of Distributed Systems

- Additional communications hardware and software must be maintained.

- Maintenance may be required on multivendor components.

- Distributed systems are somewhat more complex than dedicated or central systems because of networking requirements.

The few plants that do use distributed systems have significantly shorter response times for access control. In addition, the safety benefits gained by providing access to vital areas in the case of a central processor failure makes this the recommended design alternative for any new system or or upgrades to existing systems.

4.3.4 Systems Reliability

The primary objective of this section is to describe how reliability requirements affect computer system configuration and design. The effect of implementing redundant (duplicate, triplicate, quadruplicate, etc.) components is predictable in a statistical sense, and, using tools such as fault tree analysis, design decisions can be made such that computer system component selection can be based on reliability requirements.

To design a reliable system, the system designer must be aware of all possible hardware and software failures that could constitute a security computer system failure. This is a non-trivial task and is especially difficult for software errors.

Once sources of failure have been determined, the designer can perform a reliability analysis to show the effect that specific failures have on total system reliability. Statistical techniques are available for this type of analysis (Barlow and Proschan 1975).

Design options that need to be considered for computer-managed physical access security systems include:

- single-component systems
- redundant systems
- fault-tolerant systems.

Each of these system design concepts provide a different level of reliability. However, a more reliable system will be more complex, and the initial development and component costs will be greater.

Single-component systems provide the least reliability. A failure in a component such as the central processing unit or the disk drive would result in system degradation or unavailability. This could have a serious impact on the security and safety of the plant, and single-component systems are not adequate for computer-managed physical access security systems.

To increase system reliability, many plants have installed redundant systems. The level of redundancy may vary, but in most cases the system has a redundant central processing unit (CPU) and, in some cases, a redundant disk drive. The redundant CPU can be configured in two modes: as a back-up processor, or as a "watchdog" processor. In the backup mode a CPU failure will mean that all processing must be switched to the back-up processor. This usually requires manual intervention. In the second, "watchdog" mode, both processors are running; however, the second runs in the background, continually checking the first processor. If the second processor detects a failure, the system automatically switches to the second processor, which then performs all functions.

Redundant hard disk drives also can be used in at least two ways. If all of the data is stored on only one disk drive, a failure of that drive will result in at least the temporary loss of the historical data. The security system can still function by storing new data on the back-up disk, but there may not be access to historical data or data base information. Complete disk redundancy is achieved by storing all of the data on both disks.

4.3.5 Fault-Tolerant Systems

Industry demand is increasingly rapidly for improved reliability of computer systems and for high availability (performance time/performance and maintenance and down time). Institutions relying heavily on processing of transactions need high computer system availabilities to provide timely services. Industries using or producing large quantities of energy need very high computer system reliabilities to optimize performance by operating devices close to safety limits. System faults in some applications (such as turbine operations or commercial aircraft) need to be quickly detected and corrected to avoid compromising safety or incurring costly damage of equipment or facilities. Nuclear power plant control and monitoring systems must be highly reliable and have continual availability. If the same high availability and reliability are not applied to nuclear power plant security systems, plant safety could be affected.

Fault-tolerant technology is one of today's most successful means of incorporating high availability and reliability into complex systems. Fault-tolerant systems are designed to continue correct operation and control in the presence of faults. Fault sources may be critical components such as integrated circuits, power supplies, central processors, or disk storage devices.

Additional fault sources can result from software failures. Faults may be intermittent failures which reoccur randomly or transient failures which may occur a few times and then not reoccur in the same way.

The purpose of fault-tolerant systems is to give the right result in the right place at the right time. Fault-tolerant systems have been designed to detect faults when they occur, report correct results in spite of faults, identify the source of a fault, log fault data, and describe appropriate procedures to repair failed equipment. "The key goals of a fault tolerant system are to maintain data integrity and maximize system uptime".--(Wensley 1983)

Any component will eventually fail and will have associated with it a mean time between failures (MTBF). MTBFs can be improved for fault-tolerant systems by improving the integrity of components, by increasing the sophistication of fault recognition and correction, and by increasing the replication of components (i.e., single redundance, dual redundance, dual-dual or triple redundance, and N-redundance).

Designing a system that can detect an error and switch a crucial process to a back-up component is no easy task. The architecture of a fault-tolerant system is more complex than that of a traditional computer. The objectives of this architecture are: 1) to continue operation even when faults occur, 2) to detect dissenting inputs or outputs, and 3) to report dissenting sources. To accomplish this objective, the operating system must constantly monitor primary and back-up components and orchestrate emergency switching between them.

Fault-tolerant designs can be based on either hardware or software. Hardware-based designs rely on component redundancy. Software-based designs configure alternate data paths to isolate faulty components. Software-based designs do require some hardware redundancy, but not one-for-one replication. Several processors share a pool of work and automatically redistribute the work if one of them fails. To accomplish this, the operating system must keep tabs on every job so the system knows what a faulty processor was doing when it failed.

Besides having significantly higher reliabilities and availabilities than non-fault-tolerant computer systems, fault-tolerant systems provide other advantages:

- The failed component can be replaced without shutting down the computer system (i.e., "hot" board changes are possible).
- Self diagnosis decreases the need for highly qualified maintenance technicians.
- Maintenance can be done at the user's convenience (i.e., 24-hour maintenance is not required in most cases).

There is, however, a trade-off between performance and fault tolerance. Increasing the number of checkpoints or adding hardware redundancy may decrease the computer performance (increase processing times, for example) to give it added reliability.

Some of the manufacturers of fault-tolerant systems include: Tandem Computers (Cupertino, California), Stratus Computer (Natick, Massachusetts), August Systems (Tigard, Oregon), Sequoia Systems (Marlboro, Massachusetts), Parallel Computers (Santa Cruz, California), No-Halt Computers (Farmingdale, New York), Auragen Systems (Fort Lee, New Jersey), Synapse Computer (Milpitas, California), Tolerant Transaction Systems (San Jose, California), and Computer Consoles (Rochester, New York).

Fault-tolerant technology is a relatively new field that has been approached in several ways by the manufacturers. Further study, beyond the scope of this project, is warranted to determine the contribution that fault-tolerant systems could make toward the reliability and availability of NPP computer systems.

4.4 USE OF NEW TECHNOLOGY

Technological advances for computer-managed security systems are, in general, paralleling rapid advances in related areas. For example, distributed systems are being incorporated to prevent component failure in one area of an NPP from disabling an entire security computer system. Distributed systems also can significantly reduce processing requirements on the system central processor.

A promising access control device is the infrared retina scanner. This unit is available commercially and can be used to control access to either computer terminals or vital areas. This type of device is able to identify a person by retina scan in roughly two seconds. Retina scans provide positive identification and eliminate the potential problem of false usage of a card that does not belong to the individual requesting access. Retina scanners are more costly than card readers for initial acquisition; however, it is possible that low retina scanner maintenance costs and relatively high card administration costs may offset initial cost differences.

Some vendors offer encryption devices to control computer terminal access. The encryption devices, if used properly, virtually eliminate the possibility of unauthorized users sabotaging the security computer system through use of a terminal not designed for use in the system. Encryption devices currently available could also allow for remote central processor location for providing continuity of security system operation during disaster recovery situations. For example, a release of radioactive materials might require evacuation of the security control center, but operation could continue through use of a remote control center interfaced to a distributed security system. Currently, the planning for security surveillance during an emergency at most plants is to conduct security functions at a distance through the use of emergency perimeter barricades and patrols.

4.5 COMPUTER SECURITY

The structure of security for computer systems is analogous to the structure of site security systems as described in other parts of this document. The requirements for computer system security include the following:

- design and implementation of the computer system in such a way that access by outsiders is prevented (perimeter deterrents)
- compartmentalization of sensitive programs and data files in such a way that insider usage is limited to those individuals whose responsibility requires access (vital island concept)
- administration controls such as testing, auditing, modification procedures, training, tracking, back-up, etc
- development of a necessary emergency and/or disaster plan.

These needs can all be met by implementing security measures in the following five areas:

1. facility design
2. access control
3. administrative restrictions
4. specifications in the procurement process
5. catastrophe planning.

The remainder of this section will discuss how these needs might be met in each area.

4.5.1 Facility Design for Computer Security

Most of the security measures evident when visiting an NPP facility are considered for implementation in the design of the computer facility itself. These are physical security measures as compared to application or software security measures.

One of the major concerns is that the facility be up and available during a time of emergency. For this to occur in a computer center, several items need to be considered in designing the facility:

1. Strong consideration should be given (where possible) to physically distributing the computer capability for the CAS/SAS in such a way that some redundancy of computing capability is created and maintained. Then when a single facility is rendered unusable, either intentionally or by accident, a second facility established in another physical location will be able, at least partially, to continue to monitor the security of the facility and support any actions necessary to control the event.

Although distributing computer power to more than one location adds to the cost, it does provide the ability to continue operation of the facility while preventive maintenance and upgrades of equipment and software are taking place. Smaller, less expensive computer hardware can normally be used for back-up equipment.

In some cases where there is a higher-than-average expectation that undesirable events will occur, it may be necessary to have completely redundant systems at different locations. Redundant systems would allow the entire security program for the facility to be run on either of two or more hardware systems.

2. Since most mishaps in a computer facility occur not by intent but by accident, several kinds of warning devices should be considered for installation in any CAS/SAS facility. These include devices such as intrusion alarms, smoke and water detectors, temperature variance monitors, humidity control devices, and power supply monitors that will maintain an environment in which the computer hardware can operate dependably.

3. Since dependable, clean power is necessary for the operation of any computer hardware now available, and since access to power will more than likely be the primary target of any attack, the system should have an uninterruptable power supply or battery back-up system that will allow the hardware to continue to run for some time without access to outside power.

4. The fire protection system installed in a computer facility can be either a help in protecting the investment in the equipment or a hindrance. Dry or wet pipe sprinkling systems are not recommended for any of these facilities. A gaseous fire-extinguishing agent (for example, Halon) should be used so that no damage will occur to the computer hardware or the media (disk drives, magnetic tapes, paper, etc.)

5. A major consideration is the physical location of the facility. Areas which should not be considered for the location of the CAS/SAS facilities would be a) the border areas of the site where some kind of direct physical access to the facility would be available from outside the controlled area, b) adjacent to certain vital areas. Either of these locations would increase the probability of damage to one of these facilities.

6. The building or rooms in which the hardware is installed should be without windows, which would provide for the visual monitoring of activity within the facility.

7. Although the sensitivity of the data being processed in the facility is not likely to be such that a shielded facility would be required, some consideration during the procurement process should be given to acquiring hardware that exhibits low electronic emanation. This may

be unnecessary in those cases where the size of the site itself is such that no monitoring of facility activities with electronic surveillance equipment would be reasonably expected.

4.5.2 Control of Access to the Computer

Although the physical security measures protect the facility and the hardware involved, access controls can provide additional protection to the operation of the computer facility. Access controls are particularly helpful in preventing the accidental or unintentional destruction, manipulation, or corruption of data. There are several levels of access controls. These include:

1. access to the facility
2. access to the computer equipment
3. access to the system (user identification)
4. access within system applications (applications passwords)
5. data encryption.

A sixth consideration is that the system should be secure from unauthorized telecommunications access that could bypass the first three levels. A final part of these access controls is the administrative control of the control measures.

Access to the Facility

There are many different ways of controlling physical access to the facility; the most common method is to have guards who monitor individuals as they enter and leave. Monitoring is done by viewing some kind of identification provided by the individual, such as a badge, access card, etc. This is a reasonably sure access control method because not only is the badge or card required but a visual inspection and comparison with the individual carrying the badge is made.

Magnetic card readers are in use in some facilities. Their effectiveness for access control is probably on a par with that of a key and lock, inasmuch as they are only as good as the control of the magnetic card itself. The device is not capable of assuring that the individual using the card is the individual that should be using the card - only that the card has been issued to someone with the authority to enter certain areas of the facility. The magnetic card does have other capabilities, however, for monitoring the movement of individuals in the facility and logging which individuals were in particular areas of the facility.

These two types of physical access can be combined: the guard can be located at an access point to the facility, and the card reader can be used for access to areas inside the area controlled by the guard.

Other options include retina, palm print, and voice identification devices as well as cypher, combination, or key lock devices.

Access to the Computer Equipment

Although an individual may have gained physical access to a terminal or a keyboard that is hooked to a system, additional controls can be installed on the terminal, such as a keylock or magnetic card device, which will verify that an individual should be allowed use of the terminal.

System Access

Once someone has activated a terminal or a keyboard, access to the system will be requested. The system then should have the ability to verify through the use of a password, voice recognition, or some other key, what applications and work this particular individual is allowed to perform on the machine. Passwords should be a minimum of six characters long and randomly computer generated to eliminate the problem of using pet names, birthdates, weight, etc. for an individual's password. This level of security is only as good as the personnel choose to make it. Any sharing of or disregard for the security of individual passwords will make the entire use of passwords of little value as a security device.

Password Access within Applications

A particular application may require certain key words, codes, or phrases to be input before predefined actions can be started. This can also be used in inquiries to files where different fields within the file may have security levels such that an individual may have access to the file, but not to particular records or fields within that file. This level of password or code protection is developed and written into the application itself at the time it is developed. An important consideration here is the speed with which an individual would be able to gain access. In the case of an emergency, several layers of protection of this type may take several seconds to get through and start the action that is desired. This may not be acceptable during response to particular emergencies at the site.

Data Encryption

An additional level of protection can be created by encrypting data or passwords themselves on files in such a way that the individual that accesses the information or a particular application program not only would need to know the passwords, but also the encryption key necessary to decrypt the data. This is probably only worth the effort in those cases where the data is very sensitive, such as in the storing and administration of passwords themselves. Additional time is required in the encryption and decryption of data and should be considered when the speed of response to an emergency situation is considered.

Telecommunications Security

If telecommunication is necessary in a CAS/SAS facility, it should be an internal system using cable or leased lines in such a way that no offsite lines are necessary. If it is necessary to use offsite lines, particularly any kind of dial-in capability, an additional level of security needs to be implemented.

It is recommended that call-back devices be used on all dial-up lines to the facility. This provides a positive check on the person calling and on the telephone from which the call originates. The person dialing in would give a code number that would be checked against an account file maintained on the facility computer system. The call-back device would disconnect the telephone line, find the phone number that goes with the code number given by the user, and dial that number to reestablish the connection. Call back is important even if the dial-in capability needed is within the site because there is normally no way to eliminate dial-in from exchanges outside the site.

