EPRI-NP--2355

DE82 904679

Nuclear-Power-Plant Perimeter-Intrusion Alarm Systems

NP-2355
Research Project 1173-1

Final Report, April 1982

Prepared by

E-SYSTEMS, INC.
Greenville Division
P.O. Box 1056
Greenville, Texas 75401

Principal Investigator
D. J. Halsey

Prepared for

Electric Power Research Institute
3412 Hillview Avenue
Palo Alto, California 94304

EPRI Project Manager
B. P. Brooks

System Performance Program
Nuclear Power Division

DISCLAIMER

ORDERING INFORMATION

Requests for copies of this report should be directed to Research Reports Center (RRC), Box 50490, Palo Alto, CA 94303, (415) 965-4081. There is no charge for reports requested by EPRI member utilities and affiliates, contributing nonmembers, U.S. utility associations, U.S. government agencies (federal, state, and local), media, and foreign organizations with which EPRI has an information exchange agreement. On request, RRC will send a catalog of EPRI reports.

NOTICE

This report was prepared by the organization(s) named below as an account of work sponsored by the Electric Power Research Institute, Inc. (EPRI). Neither EPRI, members of EPRI, the organization(s) named below, nor any person acting on behalf of any of them: (a) makes any warranty, express or implied, with respect to the use of any information, apparatus, method, or process disclosed in this report or that such use may not infringe privately owned rights; or (b) assumes any liabilities with respect to the use of, or for damages resulting from the use of, any information, apparatus, method, or process disclosed in this report.

Prepared by
E-Systems, Inc.
Greenville, Texas

EPRI PERSPECTIVE

PROJECT DESCRIPTION

This project (RP1173-1) addresses the need to define and evaluate available alternatives to be utilized in achieving an effective site-perimeter security system to deter and detect site intrusion that may represent a threat to the operation and safety of a nuclear power plant. The high cost of maintaining a large staff for plant security functions and the frequency of system performance testing recommended by the Nuclear Regulatory Commission are factors that emphasize the need for critical evaluation of alternatives. This is the final report on this study; no related reports precede it, and no continuing effort is currently planned in this area.

The report presents the methods used and results obtained in conducting a study on nuclear power plant perimeter security systems to provide guidance to utilities for plant-specific application of various available systems or combinations of systems intended to provide the required information. Aspects of regulatory requirements, recommendations, and evaluations of cost effectiveness are applied in the study.

PROJECT OBJECTIVES

The objectives of this project are (1) to determine the utility-owner needs and wants for an effective site-perimeter security system for a nuclear power plant and (2) to evaluate a means to establish such a system that would provide high probability of detection with low false and nuisance alarm rates in addition to providing information to the station security personnel to aid in limiting the extent of an actual encroachment.

PROJECT RESULTS

The methodology applied in conducting the study consisted of: (1) participation in seminars and workshops on power plant security that are offered by industry societies; (2) nuclear power plant interviews,

literature search, and design evaluation of system alternatives; and (3) presentation of a workshop specific to this project to obtain direct utility input to the study. Recommendations are provided relative to perimeter barriers, lighting, intrusion detection, and alarm assessment. Results of the study indicate that the application of a multiple-layer system with time-integration processing of information from individual layers has a positive effect in achieving high probability of intrusion detection with low false and nuisance alarm rates. Cost effectiveness of the applied system should also be enhanced.

In using this report, the following should be noted:

- The unique features of each plant-specific site and application must be accounted for in determining which of the defined alternatives best satisfies performance needs.
- Multilayer alarm processors as defined in the report are not "off-the-shelf" items.
- There is no intent in the report to confirm or justify any recommendations made in other sources.

Managers responsible for the design, installation, operation, and maintenance of the site-perimeter intrusion alarm system are intended as the primary audience for this report. Potential cost effectiveness of systems, as defined in the report, should also be of interest to upper management. Evaluation of the report recommendations, leading to their site-specific implementation, is seen as the next logical step in achieving improved system performance.

B. P. Brooks, Project Manager
Nuclear Power Division

ABSTRACT

This report encourages the review of nuclear power plant perimeter security systems to assure high levels of intrusion detection and alarm performance. Perimeter security elements must enable intercept of outside intruders (as defined by NRC) in time to prevent sabotage.

Timely intercept of an intruder requires the examination of perimeter barriers and sensors in terms of reliable detection, immediate assessment and prompt response provisions. Perimeter security equipment and operations must at the same time meet the requirements of the Code of Federal Regulations, 10 CFR 73.55 with some attention to the performance and testing figures of Nuclear Regulatory Guide 5.44, Revision 2, May 1980.

A baseline system is defined which recommends a general approach to implementing perimeter security elements: barriers, lighting, intrusion detection, alarm assessment. The baseline approach emphasizes cost/effectiveness achieved by detector layering and logic processing of alarm signals to produce reliable alarms and low nuisance alarm rates. A cost benefit of layering along with video assessment is reduction in operating expense.

The concept of layering is also shown to minimize testing costs where detectability performance as suggested by Regulatory Guide 5.44, is to be performed.

Synthesis of the perimeter intrusion alarm system and limited testing of Closed Circuit Television (CCTV) and Video Motion Detectors (VMD), were performed at E-Systems, Greenville Division, Greenville Texas during 1981.

ACKNOWLEDGMENTS

Appendix A, CCTV, VMD and Lighting in Nuclear Plant Security, was prepared by Wesley D. Redus. Appendix B, The Effects of Layering on Performance Testing, was prepared by Donnie J. Pounds.

Mess'rs Redus and Pounds are employees of E-Systems at Greenville, Texas.

CONTENTS

ILLUSTRATIONS

LIST OF TABLES

ACRONYMS

AC - Alternating Current
AND - A logic gate
ANS - American Nuclear Society
ANSI - American National Standards Institute
AWG - American Wire Guage
az - Azimuth

BIT - Binary information digit (0 or 1)
BYTE - 8 bit binary word

CAS - Central Alarm Station
CATV - Cable Television
CCTV - Closed Circuit Television
CFR - Code of Federal Regulations
CPU - Central Processing Unit
CRT - Cathode Ray Tube

dB - Decibel
DC - Direct Current
DOE - Department of Energy

E-Field - Electromagnetic Field
EAROM - Electrically Alterable Read Only Memory
EIA - Electronics Industries Association
el - Elevation
EMI - Electromagnetic Interference
EPA - Environmental Protection Agency
EPRI - Electrical Power Research Institute

FAR - False Alarm Rate
f.c. - foot candle
FCC - Federal Communications Commission
FM - Frequency Modulation

FM - Factory Mutual
FOV - Field of View

H Field - Magnetic Field
HPS - High Pressure Sodium
Hz - Cycles per second

I/O - In/Out channels to microprocessor
IEEE - Institute of Electrical and Electronic Engineers
INMM - Institute of Nuclear Materials Management
IR - Infra-Red
IR&D - Independent Research & Development
ISIT - Intensified Silicon Image Tube

KVA - Kilo Volt Ampere

LLEA - Local Law Enforcement Agency
LLLTV - Low Light Level Television
LPS - Low Pressure Sodium
LRU - Line Replaceable Unit

MSTF - Multi Sensor Test Facility
MTBF - Mean Time Between Failures
MTTF - Mean Time To (First) Failure
MTTR - Mean Time To Repair
MW - Microwave

NAR - Nuisance Alarm Rate
NEC - National Electrical Code
NEMA - National Electrical Manufacturers Association
NRC - Nuclear Regulatory Commission
NUREG - A publication of the Nuclear Regulatory Commission

O & M - Operations and Maintenance
OCC - Operational Characteristic Curve
OIC - Officer In Charge
OR - A logic gate

P_D - Probability of Detection
PRST - Probability Ratio Sequential Test
PSS - Physical Security System
PTZ - Pan-Tilt-Zoom

RAM - Random Access Memory
RF - Radio Frequency
ROM - Read Only Memory

S/N - Signal to Noise ratio
SAND - A publication of Sandia National Laboratory
SAS - Secondary Alarm Station
SRI - Stanford Research International

TV - Television

UL - Underwriters Laboratory
UPS - Uninterruptable Power Supply

V - Volts
VHF - Very High Frequency (radio)
VMD - Video Motion Detection

SUMMARY

OBJECTIVES

Objectives of the project reported herein are to:

- Determine the needs and wants of nuclear power plants for effective perimeter security
- Define a baseline system and recommend features to be implemented
- Provide background information to support plant unique and site specific applications

THE DESIGN THREAT

A perimeter intrusion alarm system must be capable of responding to and providing countermeasures to likely threats. The "design basis" threat has been defined by NRC to be a small group of men in two or more teams with hand carried equipment and material which can be covertly deployed. This definition derives from analysis of worldwide terrorist activities. The threat target is defined to be radiological sabotage that may endanger the public. Specific quantification of the threat is site variable and negotiable with the NRC.

REQUIREMENTS

The Code of Federal Regulations, CFR 10, part 73.55 directs that perimeter security systems must provide:

- Measures that prevent radiological sabotage
- An immediate response to intrusions
- Yearly review and audit of security procedures
- Continual testing of security effectiveness

NRC Regulatory Guide 5.44, Revision 2 attempts to interpret these requirements and suggests the following performance goals: Probability of Detection (P_D) 0.9 with 95 percent confidence; allowable false and nuisance alarm rates (FAR, NAR) one each per day per segment if visual assessment is provided; weekly operability testing of each segment, and quarterly testing of P_D performance of each segment.

It has been shown that a knowledgeable and determined intruder can surmount a perimeter barrier, and with back-carried equipment penetrate to a vital area within about four or five minutes. This imposes a requirement on the security system for timely interdictive response in order to prevent sabotage. The perimeter must provide immediate awareness, alarm and assessment of intrusion; false and nuisance alarms must be minimized to reserve response force dispatch for genuine intrusions.

Internal barriers must provide delay of the intruder to enable the response force to confront him before he can perform an act of sabotage. Intrusion detectability performance must be at anytime verifiable, but with a cost effective use of manpower.

As determined in this project the needs and wants of the Nuclear Utilities surveyed, relate to economical perimeter alarm system operation and maintenance, economical verifiability of performance and economical use of manpower. The Utilities need assistance in identifying, acquiring and installing tested and proven security elements but more importantly, to have these elements integrated into a reliable system suited to the specific site and its environment.

These needs and wants are not inconsistent with the requirements of the Nuclear Regulatory Commission. It is believed that these requirements (and Regulatory Guide 5.44 recommendations) can be met by means of sensor layering and alarm signal processing.

SENSOR LAYERS AND ALARM PROCESSING

Sensors are layered when the time order and duration of signal receipt is used to reduce the false alarm rate. Time integration of alarm events and ORing two or three sensor outputs increases the signal to noise ratio into the detector or processor and can provide for increased probability of detection as well as a lower nuisance alarm rate.

Most nuclear plants have 2 unconnected layers, or sensor systems. Any two of these existing layers can be combined with a new layer and achieve higher probability of detection and low nuisance alarm rates. If 3 layers are thus combined, one can fail permitting routine or delayed maintenance vs. immediate response. All layers should have the same zone coincidence to identify intrusion with a segment of the perimeter.

The time integration of ANDing and ORing can be accomplished in an interface unit which should be physically located where the sensor field joins with the existing alarm stations. The interface unit, in addition to combining signals to output reliable alarms, should control hand-off to annunciation, assessment and recording equipment in the central and secondary alarm stations. It should communicate to the sensor field for line security, sensing of tampering or failure, for alarm reset, power failure indication and switching, and for the self-test function.

Available stand alone alarm processing systems were compared and evaluated in this project. No existing hardware provides all of the desired features of control and logic processing. On the other hand, a microprocessor based system can be configured to provide the desired features.

SYSTEM DESCRIPTION

The recommended perimeter intrusion alarm system is configured to enable detection and interdiction of an intruder before the sabotage target can be reached. It provides leeway for incorporation of equipment options which will best suit site specific requirements and still achieve high P_D and low NAR. The perimeter elements are described following from outside-in.

Outside Clear Zone

A 20 foot-wide outside clear zone around the perimeter permits visual awareness of encroachment. It removes any natural means that would conceal an attempt to bridge the outer fence. It discourages tunneling and delays intruder transit to the outer fence

Outer Fence And Fence Sensor

This fence turns away the casual intruder, keeps out medium and large animals, and catches blowing debris. It requires intruders to scale the outrigger barbed wire or cut fence links. It signals pedestrian or vehicle attempts to penetrate the fence and enables time for assessment of intrusion.

Cable Guard At Inner Bound Of Isolation Zone

The cable guard being open to view prevents intruder attempts to hide. It can immobilize light vehicles (3/4 ton pickup) and increase the injury risk to intruders in larger vehicles. Being inside of the fence, it discourages cutting of the cable. The cable guard should de-escalate the threat to back pack carried equipment.

Interior Clear Zone And Hardening Effects

A 100 foot interior clear zone to vital building areas provides a lighted region for video surveillance. It provides a small transit delay and provides confrontation tactical maneuver space. Hardened

outer building walls and doors and grids also provide delay time as do hardened vital area doors, grids and walls.

Layered Sensor Combinations

There are about 20 combinations of available sensor types in layers of three. Some of the most likely combinations based on already installed equipment (and selectable based on site conditions) are listed following. There is no single combination suitable for all sites.

FIRST LAYER	SECOND LAYER	THIRD LAYER
Existing E-Field Line	Add Microwave Line	Add VMD*
Existing E-Field Line	Existing Fence Sensor	Add VMD*
Existing Microwave Line	Existing Fence Sensor	Add Buried Line Sensor

*Video Motion Detection (VMD) is shown as a third layer option since it is a potentially low cost adjunct to a Closed Circuit Television System (CCTV) being used for assessment.

Alarm Processing Interface

The interface combines diverse detector signals, sensitive to different intruder and nuisance manifestations to reduce nuisance alarms and increase detection probability. It communicates with sensor segments for self test and alarm status. It accepts conditioned signals from existing sensor pre-processors or communication transducers and hands off instructions to alarm monitoring and control equipment.

Alert/Alarm/Assessment/Functions

The Central and Secondary Alarm Stations utilize existing alarm annunciation, monitoring, computing and logging equipment. Video

assessment is enabled by means of closed circuit television with appropriate external lighting.

POTENTIAL WORK FORCE REDUCTION

As compared to non-layered, non-automated systems now in use, it is believed that the perimeter intrusion alarm system just described can reduce the security workforce. A reduction by five men may be achieved with CCTV surveillance and assessment vs. two watchtowers. A three layered perimeter system may permit single shift and scheduled maintenance for an estimated work force reduction of six men. Reliable combined alarms, automated alarm keying, logging and reset, and dispatch only on true alarms should enable a work force reduction of an additional five men. Such savings in manpower can amount to as much as $640,000 per year in operating costs.

MINIMIZING PERFORMANCE TESTING COSTS

The premise is taken that utility managers as well as the NRC, should wish to realistically verify the detectability performance of their perimeters. Regulatory Guide 5.44 suggests test procedures that, depending on the P_D criterion accepted, require an inordinate number of test trials to achieve statistical proof of performance. However, the number of test trials required decreases dramatically as true P_D is increased. This increase can be effected by layering, with intrusion testing accomplished against the layered perimeter segment.

As compared to a single segment having a 0.9 P_D, requiring about 220 test trials, a two layer segment would require 68. A three layer segment would require only 34 on an average.

The savings in testing alone (if NRC Regulatory Guide 5.44 becomes a requirement) is sufficient to pay for a three layered system.

COST EFFECTIVENESS

The effects of layering and alarm processing on system costs are summarized in Table I.

Table 1
LAYERING IMPACT ON SYSTEM COST
(1600 METER PERIMETER)

	ONE LAYER	TWO LAYER	THREE LAYER
Initial Investment	171,000	194,200	292,000
Annual O & M Cost	17,300	24,500	27,500
Potential Annual Testing Cost (Reg. Guide 5.44)	334,700	89,800	51,000
Present Value of Total Cost* (For 6 year life)	1,805,000	736,700	664,500

*6 year amortization schedule, 12 percent inflation, 20 percent interest

Additionally, the value of layering (increasing detection probability) in preventing sabotage events is assessed as follows:

- The cost of one core shutdown approximates the cost of a three layer perimeter alarm system
- Any increment of true P_D over 0.90 reduces the probability of a successful penetration that would lead to a core shutdown
- For a true P_D (three layer system) greater than 0.98, extrapolation of experience data indicates that penetrations which would be undetected and result in core shutdown may be less than one in 30 years

Section 1

1.0 SCOPE

This report examines the NRC requirements for perimeter security at nuclear power plants. It extends the NRC industrial sabotage threat description and recommends performance standards to cope with the very short time that it may take a resolute outside intruder to defeat barriers, penetrate vital areas and sabotage vital equipment.