Control of Access Controls

As important as the levels of access controls is the control of the control measures themselves. The following discussions consider the control of access passwords, the need for maintaining audit files of system accesses, and the importance of screening people for access authorization.

Most of the access control measures involve the use of codes, passwords, magnetic cards, etc., and it is important that these be established in a controlled way and that they be changed regularly. It is particularly important that codes be changed when an employee who has had access to the restricted facility leaves the employment of the company or when any password, code, badge, or key has been compromised and become available to those who have no need for access. Most rules and regulations set up at other types of facilities indicate that yearly changing of passwords, etc. is usually acceptable. In a sensitive application such as an NPP, it is recommended that the change be much more frequent, possibly quarterly.

Auditing files of system accesses should be maintained. This will provide a trail in case it is necessary to find what action was taken at what location in the event some damage or corruption of data occurs. This also provides logs for monitoring attempted accesses that failed and may indicate an attempt by someone who has not been cleared to gain access to the facility.

Screening of individuals before they are given computer access is of utmost importance. It is important to remember that although someone may have access to the facility and may be able to cause damage in some physical way, significantly more damage may be done by the corruption of the security system than can be done by an individual physically attacking most equipment or devices other than the computer facility. Therefore, those gaining access to the computer facility should be screened in detail. This should be reviewed annually, particularly for those in sensitive areas such as password administration or general facility access without restrictions.

4.5.3 Administrative Measures for Computer Security

Several administrative measures should be considered for the security of the computer system:

- system manager
- risk assessment
- separation of duties during system design and applications.

All these measures are important and need management support.

System Manager

There should be one individual (a system manager) responsible for computer systems and data processing security so that a coordinated program can be implemented. This individual may come from the Information Systems Department, Plant Security, or some other organization, assigned by plant management. However, this individual should have a significant background in computer usage as well as security to assure that the correct security measures will be implemented to protect the facility.

Risk Assessment

In the process of implementing a computer security program, a risk assessment will be necessary. The types of risk to the facility and what kind of security applications may be implemented on each different system must be reviewed in detail before security measures are implemented. However, there is no such thing as total security for a computer system. Sometimes the security program can be overdone by implementing every possible kind of security in the invalid belief that this will increase the security of the system. This is not necessarily true, and the risk assessment will indicate those areas where security measures will be effective and those areas where the risk is minimal and additional measures will be counterproductive. It is important to understand that security measures affect the ability of people to do their jobs. It is possible to overburden the user or make the system unusable by trying to add too much.

Separation of Duties

Separation of duties is an important aspect of computer security. The risk of a single individual causing significant harm can be reduced, although seldom eliminated, by requiring that more than one individual be involved for any significant action to take place. It is important that these measures be designed into applications as well as in the operation of the facility. If an individual has the responsibility for designing a system, writing the code, and then implementing, testing, and putting it into production mode, then that individual can write program instructions would devastate the security or operation of the facility once it is installed. Separating these duties or requiring overchecks would be a safer policy: then two or more individuals would have to combine knowledge before they could sabotage the computer system through its programming.

Separation of duties becomes an important issue in the case of the system manager, who in most installations has carte blanche access to the system. The

ability of the system manager to access applications and data or to initiate events should be restricted. The system manager should manage the system, not necessarily the applications or the production of that system.

4.5.4 Specifications for Procurement

The needs for security must be given consideration and be included in the bid specifications during procurement of the computer system. A security program may have been developed that requires security measures that a particular piece of hardware cannot provide--password or access security features, for instance. Normally, if that is the case and the hardware has been purchased, those security measures will simply be ignored, avoided, or never implemented. Therefore, it is necessary that procurement specifications include the capabilities that are needed to implement the security measures as they have been designed. Section 5.1 discusses the system specification.

4.6 WORKSPACE DESIGN

To fully and efficiently meet the primary objectives of a physical security system, the workspace must serve the needs of both the computer manager and the security personnel. The human factors associated with a computer-managed physical security system are numerous; however, they can be organized into three primary categories:

- Equipment Layout and Displays
- System Space Needs
- Work Station Environment.

These categories are examined in the following sections. The discussions focus mainly on how each category affects hardware design, given the capabilities and limitations of the hardware and the personnel--the two major "subsystems" of the total physical security system. Human factors design principles are applied to the categories to make the hardware subsystem compatible with the human subsystem.

4.6.1 Equipment Layout and Displays to Meet Task Requirements

As previously discussed, the system must be designed to meet a specified list of functions or design goals. According to Meister (1971), the system designer and the human factors specialist must answer questions dealing with the allocation of functions, the analysis of tasks, and the identification of human-machine interfaces. As a consequence, several analyses must be performed (Meister 1971):

A. Function Allocation and Verification
   1. Determine system requirements.
   2. Determine system functions.

3. Allocate functions between humans and machines.
   a. Specify alternative configurations and functions.
   b. Verify that the human can perform the assigned functions and can satisfy system requirements.
   c. Select the most effective concepts by comparing alternative designs.

B. Task Description and Analysis
   1. Describe and analyze tasks.
   2. Determine equipment requirements implied by tasks.
   3. Analyze tasks in terms of their demands.

C. Identification of Human-Machine Interfaces
   1. Select appropriate interface components.
   2. Arrange control-display components (most efficiently and effectively).

Functional Layout to Meet Task Requirements

The placement of hardware in the CAS and SAS depends on the tasks that must be done, the hardware systems needed to do the tasks, the environment necessary for the hardware, and the space needed by personnel. In a computer-managed physical security system, the hardware generally required in the CAS and SAS includes:

- a bank of video monitors for closed-circuit television (CCTV)
- one or more data input stations, including a monitor, keyboards, or other controlling devices
- one or more printers
- communications equipment, including telephones, microphones, loud speakers
- desks, chairs, and other office furniture
- files or bookcases containing procedures and other filed or logged materials
- other equipment which may not have been specified but is necessary.

The other subsystem that must have a place designed into the CAS and SAS is the security personnel. One or two persons must have sufficient space to perform their tasks, which generally consist of using all of the above hardware and thereby coordinating all plant security efforts. All of the equipment must be easily accessed by these persons.

Display Requirements to Meet Task Requirements

As mentioned in the previous section, several types of displays are included in a physical security control center. These displays include

- CCTV monitors
- computer data monitors
- logging printers
- procedures manuals.

Each of these display devices has a different purpose and several possible design configurations.

CCTV Monitors. Closed-circuit television monitors are used in the CAS and SAS to receive visual display of remote security areas within the plant. The use of television cameras provides a continuous video image of sensitive control sites. However, for every camera to be seen continually, a dedicated TV monitor would be required for each camera. Since humans have an upper limit on the number of visual inputs they can effectively handle, a workable system must limit the number of monitors that must be observed. Also, the space available to the security station is minimal, so it is desirable to reduce the number of CCTV monitors to as few as possible.

The number of CCTV monitors in the CAS/SAS can be reduced in two ways. The first is to rotate the camera presentation by switching monitors among 3 or 4 cameras. Views should be assigned priority so that the most crucial areas are placed on the most central monitors. Also, fewer cameras should be rotated on the most critical displays. A second reduction method involves having the cameras actuated when an alarm occurs. Vital areas could always be shown, then changed when an alarm trips. The system needs enough monitors that the most important areas could alarm and be seen simultaneously. Although cameras are normally controlled by the computer system, they should be manually switchable (Sandia National Laboratories 1979).

Finally, CCTV systems should also be accessible at the operator's main data monitor, which is connected to the computer and keyboard, so that the operator can exert control from the console for activities such as routine remote access. In contrast to the dedicated camera monitors, which are mounted on a wall behind the operator, the main data monitor is located on the operator's desk or work station. Its other functions and design characteristics are discussed in the next section.

Computer Data Monitor. The computer data monitor is a second display source used in physical security control rooms with computer-managed systems. Since the early 1970s, European governments have set standards regarding the design and use of these monitors, also called video display terminals or VDTs (IBM 1984). Consequently, major computer designers and manufacturers have built VDTs to standards that meet or exceed these standards. In the process, the designers have done research in the area of human factors principles of VDTs. Recent journals have reported research concerning many human factors related to VDTs, including

- efficiency (Gould and Grischkowsky 1984)
- eyestrain (Hedman and Briem 1984)
- reading speed (Kruk and Muter 1984)
- medical effects (Smith et al. 1984)
- display format (Long et al. 1984)
- color coding (Luder and Booker 1984)
- performance (Giansas 1984).

Many more examples exist in the literature. Of course, one must exercise judgment as to the use of VDTs for information and data display. It is quite easy, for example, to include too much information on a VDT because it is technically feasible. In this example, too much information might include

- too many data points on the screen
- presentation in too little time
- presentation in a form not ordered for efficient comprehension.

Another important consideration in using VDTs for information transmittal is the style of the characters and symbols displayed. Research on display characteristics for VDTs has produced many guidelines The following list is adapted from Woodson (1981):

VDT Size--In typical console applications, the VDT diagonal screen size should be 12 to 19 in. (30 to 48 cm) for typical viewing distances of 18 to 22 in. (46 to 51 cm).

Symbol Size--Alphanumeric symbols should be about 25 minutes of arc when there is a possibility of glare or bad lighting. For typical viewing distances this is about 0.15 to 0.26 in. (0.36 to 0.65 cm).

Symbol Separation--For symbols to be seen as clearly separate, 0.1 minutes of arc is required. For typical viewing distances this is about 0.00058 to 0.0010 in. (0.0015 to 0.0026 cm).

Display Resolution--For digitally generated images that may include handwritten characters, at least 125 lines per inch are needed.

Display Brightness--A line brightener of 50 (± 40) foot-Lamberts is required under normal light levels with adjusters for different light conditions.

Alphanumeric Symbol Width/Height Ratio--A ratio of 2:3 to 3:5 is best for maximum legibility.

Between-Character Spacing--Optimal spacing between characters is 45% of character width with an acceptable range between 20% and 60% of character width.

Alphanumeric Symbol Style--The closer the characters conform to the other standards, the less this category matters. Vertical characters are preferred. However, sloping characters or bold-faced characters can be used for emphasis.

Viewing Distances--The optimum for the typical console operator is 18 to 22 in. (46 to 51 cm) for a 12- to 19-in. screen. A maximum distance of 20 ft (6 m) can be used, but all character values must be adjusted to greater size.

Viewing Angle--This should not be less than 30° from the perpendicular axis. For the seated operator, the viewing angle should not exceed 30° vertically or horizontally.

Color--Multicolor VDT displays are suggested when it is desirable to present typical encoding material for easy differentiation (enemy vs friendly targets) or other graphic information (scales, curves, callouts, etc.). Red, green, blue, and yellow are the most readily differentiated colors.

Logging Printers. Logging printers are needed in the CAS/SAS to provide a current record of access and to fulfill plant logging requirements imposed by regulatory agencies. Two problems with the printers being placed in the main security center are noise and space consumption.

Printers come in many sizes and shapes, and the principal location may be changed to an out-of-the-way place. Ideally, printers could be moved to another room, which would eliminate the space problem. However, if they must be located directly in the control room, they should be placed with three considerations in mind. First, following an analysis of personnel movements in trial arrangements of the hardware, the printer should be placed in a position that does not have much traffic. Second, the position should also be away from typical working or congregating places to avoid noise problems. Audio requirements are discussed later. Finally, paper loading for the printer should be easy enough that personnel will not injure themselves while trying to handle paper or equipment from an awkward position. Paper trays should be between 20 and 40 in. (51 to 101 cm) off of the floor. A clear path should be allowed for moving the paper to its location for loading.

Noise is one of the problems with printers in the control room. The usual noise created by printers is an explosive sound, usually in the range of 65 to 75 dB at distances over 4 ft. At this level, speaking to someone over 3 ft away requires a raised voice, and telephone use is difficult. At these levels, OSHA (Occupational Safety and Health Administration) permits unlimited exposure. However, research has shown that noise may be degrading to vigilance tasks, complex mental tasks, and tasks involving complex motor skills (Hutchinson 1981), all of which are necessary for proper security functioning. Also, these degradations are exacerbated by occasional 80-dB bursts of noise. The best solution to the noise problem would be to remove printers from the main room. If this is not possible, covers can be procured that muffle the sound to a point to which the noise is barely perceptible. If the printer is

located in the CAS and SAS, these covers could become extremely important. One of these solutions should be applied to mitigate printer noise.

Procedures Manuals. Procedures manuals can appear in two forms in the control room. First, a hard copy version may be available in which loose-leaf pages are usually bound in ring-type notebooks. A second method is to use the console computer as a presentation medium.

The use of the hard copy procedures manual is the most common method for reference presentation. In this method, ring binders are filled with loose-leaf pages containing material describing actions and precautions necessary for security personnel to perform their jobs.

The computerized version of the procedures may contain the same information and add different methods of retrieving the information. Given a certain set of circumstances, as monitored by the computer, the automated manual might suggest the proper set of procedures. Or, if needed, a specific procedure can be called to the screen without scanning pages to find it.

4.6.2 System Space Needs

As previously alluded to, the layout of the work area is quite important to the efficiency of the control room, especially if two or more persons are required to work. Space requirements can quite often lead to possible trade-offs in hardware choices with the best system being the one that fits. Within this arrangement of the hardware, however, must be the human operator. Necessary controls and displays must be available to the operator without requiring extraordinary strength or agility. Comfort must also be considered. There are three primary discussions in this section. The first involves techniques for placing hardware systems so that required operator movements can be made. The second involves the physical dimensions of the space needed by the operator at the work station. Finally, the third covers features of the ambient environment that should be specified by design.

System Placement

One of the most important but difficult aspects of human-machine design deals with arrangement of the work area, especially when more than one person must work in it. From other engineering discipline, the field of human factors design has adapted several techniques that aid in efficient and safe work area arrangements (Thomson 1972). Among the techniques listed are

- use of work area mockups (reduced scale)
- link analysis.

Using these techniques before equipment installation and operation can help to prevent many unnecessary backfits or problems associated with poor design.

Mockups (Reduced Scale). A mockup is a nonfunctional model of equipment used in a control room. A full-scale mockup is an exact duplicate of a control room, including machines, key pads, readouts, etc. However, even though a full-scale mockup is good for a realistic concept of size and an articulated measure of the effects of human body movement, they take up as much space as the normal control room and are therefore impractical. A reduced-scale mockup is also a valuable tool in the early stages of designing human-machine systems involving several people in a work area. When constructed with reasonable accuracy, tolerances can be measured and scaled very precisely. The reduced-scale mockup can be portable and is certainly more easily manipulated. Modifications can be made quickly and easily. The required clearances around machines can also be layed out to prevent possible infringement where space constraints are important.

Link Analysis. Link analysis is a second technique that provides the information needed to produce an acceptable arrangement of people and machines in a system. Used with a mockup, just described, this process could provide clearer understanding of required spaces and work areas. The rationale behind the link analysis is that the optimum arrangement can be found only by optimizing different links (such as communication and movement) that are important in that work area.

A "link" is a connection between a person and a machine or between people. When an interface occurs, this is considered a link. For example, if a security officer acknowledges an alarm, that motion is a link. Links include walking, talking, seeing, and movement of material and information. Ordinarily, links between machines can be neglected if the length of the link is of no importance in the system. Thomson (1972) describes nine steps necessary to complete a link analysis:

1. Draw a circle for each person in the system and label it with a code number for the person's function.

2. Draw a square for every item of equipment used by the human operator and label it with a code letter. It makes no difference how the circles and squares are arranged so long as there is some room between them.

3. Draw connecting lines between each person and any other people who have any direct interaction in the operation of the system.

4. Draw connecting lines between each person and any machines with which the persons must interact.

5. Redraw the resulting diagram, reducing to a minimum the number of crossing links to obtain the simplest possible arrangement.

6. Evaluate each link by one of the following methods:

    a. importance - Have an experienced person rank each link according to its relative importance by assigning low numbers to unimportant links and high numbers to important links.

b. frequency - When frequency is used as a criterion, obtain data from the simulated or operational use of the system. Use these data to rank each link according to the amount of use it gets during operation. Enter these rankings on the links.

c. both frequency and importance - Have experienced observers judge the relative weights to be given so as to assign a single composite value to each link.

7. Redraw the diagram so that the links having the higher values are shorter than those having lower link values, and reduce the number of crossing links. This is the optimum link diagram.

8. Redraw the link diagram to fit the available space, or design the space to fit the diagram.

9. Confirm the final analysis on a scale drawing or mockup (as described in the previous section on mockups) of the actual positions of people, machines, and spaces included in the system.

Work Station Dimensions

Equally important to the efficient operation of the physical security work are the dimensions of the work station, or computer console. Once again, the problems associated with the layout are specific to each console, but some general maximum and minimum dimensions can be applied.

Seat Dimensions. For a proper chair, Hutchinson (1981) reports several dimensions that should be observed for the male operator. First, seat height should be adjustable within a 15- to 18-in. (38- to 46-cm) range. The seat depth should be no more than 15 in. (38 cm). The back rest should be at least 6 in. (15 cm) high and no wider than 13 in. (33 cm) for elbow clearances. It should permit reclining 5° to 15°. Elbow rests should be 7 to 9 in. (18 to 23 cm) above the seat surface. A desirable length is 9 to 12 in. (23 to 30 cm), as measured from the seat reference point (SRP). The SRP is where the seat surface and seat back intersect. There should be about 19 in. (48 cm) between the two arm rests.

Workbench Dimensions. The height of the workbench should be between 26 to 30 in. (66 to 76 cm) for seated operations. The standard table height is 29 in. (75 cm). The work surface may be slanted toward the operator up to 15°.

The undersurface height should be a minimum of 25 in (64 cm) for thigh and knee clearances. If there is a vertical surface under the work surface, as with a console or counter, the minimum depth of the undersurface for knee clearance should be 18 in. (46 cm). The minimum depth at the floor should be 24 in. (61 cm) to allow room for the feet.

The back of the console should be 28 in. (71 cm) horizontally from the operators' shoulder level. This standard is for young, healthy males. Console

panel fronts may be angled back so that they are easier to see and reach than vertical panels. The most important displays should be immediately at eye level or just below.

4.6.3 Work Station Environment

The final work space consideration is the ambient environment--its effects on people and machine systems. The primary environmental considerations discussed in this section are lighting, noise, and temperature.

Lighting

In the physical security control room, several types of work must be performed, involving many lighting requirements. General tasks requiring the need to see include reading procedures, watching closed-circuit television (CCTV) monitors, reading information from computer monitors, and reading printouts from a logging printer. These tasks fall into two categories: reading from printed pages and watching video monitors.

The effective lighting on a work surface is the sum of all the light rays striking the surface, including rays directly from lamps and reflected from walls or other objects in the room. Usually, the source document (paper or monitor screen) is a critical factor in determining how much and what kind of light should fall on a work surface. White paper has a reflectance factor of about 70% to 80%. This means that if the desired brightness of the paper is about 30 milli-Lamberts, the intensity of the light falling on the paper should be about 400 lux. An average light level in an office is usually about 400 lux.

A monitor, on the other hand, generates its own light to create the information-carrying image on its surface. Although there is a range of the adjustability for the image brightness of a terminal, the range is limited and does not automatically change with ambient illumination. Also, glare on screens from all sources must be guarded against so that monitors may be viewed clearly.

Noise

Acoustic noise poses several engineering and human factors problems. While few machines have noise levels that could cause physiological damage to nearby workers, many machines have noise levels that require people to make compensating adjustments while talking to each other. One example is the control room printer. Other machine noises neither interfere with oral communication nor present a physiological hazard, but they are nonetheless objectionable. This is subjective, and difficult to address. In any case, attempts at reducing objectionable noises are usually associated with increased cost and operator inconvenience.

One effective way to mask unwanted noise is to introduce low-level white noise. White noise is an overall sound level without any perceptible pattern.

This type of noise does not interfere with task performance because it is heard throughout the day and people readily adapt to it. A totally quiet environment would probably be distracting. A desirable work environment would permit some ambient noise that does not interfere with desired sound.

Temperature

A final environmental consideration involves the ambient temperature of the work station. Recent temperature requirements in office situations have brought about research which suggests that temperature level affects complex mental tasks as well as motor functions. An optimum temperature range for performance seems to be between 76° and 80°F in the summer and between 68° and 72°F in the winter.

4.7 USER INTERFACE DESIGN

Good design of the physical workspace is important but by itself is not sufficient to ensure effective and reliable job performance by the CAS and SAS operators. Of equal importance is the way information is displayed to the operator at the terminal and the way in which the operator enters commands and data to the system. Documents are available that provide detail guidelines on data entry and data display (EPRI 1984; Smith and Aucella 1983). The following section of this report summarizes many of these guidelines as they apply to computer-managed physical access security systems.

4.7.1 Data Entry

Data entry refers to input by the user of data items to be processed. Command inputs or option selections are considered separately in the section on sequence control. Data entry is not the major user interface for security systems but some data entry is required for data base updates.

Data entry functions should be designed to meet the following objectives (Aucella 1983):

- establish consistency of data entry transactions
- minimize input actions and memory load on the user
- ensure compatibility of data entry with data display
- provide flexibility of user control of data entry.

The design of the data entry functions determines the speed and accuracy of operators in entering information into the system. The formats used for entries, the entry devices chosen, and the mechanisms used to identify and manage errors are each important components of the data entry task.

The following guidelines can aid the system designer in preparing the user interface necessary for data entry.

Entry Formats

- Entry methods, control groupings, and entry formats should be consistent in appearance and used consistently across applications.
- Formatting displays for data entry can greatly simplify the data entry task.
- Form-filling dialogues may be used for applications in which several related inputs are easiest to make as a group.
- Forms should be standardized as much as possible.
- Entries should be permitted in any order on the form.
- Available default values should be displayed and entry by replacement used when these values are available.
- Data entry techniques should be as simple and consistent as possible.

Entry Devices

- Switching between data entry devices should be minimized as much as possible.
- Cursor positioning devices are frequently used for position designation in the data entry process. The mouse, joystick, and function keys are the most common devices. Light pens, touch screens, and track balls are other available methods.
- Touch screens are preferable to light pens as a direct pointing technique since they do not require a cord attachment.
- All entries should result in some kind of sensory feedback, for example, visual feedback and tactile feedback for key entries or auditory feedback for touch screen entry.

Keyboard Entry Devices. Often referred to as the QWERTY keyboard, the standard arrangement of certain keys should be maintained in order not to confuse experienced users. These long-existing standards dictate the location of most of the keys, such as numbers, letters, symbol keys, and the standard function keys such as shift, new line, and backspace. These keys are in the touch typing area and are used most of the time by operators, without looking and without breaking a set rhythm for maximum speed. Special function keys, such as CLEAR, can be located outside of the touch typing locations, and usually require hand movement away from the home position. These keys are located there because they are infrequently used.

Efficient keying requires that keys function with minimum adequate force and sufficient displacement to provide muscular feedback to the operator. Key forces for current high-production keyboards are in the range of 40 to 125 grams with key displacements of 3 to 5 mm.

The more proficient the operator, the lighter the touch can be. If too little force is required, however, extra keys may be struck accidentally; if too much force is required, some keys may fail to be actuated because the operator did not press hard enough.

Designed to be comfortable for the operator's fingers, keys typically have a top surface that is about 1/2 in. square on a 3/4-in. center and have a slightly concave surface. Home position keys may be more concave than the others so that the fingers may be properly placed. Key tops may have a matte finish to prevent reflections from overhead light sources, making labels easier to read. The matte finish makes the top of the key less slippery.

Error Management

- An error management system should be incorporated into the data entry scheme for error identification and correction.
- The system should automatically check for format errors, missing data, and unlikely or destructive entries.
- Error messages should be specific and should convey all necessary information for correction.
- Errors should be correctable immediately upon notification.

4.7.2 Sequence Control

Sequence control refers to the logic and means by which inputs and outputs are linked to become coherent transactions. Sequence control governs the transitions from one transaction to the next. This section is of particular importance to computer-managed physical access security systems because the design of the sequence control affects how the CAS and SAS operators respond to alarms, communicate commands between the CAS and SAS, control CCTV cameras, and perform other functions in their day-to-day operations.

General sequence control design objectives are:

- consistency of control actions
- minimal control actions required of the operation
- minimal memory load on the operator
- compatibility with the user's needs
- flexibility of sequence control.

A fundamental decision in the design is the selection of the dialogue type(s) that will be used for sequence control. A mixture of dialogue types may be necessary since different dialogues are appropriate to different jobs and different kinds of users. The selection of dialogue types is based on anticipated task requirements and user skills. Another important aspect of dialogue choice is that different types of dialogue imply differences in system response time for effective operation. An estimate of the implied requirement for user training and for system response time is given below for eight general dialogue types (Aucella 1983):

Dialogue Type	Required User Training	Required System Response Time
Question and Answer	Little/None	Moderate
Form Filling	Moderate/Little	Slow
Menu Selection	Little/None	Very Fast
Function Keys	High/Moderate	Fast
Command Language	High	Fast
Query Language	High/Moderate	Moderate
Natural Language	Moderate (potentially little)	Fast
Interactive Graphics	High	Very Fast

The design of the dialogue should allow maximum flexibility to permit the user to undertake whatever task or transaction is needed, at any time. This is especially important to a security system since alarms and responses must occur in real time. A recommended form of flexibility is the provision of alternate modes of sequence control for experienced and inexperienced users. In a command-language dialogue, optional guidance might be provided in the form of a menu for beginning users or a menu for infrequently used commands.

Some additional guidance for the operator-computer dialogue is summarized below:

- The language that is used should be familiar to operators and conform to the standards and conventions at the facility.
- Terminology should be applied consistently throughout the dialogue.
- Excessive use of abbreviations should be avoided.
- Dialogue progression should be under the control of the operator at all times except as required to bring attention to alarms.
- Prompts should specify any required operator inputs for progressing to the next step of a sequence.

Menu selection dialogues minimize demands on operator memory and training, but require that all inputs be anticipated in advance. Guidelines for menu dialogues are:

- Menus should maximize breadth rather than depth.
- Only relevant options should be displayed on a single page if possible.
- When multiple pages of options are used, a hierarchical menu organization should be used.
- If a hierarchical arrangement of options is used, then
  - High-level items should serve as labels, not choices.
  - The hierarchy should be made apparent using indentations.
  - Items within groups should be used where possible.
  - An indication as to current position in the hierarchy should be provided.
- Point-in (touch) selection is the preferred technique for option selection, with cursor positioning as a good second choice.
- Only one option selection should be required for a given menu.

Function keys can be a useful dialogue format for a limited number of frequently used entries that are continuously available. Guidelines for the use of function keys include:

- All function keys should be clearly and distinctly labeled.
- Keys should be labelled informatively to designate a function they perform.
- For a single-purpose function that is continuously available, just one label should be on the key.
- If a function key is used for more than one function, the user should always have some convenient means of knowing which function is currently available.
- When a function key performs different functions in different operational modes, those functions should be made as consistent as possible.
- Function keys should be grouped in distinctive locations on the keyboard.
- The layout of the function keys should be compatible with their importance.

Sequence control also involves the operators' ability to advance through stored information. For advancing through alphanumeric data, the following guidelines apply:

- Whole-page advancing is preferable to scrolling.
- Function keys are desireable page advance devices rather than typed-in commands.
- A page number should be provided as well as the total number of pages in the sequence.

Graphic displays may also span more than one page, and sequence control for graphic data is also an important dialogue design consideration. Hierarchical advancement should be used, where appropriate, to provide easy access to many low-level displays and to preserve the legibility of the individual display.

Command language dialogue should be considered for the routine tasks performed by the CAS and SAS operators because the users are highly trained and require efficient performance from the system. The following guidelines apply to command language dialogue:

- An entry area for the command input should be provided in a consistent location on every display, preferably at the bottom.
- The words chosen for the command language should reflect the users' point of view.
- Abbreviation of entered commands should be permitted to facilitate entry by experienced users.
- To minimize confusion, words in a command language should be chosen to be distinctive from one another and to emphasize significant differences in function.
- When a command entry is not recognized, the computer should initiate a clarification dialogue, rather than rejecting the command outright.

4.7.3 Data Display

The design of the data display for the CAS and SAS operator consoles is extremely important. The physical characteristics of the displayed data must be made consistent with the capabilities of the human perceptual systems (primarily visual), and the data should be laid out in a way that promotes the rapid identification and understanding of relevant information.

The general objectives to be met in the design of data displays are:

- There should be as much consistency as possible over all of the displays within the system.
- The displays should be designed to enhance efficient understanding by the user.
- There should be minimal memorization required of the user.
- The data display should be flexible for user control.