Candidate equipment and procedures are described which satisfy these performance standards for each perimeter security element thus enabling selection and system definition based on further site specific criteria.

Perimeter security elements are

- Barriers
- Exterior lighting
- Intrusion detection
- Alarm assessment

Secure and reliable performance is believed best achieved if the alarm system comprising these elements is independent, self contained and kept separate from interior security. Therefore access portals and entry controls, and tactical response procedures are not included in the scope of this report.

Approaches to achieving both fast response and the performance numbers suggested by NRC Regulatory Guide 5.44, Rev. 2 May 1980 (1) are recommended in terms of detector layering and the combining of alarms through logic processing.

Regulatory guide 5.44 also suggests test procedures for verifying perimeter detection performance within statistical confidence limits. This report recommends approaches to testing against layered segments which will assure the Plant Managers of detectability yet which will minimize test trials and man hours.

Finally, relative budgetary costs are developed for candidate systems and for recommended testing procedures.

Section 2

2.0 NRC REQUIREMENTS FOR PERIMETER SECURITY

Requirements for physical protection of nuclear plants and materials are given in Title 10, Chapter 1, Code of Federal Regulations - Energy Part 73, (2). An interpretation of Part 73 is given in Nuclear Regulatory Guide 5.44, Rev. 2, May 1980 (1).

The emphasis of these two documents regarding utilities is directed toward:

- Measures that prevent radiological sabotage
- An immediate intrusion response
- Yearly review and audit of security procedures
- Continual test of security effectiveness

Reference 1 gives the following definitions and requirements for physical protection of plants and materials.

2.1 DESIGN-BASIS THREATS PER CFR PART 73.1

The following threats are given as a basis to design safeguards for nuclear power plants against radiological sabotage.

- A determined external assault, attack by stealth or deceptive actions by a small group with the following attributes, assistance and equipment:
  --Well-trained (including military training and skills) and dedicated individuals,
  --Inside assistance which may include a knowledgeable individual who attempts to participate in a passive role (e.g., provide information), an active role (e.g., facilitate entrance and exit, disable alarms and

communications, participate in violent attack), or both,

--Suitable weapons, up to and including hand-held automatic weapons equipped with silencers and having effective long range accuracy,

--Hand-carried equipment, including incapacitating agents and explosives, for use as tools of entry or for otherwise destroying reactor, facility, transporter or container integrity or features of the safeguards system, and

--The ability to operate as two or more teams.

- An individual, including an employee (in any position), and
- A conspiracy between individuals in any position who may have:

  --Access to and detailed knowledge of nuclear power plants or the facilities referred to in 73.20(a), or

  --Items that could facilitate theft of special nuclear material (e.g., small tools, substitute material, false documents, etc.), or both.

"Radiological sabotage" means any deliberate act directed against a nuclear power plant or against a component of such a plant which could directly or indirectly endanger the public health and safety by exposure to radiation.

2.2 PERTINENT DEFINITIONS PER CFR PART 73.2

"Physical barrier" means:

1. Fences constructed of No. 11 American wire gauge or heavier wire fabric, topped by three strands of more of barbed wire or similar material on brackets angled outward between 30° and 45° from the vertical, with an overall height of not less than eight feet, including the barbed topping;
2. Building walls, ceilings and floors constructed of stone, brick, cinder block, concrete, steel or comparable materials (openings which are secured by grates,

doors, or covers of construction and fastening of sufficient strength such that the integrity of the wall is not lessened by any opening), or walls of similar construction, not part of a building, provided with a barbed topping described in paragraph (f)(1) of this section of a height of not less than 8 feet; or

3. Any other physical obstruction constructed in a manner and of materials suitable for the purpose for which the obstruction is intended.

"Protected area" means an area encompassed by physical barriers and to which access is controlled.

"Vital area" means any area which contains vital equipment.

"Vital equipment" means any equipment, system, device, or material, the failure, destruction, or release of which could directly or indirectly endanger the public health and safety by exposure to radiation. Equipment or systems which would be required to function to protect public health and safety following such failure, destruction, or release are also considered to be vital.

"Material access area" means any location which contains special nuclear material, within a vault or a building, the roof, walls, and floor of which each constitute a physical barrier.

"Isolation zone" means any area adjacent to a physical barrier, clear of all objects which could conceal or shield an individual.

"Intrusion alarm" means a tamper indicating electrical, electro-mechanical, electro-optical, electronic or similar device which will detect intrusion by an individual into a building, protected area, vital area, or material access area, and alert guards or watchmen by means of actuated visible and audible signals.

"Guard" means a uniformed individual armed with a firearm whose primary duty is the protection of special nuclear material against theft, the protection of a plant against radiological sabotage, or both.

"Armed response personnel" means persons, not necessarily uniformed, whose primary duty in the event of attempted theft of special nuclear material or radiological sabotage shall be to respond, armed and equipped, to prevent or delay such actions.

"Bullet/resisting" means protection against complete penetration, passage of fragments of projectiles, and spalling (fragmentation) of the protective material that could cause injury to a person standing directly behind the bullet-resisting barrier.

"Force" means violent methods used by an adversary to attempt to steal strategic special nuclear material or to sabotage a nuclear facility or violent methods used by response personnel to protect against such adversary actions.

"Stealth" means methods used to attempt to gain unauthorized access, introduce unauthorized materials, or remove strategic special nuclear material, where the fact of such attempt is concealed or an attempt is made to conceal it.

"Deceit" means methods used to attempt to gain unauthorized access, introduce unauthorized materials, or remove strategic special nuclear materials, where the attempt involves falsification to present the appearance of authorized access.

2.3 SECURITY SYSTEM PERFORMANCE OBJECTIVES PER PART CFR 73.55

The licensee shall establish and maintain a physical protection system and security organization giving high assurance against radiological sabotage by adversaries as described in Paragraph 2.1.

At least one full time member of the security organization who has the authority to direct the physical security activities of the security organization shall be onsite at all times.

The licensee shall establish, maintain and follow written security procedures which document the structure of the security organization

and which detail the duties of guards, watchmen, and other individuals responsible for security.

2.4 PHYSICAL BARRIER REQUIREMENTS PER CFR 73.55(C)

The licensee shall locate vital equipment only within a vital area, which in turn, shall be located within a protected area such that access to vital equipment requires passage through at least two physical barriers of sufficient strength to meet the performance requirements for protection against industrial sabotage. More than one vital area may be located within a single protected area.

The physical barriers at the perimeter of the protected area shall be separated from any other barrier designated as a physical barrier for a vital area within the protected area.

Isolation zones shall be maintained in outdoor areas adjacent to the physical barrier at the perimeter of the protected area and shall be of sufficient size to permit observation of the activities of people on either side of that barrier in the event of its penetration. If parking facilities are provided for employees or visitors, they shall be located outside the isolation zone and exterior to the protected area barrier.

Detection of penetration or attempted penetration of the protected area or the isolation zone adjacent to the protected area barrier shall assure that adequate response by the security organization can be initiated. All exterior areas within the protected area shall be periodically checked to detect the presence of unauthorized persons, vehicles, or materials.

Isolation zones and all exterior areas within the protected area shall be provided with illumination sufficient for the monitoring and observation requirements of paragraphs (c)(3), (c)(4), of this section but not less than 0.2 footcandle measured horizontally at ground level.

The walls, doors, ceiling, floor, and any windows in the walls and in the doors of the reactor control room shall be bullet-resisting.

2.5 DETECTION AIDS REQUIREMENTS PER CFR 73.55(e)

All alarms required pursuant to this part shall annunciate in a continuously manned central alarm station located within the protected area and in at least one other continuously manned station not necessarily onsite, such that a single act cannot remove the capability of calling for assistance or otherwise responding to an alarm. The onsite central alarm station shall be considered a vital area and its walls, doors, ceiling, floor, and any windows in the walls and in the doors shall be bullet-resisting. The onsite central alarm station shall be located within a building such that the interior of the central alarm station is not visible from the perimeter of the protected area. This station shall not contain any operational activities that would interfere with the execution of the alarm response function.

All alarm devices including transmission lines to annunciators shall be tamper indicating and self-checking e.g., an automatic indication is provided when failure of the alarm system or a component occurs or when the system is on standby power. The annunciation of an alarm at the alarm stations shall indicate the type of alarm (e.g., intrusion alarm, emergency exit alarm, etc.) and location.

All emergency exits in each protected area and each vital area shall be alarmed.

2.6 TESTING AND MAINTENANCE REQUIREMENTS PER CFR 73.55(g)

Each licensee shall test and maintain intrusion alarms, emergency alarms, communications equipment, physical barriers, and other security related devices or equipment utilized pursuant to this section as follows:

1. All alarms, communication equipment, physical barriers, and other security related devices or equipment shall be

maintained in operable condition. The licensee shall develop and employ compensatory measures including equipment, additional security personnel and specific procedures to assure that the effectiveness of the security system is not reduced by failure or other contingencies affecting the operation of the security related equipment or structures.

2. Each intrusion alarm shall be tested for performance at the beginning and end of any period that it is used for security. If the period of continuous use is longer than seven days, the intrusion alarm shall also be tested at least once every seven (7) days.
3. Communications equipment required for communications onsite shall be tested for performance not less frequently than once at the beginning of each security personnel work shift. Communications equipment required for communications offsite shall be tested for performance not less than once a day.

2.7 RESPONSE REQUIREMENT PER CFR 73.55(h)

The licensee shall execute, when appropriate, a safeguards contingency plan for dealing with threats, thefts and industrial sabotage related to the nuclear facilities subject to the provisions of this section. Safeguards contingency plans shall be in accordance with the criteria in Appendix C to this part, "Licensee Safeguards Contingency Plans".

The licensee shall establish and document liaison with local law enforcement authorities.

The total number of guards, and armed trained personnel immediately available at the facility to fulfill these response requirements shall nominally be ten (10) unless specifically required otherwise on a case by case basis by the Commission; however, this number may not be reduced to less than five (5) guards.

Upon detection of abnormal presence of activity of persons or vehicles within an isolation zone, a protected area, or a vital area or upon evidence of intrusion into a protected area or a vital area, the facility security organization shall:

- Determine whether or not a threat exists,
- Assess the extent of the threat, if any,
- Take immediate concurrent measures to neutralize the threat by:
  --Requiring responding guards or other armed response personnel to interpose themselves between vital areas and material access areas and any adversary attempting entry for the purpose of radiological sabotage and to intercept any person existing with special nuclear material, and,
  --Informing local law enforcement agencies of the threat and requesting assistance.

The licensee shall instruct every guard and all armed response personnel to prevent or impede attempted acts of theft or radiological sabotage by using force sufficient to counter the force directed at him including the use of deadly force when the guard or other armed response person has a reasonable belief it is necessary in self-defense or in the defense of others.

To facilitate initial response to detection of penetration of the protected area and assessment of the existence of a threat, a capability of observing the isolation zones and the physical barrier at the perimeter of the protected area and assessment of the existence of a threat, a capability of observing the isolation zones and the physical barrier at the perimeter of the protected area shall be provided, preferably by means of closed circuit television or by other suitable means which limit exposure of responding personnel to possible attack.

2.8 PERFORMANCE CRITERIA OF NRC REGULATORY GUIDE 5.44

The position of Regulatory Guide 5.44, Rev. 2, May 1980, (1) is that perimeter alarm systems should continually demonstrate a probability

of detection (P_D) of at least 0.90 with 95% confidence. In addition, Guide 5.44 states the following:

> "Under normal environmental conditions including seasonal extremes, the total perimeter alarm system should not average more than one false alarm per week per segment and should not average more than one nuisance alarm per week per segment while maintaining proper detection sensitivity. Where the segment can be fully observed at all times, either visually or by closed circuit television, the false alarm rate and nuisance alarm rate may be increased to one alarm per day per segment."

Whereas these criteria are not regulations, the premise is taken that the utility operator, as well as the NRC, needs assurance through testing that the perimeter system maintains the sensitivity to detect a real intruder and that a real intrusion signal will be distinct from the "noise" of nuisance alarms.

Section 3

3.0 ADDITIONAL PERFORMANCE RECOMMENDATIONS

A security system to meet the performance requirements of the preceding paragraphs must provide the following functions.

1. Protective barriers and intrusion detection devices at the perimeter to deter attack, to provide early detection of attack, and to delay access to vital equipment.
2. Armed guards to deter attack, to respond to attack, to confront and contain intruders, to deny access to vital equipment.
3. Liaison and communication with law enforcement authorities capable of rendering assistance in countering escalation of attacks and in apprehending and charging intruders.

Implementation of these functions suggests deriving second level requirements from a further more complete description of the threat human factor and his equipment and from response force human capabilities, aids and countermeasures.

3.1 THREAT CHARACTERIZATION

The following paragraphs describe the probable types and nature of human intrusion so as to provide measures to deter or increase the difficulty of intrusion and/or increase the probability of detection. Descriptions are derived from references 3 and 4.

3.1.1 SKILLED AND WELL EQUIPPED INTRUDERS

These intruders would attempt penetrations to conduct sabotage and theft of sensitive or very high value items. They could be expected to plan their entry thoroughly and to carefully select the time and method of entry. Highly skilled intruders using professional, advanced techniques would probably attempt to covertly defeat or circumvent the intrusion detection and other physical protective measures. Personnel who work in and have intimate knowledge of vital areas and the security system itself are potential internal threats. They may be external threats as well-contributing to the skill and knowledge level of a second party. They may use their knowledge of how to defeat a sensor system in order to carry sabotage material through the perimeter without being detected. Once inside undetected, the well prepared intruder could employ normal badge identification to avoid apprehension if challenged.

On the other hand, skilled intruders, knowing the vulnerabilities of the barriers employed could well conduct a limited surprise attack with the knowledge that they could get in, accomplish their mission and escape before the guards could arrive on the scene. Such skilled intruders would be expected to transport and deploy equipment to effect quick entry and escape.

3.1.2 SEMI-SKILLED INTRUDERS

These intruders would attempt penetration to conduct terrorist or paramilitary activities, theft for profit, and/or vandalism. In addition, highly motivated and capable dissident groups or individuals may try to reduce confidence in or embarrass the nuclear establishment, embarrass the government, or create a dramatic incident to attract public attention. They would be expected to attempt entry without detailed planning or highly sophisticated equipment. They may evaluate the security posture by considering appropriate time factors, location vulnerability, and personnel/guard presence. They may attempt to bypass or otherwise defeat an intrusion detection system by covert means.

3.1.3 ORGANIZED FORCE

Well organized units can be expected to use overt force and diversionary actions to gain entry. Efficiency, depth of planning, execution, and size of acting force may vary greatly. Calling the LLEA will be necessary to upgrade the defense or security posture required to effectively counter this threat.

Demonstrators or protesting mobs may come equipped and organized to apply graduated levels of force to obtain entry or concessions. The situation could escalate to acts of sabotage, unless countered.

3.1.4 CASUAL INTRUDERS

These intruders would attempt penetration with little or no advance planning and without apparent rational purpose. They include thrill seekers and individuals who are mentally deranged or intoxicated. While they represent no sabotage threat in the usual sense, it is possible they might either inadvertently or with malicious intent cause considerable damage. An intrusion detection system should detect these intruders with very high confidence.

3.1.5 ATTRIBUTES OF THE LIKELY DESIGN-THREAT

RAND and SANDIA in reference 3 have attempted to classify potential criminal adversaries of United States nuclear programs. A composite description, which matches the design threat of paragraph 2.1, consists of three to six adversaries, armed with automatic weapons, possessing high explosives and hand and power tools, using a variety of ground transportation modes, having middle- to high-level technical skills and a varying willingness to accept high risks, possessing some inside information or assistance, and displaying a moderate to high degree of ingenuity and careful advanced planning. The typical composite profile represents one reference point on a scale of adversary capabilities. These attributes at least will be necessary for any adversary whose objectives are penetration and sabotage regardless of

whether he is a terrorist or criminal and whatever his apriori motivation. Such a small group can be assembled and brought to the perimeter without notice. The group will probably devote its resources to achieving a single breach.

According to reference 3, higher levels of attack to overrun the nuclear facility would involve a force build up and employment of special vehicles and equipment not easily disguised and would probably be discovered in the neighborhood before it could be tactically positioned. However, this is also to say that nuclear plants regardless of barriers and hardening would be vulnerable to a commando type attack which employed demolition weapons and heavy vehicles.

3.1.6 VEHICLE THREAT

Common road vehicles (e.g. 3/4 ton pickup (5)) can break most fences in negligible time and then be used to ram a building wall. A vehicle can carry equipment and explosives right up to a wall breach for further penetration into vital areas (estimated within 2 minutes) before guards can be dispatched and arrive on the scene.