Alphanumeric display codes will be part of most of the displays in the CAS and SAS. To ensure the legibility of these displays, the following guidelines apply:

- Characters should subtend between 15 and 25 minutes of arc with 17 minutes of arc as a preferred minimum.
- Character font should be simple and unembellished (for example, Leroy and Lincoln/Mitre).
- A 10 vertical component letter style or 7 x 9 matrix should be considered the minimum resolution for good legibility.
- The letter width-to-height ratio should be between 60% and 85%, with 75% as a reasonable standard.
- Between-character spacing should be between 20% and 60% of character width, with 45% as a reasonable standard.
- Upper case only should be used except where continuous prose is displayed (mixed case should be used for continuous prose).

The information on the displays should be presented in a manner that aids the operator in quickly locating information that is needed. Information can be grouped to enhance the legibility of the display. The basis for grouping data is a function of the type of data to be displayed and how they relate to the operator's task. For example, it is desirable to organize alarm messages by their importance (severity) and by their chronological order.

Displays that are designed to include graphics symbols should adhere to the following guidelines:

- Graphic symbols should subtend a minimum of 20 minutes of arc.
- Graphic symbols should be composed of at least 16 vertical elements.

- For the appearance of continuous lines, line elements should be separated by less than one minute of arc.

- Alphanumeric descriptors (for example, ON/OFF) should be unambiguously associated with their corresponding components.

Coding and highlighting can be used to bring the operator's attention to specific items on the display, for example alarm notification. The single most important guideline for coding displays is that the coding be consistent and complete. Color coding, if used sparingly, is an effective means of bringing attention to selected parts of the display. Blink coding is also an effective way of bringing attention to a part of the displayed data. Blinking should be used only to obtain the operators' attention or to indicate an urgent condition. Inverse video and brightness are another way to bring the operator's attention to specific items or areas.

4.8 OTHER DESIGN CONSIDERATIONS

The previous sections have discussed considerations that are important for the design of any computer system but which needed to be addressed in detail in the context of a computer-managed physical access security system. This section briefly considers other design issues and provides references from which you can obtain detailed guidance in areas where you desire further information. The issues are economic analysis, system integration, software design, and software development and tracking.

4.8.1 Economic Analysis

When a utility considers the feasibility of either installing a computer-managed security system or updating an existing system, decisions will need to be made on alternative designs. Many times these decisions must be based, at least in part, on an economic analysis. Rigorous guidelines to effectively aid the decision process can be found in handbooks dealing with economic analysis (Cardwell et al. 1984; DOE 1984).

The handbooks referenced can be valuable guidance sources to find out how to perform an economic analysis. The analysis described in the handbook is based on events (what steps to take when) and techniques (present value analysis, uniform annual cost, savings/investment ratio, discounted payback analysis, break-even analysis, benefit/cost ratio, and sensitivity analysis).

The system integrater should be involved with this process from the outset to help provide a smooth transition from system conception and design to implementation and maintenance.

4.8.2 System Integration

Regardless of the apparent simplicity of requirements for implementing a computer-managed security system, and regardless of which vendor is selected to supply hardware and software, short-term and long-term problems are certain unless the system is effectively integrated. The system integrater should be involved at the outset of the planning and design of the security computer system to avoid expensive redesigning or retrofitting. A capable integrater is knowledgeable of NPP's and computer technology and system implementation practices. The integrater should be able to follow requirements development and implementation and effectively coordinate user and supplier communications. The system integrater needs to be able to aid the NPP in providing continuity of services between vendor products and support and NPP support.

The utility should use great care in choosing the person who will be the integrater. The integrater's value to the organization depends on three attributes. These are technical talent, the ability to understand management concepts, and the ability to communicate.

4.8.3 Software Design

Software design, whether done by the utility or a vendor, is an important part of the overall system design and has a tremendous impact on the final system. The goal is to configure and design software such that the limited testing possible can provide a reasonable degree of reliability.

Software design begins with formally defining the requirements of the users. Formalizing these requirements can be a difficult task, but avoidance of this basic task can result in a system that does not do the needed job. The next step is to translate the users' requirements into a system design. In this phase, the hardware configurations must be specified along with communication links between components of the system. After this has been completed, the software design phase can occur. Continuous verification and validation is necessary in each of the design phases. Verification emphasizes checking the consistency of the design at each step, and validation emphasizes checking the design for consistency with the users' requirements before implementation.

The design process can be a difficult stage of the project. In recent years, software engineering methodologies have been developed to aid the designer. These methodologies have been effective in opening up communication between the designer and the user and in verifying the consistency of the design. Several methodologies are now in use by software engineers and computer scientists (Jensen and Tonies 1979; Dahl, Dijkstra, and Hoare 1972; Jackson 1975; Yourdan and Constantine 1976). The choice may depend on the application or the designer's preference.

4.8.4 Software Development Tracking

In many cases the utility will purchase a "turn-key" security computer system from a vendor and will not find it necessary to predict and plan an extensive software development project. However, security systems may need comprehensive upgrading, and some utilities may have sufficient expertise to undertake the initial development or upgrades in-house. For those cases tools are available to project and track the progress of the project.

The Gantt chart can be used as a scheduling device (Gido 1974; Harrison 1981). It is a simple bar chart that shows each event and its duration and is used primarily to compare the project's schedule with its actual progress. The Gantt chart fails to show the relationship between one event and another. However, it's simplicity is an important advantage over other methods. Managers are used to working with charts, and in relatively simple projects a Gantt chart will easily communicate a schedule and its status.

A PERT (Program Evaluation and Review Technique) chart is a diagramming technique for planning and evaluating progress on complicated projects (Evarts 1966; Hansen 1965; Harrison 1981). Two symbols are usually in a PERT network: the circle, which is used for an event (milestone) in a project, and the line, which represents the activity to be completed before the milestone is reached.

The planner must first determine and list all of the steps in a project. A significant step in creating a PERT chart is then determining which events are dependent upon others. Then the planner must estimate the time for each step. The completed PERT chart will show the steps in the project and the dependencies within the steps. By studying a PERT chart a manager can recognize critical steps and track these closely to determine when a critical step falls behind schedule. Another advantage of PERT charting is that it requires thoughtful project planning from the manager to create the PERT chart.

Warburton (1983) recommends a variation of the Putman model to predict and manage software development projects. This is a management tool that uses manpower data as input and produces cost and schedule estimates. Using the Putman model, historical data on completed projects can be used to generate likely cost and schedule estimates on future projects. The second use of the model is to predict costs and schedules while a job is progressing. The model provides realistic projections that can be compared with actual milestones. A complete description on the use of this model can be obtained from Warburton (1983).

5.0 SYSTEM SELECTION AND INSTALLATION

The system design phase determines and documents the functions to be performed, the performance standards to be met, the inputs and outputs to be processed, and the reliability requirements to be imposed upon the system. Once the design of the system has been completed, the next step is the development of system specifications for the purchase of hardware and software. Most nuclear power plant staffs do not have sufficient resources internally to develop software and assemble the hardware. Therefore, they will need to write system specifications and select a vendor to provide and install the system. This section of the report outlines the preparation of a system specification, discusses vendors and vendor selection, and provides guidance on system installation.

5.1 SYSTEM SPECIFICATION DESIGN

The system specification has two major functions: 1) it serves as an aid in the selection of a vendor, and 2) it provides a way of specifying exactly what the selected vendor must provide. The specification is very important to the bidding process. Competing vendors are encouraged to bid the costs of functionally similar equipment and software. This gives the utility a meaningful basis for comparing prices. The utility can then select the vendor that can provide the most cost-effective system that meets the performance specifications.

A good specification is very important to the implementation of a computer-managed physical access security system. Before a good specification is written, the system performance criteria must be established and the system well-planned. The specification lists the functions that the system must perform as well as required vendor support services. The utility should provide vendors with all the information needed to price equipment and services and to write an acceptable bid proposal.

The system specification should deal primarily with the functions of the computer system and specify what the system should do rather than how it should be done. There may be alternative ways to perform the specified functions, so the bidders should have the freedom to propose different methods. This approach benefits the utility staff by providing the opportunity to review different system designs and choose the system that best accommodates the utility's security requirements.

Based upon start-up ideas from Shidal (1979), there are five suggestions to follow before writing the specification.

1. Obtain copies of system specifications that were successful for similar applications. These may be obtained from other utilities or they may be provided by prospective vendors. Although the system requirements may not be exactly the same, there will be much valuable

information that should provide a starting point and help to develop a check list of things which are important.

2. Communicate with other utilities who have recently purchased and installed computer-managed physical access security systems. This communication will be more helpful if it occurs between both security personnel who use the systems and the engineering staff who are responsible for the installation and maintenance of the system. Maximum benefit can be gained by contacting enough utilities to obtain information on each vendor's system. Finding out the problems other utilities encountered and their solutions to these problems can save many headaches later on.

3. Use professional organizations. These may be computer-oriented organizations or industry-related organizations. The goal of these organizations is to share technical and professional knowledge. These are excellent places to make contacts. The shared learning experiences of the members can prove to be invaluable.

4. Review technical journals to obtain evaluations on hardware and software. Magazines, journals, and newsletters can also offer research material. In addition to general computer journals, security publications can be reviewed to obtain information specific to security systems.

5. Obtain information from vendors. Many times it is possible to arrange for a demonstration of their equipment. They are always willing to provide literature on their systems.

The following is an outline of a typical system specification. Appendix A explains the purpose of each component of the specification and suggests details to include. A specific example of a system specification for an industrial process control system is given in Skrokov's (1980) handbook on the subject.

Outline of
Typical System Specification

1.0 Introduction
- 1.1 Scope
- 1.2 Bidder Qualifications
- 1.3 Bidding Instructions

2.0 Functional Description
- 2.1 (Function Specification 1)
- :
- 2.N (Function Specification N)

3.0 Hardware Configuration
    3.1 Major Configuration of (Item 1)
    :
    3.N Major Configuration of (Item N)

4.0 Environmental Constraints

5.0 Programming Languages

6.0 Operating System Software and Diagnostics

7.0 Documentation

8.0 Acceptance Testing

9.0 Installation and Maintenance
    9.1 Installation
    9.2 Maintenance
    9.3 Spare Parts
    9.4 Consumables Supplies

10.0 Training

11.0 Project Management

12.0 Terms and Conditions

5.2 SELECTION OF SYSTEMS

Earlier sections of this document discussed NPP security system components and functions, requirements for computer-managed security systems, design methodology, and the generic translation of functional requirements into specific hardware, software, and associated documentation. This section reviews methodology for system selection.

The task of system selection is more complex than reviewing manufacturers' responses to a bid proposal. System selection begins during the functional requirements phase and extends into analysis and design. Proper system selection should include long-range planning integrated into the system requirements and the synthesis of information from a variety of reliable sources. The system selection process includes using proven methods to select a vendor from those submitting proposals. The selection process ends when a system has been delivered and acceptance testing has been satisfactorily completed.

Even though the selection process appears routine, it is a process that is laden with potential problems and has negatively affected many computer system users. One author has stated that somewhere between one-third and one-half of computer systems installed were improperly selected (Edward 1977).

System selection methodology as presented in this section focuses on current vendor information and bid review procedures. A list of important items to consider are presented, and information sources for vendors are discussed. Typical vendors of computer-managed security systems are listed and some general comparisons made.

To aid utilities in making a system selection, four general approaches to bid review are outlined. The goals of using these methods are to

- select the best system available for a specific application
- be more objective in evaluation approaches
- be systematic when considering intangibles
- be as open and fair as possible.

5.2.1 Current Vendor Information

The primary sources for information on vendors were NPPs that are using or are planning to implement computer-managed security systems. Their input was used to obtain an initial list of vendors and to gain insight on system experiences and problems. Every effort was made to locate suppliers of complete computer-managed security systems for NPPs. Vendors who may have been omitted were overlooked inadvertently.

Seven NPPs were visited to obtain direct information on how computer-managed security systems functioned, on the strengths and weaknesses of typical systems, and on the suppliers of these systems. Most of the users surveyed were satisfied with the systems that they were using; however, all sites indicated that most problems occurred just after installation and that these problems had been corrected after the first year.

All of the computer-managed security systems that were reviewed performed some combination of the following functions:

- perimeter intrusion alarm monitoring
- access monitoring and control
- closed-circuit television monitoring
- data gathering, processing, and archiving
- personnel access data base capability
- computer access control for data and/or command privilege
- communications
- watchtour and duress alarm features
- tamper-sensing sensitive cabling and alternate route communications on communications failure.

Table 5.1 lists the major computer-managed security system vendors and shows the features available in the systems that they are offering. The following is a list of those vendors with addresses for user reference.

Arvin Diamond
P.O. Box 400
Lancaster, Ohio 43130

Barnes Engineering
44 Commerce Road, P.O. Box 53
Stamford, Connecticut 06904

Johnson Controls
507 East Michigan Street, P.O. Box 423
Milwaukee, Wisconsin 53201-0423

Sygnetron
2103 Greenspring Drive
Timorium, Maryland 21093

Stoller
1250 Broadway
New York, New York 10001

Tera
2150 Shatluck Avenue
Berkeley, California 94704

In addition to the computer system vendors, other vendors can supply alarms, alarm monitors, access devices, etc. Information on these components is available in the Security and CCTV Handbook (1984).

5.2.2 Bid Review Procedures

This section describes four approaches to bid review: low bid, fixed price selection, evaluation of intangibles, and analytic hierarchic process. These are not all of the procedures available but are the ones that the authors felt would be most useful to the utilities.

Low Bid Approach

Low bid is the approach most commonly used by public institutions. A set of specifications is prepared, and the request for proposal is distributed to potential bidders. The vendor offering equipment and services that meet the specified requirements for the lowest cost is awarded a purchase contract.

The following are advantages of the low bid method:

- There are only two decision criteria: the satisfaction of required specifications and price.
- The procedure is widely used and accepted.
- The analysis of bid responses is relatively simple and can be done quickly.
- Vendor-initiated protests and/or legal actions are minimized.
- Buyer and engineer proposal analysis costs are relatively low.