Some power plant perimeter systems do not have barriers which either will prevent vehicle penetrations or pose risk of injury to the vehicle occupants.

Therefore, a common, available, perhaps unsuspicious vehicle will be a likely assault tool for an intruder bent on sabotage. It buys him unopposed time to accomplish his mission. It is therefore suggested that the outside threat definition include common road vehicles (implying that vehicle countermeasures be considered).

3.2 RELIABLE ALARMS

A sensor system producing many false alarms (several per day) will tend to become ignored by the human surveillance factor.

Some perimeter sensors such as microwave and the E-field fence produce false alarm rates (FAR) higher than several per day.

Consequently, in single layer perimeter systems, true alarms may tend to be overlooked increasing the likelihood of successful perimeter intrusion.

Regulatory Guide 5.44 suggests that a combination of sensors (such as provided by layering and logic processing) in addition to alternative assessment capabilities such as video, may decrease nuisance alarm rates and also increase the probability of detection.

3.3 PROMPT RESPONSE CAPABILITY

Given a vehicle barrier which will prevent transport of ramming means and other penetration aids close to a vital area, the threat de-escalates to being man carried. However, the time it takes an intruder to cross perimeter barriers, to carry explosives across clear zones and to actually breach two layers of walls or doors is still very short per the SANDIA Barrier handbook(5). This time for a resolute knowledgeable intruder is about 4 minutes to 5 minutes per Table 1.

Table 3-1
ESTIMATED TIME TO REACH/BREACH VITAL AREA

Event	Response	Mean Time For Event
Climb 1st Fence	Signal	10
Run 20 Feet	Alarm-Locate-Dispatch	2
Climb Vehicle Barrier	Video Locate - Call LLEA	4
Jog 100 Feet	Video Locate	16
Drill Door - 1st Wall	Alarm-Locate	102
Find Vital Area		4
Drill Door - Vital Area	Alarm-Locate	102
		240 seconds

: Required Guard Intercept Time - 4 Minutes

Source: Barrier Technology Handbook (Sand 77-0077) (5)

Some nuclear power plant security force perimeter surveillance, alarm assessment, response force manning and dispatch procedures assume a much longer time interval available to classify alarms, to analyze the threat, to confront the intruders and to call in local law enforcement agencies (LLEA) to neutralize the intruders (6).

Consequently sabotage may be accomplished before a cognitive threat evaluation can be completed and before the LLEA can arrive.

Given the provision of reliable alarms and immediate CCTV location assessment, it is suggested that guard force manning, guard post location, guard equippage and rapid travel routes to all vital locations be established to enable prompt response in the time required to prevent sabotage.

Section 4

4.0 SYSTEM CONSIDERATIONS

It is probably not demonstrable that present power plant security forces can respond to a detected outside intruder and intercept him before he can do damage. On the other hand, it is hypothesized that a security system can be designed to effectively deter vehicles, reliably alarm upon intrusions and procedurally enable intruder inderdiction within a 5 minute critical time frame.

The premises and conclusions of Section 3.0 suggest an approach to achieving time for response by means of reliable detection and assessment equipment and by means of barriers, isolation zones and open terrain - all of those perimeter elements now employed, but perhaps in new arrangements which can benefit from existing signal processing technology.

4.1 SENSOR LAYERING AND PROCESSING OPTIONS

Various types of commercially available sensors can be installed along a perimeter to provide a single layer of intruder detection capability. Each of these sensor types will provide a high probability of detecting certain attributes of an intrusion act, i.e. running or walking, climbing, cutting, etc. However, each sensor type will also:

- Falsely alarm due to other than intruder-related events and stimuli, referred to as nuisances, and
- Can be defeated or by-passed by a skilled intruder by some unorthodox intrusion method, for example bridging, vaulting, tunneling, or even target masking.

To overcome these deficiencies and improve system performance, it is prudent to install two or more layers of diverse sensors along the

perimeter. Sensor arrays in layers which are combined or connected so that intrusions detected in one phenomenon are serially detected in another, hold promise for processing discrimination. Two or more phenomenological echelons of detection can assure that nuisance sources are rejected and that only credible alarms are acted upon.

In such layered combinations, detection becomes conditional. Therefore if an intrusion has a given probability of alarming in one layer, the combined probability of alarm is increased as each subsequent layer is passed. For example, if each layer has an inherent P_D of 0.95, the P_D for two layers becomes $1-(1-.95)^2 = 0.9975$, and so on.

4.1.1 COMPLEMENTARY SENSOR LAYERING

The layered system design concept colocates complementary sensors which are based on different detection principles to extend the system's sensitivity to alternative intrusion methods. For example, the taut wire sensor virtually precludes undetected penetration of the fence plane itself, and exhibits extremely low false alarm rates. However, this sensor can be defeated by bridging over or tunneling under the fence structure. A complementary sensor, for example, a video motion detector will detect intruder movement within the camera field-of-view; however, it will also produce nuisance alarm due to movements of animals, vegetation, and wind-blown debris. These sensor types can complement each other in the following ways:

- The fence itself eliminates most video motion detector nuisance alarm sources of origins exterior to the fenced perimeter. The taut wire sensor precludes undetected intruder breach of the fence structure.
- The video motion detector's sensitized field-of-view, restricted to the region internal to the fence plane, provides for detection of a fence bridging attempt, a tunneling attempt, or other motion within the isolation zone.

The layered sensor design concept places multiple sensors along the possible intrusion paths. Although the intruder's probability of

undetected penetration of one layer may be attractive (to him), the joint probability of undetected penetration through all sensor layers can be made arbitrarily small as the number of layers is increased.

4.1.2 SENSOR ALARM PROCESSING

Intrusion sensor alarm signals are data-linked to a central Alarm Station for display to the security operator and officer in charge (OIC). An Alarm Station terminal which simply indicates the alarm status of each installed sensor does provide the basic alarm information of potential intruder presence and location, but will also indicate all false or nuisance alarm conditions. In a layered sensor design, the percentage of false or nuisance alarm conditions reported can be significantly reduced by computer preprocessing of the raw sensor alarm data. Such interface processing reflects the complementary character of the installed sensor types, and permits measures of nuisance alarm sources such as meteorological and power load switching phenomena to be considered in determining the significance of raw sensor alarm data. The interface processor may also be configured to provide display outputs which assist the operator in differentiating between a confirmed intrusion, requiring an immediate and maximum response, and a possible intrusion warranting remote video assessment and confirmation before committing a maximum response.

An Alarm Station interface processor might additionally be programmed to:

- Automatically display alarmed sector video on the CCTV monitors if any single layer is alarmed,
- signal (audible and visual output) a "certain" intrusion requiring maximum immediate response if two or more layers alarm in the same perimeter segment.
- Signal a "probable" intrusion requiring limited immediate response if only the fence sensor alarm is received,
- Signal a "potential" intrusion requiring remote CCTV assessment before commitment of response forces if only an isolation zone alarm is received.

4.1.2.1 The Reduction of Nuisance Alarms

Nuclear Regulatory Commission guidelines suggest false and nuisance alarm goals of one per week per segment for a system without surveillance of the isolation zone. This is relaxed to one per day if surveillance of the isolation zone is present.

Raw sensor outputs may not now satisfy these recommendations. For example, false and nuisance alarm rates are in the order of 24 per day for a video motion detector, and 10 per day with an E-field fence. One per day for a fence disturbance sensor is expected under normal conditions; but in high winds the nuisance alarm rate increases significantly.

One solution to this dilemma is the use of time integration signal processing supplemented with an "And Mostly" logic circuit.

Processing gain is enabled by time integration sequencing; and, for any single sensor with a "time window", the false or nuisance alarm rate, NAR, approaches:

$$NAR_P = NAR_R \exp\left(-\frac{T}{t_{FA}}\right) \qquad (4\text{-}1)$$

NAR_P = processed false alarm rate

NAR_R = raw false alarm rate

where T = time of integration

t_{FA} = time duration of false alarm.

For example, if for the fence sensor T = 10 seconds, t_{FA} = 1 second and NAR_R = 1 per day, then

$$NAR_P = \exp\left(-\frac{10}{1}\right) = .000045 \text{ per day} \qquad (4\text{-}2)$$

For the E-field fence let t_{FA} = 1/4 second, T = 1 second, and NAR_R = 10 per day then:

$$NAR_P = 10 \exp\left(-\frac{1}{1/4}\right) = 0.183156 \text{ per day} \quad (4\text{-}3)$$

For the video motion detector let t_{FA} = 1/30 second, T = 8/30 second and NAR_R = 24 per day, then:

$$\text{then } NAR_P = 24 \exp\left(-\frac{8/30}{1/30}\right) = 0.008051 \text{ per day} \quad (4\text{-}4)$$

The expected combined false alarm rate for this 3 layered system would be:

$$NAR_{SYSTEM} = NAR_{VMD} + NAR_{E\text{-}FIELD} + NAR_{FENCE} \quad (4\text{-}5)$$
$$= 0.191253 \text{ per day or } 1.338770 \text{ per week}$$

This expected rate is within NRC guidelines for visual or video assessment.

An example of time integration, sequencing and "and mostly" processing is shown in Figure 4-1.

Consider the fence sensor. The first signal above threshold sets the logic for one input to an AND circuit and opens a second channel 1 second later. If during the following 9 seconds a signal above threshold occurs, the second input to the AND circuit is set and an alarm is output through the OR circuit. If no other signals above threshold occur during the next 9 seconds, the input to the AND is reset and no alarm is output. Alternatively, time integration may be implemented through a counter which would accumulate a set number of disturbances before alarming. The E-field fence is handled similarly except that the time periods have been shortened to 1/4 second and one second.

The first frame of the Video Motion Detector which detects movement initializes a counter to one and starts counting succeeding frames where motion occurs. If 8 consecutive frames indicate motion, a detection is output to be ANDed with other sensors.

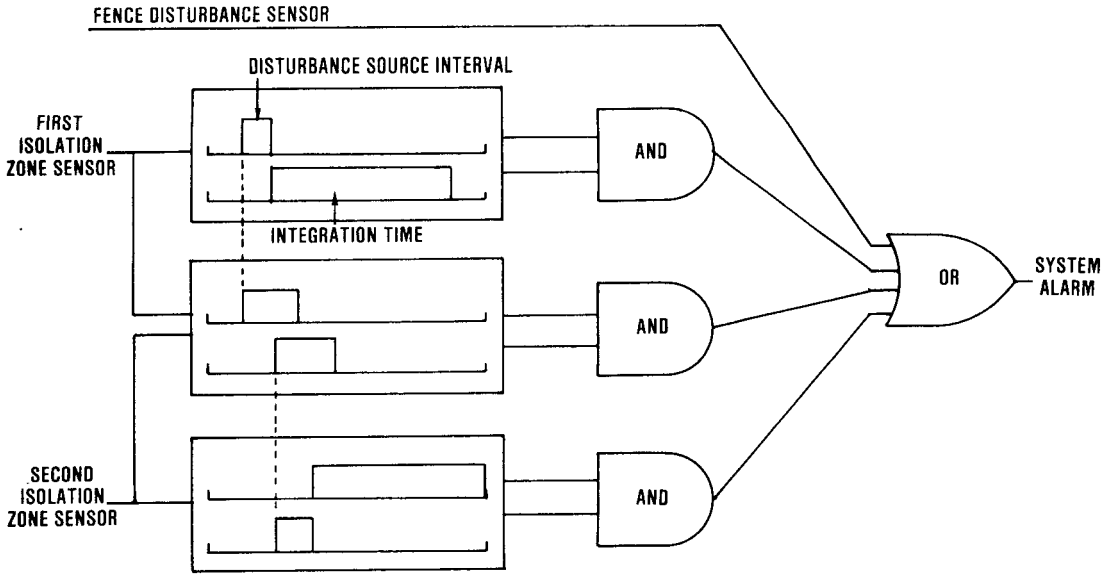


Figure 4-1 Layered Sensor Logic

The processor can be set up to work with sensor pairs using time sequencing appropriate to the specific detection phenomena. The fence borders the isolation zone covered by the video motion detector.

Therefore a signal from the fence sensor sets one input of an AND circuit and opens the gate to accept video motion detector signals for the next 9 seconds. If a motion detection in signal occurs within this time period an alarm is output, otherwise the inputs to the AND gate are reset.

Similar pairing can be performed using the E-field fence and VMD as a pair and the fence sensor and E-field fence as a pair. This is illustrated in Figure 4-1.

This type of signal processing on sensor signals allows a high probability of detection while holding false alarms to an acceptable level.

In operation, a strong persistent signal from a single layer will activate the alarm. A transient activation of a sensor requires confirmation of another and diverse sensor before an alarm is sounded. This allows the system to approach the high P_D of layers connected with OR circuitry and maintain a false alarm rate which approaches that of sensors connected by AND circuitry. The specific sensors' integration times, and logic chosen for a particular installation must be tailored to the environment and requirements at a specific plant site. Individual integration and delay times can be set independently for each sensor and sensor pair utilizing an alarm processing interface.

Examples of both FAR/NAR and P_D improvement are shown in Figure 4-2.

4.1.2.2 EVALUATION OF STAND-ALONE ALARM PROCESSORS

Several micro-computer based alarm processors are available which perform some of the control functions discussed in preceding paragraphs but which are not programmed to combining signals from sensor layers.

SENSOR TYPE	FAR/NAR ALARM CATEGORY	CALCULATION PARAMETERS	SINGLE SENSOR P_D	SINGLE SENSOR FAR	TWO LAYER COMBINED FAR	TWO LAYER P_D
PORTED COAX	NUISANCE ALARMS	3 SEC. AVG. DURATION OF ALARM	0.95	0.5/DAY	0.037/DAY	0.9975
MICROWAVE			0.95	0.5/DAY		
ACOUSTIC TRANSDUCER	BACKGROUND NOISE	1-10 HZ B.W. 5 dB S/N 1 SEC AVG DURATION OF ALARM	0.95	50/DAY	0.24/DAY	0.9848
GEOPHONE			0.85	50/DAY		
MICROWAVE	NUISANCE ALARMS	3 SEC AVG DURATION OF ALARM	0.95	0.5/DAY	0.578/DAY	0.99622
VIDEO MOTION DETECTION		8 FRAME ALARM SOURCE 1 SEC ALARM DURATION	0.99	24/DAY		

NAR (AND MOSTLY) = NAR ss $(e^{\frac{-t_1}{\Delta t}})$

P_D (AND MOSTLY) = $P_{D_{ss}}$ $(1 - e^{\frac{-t_1}{\Delta t}})$

t_1 = FIRST TIME INTEGRATION INTERVAL

Δt = DURATION OF FALSE ALARM SOURCE

Figure 4-2 Reduction of False & Nuisance Alarms "And Mostly" Examples

Their features are evaluated and compared to recommended features and functions of a multi-layer processing interface as developed from Section 3.0 requirements and the system considerations of previous paragraphs. A study of this comparison shown in figure 4-3 leads to the conclusion that none of the hardware listed (which may not be all inclusive) has all of the features desired, but that a microprocessor (micro computer) based system can provide all of these features if configured and programmed to do so. The flexibility of a microcomputer system is indicated by its conceptual configuration blocked out in figure 4-4.

4.2 SENSOR EVALUATION CRITERIA

Candidate individual sensors will be screened by application of the following criteria taken in order.

- Commercial availability of the sensor, and any applicable test or field experience.
- Low vulnerability to defeat, either inherent in the sensor technology or determined by test experience.
- Performance potential as demonstrated by a high single sensor P_D and low FAR based on field or test experience, or based on theoretical S/N predictions.
- Potential for array correlation or cross-phenomenon signal matching and processing.
- Life Cycle Cost/Effectiveness.
- Mean time between failures (MTBF).

Individual sensor performance values become the critical consideration in evaluating and predicting a total system capable of meeting the required P_D and NAR. P_D and NAR values for individual sensors determine the technologies to be combined, the number of elements in an array, the number of layers of different detection phenomena and the complexity of processing required. Vendor claims lacking backup data are suspect. Therefore, only systems will be considered which previously have been used on similar sites, and for which test or field experience is available.

ALARM PROCESSOR	GENERAL DESCRIPTION	HARDWARE: MAIN PROCESSOR (CPU)	HARDWARE: SECONDARY/ PRE-PROCESSOR	HARDWARE: MEMORY VOLATILE	HARDWARE: MEMORY NON-VOLATILE	HARDWARE: SERIAL I/O CAPABILITY	HARDWARE: PARALLEL I/O CAPABILITY	HARDWARE: SPECIAL LINE DRIVERS/RECEIVERS	INTERFACE CHARACTERISTICS: SENSOR INTERFACE: ADAPTABILITY: LAYERED ALARM SEGMENTS	ADAPTABILITY: MAXIMUM NUMBER ALARM SEGMENTS	ADAPTABILITY: MAXIMUM NUMBER SENSOR POINTS	ADAPTABILITY: TRANSPONDER COMPATIBILITY	ADAPTABILITY: DIRECT SENSOR COMPATIBILITY	POLLING TECHNIQUE: DUPLEX POLLING	POLLING TECHNIQUE: RS422 COMPATIBLE	POLLING TECHNIQUE: DATA RATE	POLLING TECHNIQUE: POLLING TIME	MULTIPLEXED SIGNALS	CAS/SAS INTERFACE
RECOMMENDED MULTI-LAYER ALARM PROCESSING INTERFACE	ALARM PRE-PROCESSOR INTERFACES CAS/SAS WITH PERIMETER SENSOR FIELD OF UP TO THREE LAYERS	INTEL 80/10 SINGLE BOARD COMPUTER 8085A MICROPROCESSOR	INTEL SBC 544 INTELLIGENT COMMUNICATIONS CONTROLLER 8085A MICROPROCESSOR	STATIC RAM/ DYNAMIC RAM	EPROM - FIRMWARE STORAGE EAROM - RELIABLE, INTERNALLY ALTERABLE FIRMWARE STORAGE	5 RS232C SERIAL PORTS AND 52 PARALLEL I/O LINES OR 6 RS 232C SERIAL PORTS AND 34 PARALLEL I/O LINES		UNDEDICATED WIRE WRAP BOARD SPACE ALLOWS NEW DEVICES/ DIFFERENT CONFIGURATIONS	YES 3 LAYERS/ SEGMENT	256	2048	PARALLEL OR SERIAL DIGITAL DATA, VARIABLE FORMAT	SWITCH CONTACT OR SERIAL DIGITAL	YES	YES	9600 BAUD	1.5 SEC	YES	YES
VINDICATOR SMS-2000M	STAND-ALONE ALARM MONITOR/ RECORDER	CUSTOM PROCESSOR CARD	NONE	ERROR CORRECTING RAM	EPROM - FIRMWARE STORAGE	5 SERIAL PORTS 2 POLLING 2 RESPONSE 1 PRINTER	16 PARALLEL LINES 8 KEYBOARD 8 DISPLAY	ONLY AS AN ADDITIONAL INTERFACE UNIT	NO	255	1020 (WITH DUAL LOOP)	ASYNCHRONOUS SERIAL DIGITAL DATA, PROPRIETARY FORMAT	NONE	OPTIONAL, WITH TWO TRANSPONDERS PER SEGMENT	NO	10000 BAUD	1.22 SEC	YES	NOT PRESENTLY CONFIGURED AS A PRE-PROCESSOR
STELLAR SYSTEMS MARS-1000	STAND-ALONE ALARM MONITOR/ RECORDER	PROPRIETARY SINGLE BOARD COMPUTER	NONE	DYNAMIC RAM	EPROM - FIRMWARE STORAGE	6 RS232C SERIAL PORTS (2 FOR POLLING)	NONE	NONE	NO	128	1024	ASYNCHRONOUS SERIAL DIGITAL DATA, PROPRIETARY FORMAT	NONE	YES: RANDOMLY CHANGES TRANSPONDER ADRESSES	YES	4800 BAUD	1.5 SEC	YES	NOT PRESENTLY CONFIGURED AS A PRE-PROCESSOR
STELLAR SYSTEMS 2450	ADD-ON CARD PRE-ANNUNCIATOR	CUSTOM PROCESSOR CARD	NONE	N/A	N/A	RELAY CONTACT INTERFACE 2 INPUTS 1 OUTPUT		NONE	YES 2 LAYERS/ SEGMENT	N/A	N/A	N/A	SWITCH CONTACT SIGNALS	N/A	N/A	N/A	N/A	N/A	INTENDED AS AN ADD-ON CARD
KELTRON SIRS 700	COULD FUNCTION AS CAS/SAS; ADAPTIBLE TO MULTI-LAYER PROCESSOR IDEA	DEC PDP-11/03 MINI-COMPUTER	NONE	STATIC/DYNAMIC RAM POSSIBLY SOME CORE MEMORY	FLOPPY DISCS - PROGRAMS ARE LOADED INTO RAM ON EACH POWER-UP	CAN INTERFACE TO DM-701 OR TO OTHER SENSOR SYSTEMS THROUGH A CUSTOM INTERFACE		ONLY AS AN ADDITIONAL INTERFACE UNIT	POSSIBLE, BUT NO ALARM PROCESSING IS PRESENTLY PROVIDED	DEPENDS ON SOFTWARE AND INTERFACE	DEPENDS ON SOFTWARE AND INTERFACE	PARALLEL OR SERIAL DIGITAL DATA, VARIABLE FORMAT	SWITCH CONTACT OR SERIAL DIGITAL	DEPENDS ON INTERFACE	DEPENDS ON INTERFACE	DEPENDS ON INTERFACE	DEPENDS ON INTERFACE	YES	NOT PRESENTLY CONFIGURED AS A PRE-PROCESSOR
KELTRON DM-701	STAND-ALONE ALARM MONITOR/ RECORDER	CUSTOM PROCESSOR CARD	NONE	DYNAMIC RAM	EPROM - FIRMWARE STORAGE	25 TWISTED PAIR LINES (PROPRIETARY) PRESENTLY DEDICATED TO KELTRON TRANSPONDERS AND CAS/SAS		NONE	NO	56, WITH DEP32 TRANSPONDER	1000	COMPATIBLE WITH KELTRON TRANSPONDERS ONLY	NO	NO	NO	N/A	200 mS	YES: WITH AUXILLIARY MONITOR DM-600	YES
RECEPTORS, INC. CP 8400	STAND-ALONE ALARM MONITOR/ RECORDER	CUSTOM PROCESSOR CARD	MODULE OFFERED TO SWITCH BETWEEN DUAL 8400 CPU'S	DYNAMIC RAM	EPROM - FIRMWARE STORAGE	4 RS232C SERIAL PORTS (DLV11-J OPTION)	NONE	NONE	NO	32	4096	ASYNCHRONOUS SERIAL DIGITAL DATA, PROPRIETARY FORMAT	YES	YES	YES	38,400 BAUD	15 mS	YES	NOT PRESENTLY CONFIGURED AS A PRE-PROCESSOR
VIDEO TEK, INC. SLS-100	ALARM SYSTEM MONITOR/RECORDER	CUSTOM PROCESSOR CARD: 6809 MICRO-PROCESSOR	NONE	DYNAMIC RAM	ROM - FIRMWARE STORAGE	2 SERIAL PORTS 1 RS 232C 1 PROPRIETARY	96 PARALLEL LINES 64 SENSOR INPUT 16 INTERFACE 16 CONTROL	NONE	POSSIBLE, BUT NO ALARM PROCESSING IS PRESENTLY PROVIDED	PROCESSES DATA FROM EXISTING SENSOR INTERFACE		PARALLEL OR SERIAL DIGITAL DATA, VARIABLE FORMAT	YES	YES	N/A	2400 BAUD	N/A	YES	YES
ICI SYSTEMS, LTD.	DISTRIBUTED PROCESSOR FOR CENTRAL COMPUTER BASED SYSTEM	CUSTOM PROCESSOR CARD: 6800 MICRO-PROCESSOR	NONE	DYNAMIC RAM	ROM - FIRMWARE STORAGE	10 SERIAL PORTS RS 232C (WITH 8 CS-1008 I/O BOARDS)	128 PARALLEL LINES (OPEN COLLECTOR)	SPACE PROVIDED FOR OPTIONAL I/O BOARDS	PROCESSING PROVIDED ON A CUSTOMIZED BASIS		10000	ASYNCHRONOUS SERIAL DIGITAL DATA, VARIABLE FORMAT	YES	YES (AT 4800 BAUD)	YES	9600 BAUD	0.5 SEC	YES	YES: SPECIALLY CONFIGURED FOR A CAS/ SAS INTERFACE

ALARM PROCESSOR	PROGRAMMING FEATURES: ALARM PROCESSING: COMBINING LOGIC	ALARM PROCESSING: ANNUNCIATION OF SINGLE SENSOR EVENTS	FIELD PROGRAMMABILITY: TIME WINDOW ADJUSTMENT	FIELD PROGRAMMABILITY: PRIORITIZED ALARM REPORTING	FIELD PROGRAMMABILITY: ALARM RESET	FIELD PROGRAMMABILITY: SENSOR ACCESS COMMAND	SELF-ADJUSTING SENSOR THRESHOLDS: ENVIRONMENTAL ADAPTABILITY	SELF-ADJUSTING SENSOR THRESHOLDS: SENSOR NOISE IMMUNITY	SELF-TEST: PROCESSOR SELF-TEST	SELF-TEST: SENSOR TEST	FAILURE ANNUNCIATION: PROCESSOR	FAILURE ANNUNCIATION: SENSOR NETWORK	GROWTH POTENTIAL: COMPATIBLE WITH PROGRAMMABLE TRANSPONDERS	GROWTH POTENTIAL: REDUNDANT I/O ALLOWS EXPANSION	SECURITY FEATURES: RELIABLE DATA STORAGE (NON VOLATILE)	SECURITY FEATURES: TAMPER INDICATOR	SECURITY FEATURES: UNINTERRUPTIBLE POWER SUPPLY	SECURITY FEATURES: BUILT-IN HARDWARE REDUNDANCY	SECURITY FEATURES: LINE SUPERVISION	SECURITY FEATURES: OVER-VOLTAGE PROTECTION
RECOMMENDED MULTI-LAYER ALARM PROCESSING INTERFACE	MULTI-LAYER APPROACH: "AND-MOSTLY" LOGIC/ TIME INTEGRATION OF EVENTS	YES	1 SECOND TO 60 SECONDS	YES: PER ALARM SEGMENT	YES: MANUAL AND PROGRAMMABLE	YES	ADAPTS TO WEATHER AND SOIL CHANGES	RESISTANT TO BACKGROUND SENSOR NOISE	YES	YES	YES: NOTES PROCESSOR FAILURE AS AN ALARM	NOTES INDIVIDUAL SENSOR FAILURES	YES: VARIBLE INTERROGATION FORMAT	3 SPARE RS232C SERIAL CHANNELS	ALL LONG-TERM STORAGE IN PROM & EAROM	YES	YES: 4 HR BATTERY BACKUP	YES: SECONDARY PROCESSOR AND SPARE I/O	YES: TIME DOMAIN REFLECTOMETRY	YES
VINDICATOR SMS-2000M	SINGLE EVENT REPORTING: NO PRE-PROCESSING	YES	NO	5 LEVELS	MANUAL ONLY	YES	MANUAL DIGITAL THRESHOLD ADJUST	NON-ADAPTIVE; RESISTANT TO ELECTRICAL NOISE	YES	YES	YES: NOTES PROCESSOR FAILURE AS AN ALARM	NOTES INDIVIDUAL SENSOR FAILURES	NO	NO	NO: SOME LONG-TERM PROGRAMMING STORED IN RAM	YES	YES: 4 HR BATTERY BACKUP	REDUNDANT DATA FORMATTING; LITTLE HARDWARE REDUNDANCY	YES	YES
STELLAR SYSTEMS MARS-1000	SINGLE EVENT REPORTING: NO PRE-PROCESSING	YES	NO	16 LEVELS, ASSIGNABLE TO EACH SENSOR	MANUAL ONLY	YES	MANUAL DIGITAL THRESHOLD ADJUST	NON-ADAPTIVE	NO	YES	NO	NOTES GENERAL SENSOR NETWORK FAILURES	NO	NO	NO: LONG-TERM STORAGE PROBABLY IN RAM	NO	YES: 1 HR BATTERY BACKUP; SEPARATE TRANSPONDER SUPPLIES	YES: REDUNDANT I/O PORTS	YES	NO
STELLAR SYSTEMS 2450	"ANDS" ALARM GROUPS TOGETHER BEFORE REPORTING	NO	15 SECONDS TO 120 SECONDS	N/A	N/A	N/A	MANUAL ANALOG THRESHOLD ADJUST	NONE	N/A	N/A	N/A	NO	NO	NO	N/A	NO	N/A	NO	NO	NO
KELTRON	NO MULTIPLE ALARM PROCESSING PRESENTS HISTORY WITH ALARM	YES	N/A	HISTORY AND PERTINENT DATA PRESENTATION ALLOW OPERATOR TO PRIORITIZE	MANUAL ACKNOWLEDGEMENT ONLY	YES	NONE	NONE	YES	POSSIBLE, BUT NOT OFFERED	YES: PROVIDES A COMPLETE ERROR MENU	NO	YES, WITH NEW SOFTWARE	N/A	LONG-TERM STORAGE ON FLOPPY DISC BACK-UPS REQUIRED	NO	YES	NO	YES	YES
KELTRON DM-701	NO PROCESSING: FUNCTIONS SIMPLY AS A MONITOR FOR CAS/SAS	YES	N/A	2 LEVELS, ASSIGNABLE TO EACH SENSOR	MANUAL ONLY	YES	NONE	NONE	YES: CHECKS ONLY FRONT PANEL FUNCTIONS	NO	YES: PROCESSOR FAILURE LIGHTS PCB-MOUNTED LED'S	NOTES INDIVIDUAL SENSOR FAILURES	NO: POLLING METHOD FIXED	NO	LONG-TERM STORAGE IN PROM	NO	YES	SOME REDUNDANT CONTROL FEATURES	YES	YES
RECEPTORS, INC. CP 8400	SINGLE EVENT REPORTING: NO PRE-PROCESSING	YES	N/A	YES: 8 LEVELS	MANUAL ONLY	YES	NONE	NONE	YES	YES	YES: NOTES PROCESSOR FAILURE AS AN ALARM	NOTES INDIVIDUAL SENSOR FAILURES	NO	YES: WITH OPTIONAL BOARDS	LONG-TERM STORAGE ON FLOPPY DISC BACK-UPS REQUIRED	YES	YES	PROVIDES SWITCHING CONTROL FOR DUPLICATE HARDWARE	YES	NO
VIDEO TEK, INC. SLS-100	SINGLE EVENT REPORTING: NO PRE-PROCESSING	YES	N/A	N/A	MANUAL ONLY	YES	NONE	NONE	NO	YES	N/A	NOTES INDIVIDUAL SENSOR FAILURES	NO	NO	LONG-TERM STORAGE IN ROM	NO	NO	NO	NO	NO
ICI SYSTEMS, LTD.	PROCESSING IS USER TAILORED	YES	N/A	SOFTWARE DEPENDENT			NONE	NONE	YES	YES	YES: NOTES PROCESSOR FAILURE AS AN ALARM	NOTES INDIVIDUAL SENSOR FAILURES	YES	PRESENT DESCRIPTION IS AT MAXIMUM EXPANSION OF I/O	LONG-TERM STORAGE IN ROM	YES	YES	YES: BUILT-IN SPARE I/O	YES	YES

Figure 4-3 Comparison of Some Available Stand-Alone-Alarm Processors

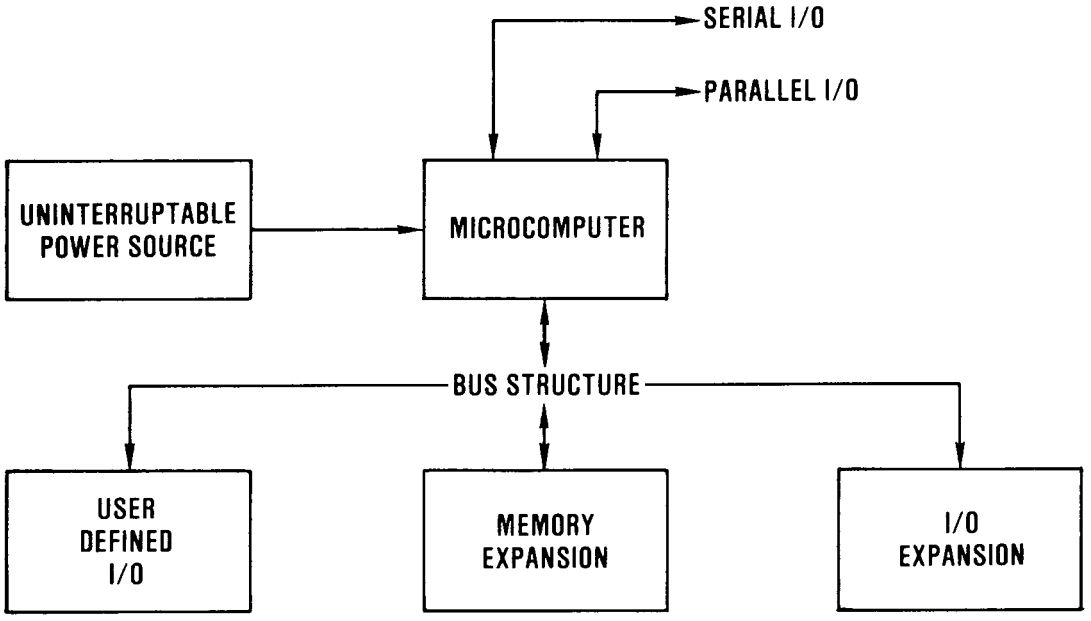


Figure 4-4 Micro Computer System Flexibility

Vendor claims will be derated, depending on the time accumulation of credible performance, and identification of FAR/NAR sources. Site dependent systems require a "back-in" strategy in which measurement of site characteristics and on-site calibration of thresholds and dynamic range will determine array configuration and processing to meet P_D, and NAR goals.