TABLE 5.1. Major Computer-Managed Security System Vendors

Item	Arvin Diamond	Barnes Engineering	Johnson Controls	Sygnetron	Stoller	Tera
System design report	Y	Y	Y	Y	Y	Y
Software development support	Y	Y	Standard package, will assist in using	Y	Y-(Delivered system) No-User custom software)	Y
Software maintenance support	Y	Y	Will assist in using standard package	Y	Y-(Package software) No-User custom software	Y
Install hardware system	Y	Y	Y	Y	Y	Y
Perform hardware maintenance	Y	Y	Y	Y	Y	Y
Provide hardware and software updates	Y	Y	Y	Y	Y	Y
System operator training	Factory or on site	Factory or on site	Factory	Factory or on site	Usually on site, factory optional	Factory or on site
Warranty period (new system)	1 Year/ Manufacturer	1 Year	1 Year	Manufacturer of components	1 Year	1 Year
Lease option	No	--	Y	No	Y	No
Years of experience	10	23	13	11	11	6
Central processor	DEC PDP series	DEC PDP series	Current = TI 990 Prior = MODCOMP	Data general S series and DEC	Honeywell	Data general S series
Programming language	FORTRAN or ASSEMBLER	PASCAL	User Programming Package	C and ASSEMBLER	FORTRAN or ASSEMBLER	FORTRAN
Card reader type	Magnetic strip or Weigand effect readers	Proximity	Magnetic strip	Proprietary coding technique	All types	Weigand effect readers

TABLE 5.1. (Contd)

Item	Arvin Diamond	Barnes Engineering	Johnson Controls	Sygnetron	Stollor	Tera
Data archival	Y	Y	Y	Y	Y	Y
Data base capability	Y	Y	Y	Y	Y	Y
Distributed systems	Y (Custom)	Y	Y	No	Y	Y
Modular system expansion	Y	Y	Y	Y	Y	Y
Fire alarm monitoring capability	Contractual add-on	Y	Y	Y	Y	Contractual add-on
Graphics display	Color CRT, map/alarm display	Color CRT, map/alarm display	Color CRT, map/alarm display	Color CRT, map/alarm display	Color CRT, map/alarm display	Color CRT, map/alarm display

The following are disadvantages of the low bid method:

- Changes to specifications during proposal evaluation often results in the need for new proposals and re-analysis.
- Intangible criteria that are vital to system selection are usually not considered.
- Emphasis on quick vendor selection can lead to improper analysis and result in improper system selection.
- There is often a tendency to orient the specification to a particular vendor before issuing the RFP.

Fixed Price Selection Approach

Another selection process is fixed price selection. This approach was addressed by Klein, Obel and Soren (1979) as a method which reverses phases of competitive bidding. Here the buyer discloses a budget limit for a system and furnishes prospective suppliers with functional requirements and specifications. Competing vendors then are expected to analyze the specified needs and propose their solutions (packaged systems). The buyer then can use analytical tools such as those techniques discussed later in this section to select the system that provides the best selection for the budget limit.

This method may also include an iteration process that would allow the buyer to provide confidential feedback to the vendors. The feedback would be based on results of analyzing each proposed solution, including comments about strengths and weaknesses of the proposal. The feedback might also include data on benchmark performance. The buyer would then allow the competing manufacturers to re-evaluate their own systems and submit revised proposals. The buyer would then re-analyze any modified proposals and select a system.

The advantages of the fixed price selection process are:

- Primary emphasis is on obtaining the best relative solution to the problem within budget constraints.
- The buyer has the opportunity to interact with prospective vendors before purchasing commitments are made.
- Iterative proposals give vendors an opportunity to be made aware of deficiencies and correct them.
- Manufacturers who have invested resources during the course of this iterative approach probably will offer a better package than if they had been asked to submit a routine proposal.

- Very strong competitive pressures are likely to be felt by prospective manufacturers.

- Requests for component or configuration changes are more acceptable to manufacturers than requests for price reduction (Klein, Obel and Soren 1979).

The disadvantages of the fixed price selection process are:

- This method is most effective only for very competitive situations.

- A utility would need to invest extensive personnel resources to properly coordinate the process.

- This technique would take longer than more conventional methods.

- Disgruntled manufacturers would be more inclined to file protests or initiate litigation because of their resource investments.

Evaluation-of-Intangibles Approach

In the trend toward total objectivity in system selection, some important aspects that significantly affect the eventual success of an acquired system are sometimes ignored. Hardware requirements such as memory cycle speed, on-line and off-line storage capability, input-output capacity, and bus type may satisfy the buyers and sellers, but the installed system may not meet the needs of the end user.

To avoid this problem, Vaid-Raizada (1983) has stressed the importance of integrating intangibles into the computer selection process. The following is a list of intangibles which should not be overlooked when attempting to select a computer-managed security system:

- compatibility with existing equipment

- modular expansion capability to allow for system changes

- ease of learning and using the software (operating systems, special function packages such as graphics, data base, report generation, etc., and applications software developed by the vendor)

- results of benchmark comparisons

- reliability (fault-tolerant versus single-component systems)

- proven systems and software versus new systems

- completeness and effectiveness of error handling methods

- maintenance support ability (large or small firm or location of support people)
- established or relatively new vendor
- hardware and software documentation
- system security (i.e., command and file access system)
- the experience of other utilities with similar systems.

The method recommended by Vaid-Raizada (1983) for integrating firm requirements evaluation with intangible considerations and then selecting systems based on the combined results is a seven-step procedure:

1. Make a list of all the intangible factors that apply to the system under consideration.

2. Determine the relative importance of each of the intangible factors and list them from the most important to the least important; for example, most important might be "ease of use" and least important might be maintenance service. The ranking of the intangibles depends upon the relative importance of each intangible to the requirements of a system. For instance, if security is of utmost importance in a system, it would be ranked close to the top.

3. Assign an importance value to each of the intangible factors in terms of the user's requirements, using 100 for the most important and a lesser value for each of the others.

4. Adjust the importance values from Step 3 so that they add up to 100. The adjusted importance values are calculated by dividing the importance values by the total of all importance values.

5. Evaluate each intangible factor for each available alternative system on the basis of 100 for the best alternative and so on.

6. Determine the weighted evaluation ratings by multiplying the adjusted importance values from step 4 by the evaluation ratings from step 5 for each of the alternatives.

7. Calculate the total weighted evaluation for each alternative by adding weighted evaluation ratings.

The totals from step 7 are the intangible rating evaluations for each of the systems. For additional information on decision analysis methodology, see Clark and Reardon (1982).

To combine the cost analysis with the intangible analysis, divide the comparative system costs by the total fractional weighted evaluation rating for each vendor. The adjusted costs can be compared and used as a selection criterion to determine the successful vendor.

A utility may choose to use the method just described to include intangibles in the selection process, or it may decide to adopt or develop another method; however, intangibles should be identified and considered regardless of the selection methodology that is used.

Analytic Hierarchic Process (AHP) Approach

The prior section discussed how tangible and intangible factors for system selection can be analyzed separately and then merged using a mathematical approach to choose an optimal system. Other available methods that could help in the selection process include criteria weighting and ranking (Smith 1967) and operation-research procedures (Morris 1977). Weighting and ranking is not discussed here because of its subjectivity. Operations-research methods also are not addressed because of their complexity.

This section discusses a relatively new approach that is felt to be strong in handling judgement factors (Narasimhan 1983). This method is called the analytic hierarchic process because alternative proposals are compared by constructing a hierarchy of criteria and then evaluating alternatives for each level of the hierarchy. Then a composite analysis is performed to determine which system should be selected. The following discussion briefly explains the approach. Appendix B details a specific example of calculations in applying the analytic hierarchic process.

The system selection hierarchy example shown in Figure 5.1 illustrates a way of decomposing a complex problem into a hierarchy. The evaluation criteria (system cost, delivery, quality, service, and experience) make up the first level of the hierarchy. The second level shows the dimensions of each of these criteria.

Each criterion has a different degree of importance to the system selection. The lowest level on the hierarchy consists of the alternatives, or vendors. Vendors will measure up differently when evaluated on the various criterion dimensions.

The first step in this approach is to create a hierarchy similar to the one just shown. The criteria and criterion dimensions depend on the product to be supplied. After this has been completed, relative weights are established for the elements within each level of the hierarchy. This is accomplished by making pairwise comparisons of the elements in each level relative to the elements in a higher level. For example the evaluator would decide how much more important is "cost" than "quality" in selecting a vendor. The answers to these questions are put in pairwise comparison matrices such as in Figure 5.2.

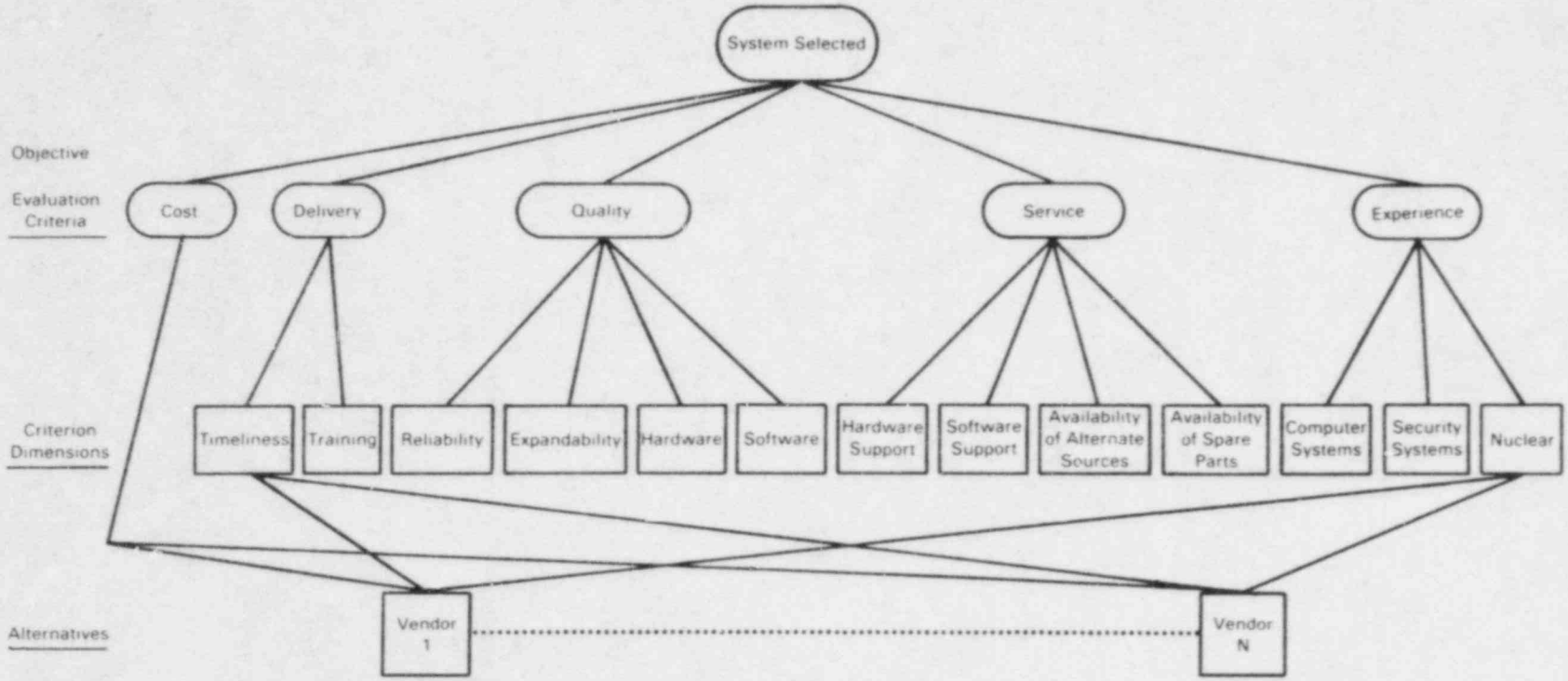

FIGURE 5.1. System Selection Hierarchy Example

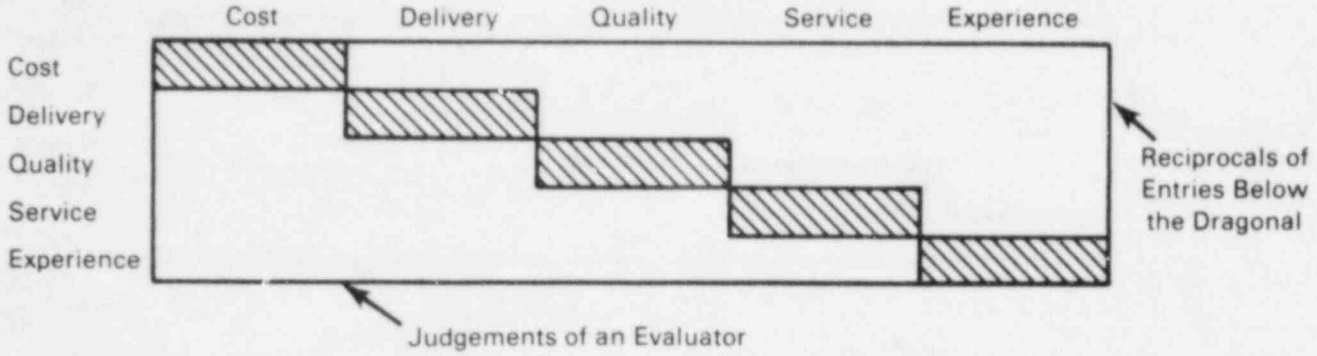

FIGURE 5.2. Pairwise Comparison Matrix for Rating the Relative Importance of Criteria (i.e., elements of a level of the hierarchy)

Pairwise evaluations provide the data needed to derive the relative weights of the evaluation criteria. Pairwise comparisons of the vendors, relative to the criterion dimensions, results in a relative ranking of the vendors.

After putting together all of the pairwise comparison matrices, an approximation of the criterion weights is obtained by taking a "geometric average" of the entries in each row and "normalizing" them so they add up to 1.0. These numbers then represent the relative importance of the criteria. This procedure is repeated for each of the linkages in the hierarchy.

Next, the normalized weights derived for elements in a lower level (for example, vendors) are combined using the weights for the elements in the next level up (for example, expandability, reliability). This is called hierarchical composition and involves computing weighted average ratings for the vendors. After the process is carried out, moving upward through the hierarchy, a final ranking will be available for each vendor. Appendix B details a specific example of how the ratings can be calculated. This example should clarify the procedure for the reader.

The advantages of the analytic hierarchic approach are:

- Tangibles and intangibles can be analyzed and integrated using the same method.
- Complex computing resources are not required.
- Weighting can be easily and quickly changed to do sensitivity analysis.
- Judgements are made by following specific procedures.
- The procedure is applicable to group evaluations as well as evaluations by a single individual.