Mean-time-between-failure, (MTBF) is a major systems consideration affecting the control of cost and performance. It is manifested in a parts count of high individual reliability and/or redundancy. Equipment failures can impose operational maintenance penalties, and by definition of failure-in-the-alarm-state, will contribute to the false alarm budget. The sensor count in an array, and the number of arrays, becomes an MTBF trade-off against processing capability to be provided.

4.3 CENTRAL AND SECONDARY ALARM STATIONS AND ASSESSMENT

The Alarm Station is the focal point for command and control of security resources and activities. A Central Alarm Station (CAS) is equipped to serve as a primary command and control center. The Secondary Alarm Station (SAS) is equipped both to validate the operations of the CAS, and to serve as a back-up security command and control center if the CAS becomes inoperative through equipment failure or adversary take over.

The dedicated operator at each Alarm Station is provided with control and display interfaces to the Security System and with controlled access to security communications, as shown in Figure 4-5.

Under normal conditions, the operator's principal interaction with the Security System is through a Status and Control Unit. This unit typically includes switch controls and status lights to set individual remote sensors in an ACCESS or SECURE state, to test their operability, and to indicate their current alarm state. The Status and Control unit will also permit operator selection of scene video from specified remote CCTV cameras and provide a keyboard entry to annotate the Data Log maintained for each Alarm Station. The Video Assessment

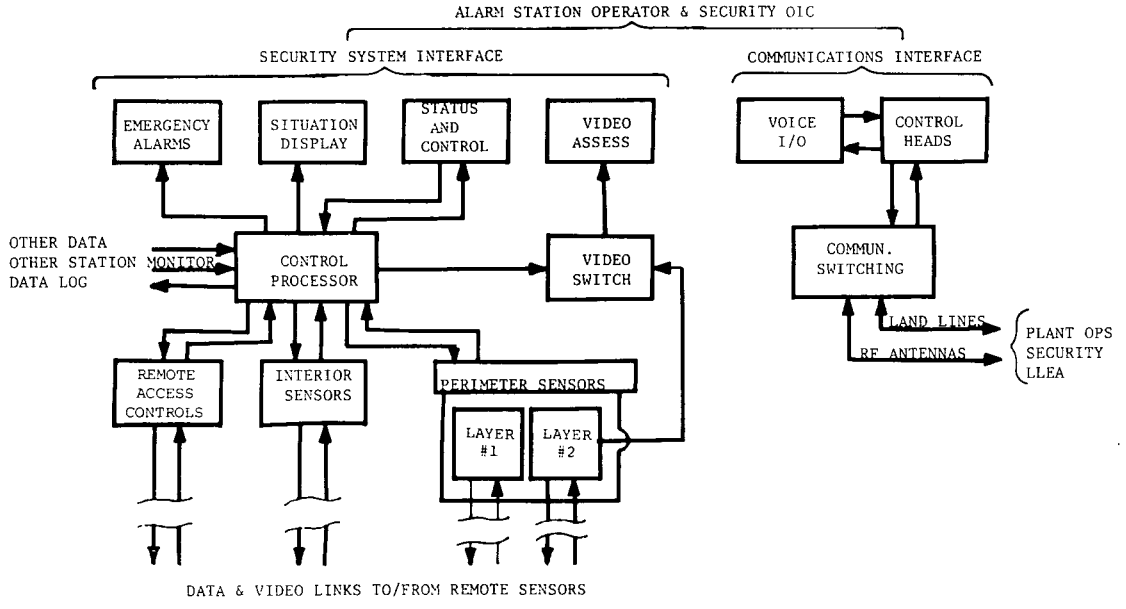


Figure 4-5 Typical Alarm Terminal Block Diagram

unit will include CCTV monitors which permit visual assessment of circumstances at remote CCTV camera locations. Under normal conditions this unit supports remote access control operations conducted from the Alarm Station, and permits a supplemental watch to be maintained with respect to perimeter and interior security. The Situation Display Unit is frequently a map display on which lighted points or segments indicate the status of security at all site access control points, and for each perimeter and interior security sector. The Situation Display represents a snap shot of the overall security posture at the site. It is an invaluable assessment tool for the Security OIC when determining and commanding response for operations during emergencies. The Situation Display also provides plant management, as well as the Security OIC with " at a glance" capability to monitor and review plant security provisions under normal conditions.

When a security alarm conditon arises, the Security System automatically provides the Alarm Station operator with location data, implied

response action cues, and live scene video from the alarmed sector. The Situation Display also responds immediately to represent current conditions.

Figure 4-5 identifies the several subsystems of the Security System console which interface, process, and route alarm, control, and video information between the operator and the remote sensor installations. The illustrated system organization is general in all respects except for the Perimeter Sensors which here depict the use of two or three diverse sensors.

Stations for monitoring access control activities and intrusion alarms are usually custom tailored for individual power plants to accommodate 1000 or more alarm points. Some of the existing systems have been provided by companies such as Sylvania and Honeywell, and Stellar Systems. These have generally been configured to include main frame central processing, lighted segment situation displays, video monitor banks, line printers, video recorders, etc.

The commercial security operator interface requires greater than normal automatic video switching capability, and integration of the video motion detection processor, if used. Existing central and secondary alarm stations can be expanded through the judicious addition of modular interface units to achieve the capability of prompt response to genuine alarms. Such an alarm processing interface would be programmed to perform layered sensor processing; sensor hardware self test, interrogation and response; data link supervision, and to log data pertinent to service life, reliability and maintainability.

4.4 DATA LINK SUPERVISION

An intrusion detection system is no better than the security of the conductors that transmit the alarm signal to the monitor unit. These conductors must be sensitive enough to cause an alarm in the event of tampering.

Requirements for line supervision and implementation recommendations have been extracted from reference 4 as follows:

- An intrusion detection system may be defeated regardless of the effectiveness of its sensor if the signal transmission line is not functioning properly. Conductors may be made ineffective by an intruder who has sufficient knowledge of electricity and the necessary equipment to adjust the resistance in the signal transmission lines.
- Signal transmission lines may be supervised in a variety of ways, according to location of the lines and the security required.
  --The simplest means of line supervision is to monitor whether an electrical circuit has been broken, grounded, or shorted.
  --The most common means is to monitor whether a predetermined variation to an electrical current has occurred. For example, an alarm light might be created if a 30-milliamp current has been increased or decreased five percent.
- A more sophisticated means is to monitor two or more features of a complex signal, such as current and frequency. If the signal is changed on a random basis, the likelihood of the signal being recorded and replayed successfully is very remote.
- Another approach is to monitor a digital- or tone-type signal transmitted through a telephone system. An investigation and reply scheme is ordinarily employed. Since an electrical current is not being monitored in this case, the distance limitation (a few miles) of the other types does not apply.
- The need for constant electronic or other type surveillance of signal transmission lines must be emphasized to insure awareness of security personnel that this is normally the weakest link in the system. Emphasis must also be placed on the necessity to maintain records of both nuisance alarms and scheduled/unscheduled maintenance to insure proper operation of the system at all times.

- Signal transmission lines can be secured by locating them on high overhead poles, burying them, leading into buildings as high as possible, locking terminal cabinets, and comparable measures.

Protective communication systems will vary in size and type with the vulnerability, size, location, radio receptivity, and other factors affecting a specific installation, and must be largely subject to local determination.

4.5 RELIABILITY AND MAINTENANCE

Demonstrated reliability will be a system selection criterion. Reliability is an important parameter in determining life cycle cost, maintenance force, and initial response force requirements because of its impact on false alarm rate. Some of the factors influencing reliability are as follows:

- Detection equipment must be fail-safe (i.e., alarm on failure).
- Unless redundancy is present each equipment failure represents an alarm requiring action.
- Each equipment-failure caused alarm will require both a guard response and maintenance response.
- Equipment and subsystems must have a high MTBF.

4.6 LIFE CYCLE COSTING CONSIDERATIONS

Threat, vulnerability, and countermeasure definitions have been developed for the "typical" nuclear power plants. However, geopolitical, economic, and environmental factors which result in significant differences among individual plants produce variances in the design and operation of an acceptable security system plan.

The plant management must measure plan acceptability not only in terms of regulatory compliance, but also in terms of the life cycle cost of alternative system implementations. General contributors to the life

cycle cost of a candidate security system must include:

- Modifications to existing facilities,
- New security equipment and construction:
  --Initial procurement and installation costs,
  --Maintenance and replacement costs over system lifetime.
- Guard force modifications:
  --Retraining and/or recruiting
  --Equipment
  --Logistics Support

Cost data developed herein for the system definition are meant primarily to use for comparing and optimizing perimeter security systems rather than as a firm pricing exercise. Most figures are based on order of magnitude equipment estimates from vendors and on linear, areal or volume measures for bulk materials of construction.

Of course, the final costing basis, that is, rates and conversion factors to use, will vary with each plant and its individual evaluation of return on investment realities.

Life cycle costs comprise the following additional items:

- Research, development, test, and evaluation costs.
  --The system design and limited site specific environmental and terrain compatibility testing.
- Investment costs.
  --The initial purchase price of the equipment.
  --The cost of initial installation, check out, and alignment of the equipment.
  --Costs involved in setting up an initial inventory.
  --Purchase costs of spares and parts for the initial inventory.
  --Purchase of training equipment.
  --Cost of student and instructor time for initial training.
  --The cost of preparing and reproducing technical manuals for the equipment.
  --Purchase of test equipment.

--Non-recurring cost of developing alarm response procedures.

- Operating and maintenance costs.
  --Energy costs
  --Student and instructor time for recurring training for replacement personnel.
  --Charge for items in inventory.
  --Parts costs for repairs.
  --Labor costs for repairs
  --Pro-rata costs of vehicles used by repair personnel.
  --Transportation and handling for repair parts.
  --Penalty for excessive dispatches for equipment failure.
  --Labor for preventive maintenance.
  --Labor and personal equipment for additional guards, if any, required to implement speedy response to positive alarms.

4.7 SPECULATION ON THE COST OF OUTAGE VS. P_D

The cost of an outage due to a successful sabotage attempt in which the core is shut down (even though there has been no radiation release) is a consideration in specifying the performance of a perimeter security system. So far, the greater number of perimeter penetrations reported have been by people bent on objectives other than radiological sabotage. The following assumptions extrapolate the trend of these intrusions experienced since 1971 at U.S. and foreign nuclear facilities (3) and considers that in the future nuclear plants will become somewhat more attractive targets to champions of causes.

The following assumptions are made:

- Over the thirty year life of the plant, 100 attempts will be made to penetrate the secure area. Of these, it is assumed that half will be for hostile purposes, i.e. to force plant shut down.
- If the hostile intruder is detected by the security system, he will be prevented from causing a shut down.
- If the hostile intruder is not detected, he will be

successful in shutting down the plant for 3 days at a cost of $600,000 per day in assignable costs.

- Additional assignable costs related to plant shutdown, damages, repair, cleanup, and restart will total $200,000.00 per outage.
- Life expectancy of the security system is 6 years.
- No monetary value is assigned to the distractive administrative consequences, loss of good will, negative public reaction, and actual damages to utility customers although a sudden shutdown of a large nuclear plant would almost certainly precipitate these consequences.

Given these assumptions, if a security system has a P_D of 0.90, 10% of 50 intrusions or 5 hostile intruders would be expected to succeed in causing plant shutdowns at a cost of 2 million dollars (assignable cost only) per 3 day outage, or an expected cost of 10 million dollars for 5 outages. Maintaining P_D at 0.98 would reduce the expected number of outages from five to one per plant, and the expected total cost would be two million dollars.

Even if expectation of sabotage outage were one less, instead of four less, the value of avoiding it would balance an increased annual expenditure of $66,700 or an initial security system investment of $400,000. This is more than the cost of the additional perimeter detection layer which enables achieving the higher P_D.

This is obviously an oversimplified model but it can easily be scaled by the expected probability of the intruder successfully sabotaging the plant, the actual anticipated losses and duration of shutdown, and the number of hostile intruders expected during the lifetime of the plant.

4.8 REVIEW OF NUCLEAR UTILITY NEEDS AND WANTS

4.8.1 REASONS FOR REVIEW OF SECURITY NEEDS

According to "Security World" Feb 1981 (7) most industrial companies having physical security provisions, review their security needs on an

average of once every seven months. They upgrade or replace perimeter protection equipment on an average of once every two years. The reasons for such short review and action cycles as they apply to the industrial community and specifically as they also apply to the nuclear utility community, are listed following:

- New detection performance criteria (e.g. Regulatory guide 5.44)
- New interpretations of security system regulations to meet the "negotiated" threat
- Obsolescence, failure, or poor performance of equipment in use
- Economics and technological advancement
  --Replacement of manpower with new equipment,
  --CCTV vs. watchtowers,
  --Processor control vs. manual alarm reset,
  --Nuisance alarm reduction vs. continuous patrol,
  --Alarm keyed monitor vs. continuous operator surveillance,
  --Reduction in maintenance and spares
  --Effective probability testing

4.8.2 NUCLEAR POWER PLANT SURVEY

An objective of this report is to establish the basis for system definition through a survey of the needs and wants of the nuclear utilities. This was done by visiting several power plants, talking to security personnel and observing equipment and procedures in actual use. Additionally, visits were made to SANDIA; and various symposia were attended. Much information of value, reflected in this report was gathered at conferences and workshops devoted specifically to physical security sponsored by ANS, INMM and the University of Kentucky (Carnahan).

The content and recommendations of this report were the subject of an independent workshop at E-Systems Greenville, Texas held on Oct 6 and 7, 1981. This workshop was sponsored by EPRI. Thirty-one Nuclear

Utility representatives participated and exchanged ideas on the following topics:

- E-Field fence experience
- CCTV, VMD test experience
- Alarm processing systems
- Probability testing
- Tentative perimeter intrusion alarm system specification
- Sensor test bed benefits

Summary statements of the workshop chairmen have been transcribed and appear in Appendix C.

4.8.2.1 Equipment Now In Use At Nuclear Power Facilities

SANDIA, in report SAND80 7046, (8) April 1981, shows the incidence of use of equipment comprising perimeter security elements at nuclear power facilities. These are listed following in the interests of identifying those existing building blocks which may be available to alarm segment layering, combined alarm processing and assessment.

	PRESENT USE
• Perimeter intrusion sensors	
--Microwave (primarily at gates)	<75%
--E-field	>75%
--Buried line magnetic	0%
--Buried line pressure/strain	0%
--Infrared beam interrupt	0%
--Fence mounted vibration strain	<75%
--Fence disturbance and free standing sensor combination (E-field or microwave)	45%
• Alarm assessment	
--CCTV (fixed mounted)	>75%
--One monitor per camera	>50%
--Video recording	0%
--Guard towers	<25%
• Barriers	
--Vehicle (earthen type)	Infrequent
--Double fence	Prevalent

- Lighting
  --High mast sodium — Prevalent

4.8.3 SUMMARY OF PERIMETER SECURITY NEEDS AND WANTS

The needs (but not all of the wants) are reflected in later paragraphs which define a recommended perimeter security system. Needs and wants fall into the categories of function, operations, equipment, installation, procurement and testing.