The analytic hierarchic approach has the following disadvantages:

- Subjectivity has not been completely eliminated.
- Vendors may initiate protests or litigation if they disagree with the weighting approach.

5.3 SYSTEM INSTALLATION

The installation of the computer equipment for the security system is an extremely important part of the system implementation. Improper installation would adversely affect the reliability, availability, and usability of the system. Site preparation and system installation requirements varies from site to site. The degree of site preparation needed depends on the size of the system to be installed and on whether the proposed installation is to be in a new building or a previously existing facility. For the latter case, there may be extensive renovation or reconstruction needed to meet the demands of the computer system.

This section of the document provides some general guidance about installation and delineates those items that should be considered before system installation. Some of the computer vendors have site preparation guides that provide specific information pertinent to the installation of their systems (DEC 1978).

5.3.1 Selecting a Site

The same amount of emphasis that is placed on programming and systems design should be placed on proper site selection and planning. The location and environmental aspects of the computer system are as significant as the inherent reliability of the equipment itself. The following criteria can be used to evaluate proposed sites for security computer system installation:

- Space - The system needs adequate space for system installation, operation, potential expansion, service, storage of supplies, and maintenance area (if applicable).
- Location - Consideration should be given to the convenience of delivery of equipment and supplies.
- Power - There needs to be adequate power for system requirements and potential expansion. Items that need to be considered include the computer facility power distribution system, power conditioning, availability of uninterruptible power supplies, and emergency power systems.
- Mechanical Support Systems - Adequate mechanical support systems such as heating/cooling systems need to be available.

- Structural Integrity - The floor of the proposed computer area must be strong enough to withstand anticipated loads.

- Security - The equipment should be located in an area where access to the room can be restricted to those individuals responsible for the system.

Once a site has been selected to house the computer equipment, some additional factors need to be kept in mind during site development:

- Work Flow - Consideration should be given to related work areas, human factors, and storage.

- Fire and Safety - Fire and safety precautions must be implemented. These are discussed in further detail in Section 5.3.2.

- Environment - There are several environmental considerations that are discussed in Section 5.3.5.

5.3.2 Site Planning

Adequate site planning and preparation is necessary to simplify the installation process and produce efficient, reliable system operation. Site planning considerations should include space and layout requirements, floor construction requirements, fire and safety precautions, and security.

Space and Layout Requirements

Space and layout requirements will differ depending on the computer system selected and the available physical area. There are four categories of required space that need to be considered: primary computer system, maintenance work space, storage areas, and operational work area. The floor area required for the computer system itself depends on the components selected, the dimensions of the setup, and the location of walls, partitions, windows, and doors. A layout can be prepared using scaled layouts of the area being considered. The layout needs to provide room for service areas that the manufacturer feels are necessary to perform service on equipment. Free-standing peripherals must be located so that the length of connecting cables will not exceed the maximum limit allowed. Space needs to be provided for the storage of tapes, paper, and other supplies that are needed daily. A maintenance area for storage of spare parts and necessary maintenance supplies would be useful to optimize system availability. The area surrounding the equipment that is designated as the operator work station should allow operators to perform efficiently all normal and emergency functions. Space needs to be allocated based on the number of personnel located around the workstation. The number of personnel will depend upon the staffing requirements of the utility.

Floor Construction Requirements

The computer room floor needs to support the total weight of all the components of the system as well as the localized weight at each caster. The preferred method of floor preparation is to construct a raised floor over the building floor. The advantages of a raised floor are:

- simplification of installation and flexibility for subsequent layout changes or expansion,
- distribution of computer load while adding relatively little to the total floor load
- protection of interconnecting cabling, plugs, and power connections
- safety to personnel by eliminating the hazard of cabling underfoot
- optimization of air conditioning efficiency.

The desired type of raised flooring for computer rooms is the pedestal type because it allows cable routing in any direction, minimizes cable lengths, and increases layout flexibility. Raised floors are usually tile-covered panels supported by a grid system. The raised floor should support a load of 200 lb/ft^2 with a concentrated load of 1,000 lb at any point. The preferred height of raised floors is 12 inches, but the minimum height is 4.5 inches. Surface resistivity, ease of maintenance, durability, appearance, and cost are further considerations for the floor covering.

Fire and Safety Precautions

Several fire precautions can be implemented during the construction phase of a computer installation:

- Walls enclosing a computer area should extend from floor to true ceiling.
- Walls, floors, and the dropped ceiling, if applicable, should be constructed of noncombustible materials.
- If the structural floor is made of combustible materials, it should be covered with a noncombustible covering.

Fire protection systems should be included in the facility design. Automatic fire detection systems should be installed to alarm in the room and at a central alarm station. There should be a master fire extinguishing system that is of the water sprinkler, carbon dioxide, or hydrocarbon bromide type. The use of hydrocarbon bromides, such as Halon 1211 and 1301, is recommended because it reduces equipment damage to a minimum with virtually no personnel hazard.

At least two carbon dioxide fire extinguishers should be available in each room where computer equipment is located. These should be clearly marked and regularly inspected.

As a safety measure, it is important to train personnel in emergency measures that are required in the event of a fire. These may vary from plant to plant and will depend on the location of the computer system. Good safety practices reduce the chance of damage to the equipment in the event of a fire.

Security

Safeguards such as tamperproof door controls and electrically taped glass doors and windows can be tied to the alarm system. Duplicates of master records and system back-up tapes or disks should be maintained in a separate storage room or vault. That room should be of fire-resistant material and located in a building separate from the computer area. Computer facility environmental information such as temperature, humidity, liquid detection, and mechanical system status should be monitored and alarms reported for off-standard conditions.

5.3.3 Supply Storage

Sufficient storage in a closed cabinet should be provided for magnetic tapes, disk packs, and line printer paper. Tapes and disk cartridges should be protected from rough handling, magnetic fields, dust, and extremes of temperature and humidity. The storage area should be maintained between 60° and 80°F with a relative humidity of from 40 to 60 percent.

5.3.4 Acoustics

Acoustic treatment is an important consideration in a computer room. If it is impossible to reduce the noise level at its source, there are three other techniques to consider for sound isolation:

- Relocate the noise source.
- Use sound-absorbing material on floors, ceilings, and walls.
- Place barriers between the source of the noise and the listeners.

The best design feature to reduce ambient noise is to physically isolate the computer equipment from system operators by installing it in its own room. If this is not possible, then sound-absorbing materials will need to be used. Ceilings properly treated with acoustic dampeners or acoustic material provide the greatest reduction in noise levels. The floor is the secondmost effective area for acoustic dampening.

Special consideration needs to be given to acoustics if a line printer is located in the CAS or SAS. Because of the size of these rooms and the importance of operator surveillance, the noise generated by the line printers may

adversely affect the CAS and SAS operators' performance. Line printer enclosures are now commercially available; these significantly reduce the noise level from the printers.

5.3.5 Environmental Specifications

The recommended lighting in the computer room area is 60 ft-c (foot-candles) measured at desk level. In the areas immediately surrounding VDTs, illumination should be reduced to 40 ft-c. Flourescent lighting provides little heat and even area illumination.

The computer room temperature should be maintained between 65° to 75°F and the humidity between 40% to 60%. The temperature rate of change should not exceed 3.6°F/hour, and the humidity rate of change should be within 2%/hour.

5.3.6 Electrical Considerations

The power source must be of sufficient capacity to handle the present computer load and loads likely to be imposed by future system expansion. Because of the need for high reliability and availability of security systems, the computer system should be supplied by an uninterruptible power supply (UPS), which should be capable of carrying the required load until input power is restored. A grounding system exclusively for the computer system should also be provided.

6.0 REFERENCES

Barlow, R. E., and F. Proschan. 1975. Statistical Theory of Reliability and Life Testing. Holt, Rheinhart and Winston, New York.

Cardwell, R. G., D. A. Moal, J. A. McBride, and C. W. Wilson. 1984. The Role of Security During Safety-Related Emergencies at Nuclear Power Plants. NUREG/CR-3251 (YYDS-178), Union Carbide Corporation, Oak Ridge, Tennessee.

Clark, R. G., and P. T. Reardon. 1982. Notes on Performing Value - Impact Analysis Using a Weighted Matrix Decision Technique, PNL-3763, Pacific Northwest Laboratory, Richland, Washington.

DOE. 1984. Economic Analysis Guidelines and Procedures for ADP Resources - Users Handbook. Volumes 1 and 2, Office of ADP Management, U.S. Department of Energy.

DEC. 1978. Digital Site Preparation Guide. EK-CPRP-SP-002, Digital Equipment Corporation, Maynard, Massachusetts.

Dahl, O. J., E. W. Dijkstra, and C. A. Hoare. 1972. Structured Programming. Academic Press, New York.

EPRI. 1984. Computer-Generated Display System Guidelines. EPRI NP-3701. Prepared for the Electric Power Research Institute by Oak Ridge National Laboratory.

Edward, J. 1977. Computer Selection. Addison-Wesley Publishing, Menlo Park, California.

Eidsmore, D. 1983. "Fault Tolerant Architectures." Digital Design. 13(8):70-82. August 1983.

Energy Regulations. 1981. U.S. Code of Federal Regulations (CFR). Title 10, Parts 9 to 99, Chapter I, "Energy."

Part 73 - "Physical Protection of Nuclear Power Plants"

Part 73.55 - "Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors Against Radiological Sabotage"

Part 73.70 - "Records"

Evarts, H. F. 1966. Introduction to Pert. Bacon, Inc., Boston, Massachusetts.

Fainberg, A., and A. M. Bieber, Jr. 1978. Barrier Penetration Database. NUREG/CR-0181, Brookhaven National Laboratory, Upton, New York.

Giansas, M. 1984. "Reading Moving Text on a CRT Screen." Human Factors. 26:98-105.

Gido, J. 1974. An Introduction to Project Planning. Educational Methods, Chicago.

Gould, J., and N. Grischowsky. 1984. "Doing the Same Work with Hard Copy and with Cathode-Ray Tube (CRT) Computer Terminals." Human Factors. 26: 323-339.

Hansen, B. J. 1965. Practical Pert. America House, Washington, D. C.

Harrison, F. L. 1981. Advanced Project Management. John Wiley & Sons, New York.

Hedman, L., and V. Breim. 1984. "Short-Term Changes in Eyestrain of VDU Users as a Function of Age." Human Factors. 26:357-376.

Hendrie, G. 1983. "Fault-Tolerant Computers. A Hardware Solution to Port Failures Totally Insulater Programs." Electronics. 56(2). January 27, 1983.

Hutchinson. R. 1981. New Horizons for Human Factors in Design. McGraw Hill Book Company, New York, New York.

IBM. 1984. Human Factors of Workstations with Visual Displays. IBM Corporation, San Jose, California.

Jackson, M. 1975. Principles of Program Design. Academic Press, New York.

Jensen, W., and C. C. Tonies. 1979. Software Engineering. Prentice-Hall, Inc., Englewood Cliffs, New Jersey.

Kartashev, S. P. and S. I. Kartashev. 1983. "Reconfigurable Fault-Tolerant Multicomputer Network." 1983 National Computer Conference AFIPS Conference Proceedings. Anaheim, California, USA, May 16-19, 1983, AFIPS Press, Arlington, Virginia.

Klein, D., B. Obel, and J. H. Soren. "Soliciting and Evaluating Bids for a Complex Big Ticket Item." Industrial Marketing Management. 8(2):154-160.

Kruk, R., and P. Muter. 1984. "Reading of Continuous Text on Video Screens." Human Factors. 25:339-341.

Luder, C., and P. Booker. 1984. "Redundant Color Coding on Airborne CRT Displays." Human Factors. 26:19-32.

Long, G., et al. 1984. "The Effect of Display Format on the Direct Entry of Numerical Information by Pointing." Human Factors. 26:3-19.

Morris, W. T. 1977. Decision Analysis. Grid Publishing Company, Ohio. pp. 80-82.

NRC Information Notice. 1983. "Impact of Security Practices on Safe Operations." IN 83.36, U.S. Nuclear Regulatory Commission. June 9, 1983.

NUREG-0992. May 1983. Report of the Committee to Review Safeguards Requirements at Power Reactors. Nuclear Regulatory Commission, Washington, D.C.

Narasimhan, R. 1983. "An Analytical Approach to Supplier Selection." Journal of Purchasing Materials Management. 19(4):27-32.

Richardson, J. M. April 1982. Rank Ordering of Vital Areas within Nuclear Power Plants. NUREG/CR-2551, Sandia National Laboratories, Albuquerque, New Mexico.

Rountree, S. L. K. March 1982, Security Officer Response Strategies (SECURORS). SAND82-0410, Sandia National Laboratories, Albuquerque, New Mexico.

Saaty, T. L. 1980. The Analytic Hierarchy Process. McGraw Hill, New York.

Sandia National Laboratories. 1979. Safeguards Control and Communications Systems Handbook. SAND78-1785, Sandia National Laboratories, Albuquerque, New Mexico.

Schiff, W. 1980. Perception: An Applied Approach. Houghton Mifflin Company, Boston, Massachusetts.

Security and CCTV Handbook. Bill Daniels Company, Inc. Publisher. ISSN 0740-6622, 1984.

Shidal, J. G. 1979. "Preparing an Objective RFP." Journal of Systems Management. February, 1979.

Skrokov, M. R. 1980. Mini- and Microcomputer Control in Industrial Processes - Handbook of Systems and Applications Strategies. Van Nostrand Reinhold Company.

Smith, A., et al. 1984. "Correlates of Ocular and Somatic Symptoms Among Video Display Terminal Users." Human Factors. 26:143-157.

Smith, D. V. 1967. "Vendor/Supplier Evaluation." N.A.P.M. Guide to Purchasing. pp. 1.6.0 - 1.6.18.

Smith, S. L., and A. F. Aucella. 1983. Design Guidelines for the User Interface to Computer-Based Information Systems. ESD-TR-83-122, USAF Electronic Systems Division, Hanscom Air Force Base, Massachusetts. Also: National Technical Information Service No. AD A127 345, Springifeld, Virginia.

Thomson, R. 1972. "Design of Multi-Man-Machine Work Areas." In Human Engineering Guide to Equipment Design, Joint Services Document, eds, H. Van Colt and R. Kinkade.

Vaid-Raizada, V. K. 1983. "Incorporation of Intangibles in Computer Selection Decisions." Journal of Systems Management. November 1983.

Warburton, R. D. H. 1983. "Managing and Predicting the Costs of Real-Time Software." IEEE Transactions on Software Engineering. Vol. SE-9, No. 5, September 1983.