4.8.3.1 The perimeter security operations and equipment should:

- Minimize false and nuisance alarm rates to reserve dispatch of the response force for genuine intrusions.
- Promptly assess the intruder and his location so that the response force can be dispatched to intercept the intruder with appropriate tactics and countermeasures.
- Continually verify detectability
- Minimize maintenance (use high reliability equipment)

4.8.3.2 The equipment should be configured to provide the following:

- Nuisance alarm reduction
- Equipment failure reduction
- Logical connection of diverse sensors and multilayer alarm processing interface
- Generic detection and assessment supplements that are not site specific
- Nonlabor intensive alarm assessment, logging, and reset

4.8.3.3 Installation whether for new sites or modification of existing sites should consider the following:

- Site preparation by segments for sensor layers
- Minimal disturbance of the ground, common trenching
- Serial bus multiplexing of sensor reporting segments

4.8.3.4 Performance and operability testing of the perimeter should be reduced and minimized. Criteria other than the statistical testing suggested by NRC Guide 5.44 should be developed. One approach to

minimizing testing is utilization of the longest practical segment - say 200 meters. Another approach is to minimize the number of test trials in probability testing by solving type I error problems. An approach to this is recommended in Appendix B.

4.8.3.5 Procurement needs are listed following:

- Acquire only tested and proven security elements
- Choose a single system contractor to procure, install, integrate, and test system equipment
- Require site specific pre-award and post installation testing
- Require a warranty

4.8.3.6 In summary, the overall perimeter security system must:

- Provide layers of different sensor types to achieve high probability of detection
- Process false and nuisance alarm signals to output reliable alarms
- Link the video display to perimeter alarms for immediate visual assessment of the intrusion scene
- Verify detectability against layered segments with a minimum number of test trials

Most nuclear plants have 2 unconnected layers, e.g. E-field fence, fence protection sensor. Any two of these existing layers can be combined with a new layer and achieve high probability of detection and low nuisance alarm rates. If 3 layers are combined, one can fail permitting routine or delayed maintenance versus immediate response. All layers should have the same zone coincidence to identify intrusion with a segment of the perimeter.

Section 5

5.0 BASELINE SYSTEM DEFINITION

The recommended baseline perimeter intrusion alarm system has been synthesized from the CFR 73.55 requirements and threat definition, from resulting systems considerations and from the needs and wants of the nuclear utilities as determined in surveys and nuclear community workshops. The synthesis tests and answers the reliable alarm rapid response hypothesis put forth in paragraph 4.0. It is suggested as a design guide for reducing the layered system concept to practice and demonstration at a nuclear power plant.

The approach to the baseline system is summarized as follows:

- Provide a vehicle barrier or interior fence
- Retain existing perimeter detection sensors
- Employ phenomenologically different sensors to achieve three detection layers
- Provide processing interface for combined alarm output
- Employ CCTV for intrusion assessment
- Key assessment scene to combined alarm
- Utilize control processor for video and alarm peripherals
- Establish guard force functions and procedures for tactical command and communication response
- Perform probability testing against layered perimeter segments

5.1 APPLICABLE SOURCE DATA

5.1.1 PLANNING AND DESIGN

The following documents have been developed by the Department of

Energy (DOE), the Nuclear Regulatory Commission (NRC) and others to aid physical security planning both for new installations and for upgrading existing nuclear facilities. Emphasis in these documents is on DOE nuclear fuel cycle facilities but the contents are applicable as well to power utilities.

- Regulatory Guide 5.44 Revision 2, May 1980. Perimeter Intrusion Alarm Systems, U.S. Nuclear Regulatory Commission Office of Standards Development. (1)
- SAND 76-0554 Intrusion Detection Systems Handbook Volume I, Volume II with revisions as of July 1980. Sandia National Laboratories, Albuquerque, New Mexico. (9)
- NUREG/CR-0484 (MH-7814) Vehicle Access and Control Planning Document, October 1979. U. S. Nuclear Regulatory Commission Office of Standards Development. (10)
- Regulatory Guide 5.61 Intent and Scope of the Physical Protection Upgrade Rule Requirements for Fixed Sites. U. S. Nuclear Regulatory Commission Office of Standards Development June 1980. (11)
- NUREG/CR-0509 (Y/DA-7678). Emergency Power Supplies for Physical Security Systems, November 1979. U. S. Nuclear Regulatory Commission Office of Standards Development. (12)
- NUREG/CR-0543 (MHSM-SD-7816). Central Alarm Station and Secondary Alarm Station Planning Document, June 1980. U. S. Nuclear Regulatory Commission Office of Standards Development. (13)
- NUREG/CR-1327 (MHSM-SD-7911). Security Lighting Planning Document for Nuclear Fixed Site Facilities, April 1980. U. S. Nuclear Regulatory Commission Office of Standards Development. (14)
- Part 73.55 Title 10, Code of Federal Regulations "Physical Protection of Plants and Materials". (2) This part specifically is applicable to nuclear utilities.
- IEEE Standard 308-1974 as endorsed by Regulatory Guide 1.32, "Criteria for Safety-Related Electric Power Systems for Nuclear Power Plants". (15)
- IEEE Standard 450-1975 as endorsed by Regulatory Guide 1.129, "Maintenance Testing and Replacement of Large Lead Storage Batteries for Nuclear Power Plants". (16)
- SAND 80-1046. Physical Protection Technology for

Nuclear Power Plants, April 1981, Sandia National Laboratories, Alburquerque, New Mexico. (8)

5.1.2 STANDARDS

The following standards and codes should apply to security system construction:

- American National Standards Institute (ANSI) X4.14-1971 ANSI Standard Keyboard (17)
- Electronics Industries Association (EIA)
  --EIA RS-170 Electrical Performance Standards for Monochrome Television Studio Facilities (18)
  --EIA RS-232-C Interface between Data Terminal Equipment and Data Communication Equipment employing Serial Binary Data Interchange (19)
  --EIA RS-330 Electrical Performance Standards for Closed Circuit Television Camera 525/60 Interlaced 2:1 (20)
  --EIA RS-375-A Electrical Performance Standards for Direct View Monochrome Closed Circuit Television Monitors 525/60 Interlaced 2:1 (21)
- Federal Communications Commission (FCC) Part 15 Sub. "F" Title 47-76-605, Paragraph 12 (22)
- Interim Federal Specification GSA-FSS W-A-00450B (23)
- National Electrical Code (NEC) NFPA #70-1981 Article 725 Class 1, Class 2 and Class 3 Remote - Control, Signaling, and Power-limited Circuits (24)
  --Article 800 Communication Circuits
  --Article 820 Community Antenna Television and Radio Distribution Systems
- National Electric Manufacturers Association (NEMA) (25)
- National Electrical Safety Code (ANSI-C2) - 1981 Section 9 Grounding Methods for Electrical Supply and Communication Facilities (26)
- Underwriter's Laboratory, Inc. (27)
  --UL-198 Fuses
  --UL-512 Fuse-holders
  --UL-796V Printed Circuit Boards

5.2 OPERATIONAL CONCEPT

The basic operational concept is to provide reliable alarms and quick video assessment of an alarmed segment so as to enable prompt dispatch of a response force to the intruder's target area. The concept also enables the conservation of manpower in both presently operating and new plants as follows:

- Combining of perimeter sensor signals by means of a processor. Operator assessment and guard dispatch only on true alarms. False and nuisance alarms would not require guard response. These are alarms or signals that are not combined by the processor because they do not appear on each channel of the AND circuit in its pre-set time "window". Additionally, these are signals coming from, for instance, fence sensors caused by wind or animals which can be visually assessed as nuisances.
- Operator assessment of alarms utilizing CCTV, automated alarm keying of video monitors, automated alarm logging and reset.
- Incorporation of presently installed sensors (as applicable) in a 2 or 3 layered perimeter intrusion detection system to produce reliable alarms.
- Use of proven high Mean Time Between Failure (MTBF) equipment. Scheduling of maintenance on a one shift basis. (High MTBF equipment and three sensor layers allows one to fail and still retain a high P_D until routine repair can be accomplished).
- Designation of perimeter segment lengths of 200 meters (rather than 100 meters or shorter) results in fewer alarm reporting cells and perimeter segments to be periodically tested for detectability performance. Yet this length is about optimum for either visual or video assessment.
- A layered segment of two or more sensors can achieve, through alarm processing, a higher P_D than a single sensor segment. Periodic penetration testing by the user and qualification testing by the vendor against a layered segment will permit verification of the single

sensor P_D criterion. Most importantly, layering will at the same time minimize the number of test trials otherwise made necessary by the expected probability of single sensor Type I errors. Such errors are statistically inherent if the NRC test sequence of Regulatory Guide 5.44 is applied. Fewer trials means fewer manhours expended for detection probability testing.

5.3 SYSTEM ELEMENTS

Functions of a perimeter security system are to provide deterrent barriers bounding an isolation zone, detection and reporting of intrusion alarms and assessment of alarms. Equipment and procedural elements necessary to satisfy these functions are described in the following paragraphs.

5.3.1 BARRIERS

- An outer clear zone.
- An outer fence deterrent barrier.
- A segmented isolation zone interior to the fence.
- A vehicle barrier forming the interior bound of the segmented isolation zone.

If a present facility has a second fence bounding the isolation zone or some other means for delineating the zone and keeping it free from casual intrusion and traversing debris, then a vehicle barrier is optional.

5.3.2 LIGHTING

Provision of illumination permitting visual and video surveillance of the perimeter and facilitating detection and assessment of intrusion attempts.

5.3.3 INTRUSION DETECTION

- Perimeter intrusion alarm segments incorporating two or more phenomenologically diverse layers of intrusion sensors.
- A non-interruptable power supply.
- Supervised signal lines.
- A multilayer alarm processing interface to combine alarm signals from each segmented layer in such a manner as to identify and appropriately treat false and nuisance alarms, yet assure high overall probabilities of detection. Additionally, to communicate commands to perimeter sensor elements and hand-off control signals either to a central computer or to a variety of stand-alone peripherals in the Central and Secondary Alarm Stations (CAS and SAS).

5.3.4 ALARM ASSESSMENT

Monitors, annunciators, displays and controls identifying alarms to an operator and logging the alarmed perimeter segment and its disposition. In addition, an alarm-keyed, closed circuit television (CCTV) system enabling an operator to assess alarmed segments and to automatically record alarms for recall on operator command.

5.3.5 PHYSICAL INTERFACES

Each perimeter segment and layer interfaces with the isolation zone terrain and environment. Site preparation should encompass the installation of each layered segment as one task including common trenching, power and signal wiring from perimeter to the multilayer processor. This processor should be the alarm signal and control interface to and from the perimeter sensor field and the CAS and the SAS, and in turn to the response force command.

5.4 SYSTEM PERFORMANCE

5.4.1 CLEAR ZONE

The clear zone should not permit the intruder to hide or to bring scaling constructs to the perimeter without being observed. Vegetation should be cut and controlled so as not to become a source of nuisance alarms to the perimeter sensors.

5.4.2 OUTER FENCE

The outer fence should be of strong and formidable appearance so as to deter trespass.

5.4.3 ISOLATION ZONE

The isolation zone should be free of vegetation, obstacles and terrain features which would either be nuisance alarm sources or obstacles to a clear view of each segment length.

5.4.4 VEHICLE BARRIER

The vehicle barrier, if installed, should stop or seriously disable a 3/4 ton pick-up truck or heavy automobile.

5.4.5 INTRUSION DETECTION

A detector is a sensing device in combination with a processor. An intrusion detector layer comprises one or several like sensors which are phenomenologically distinct from other layers used in the same perimeter segment.

Each layer individually should have demonstrated in field testing (preferably tested by SANDIA) a point estimate of probability of

detection (P_D) of at least .90 based on required trials in each of the modes and conditions described in NRC Regulatory Guide 5.44.

The combination of two sensor layers internal to the isolation zone (not including fence disturbance sensor type) should have as a goal, a point estimate P_D of at least 0.95 for each segment under each of the modes and conditions described in NRC Regulatory Guide 5.44. A three layer segment should have as a goal, a point estimate P_D of at least 0.98.

False alarms are defined as appearing without apparent cause. They are usually artifacts of system and environmental noise.

Nuisance alarms are identifiable as to cause, e.g., animals, vegetation, weather, and do not comprise an intrusion threat.

The objective for a single layer segment should be on the average not more than one false alarm and ten nuisance alarms per day. A processed 2 or 3 layered complete perimeter should exhibit no more than one false alarm and no more than one nuisance alarm per day. False or nuisance alarm signals occurring on any single layer (and not given a combined alarm) should be annunciated as a low level indication of environmental activity, logged and automatically reset.

Each segment of the perimeter alarm system should be capable of detecting an intruder disturbing the fence or traversing the isolation zone. By definition, the intruder will weigh a minimum of 35 kilograms and will traverse the zone at a rate between 0.15 and 5 meters per second whether walking, running, jumping, crawling or rolling.

The following specific detection requirements are applicable only if the particular sensor is used in the perimeter.

A ferrous metal detector should be able to detect this intruder with a factor 20 (13 dB) insertion loss due to atmospheric attenuation (e.g., fog) at a maximum range of 100 meters.

Fence mounted vibration or strain sensors should detect this intruder attempting to climb or cut the fence or to lift the fence more than 15 cm above grade. Fence sensors should not generate alarms from wind forces up to 48 km/hr.

Sensor layers may come with vendor supplied terminals for gathering and formatting data from individual transducers. The multi-layer processing interface should then accept signals from these terminals either as switch closure voltage levels or as digital words containing sensor address, sensor status or alarm data. The interface ties the perimeter elements to the alarm stations. It allows for self-test commands to be sent to perimeter sensors and hand off command to be sent to a central computer and/or to peripheral assessment and logging devices at the alarm stations.

5.4.6 LIGHTING

The perimeter lighting element should provide night time illumination of the isolation zone to a minimum of two footcandles with an illumination ratio 3:1, maximum to minimum.

5.4.7 ALARM ASSESSMENT

Intrusion alarms processed by the multi-layer alarm processor should be separately sent to the CAS and SAS for annunciation, assessment, recording and logging. Cameras, processor and monitors should be configured to provide a high contrast, high resolution alarm segment scene sufficient to assess the threat, to make the dispatch decision and to continue surveillance of the isolation zone for tactical command purposes.

Recording should be made of each sensor signal whether layer processed alarm, nuisance alarm, sensor self test or access command, tamper indication or power switching. The recording should maintain the following data:

- Type of Alarm
- Alarm Segment
- Data and Time
- Acknowledgement
- Guard Response Action

5.4.8 COMMUNICATIONS

Supervised signal transmission lines must be provided between the sensor segments and the alarm processing interface and between the interface and the CAS/SAS. Any attempt at tampering with these lines will cause an alarm to be annunciated and logged.

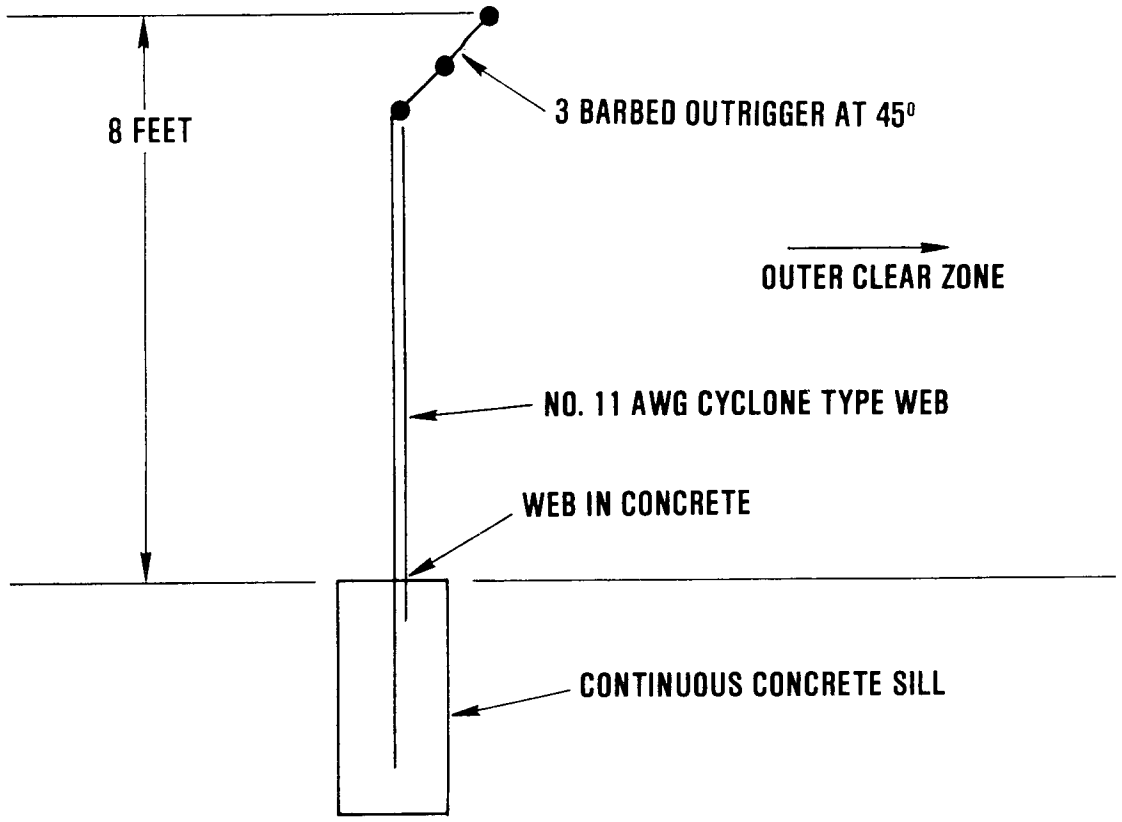
5.5 PHYSICAL CHARACTERISTICS OF SYSTEM

5.5.1 CLEAR ZONE

The clear zone exterior to the outer fence should be a minimum of 6 meters wide, clear of vegetation and major terrain discontinuities.