Wensley, J. H. 1982. "A Fault Tolerant Computer for Industrial Control." In Mini/Micro 82 Conference Record. Anaheim, California. September 14-16, 1982.

Wensley, J. H. 1983. "Fault-Tolerant Computers. Industrial-control System Does Things in Threes for Safety." Electronics. 56(2):98-102. January 27, 1983.

Wensley, J. H. 1983. "The Analysis of the Use of a Fault-Tolerant Computer for Control Functions." Presented at the Fourth Annual Conference on Computer Developments, Houston, Texas, November 1983.

Woodson. W. 1981. Human Factors Design Handbook. McGraw Hill Book Company, New York, New York.

Yourdan, E. Y., and L. L. Constantine. 1979. Structured Design, Fundamentals of a Discipline of Computer Program and Systems Design. Prentice-Hall, Inc., Englewood Cliffs, New Jersey.

Zimmerman, D. C. 1980. Economic Analysis Procedures for ADP. Naval Data Automation Command, Washington Navy Yard, Washington, D.C., March 1980.

APPENDIX A

TYPICAL SYSTEM SPECIFICATION

APPENDIX A

TYPICAL SYSTEM SPECIFICATION

1.0 INTRODUCTION

The utility can assist the vendors' understanding of the system to be bid by providing background information on the nature of the problem and the need for the specific system. The background might include a brief description of the current system or manual operating procedures that are used.

1.1 Scope

The scope section allows prospective bidders to determine the type and size of the system to be supplied. Prospective bidders should be able to read this section and determine whether they would like to submit a bid. This section should provide a brief description of the system and summarize the functions it must perform.

1.2 Bidder Qualifications

In nuclear industry security applications, a field-proven system is desirable. The system needs to be highly-reliable, and a short start-up effort is important. The utility must be concerned with software reliability as well as hardware reliability. The vendor must be able to provide maintenance and spare parts to minimize the time that the system is not operating.

This section should describe any qualifications the utility requires the bidder to meet for their bid to be considered. To gain some assurance that the vendor can provide reliable, field-proven systems, a user's list describing each computer-managed security system the vendor has supplied can be required. The vendor may also be required to demonstrate field maintenance capability and maintain a stock of spare parts. Any requirements for small, disadvantaged, or minority-owned businesses would also be specified in this section.

1.3 Bidding Instructions

Instructions on the date the bid proposal must be returned and the address to which bids should be sent can be specified here. Bid review will be easier if a consistent format is suggested for the bid proposals. The protocol for interface between the buyer and the vendor that is to be followed during the bid process can be described in this section.

The basis on which the winning vendor will be selected (i.e., low bid, low bid with consideration to specified options, lowest life cycle cost, etc.) are specified. Specifying the length of time the bid prices must be guaranteed from the time of bid opening will ensure that the bid will still be valid after the lengthy processes of bid evaluation and the selection of a winning proposal are completed. If a benchmark is to be used, specify the way in which it is to be conducted and what will be determined as a result of the benchmark.

If the utility does not wish to negotiate on the price, the specification should state that the vendor bid their best prices since the buyer reserves the right not to negotiate.

This section may include instructions on the type of equipment the vendor can provide. For example, the specification could require field-proven products rather than custom-designed hardware or software. The specification should state whether third party components are acceptable. If third party components are acceptable, the specification should state that the bidder will be held responsible for the total package bid. The specification might also state that all equipment be currently manufactured and part of the standard offering of the manufacturer. This will eliminate bids proposing out-of-date equipment.

An additional instruction that would aid bid review is to require bidders to specify, item-by-item, any specifications they do not meet. However, systems that do not meet certain specifications may still be considered if supporting information supplied by the vendor acceptably demonstrates that the system will function as required by the utility.

2.0 FUNCTIONAL DESCRIPTION

The functional description will provide the basis from which the vendor prepares the bid, so this is an extremely important section of the specification. The utility should provide the detail required to ensure that the system will perform all of the required functions within a specified response time and within tolerance-levels for reliability and availability. The functional needs for security, such as system access control, should be clearly specified.

An introduction can list the functions the system should perform. Examples of the functions that could be included are:

Data Acquisition and Storage
Alarming
Logging
Access Control
Data Display.

2.1 (through 2.N) Function Specification 1 (through N)

For each of the functions, a detailed specification should be provided. Each of these sections will include details such as sensor scan rates, alarm processing, alarm limit checks, logging reports, historical data storage, the type and frequency of data displays, and required response time. The kind of user interfaces should be specified. The specification should state whether the system is to be programmable by the user or if all interaction is specified by parameter changes.

3.0 HARDWARE CONFIGURATION

The hardware configuration depends on the functional requirements of the system. The utility may wish to have the vendor propose the configuration for the system. However, the utility may have overriding factors it feels dictate a specific hardware configuration such as a distributed system, a fault-tolerant system, or a redundant system. Details of any required hardware configuration should be provided.

For distributed systems, the configuration needs to specify the general processing to be performed by the host processor and that performed by the intelligent front-end processors.

3.1 (through 3.N) Major Configuration of Item 1 (through N)

A section specifying specific configuration details should be included for the computer, intelligent multiplexers, bulk memory, line printer(s), tape drive(s), operator console, VDTs, communications equipment, etc.

4.0 ENVIRONMENTAL CONSTRAINTS

This section should include any special environmental requirements imposed on the system. The footprint (area and arrangement) of the system is important because the vendor must be prevented from bidding equipment that could not physically fit in to the facility for which it is intended. On the vendor's part, the system vendor should be required to state any needs for facility modifications necessary to accommodate the vendor's system. For example, the system the vendor bids might require special power and air conditioning needs that would require major and costly facility modifications.

5.0 PROGRAMMING LANGUAGES

All of the programming languages that are to be included in the system should be specified. If a high-level language compiler (e.g., FORTRAN) is required, the utility should specify industry standards to which the compiler must conform. Another item to consider is a report generator program so that the system user can develop special reports without program development.

If there is a requirement for a database management system (DBMS), the specifications for this system should be provided. For example, the vendor might be required to supply a DBMS that supports small-to-medium-sized files with concurrent, multiple, on-line, and batch updating processes. The DBMS should provide a comprehensive back-up and recovery procedure. Any additional DBMS requirements, such as interaction with a high-level language or graphics applications, on-line dictionary, on-line query capability, user-defined command procedures, access control, report formatting, etc., should be specified.

6.0 OPERATING SYSTEM SOFTWARE AND DIAGNOSTICS

The specification for operating system software and diagnostics depends on how the utility expects to operate the system. The utility may purchase a completely turn-key system and specify that the vendor will perform all of the software development, both initially and for future maintenance and upgrades. However, if the utility is going to do software development and maintenance in-house, it should specify that the operating system must provide the tools to perform these functions. Items to be considered are an on-line editor, a file manager, input/output programs, and on-line and off-line diagnostics.

This section should specify access security requirements. These specifications would include such things as:

- description of password levels and user code access criteria
- specifications for physical access restrictions; i.e., terminal key locks, power access locks, coder card, etc.
- encryption requirements for data and passwords.

7.0 DOCUMENTATION

This is an extremely important section that is too often neglected. The specification should define a minimum list of documentation that is required, the time frame in which it is to be delivered, and the number of copies of the document sets. The requirements for future updates to the documentation should also be addressed.

8.0 ACCEPTANCE TESTING

Both factory acceptance test and field acceptance test requirements should be specified. These tests should include the running of all hardware diagnostics and running of the total system program. The factory acceptance test should also check the software, system documentation, diagnostic programs, and spare parts. Documentation should be checked for correctness and completeness. The vendor may be required to submit a test plan with the bid or at some point before delivery of the system. The utility can use the test plan to determine how it will be able to verify that the system is operating correctly.

9.0 INSTALLATION AND MAINTENANCE

Specifying the system to be developed is only one part of the task the utility must undertake. It is equally important that specifications be defined for installation, maintenance, and training. Before writing these specifications, the utility should carefully evaluate the availability of in-house expertise to perform any or all of these functions. If the expertise is not available, then the specification should be written to ensure that the vendor will provide it.

9.1 Installation

Details of the actual installation process are specified here. The utility may require the vendor to provide trained engineers and programmers to supervise the installation and start-up of the computer system. The utility should also include the time frame in which it expects the system to be installed.

9.2 Maintenance

This section specifies any maintenance requirements to which the vendor must agree. This may vary greatly because it depends on the utility's computer expertise and availability of personnel. The utility must determine 1) what items are to be maintained by the vendor, 2) whether there is a requirement for 24-hours-a-day, seven-days-a-week service, 3) what spare parts the vendor must stock nearby, 4) the hardware and software maintenance training requirements, (5) the expected mean time between failure (MTBF) requirements, (6) the time in which the vendor must respond for repair, and (7) the preventative maintenance schedule that will be required. The specification may include penalties for failing to have the system up and running within a reasonable time after system failure as well as for failing to meet the MTBF criteria. The need for special clearances for the personnel maintaining the system should be specified, as well as who will be expected to meet the cost of any clearance investigations that are required.

9.3 Spare Parts

The specification should require the vendor to provide a recommended list of spare parts and respective prices. The purchase of spare parts should be included in the purchase of the total system. An alternative to buying spare parts is to require the vendor to maintain an agreed-upon minimum level of spares onsite or at a nearby location. The specification might specify that some combination of these options is acceptable.

9.4 Consumable Supplies

This section is used to specify the consumable supplies, such as line printer paper, and ribbons, that the vendor must supply.

10.0 TRAINING

This section should specify the training that the vendor must supply for both hardware and software, exclusive of maintenance training. The utility may also specify that the vendor must provide training for the security personnel who will operate the system. The location of the training should be specified because this could be a significant cost to the utility if the trainees must travel off-site.

11.0 PROJECT MANAGEMENT

This section specifies the liaison that will occur between the utility and the vendor.

12.0 TERMS AND CONDITIONS

This section specifies how the payments will be made and discusses warranties, disclaimers, and liabilities.

APPENDIX B

EXAMPLE OF THE ANALYTIC HIERARCHIC PROCESS

APPENDIX B

EXAMPLE OF THE ANALYTIC HIERARCHIC PROCESS

The analytic hierarchic process (AHP) is an approach to vendor selection that was described in Section 5.2 of this report. The approach involves the creation of a decision hierarchy and the calculation of relative weights for elements in the hierarchy to determine final rankings for vendors. This appendix provides a hypothetical example to illustrate the methodology.

The first step in the process is to create a decision hierarchy, as shown in Figure B.1. Each level of the hierarchy consists of elements or criteria to be considered about the next higher level. The second step is to establish the relative importance (weights) of the elements within each level. This is done by pairing elements from one level and evaluating their relative importance to the single elements in the next higher level. These evaluations require a scale for coding importance. The scale is arbitrary; this example uses the one established by Narasimhan (1983), as shown in Table B.1.

The importance codes are used to create pairwise comparison matrices for each level of the hierarchy. For example, consider the comparison matrix for "System Selected," as shown in Figure B.2. The entries in the matrix compare the row factors on the left with the column factors on the top. The element (i,j) shows how much more important the ith criterion is relative to the jth criterion, and the (j,i) element is the reciprocal of the element (j,i). The pairs in the matrix are evaluated by considering how one item of the pair dominates the other relative to the higher level of the hierarchy--in this case, System Selected.

Cell (2,1) implies that cost and delivery have "equal importance" in system selection. Cell (3,2) implies that quality has "weak importance" over delivery. The last column in Figure B.2 shows the normalized, relative weights for the evaluation criteria. Figure B.3 shows how the weights are calculated using the geometric averaging procedure.

The numerical values shown in Figures B.4 and B.5 are derived in the same way. The next step is to move through the hierarchy starting at the lowest level and combine the weights to determine the overall weights for vendors A, B, and C. Figure B.6 illustrates this procedure, which is simply a process of computing weighted average ratings for the vendors.

The method of hierarchical compositions is as follows:

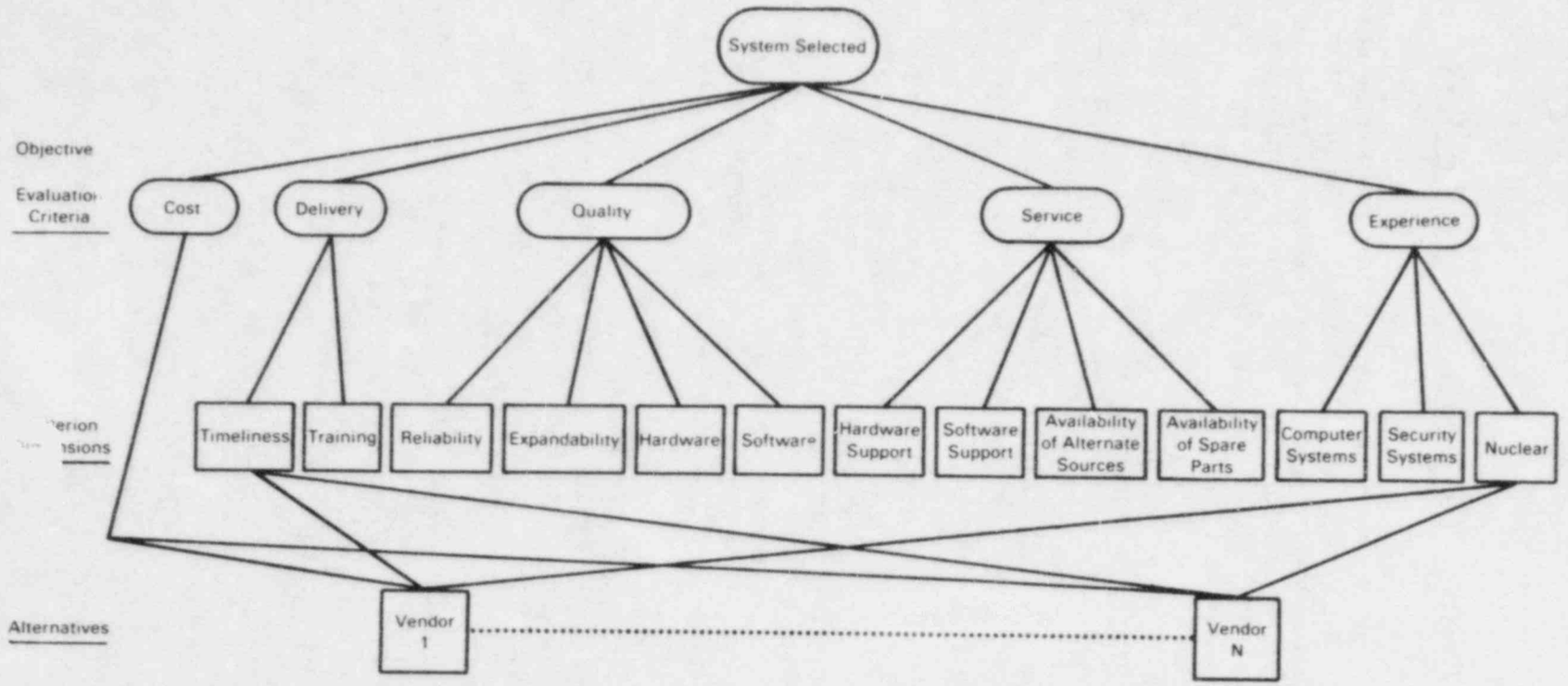

FIGURE B.1. System Selection Hierarchy Example

TABLE B.1. Scale for Coding Responses

Importance Code	Definition	Explanation
1	Equal importance	Two activities contribute equally to the objective.
3	Weak importance of one over another	Experience and judgment slightly favor one activity over another.
5	Essential or strong importance	Experience and judgment strongly favor one activity over another.
7	Demonstrated importance	An activity is strongly favored, and its dominance is demonstrated in practice.
9	Absolute importance	The evidence favoring one activity over another is of the highest possible order of affirmation.
2,4,6,8	Intermediate values between the two adjacent judgments	When compromise is needed.
Reciprocals of above number codes	If activity i has one of the above numbers assigned to it when compared with activity j, then j has the reciprocal value when compared with i.	