5.5.2 OUTER FENCE

The outer fence should be a minimum 8 feet (2.44 meters) high with the top 1 foot (0.3 meter) comprising 3 strands of barbed wire on extension arms. The lower 7 feet (2.14 meters) should be minimum #11 AWG chain link to be anchored in a reinforced concrete curb or pier, 8 inches (0.2 meters) wide with 4 inches (0.1 meters) above ground. The chain link material should be treated to prevent corrosion while imbedded in the concrete. The below ground pier should extend below the frost line but should be a minimum 18 inches (0.46 meters) below ground level. The curb is meant to discourage tunneling but also to avoid the creation of ditches by water erosion which could permit defeat of the fence. The fence is schematically shown in figure 5-1.



- TURNS AWAY THE CASUAL INTRUDER
- KEEPS OUT MEDIUM AND LARGE ANIMALS
- CATCHES BLOWING DEBRIS
- REQUIRES INTRUDERS TO SCALE OUTRIGGER BARBED WIRE OR CUT FENCE LINKS
- SIGNALS PEDESTRIAN OR VEHICLE ATTEMPTS BY INTRUDER TO PENETRATE FENCE (WILL NOT DETECT BRIDGING ATTEMPTS)
- ENABLES TIME TO ASSESS

Figure 5-1. Outer Fence and Fence Sensor

If the present facility has an existing similar outer fence not anchored to a curb, then the curb becomes optional. Instead the fabric should be tied every 6 inches (0.15 meters) to the bottom rail and no gaps should be allowed to form beneath the fence.

5.5.3 ISOLATION ZONE

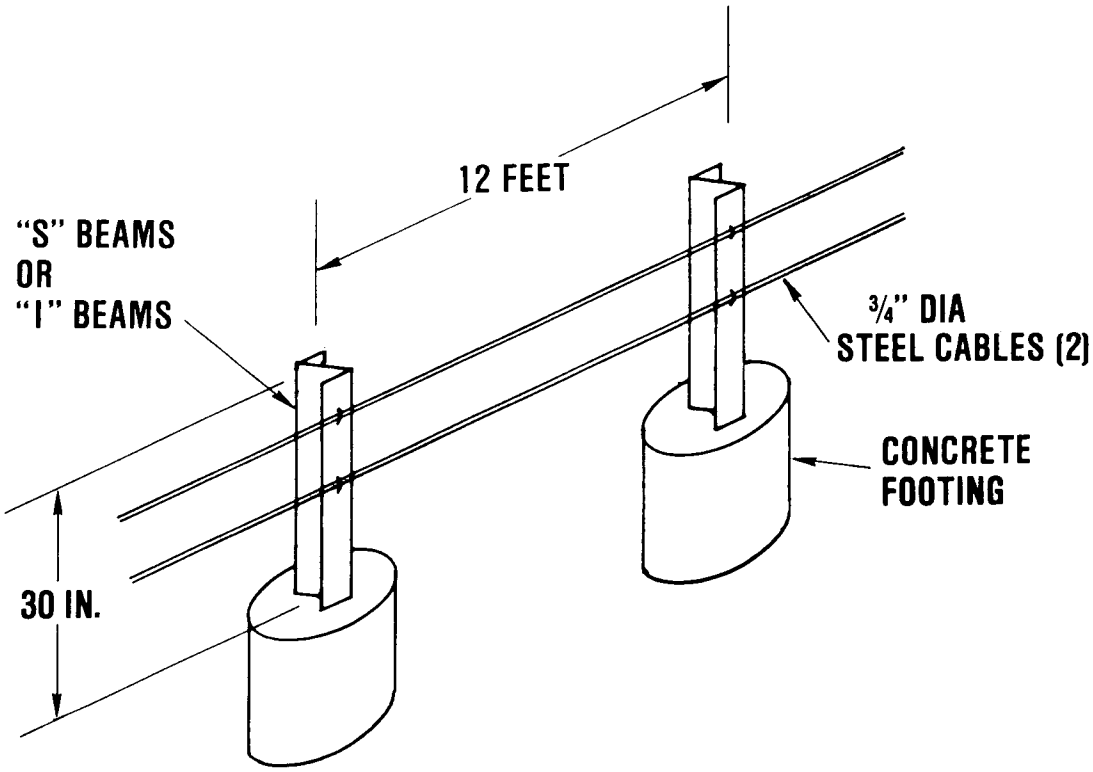
The isolation zone should be at least 6 meters wide, free of vegetation, obstructions and terrain discontinuities. Fence or fences should bound the isolation zone continuously around the periphery except at portals (portals are specified elsewhere). The isolation zone should be segmented for purposes of intrusion detection and location and each segment should have a length of 200 meters as a goal, or 100 meters for small perimeters. It is recognized that a few segments, like at portals, will be shorter.

5.5.4 VEHICLE BARRIER

A vehicle barrier should be located at least 6 meters interior to the outer fence of the protected area. As shown in figure 5-2, it should consist of steel S beams or I beams anchored vertically in cylindrical concrete footings spaced 12 feet (3.66 meters) apart with two continuous 3/4 inch (1.9 cm) diameter steel cables attached at each beam. The vehicle barrier should be continuous around the perimeter except at portals which will have separate vehicle barriers. The vehicle barrier is optional if a second fence has already been provided as the inner boundary to the isolation zone.

5.5.5 LAYERED INTRUSION DETECTION

Two or three intrusion detection layers using diverse sensing processes may be selected from among the six categories specified herein. The six categories are Microwave, E-Field, Buried Line, Infra red, Fence Sensor, Video. Each layer selected should be in a different category. For example, a power plant already having two uncombined



- PREVENTS INTRUDER ATTEMPTS TO HIDE
- IMMOBILIZES LIGHT VEHICLES (3/4 TON PICKUP)
- INCREASES THE INJURY RISK TO INTRUDERS IN LARGER VEHICLES
- INSIDE FENCE DISCOURAGES CUTTING OF CABLE
- SHOULD DE-ESCALATE THREAT TO BACK PACK CARRIED EQUIPMENT

Figure 5-2. Cable Guard Rail Vehicle Barrier

sensor layers and CCTV alarm assessment equipment might choose one of the following sets, depending on what is already there (VMD is Video Motion Detection, MW is microwave).

1.	EXISTING E-FIELD LINE	ADD POLYSTATIC M.W.	*ADD VMD
2.	EXISTING E-FIELD LINE	EXISTING FENCE SENSOR	*ADD VMD
3.	EXISTING MICROWAVE LINE	EXISTING FENCE SENSOR	*ADD VMD

*Video Motion Detection (VMD) is shown as the third option example here only because it is a potentially low cost adjunct to an existing CCTV system. The third sensor may be selected from among the combinations listed on page 5-15.

Because fences in themselves are most easily defeated, fence disturbance sensor types are not recommended for new equipment layering, even though they may have a high P_D and low FAR/NAR. Any supplementary layer should employ sensors in or projecting into the isolation zone; and existing fence sensors will comprise the 3rd or backup layer.

Sensor layer selection, particularly for new installations and old installations adding new reactors, may be made from the Table 5-1 matrix of 20 possible combinations of 6 sensor categories into 3 layers. Magnetic, pressure/strain and seismic sensors are included under "buried sensors". The ported coax, although buried, is considered as a microwave system. Individual sensors and viable combinations have been identified further in Figure 5-3.

Selection of appropriate sensor types from among these categories (e.g., seismic type from buried line category) should consider requirements imposed by intended site and environment. A northern site having winter weather extremes, could well opt for a buried sensor instead of a free standing sensor in the isolation zone to enable snow removal without obstruction.

Choice for this environment for example, might be one of the following sets.

1.	Buried Ported Coax	Buried Seismic Line	Fence Sensor
2.	Pressure Strain Buried Line	Buried Ported Coax	Fence Sensor
3.	Fence Sensor	Buried Seismic Line	VMD

Table 5-1

20 POSSIBLE COMBINATIONS OF 6 SENSOR CATEGORIES INTO 3 LAYERS

MICROWAVE	E-FIELD	BURIED LINE
MICROWAVE	E-FIELD	IR
MICROWAVE LINE	E-FIELD	FENCE SENSOR
MICROWAVE	E-FIELD	VIDEO
MICROWAVE	BURIED LINE	IR
MICROWAVE LINE	BURIED LINE	FENCE SENSOR
MICROWAVE	BURIED LINE	VIDEO
MICROWAVE	IR	FENCE SENSOR
MICROWAVE	IR	VIDEO
MICROWAVE	FENCE SENSOR	VIDEO
E-FIELD	BURIED LINE	IR
E-FIELD LINE	BURIED LINE	FENCE SENSOR
E-FIELD	BURIED LINE	VIDEO
E-FIELD LINE	IR	FENCE SENSOR
E-FIELD	IR	VIDEO
E-FIELD LINE	FENCE SENSOR	VIDEO
E-FIELD LINE	FENCE SENSOR	VIDEO
BURIED LINE	IR	FENCE SENSOR
BURIED LINE	IR	VIDEO
BURIED LINE	FENCE SENSOR	VIDEO
IR	FENCE SENSOR	VIDEO

5.5.6 PERIMETER ALARM SENSOR CANDIDATES

Physical characteristics of the six types of perimeter intrusion alarm sensors described by NRC in regulatory guide 5.44 are repeated following. Supplementary information is given for ported coax and VMD sensors.

5.5.6.1 Microwave Perimeter Alarm Sensor

Each link of a microwave perimeter alarm system is composed of a transmitter, receiver, power supply, signal processing unit, signal

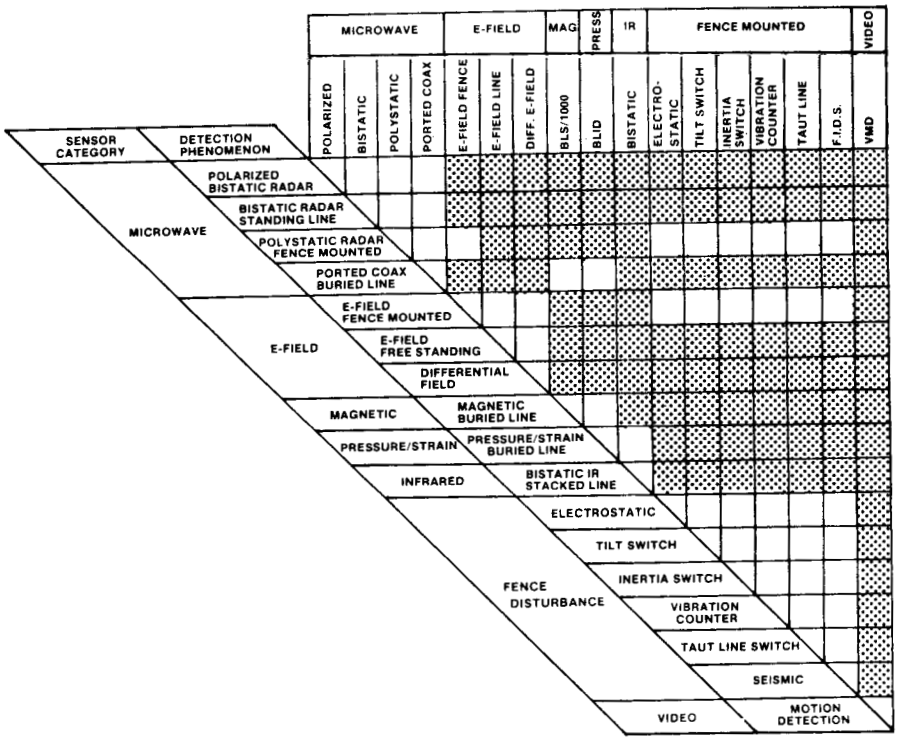


Figure 5-3. Alarm System Combinations

transmission system, and annunciator. The microwave transmitter produces a beam-like pattern of microwave energy directed to the receiver, which senses the microwave beam. A partial or total interruption of the beam will cause an alarm. The microwave beam can be modulated to reduce interference from spurious sources of radio frequency energy, to increase sensitivity, and to decrease the vulnerability to defeat from "capture" of the receiver by a false microwave source.

Successive microwave links can be overlapped to form a protective perimeter around a facility. Since the transmitter/receiver link is a line-of-sight system, hills or other obstructions will interrupt the beam, and ditches or valleys may provide crawl space for an intruder. Moreover, objects such as tumbleweed, paper, and bushes moving in the path of the beam can cause nuisance alarms. Since the beam is wider than other systems, care must be taken to ensure that authorized activities do not create nuisance alarms. Systems using the Doppler shift for motion detection are especially sensitive to the motion of trees and grass and to falling rain and snow. Typically, a microwave perimeter alarm system will operate effectively in the range between 70 and 150 meters. However, the maximum and minimum separation of the transmitter and receiver should be specified by the manufacturer.

For this application, the microwave beam should be modulated, and the receiver should be frequency selective to decrease susceptibility to receiver "capture". The transmitters and receivers should be installed on even terrain clear of trees, tall grass, and bushes. Each unit should be mounted rigidly at a distance of about 1 meter above the ground. Because of variances in the antenna pattern of different microwave systems, this height may have to be varied slightly in order to obtain proper ground coverage. The distance between a transmitter and its receiver should be in accordance with both the manufacturer's specifications and site-specific requirements. To prevent passage under the microwave beam in the shadow of an obstruction, hills should be leveled, ditches filled, and obstructions removed so that the area between transmitter and receiver is clear of obstructions and free of

rises or depressions of a height or depth greater than 15 cm. The clear area should be sufficiently wide to preclude generation of alarms by objects moving near the microwave link (e.g., personnel walking or vehicular traffic). Approximate dimensions of the microwave pattern should be provided by the manufacturer.

If the microwave link is installed inside and roughly parallel to a perimeter fence or wall, the transmitter and receiver should be positioned so as to prevent someone from avoiding detection by jumping over the microwave beam into the protected area from atop the fence or wall. Typically, a chain link security fence with an overall height of 2.4 meters will require a minimum of 2 meters between the fence and the center of the microwave beam.

Successive microwave links and corners should overlap at least 3 meters to eliminate the dead spot (areas where movement is not detected) below and immediately in front of transmitters and receivers. The overlap of successive links should be arranged so that receiver units are within the area protected by the microwave beam.

Buried ported coax microwave and fence mounted microwave systems are excepted from the above dimensional requirements which are meant for free-standing equipment.

5.5.6.2 E-Field Perimeter Alarm Sensor

An E-field perimeter alarm system consists basically of a field generator that excites a field wire, one or more sensing wires, and a sensing filter; and amplifier; and a discriminatory annunciator unit. The field wire transmits essentially and omnidirectional E-field to ground. A large body approaching the system changes the pattern of the E-field. When sensing wires are placed at different locations within the transmitted E-field pattern, they pick up any changes occurring in that pattern. If the changes are within the frequency bandpass of human movement, an alarm signal is generated. The field wire and one or more parallel sensing wires can be either connected

to a chain link fence or mounted as an above-ground, freestanding system within an isolation zone.

The E-field system can offer about 300 meters of perimeter protection per segment, but shorter lengths are recommended in order to have effective alarm assessment and response capabilities. The system can be mounted on metal, plastic, or wooden posts using specially designed electrical isolators that allow for small movements of the posts without disturbing the field and sensing wires. Both the field and sensing wires need to be under a high degree of spring tension to produce high-frequency vibrations when they are struck by small foreign objects or blown by the wind, both of which are out of the passband of the receiving circuitry. In addition, in order to keep the sensitivity of the system from varying, the E-field detector needs to be well grounded in accordance with vendor specifications.