Let

$$R(mxn) = \begin{matrix} r_{11} & r_{12} & \cdots & r_{1n} \\ \vdots & & & \\ r_{m1} & r_{m2} & \cdots & r_{mn} \end{matrix}$$

where R is the matrix of weights for the elements of one level of the hierarchy. The jth column of the matrix is the relative ranking of the alternatives (the lowest level in the hierarchy) with respect to the jth (applicable) elements in the level immediately above.

Matrix Factor	Cost	Delivery	Quality	Service	Experience	Weights
Cost	1	1	3	2	3	0.30
Delivery	1	1	1/3	1/2	1	0.13
Quality	1/3	3	1	2	2	0.25
Service	1/2	2	1/2	1	3	0.21
Experience	1/3	1	1/2	1/3	1	0.11

FIGURE B.2. Pairwise Comparisons of Evaluation Criteria for System Selected

Matrix Factor	Geometric Mean (M)			Normalized Weights (M/T)
Cost	$(1 \cdot 3 \cdot 2 \cdot 3)^{1/5}$	=	1.5518	0.30
Delivery	$(1 \cdot 1/3 \cdot 1/2 \cdot 1)^{1/5}$	=	0.6988	0.13
Quality	$(1/3 \cdot 3 \cdot 2 \cdot 2)^{1/5}$	=	1.3195	0.25
Service	$(1/2 \cdot 2 \cdot 1/2 \cdot 3)^{1/5}$	=	1.0845	0.21
Experience	$(1/3 \cdot 1 \cdot 1/2 \cdot 1/3)^{1/5}$	=	0.5610	0.11
		T =	5.2156	

FIGURE B.3. Computation of Normalized Weights

And

$$W_{(nx1)} = \begin{matrix} W_1 \\ W_2 \\ \vdots \\ W_n \end{matrix}$$

is the vector of weights for the elements of the higher level. The weighted ranking of the alternatives with respect to the elements in the immediately higher level is computed as:

$$\begin{matrix} r1 \\ r_2 \\ \vdots \\ r_n \end{matrix} = R \times W$$

For example, after one level of composition, the average ratings for vendors A, B, and C with respect to delivery (see Figures B.4 and B.5) are:

Delivery

	Time-liness	Training	Weights
Time-liness	1	3	0.75
Training	1/3	1	0.25

Experience

	Computer Systems	Security Systems	Nuclear	Weights
Computer Systems	1	2	3	0.54
Security Systems	1/2	2	1/3	0.16
Nuclear	1/3	3	1	0.30

Quality

	Reliability	Expandability	Hardware	Software	Weights
Reliability	1	4	1/2	1/2	0.22
Expandability	1/4	1	1/3	1/3	0.10
Hardware	2	3	1	1	0.34
Software	2	3	1	1	0.34

Service

	Hardware Support	Software Support	Availability of Alternate Sources	Availability of Spare Parts	Weights
Hardware Support	1	1	5	3	0.40
Software Support	1	1	5	3	0.40
Availability of Alternate Sources	1/5	1/5	1	2	0.10
Availability of Spare Parts	1/3	1/3	1/2	1	0.10

FIGURE B.4. Pairwise Comparisons of Criterion Dimensions for Delivery, Experience, and Quality (Second-Level Elements in the Hierarchy)

System Cost

Vendor	A	B	C	Weights
A	1	1	1/5	0.157
B	1	1	1/3	0.185
C	5	3	1	0.658

Timeliness

Vendor	A	B	C	Weights
A	1	5	3	0.659
B	1/5	1	1	0.156
C	1/3	1	1	0.185

Training

Vendor	A	B	C	Weights
A	1	1/3	2	0.23
B	3	1	5	0.65
C	1/2	1/5	1	0.12

Reliability

Vendor	A	B	C	Weights
A	1	1/2	1/3	0.16
B	2	1	1/2	0.30
C	3	2	1	0.54

Expandability

Vendor	A	B	C	Weights
A	1	1	1/2	0.25
B	1	1	1/2	0.25
C	2	2	1	0.50

Hardware Quality

Vendor	A	B	C	Weights
A	1	1/5	2	0.20
B	5	1	3	0.65
C	1/2	1/3	1	0.15

Software Quality

Vendor	A	B	C	Weights
A	1	1	1	0.333
B	1	1	1	0.333
C	1	1	1	0.333

Hardware Support

Vendor	A	B	C	Weights
A	1	1/3	1/3	0.14
B	3	1	1	0.43
C	3	1	1	0.43

Software Support

Vendor	A	B	C	Weights
A	1	3	1	0.42
B	1/3	1	1/4	0.12
C	1	4	1	0.46

Availability of Alternate Sources

Vendor	A	B	C	Weights
A	1	1/2	1/3	0.16
B	2	1	1/2	0.30
C	3	2	1	0.54

Availability of Spare Parts

Vendor	A	B	C	Weights
A	1	1	1/2	0.25
B	1	1	1/2	0.25
C	2	2	1	0.50

Computer Systems Experience

Vendor	A	B	C	Weights
A	1	1	1	0.333
B	1	1	1	0.333
C	1	1	1	0.333

Security Systems Experience

Vendor	A	B	C	Weights
A	1	1/3	1/3	0.14
B	3	1	1	0.43
C	3	1	1	0.43

Nuclear Experience

Vendor	A	B	C	Weights
A	1	1	1/5	0.157
B	1	1	1/3	0.185
C	5	3	1	0.658

FIGURE B.5. Pairwise Comparison of Vendors A, B, C (Elements of the Lowest Level in the Hierarchy with Respect to Criterion Dimensions)

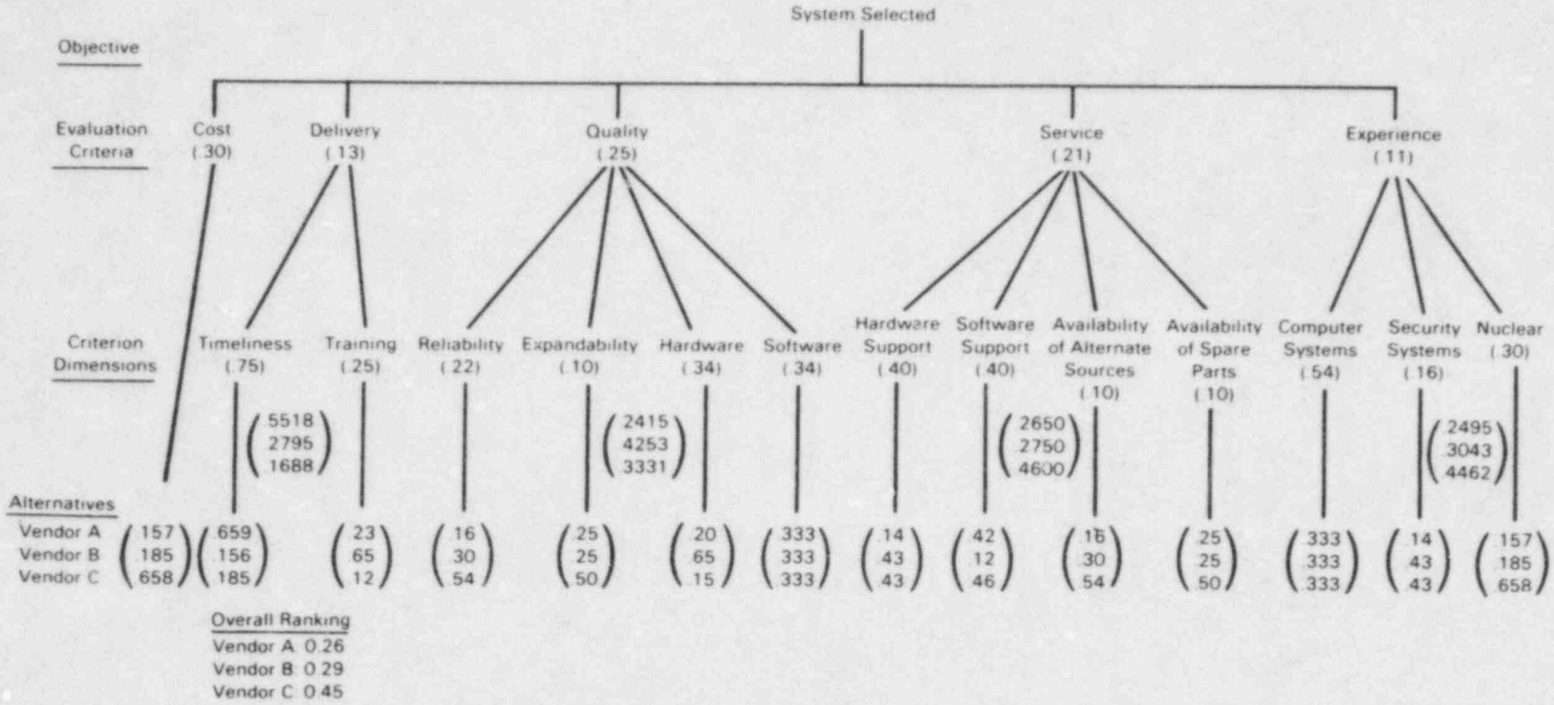

FIGURE B.6. Hierarchial Composition of Weights for the System-Selected Decision

$$\begin{pmatrix} .5518 \\ .2795 \\ .1688 \end{pmatrix} = \begin{pmatrix} .659 & .23 \\ .156 & .65 \\ .185 & .12 \end{pmatrix} \begin{pmatrix} .75 \\ .25 \end{pmatrix}$$

$$\begin{matrix} r_1 \\ \vdots \\ r_n \end{matrix} = (R) \quad (W)$$

This process is continued through the hierarchy until the overall vendor rankings are obtained. For this example, the rankings were 0.26 for Vendor A; 0.29 for Vendor B; and 0.45 for Vendor C. Thus, Vendor C ranked considerably higher than the other two.

NUREG/CR-4298
PNL-5490
RS, 1S

DISTRIBUTION

No. of Copies

OFFSITE

10 S. P. Turel
Human Factors & Safeguards Branch
U.S. Nuclear Regulatory Commission
5650 Nicholson Lane
Rockville, MD 20850

U.S. Nuclear Regulatory Commission
Division of Technical Information and Document Control
7920 Norfolk Avenue
Bethesda, MD 20014

No. of Copies

34 Pacific Northwest Laboratory

K. R. Byers
M. D. Erickson
J. D. Fluckiger
N. L. Harms
J. R. Lewis (20)
K. C. McBride
R. J. Sorenson
C. S. Vickroy
Publishing Coordination (2)
Technical Information (5)

NRC FORM 335 (2-84) NRCM 1102, 3201, 3202

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

SEE INSTRUCTIONS ON THE REVERSE

1. REPORT NUMBER (Assigned by TIDC, add Vol. No., if any)
NUREG/CR-4298
PNL-5490

2. TITLE AND SUBTITLE
Design and Installation of Computer Systems to Meet the Requirements of 10 CFR 73.55

3. LEAVE BLANK

4. DATE REPORT COMPLETED
MONTH: May YEAR: 1985

5. AUTHOR(S)
J. R. Lewis
K. R. Byers
J. D. Fluckiger
K. C. McBride
S. C. Vickroy

6. DATE REPORT ISSUED
MONTH: July YEAR: 1985

7. PERFORMING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code)
Pacific Northwest Laboratory
P.O. Box 999
Richland, Washington 99352

8. PROJECT/TASK/WORK UNIT NUMBER

9. FIN OR GRANT NUMBER
B2877

10. SPONSORING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code)
Division of Risk Analysis and Operations
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555

11a. TYPE OF REPORT
Task Final Report

b. PERIOD COVERED (Inclusive dates)
May 1984 - June 1985

12. SUPPLEMENTARY NOTES

13. ABSTRACT (200 words or less)

The Pacific Northwest Laboratory has studied the design and installation of computer-managed systems that can help nuclear power plant licensees to meet the physical security requirements of 10 CFR 73.55 (for access control, alarm monitoring, and alarm recording.) Two objectives were to study the power plant security functions that could be aided by a computer-managed physical security system and to evaluate the safety and security considerations of such a system. A further objective was to develop guidance on system design, selection, and installation. The design guidance includes safety and security requirements, design alternatives, computer security, workspace design, and user interface design. Guidance is also provided on writing a system specification for procurement, bid review procedures, and site preparation.

14. DOCUMENT ANALYSIS - a. KEYWORDS/DESCRIPTORS

b. IDENTIFIERS/OPEN-ENDED TERMS
computer security, security systems, power plant security, access control, physical security

15. AVAILABILITY STATEMENT
unlimited

16. SECURITY CLASSIFICATION
(This page) unclassified
(This report) unclassified

17. NUMBER OF PAGES

18. PRICE

*U.S. GOVERNMENT PRINTING OFFICE: 1985-461-721:20208

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555