The E-field detector is not line-of-sight limited and therefore can be installed on uneven terrain and in an irregular line. The surrounding terrain should be kept clear of shrubs, tree limbs, and undergrowth since they act as moving ground objects. The basic system has either three or four wires comprising sensing wires and a field wire. The width of the detection zone is variable and depends to a large degree on the size of the target. Generally, it is approximately 0.6 meter wide on either side of the field wire. To prevent an intruder from jumping over the top of the E-field detector, a sensing wire can be installed approximately 1 meter above the field wire. When installed on a chain link fence, standoffs approximately 0.5 meter long are used for mounting the wires. The E-field generated in this configuration does not penetrate the fence but parallels it.

The field and sensing wires should be supervised to prevent the undetected cutting or bypassing of the system through electronic or clandestine means. The system design should employ techniques to minimize alarms caused by high winds, thunderstorm-related electrical phenomena, and small animals.

The E-field sensor should consist of a minimum of one field wire and two sensing wires. One sensing wire should be located no more than

0.45 meter above ground level with the second located approximately 2.6 meters above ground level. The field wire should be located between the sensing wires approximately 1 meter above ground level. The surrounding terrain within 3 meters of E-field wires should be free of all shrubs, trees, and undergrowth. The control unit should be well grounded using a 1-meter or longer grounding rod or equivalent electrical ground. When mounted to a chain link fence, the fence should also be well grounded approximately every 23 meters using a 1-meter or longer grounding rod or equivalent electrical ground.

5.5.6.3 Buried Sensors

5.5.6.3.1 Ferrous Metal Detector Perimeter Alarm Sensor.

A ferrous metal detector system consists of buried electrical cables, amplifiers, inhibitors, power supply, signal processing unit, signal transmission lines, and annunciator. The system is passive and is responsive to changes in the earth's ambient magnetic field. Such changes are caused either by electromagnetic disturbances such as lightning or by ferrous metal being carried over the buried cables. The change in the local ambient magnetic field induces a current in the buried cable which is filtered and sensed by the electronics. If the change exceeds a predetermined threshold, an alarm is generated. To reduce nuisance alarms from external electromagnetic sources (e.g., electrical power transmission lines), the electrical cable is laid in loops that are transposed at regular intervals. Also, an inhibitor loop can be used to reduce nuisance alarms from electromagnetic interference. The inhibitor which operates on the same principle as the sensor cable loops and is buried near the sensor cable, senses strong temporary electromagnetic interferences (e.g., lightning) and disables the alarm system for approximately one second, thus reducing nuisance alarms.

The ferrous metal detector system is not a line-of-sight system and therefore can be installed on uneven ground in an irregular line. The sensor subloops formed by the cables must be fairly regular, however. Since the system will detect only ferrous metal, animals,

birds, or flying leaves will not initiate alarms. However, electromagnetic interferences can cause nuisance alarms or disable the alarm system when the interference is severe.

Each sensing cable (and amplifier) can monitor a security segment up to 500 meters in length. Increasing the length of the security segment beyond 500 meters usually results in a high nuisance alarm rate. Multiple cables and amplifiers can be used to extend the monitoring length.

The detection system should be equipped with inhibitor coils to minimize nuisance alarms due to electromagnetic interference. No more than six sensing loops per inhibitor coil should be used in order to prevent simultaneous desensitizing of the entire system.

To determine if the ferrous metal detection system will operate in the proposed environment, a preengineering site survey should be made using an electromagnetic detection survey meter. This survey meter can be furnished by the manufacturer. If the electromagnetic disturbances are within the limits prescribed by the manufacturer, this type of system can be used effectively. Special looping configurations can be made in areas of high electromagnetic interference to reduce the incidence of nuisance alarms.

The sensing loops of electrical cable should be buried in the ground according to the manufacturer's specification. Multiple units (cable and amplifier) should be used to protect a perimeter. All associated buried circuitry should be buried within the protected zone and packaged in hermetically sealed containers. The cable should be laid in accordance with the manufacturer's recommended geometrical configurations to reduce nuisance alarms from external sources. When cable is being installed in rocky soil, care should be taken to remove sharp rocks during backfilling over the cable. Inhibitors should be buried in the ground at least 6 meters from the cable inside the protected perimeter.

Continuous electromagnetic interference obstructs the detection of an intruder carrying ferrous metal over the buried cable by keeping the inhibitor activated, thereby preventing the alarm unit from responding

to a change in flux caused by the intruder. The device should therefore be used only where the environment is relatively free of severe man-made electromagnetic interference (e.g., overhead power cables pole-mounted transformers, generators). The cable should never be installed close to overhead power transmission lines. Moreover, the cable should be placed at least 3 meters from parallel-running metal fences and at least 20 meters from public roads to minimize nuisance alarms.

5.5.6.3.2 Pressure/Strain-Sensitive Perimeter Alarm Sensor.

Buried pressure/strain transducers detect small variations in the mechanical stress exerted on the surrounding soil by the presence of an individual passing above the sensor. The signals produced by the transducers are amplified and compared with a preestablished threshold. If the signal exceeds the threshold, an alarm occurs. The transducer may be a set of piezoelectric crystals, a fluid-filled flexible tube, a specially fabricated stress/strain electrical cable, an insulated wire in a metallic tube or an interconnected set of seismic transducers. Seismic transducers detect low frequency pressure waves.

Like the ferrous metal detector system, the pressure-sensitive system does not require line-of-sight installation and can be sited on uneven terrain. However, soil condition and composition have a significant effect on sensor sensitivity. Installation in rocky soil may result in damage to the pressure transducers either during installation or as a result of soil settlement after installation. Wind-generated movement in trees and poles can create nuisance alarms. High winds can produce pressure waves on the ground surface which, if sensed by the transducer, could necessitate operation at reduced sensitivity in order to avoid nuisance alarms. Features to compensate for wind-generated noise can be designed into the equipment but in turn may cause a decrease in system sensitivity. Pressure systems will lose sensitivity when the buried sensors are covered by snow, by snow with a frozen crust that will support the weight of man, or by frozen ground. Seismic sensors may detect an intruder on frozen ground although not in deep snow. Other natural phenomena such as hail and rain can cause nuisance alarms.

A typical length monitored by buried line transducers is about 100 meters. The sensors should be installed at the depth below the ground surface stated by the manufacturer. To obtain a high probability of detection, the sensors should be in two separate parallel lines at a distance of 1.5 to 2 meters apart. The sensors and electronic circuitry buried in the ground should be of a durable, moistureproof, rodent-resistant material. When a pressure-sensitive perimeter alarm system is being installed in rocky soil, all rocks should be removed during backfilling to prevent damage to sensors. If the frost line exceeds 10 cm, a buried pressure-sensitive system (other than seismic) should not be used unless the soil is specifically prepared to eliminate freezing above the sensor. The system design should employ techniques (e.g., electronic signal processing) to eliminate nuisance alarms from wind and other environmental phenomena.

5.5.6.4 Infrared Perimeter Alarm Sensor.

Each link of an infrared system is composed of a transmitter, receiver, power supply, signal processor, signal lines, and alarm annunciator. There may be two links in a perimeter segment. The transmitter directs a narrow modulated infrared beam to a receiver. If the infrared beam line-of-sight between the transmitter and receiver is interrupted, and alarm signal is generated. Since the modulated beam does not diverge significantly, multiple infrared beams between transmitter and receiver can be used to define a "wall". If this wall is then penetrated by an individual, an alarm will result.

Fog both attenuates and disperses the infrared beam and can cause nuisance alarms. However, the system can be designed to operate properly with severe atmospheric attenuation. Dust on the faceplates will also attenuate the infrared beam as will an accumulation of condensation, frost, or ice on the faceplates.

Such condensation, frost, or ice, however, may be eliminated through the use of heated faceplates. Sunshine on the receiver may cause an alarm signal. Misalignment of transmitter and receiver caused by frost heaves may also cause an alarm signal. Like the microwave system, vegetation such as bushes, trees, or grass and accumulated snow

will interfere with the infrared beam; and ditches, gullies, or hills will allow areas where the passage of an intruder may go undetected.

The typical distance between transmitter and receiver is about 100 meters; some systems are capable of monitoring a distance up to 300 meters under ideal conditions.

An infrared perimeter alarm system should be a multibeam modulated type consisting of a minimum of three transmitters and three receivers per unit. The system should be installed so that, at any point, the lowest beam is no higher than 21 cm above grade and the highest beam at least 2.6 meters above ground. Sufficient overlap of beams should exist such that an individual could not intrude between the beams and remain undetected. The ground areas between the infrared beam posts should be prepared to prevent tunneling under the lower beam within at least 15 cm of the surface. This may be accomplished by using concrete, asphalt, or a similar material in a path at least 1 meter wide and 15 cm deep or alternatively 15 cm wide and 1 meter deep between the posts.

The transmitters and receivers should be mounted rigidly, (e.g., installed on a rigid post or concrete pad) to prevent nuisance alarms from vibrations. Each transmitter and receiver post should be provided with a pressure-sensitive cap to detect attempts at scaling or vaulting over the infrared beam post. The maximum distance between transmitter and receiver should be selected to permit proper operation during conditions of severe atmospheric attenuation. The system should be able to detect with a factor of 20 (13 dB) insertion loss due to atmospheric attenuation (e.g., fog) at maximum range (100 meters).

The infrared perimeter alarm system should be installed inside the isolation zone with the transmitter and receiver units positioned a minimum of 3 meters from the fence. Installation of the infrared alarm system directly adjacent to the perimeter fence should be avoided since the barrier may provide a solid base from which an intruder can jump over the beams into the protected area.

5.5.6.5 Fence Mounted Vibration- Or Strain-Detector

A variety of devices that detect strain or vibration are available for use as fence protection systems. Vibration sensing may extend into the acoustic and seismic frequency regimes. Although the devices vary greatly in design, each basically detects strain or vibration disturbances of the fence such as those produced by an intruder climbing or cutting the fence. In the simplest devices, the disturbance makes or breaks electrical continuity and thereby generates an alarm.

Unless set to a high threshold, most fence protection sensors are susceptible to nuisance alarms caused by wind vibrating the fence, by hail stones or by blowing debris. The frequency of nuisance alarms due to the wind can be reduced by rigidly mounting the fence and thereby lessening the propensity of the fence to vibrate in the wind. This situation is especially common with post-mounted switch-contact-type alarm systems. The use of electronic signal processing equipment in conjunction with signal-generating strain transducers can effectively reduce nuisance alarm rates without sacrificing sensitivity to climbing or cutting the fence. However, most fence alarm systems can be easily bypassed by a variety of methods.

Fence disturbance sensors should be used only as a secondary or backup perimeter alarm system (i.e., 3rd sensor) except when one of the other types of perimeter alarm systems will not work (e.g., because of the environment) and after the NRC's approval has been received.

If approved the vibration or strain sensors should be attached firmly to the fence (post or fabric, as appropriate) so that the vibration/stress caused by an intruder climbing, cutting, or lifting the fence fabric will generate an alarm.

5.5.6.6 Ported Coax Microwave Perimeter Alarm Sensor.

The ported coax detector comprises an electromagnetic sensor and a signal processor. The electromagnetic sensor consists of a transmitter/receiver connected to two parallel "leaky" coax cables spaced 3

to 5 feet apart. The processor unit performs the required signal processing and provides a display and alarm function to the operator. The sensor concept is based on the properties of lossy coax cables. Openings fabricated in the outer shield allow a portion of the electromagnetic energy traveling within the cable to escape (radiate) in controlled fashion. This energy creates a traveling wave external to the cable but within a defined zone near the cable. The second cable, identical to the first, is placed within this irradiated zone. The energy coupled into the second cable is dependent upon the geometry of the cable placement and the electrical properties of the intervening media. Any change in the propagating medium will effect the magnitude and phase of the coupling.

Thus, if the magnitude of the intrusion signal exceeds a predetermined threshold, a target is declared and an alarm generated. Measurement of the time between the transmitted pulse and the receiver output provides the location of the intruder.

For a given installation environment and uniform processor excitation, the received energy remains constant and its character is referred to as the profile of that installation.

Environmental changes, for example rainfall, cause a change in the received energy profile by changing the characteristics of the propagation medium. However, these changes occur much more slowly than the perturbations practically attributed to an intrusion event. The processor receiver adapts to environmental changes by continuously performing a moving average calculation of the profile or reference energy characteristics.

For purpose of setting signal-to-threshold margins for detection along the perimeter, range resolution should be 100 meters. The perimeter length accomodated by a single processor should be a minimum of 1600 meters.

Operational frequency and radiated power should be compatible with FCC regulations.

The processors should be configured to be installed in a standard 19 inch rack and to interface with the multi-layer alarm processor.

5.5.6.7 Video Motion Detection Perimeter Alarm Sensor.

Video Motion Detection (VMD) is a means whereby a CCTV system can be used for detection and quick assessment of alarms without the need for constant viewing. A VMD channel samples the video signal from a TV camera so that the light levels in several areas of the TV camera's field-of-view are monitored.

The video signal from each area is digitized and stored for comparison with future signals from the same area as they are repeatedly sampled. When the light level in the sample area changes, the signal from the TV camera will also change. If the signal changes enough, the newly digitized signal will disagree with the previously stored signal. This disagreement is then noted by the VMD processor which transmits an alarm when the number of disagreements exceeds a preset number.

Video motion detection systems for exterior perimeter security are subject to nuisance alarms from the following causes.

- Personnel and equipment movement in TV camera field-of-view,
- Reflections from objects in field-of-view,
- Blowing litter in field-of-view,
- Animal intrusion (birds, rabbits, insects, etc.)
- TV camera support movement,
- VMD system equipment failure,
- Natural and artificial lighting changes, e.g. cloud shadow edge movement,
- Power line and video transmission system EMI.

As with other detection systems, nuisance alarms can be controlled and significantly reduced by proper equipment siting and attention to keeping the isolation zone clear. In addition, the VMD processor is capable of masking or desensitizing areas of the scene outside of the isolation zone so that outside movements do not cause alarms. Detection

thresholds are adjustable to minimize nuisance alarms as from clouds, birds or debris.

The video motion detection alarm system may utilize existing CCTV cameras if suitable, or independent cameras. Camera tubes should be capable of "seeing" under 1 footcandle illumination (10.75 lux). The multilayer processing interface should automatically key a TV monitor to view an alarmed segment and provide a control signal for video tape recording of the scene.

Video Motion Detection Processors should be configured for standard 19 inch rack mounting and housed in a building environment. The container should be provided with a tamper switch. Camera and enclosure should be rigidly mounted on a double pole where the inner pole holding the camera is isolated from the outer pole so that wind caused deflections are decoupled from the camera. Alternatively, the camera can be mounted atop a 2 ft. (0.6 meters) diameter tower made of joined concrete sewer pipe filled with reinforced concrete for rigidity. Footings should be a minimum of 4 ft. (1.2 meters) deep and of a strength and mass consistent with the doublepole or tower.

VMD is supplemental to CCTV, and common features are further specified in Section 5.5.9, alarm assessment element.

5.5.7 MULTI-LAYER ALARM PROCESSING INTERFACE

The multi-layer alarm interface should use firmware-based majority logic to combine and process alarm data from the perimeter sensor layers. Because data will be transferred to and from a variety of sensor and CAS/SAS hardware, the processor must offer a highly flexible interface.

Particularly, this interface should enable adaptability to unique on-site requirements and compatibility with various existing alarm system equipment and sensor polling formats.

In layered processing, alarms result from a logical combination of individual events which occur within predetermined time windows. The

multilayer alarm processor uses this method to identify sensor layer and segment intrusion, tampering or equipment failure. Any alarm reporting priorities are pre-programmed by the user. Processed and prioritized alarm data are transmitted to both CAS and SAS for annunciation, and assessment.

Specifically, alarms will be generated under any of the following conditions.

- Detection of a stimulus or condition for which the system was designed to react. (A response force will be dispatched only upon assessment of a layered intrusion alarm; other lower priority alarms will be handled either manually or by automatic logging and reset).
- Indication of a switchover to the emergency or secondary source(s) of power and also upon loss of emergency power.
- Indication of any tampering (e.g., opening, shorting, or grounding of the sensor circuitry) which renders the device incapable of normal operation.
- Failure of any component(s) to the extent that the device is rendered incapable of normal operation. The alarm processor should incorporate a self-test to check itself and the sensor net for proper functioning. Identification of the failed sensor shall be provided.

In order to accommodate unique sites and environments and to ensure ready adaptability to future system modifications, strategic portions of the processor's programming will reside in non-volatile Electrically Alterable Read Only Memory (EAROM). Custom programming should be done through an external data terminal at the user's location. Procedures such as changing alarm priorities, adding and deleting sensor addresses, and changing sensor threshold can thus be done at the user's convenience. In addition, the selected threshold can be made self-adjusting in response to appropriate weather station information inputs. This is possible because EAROM requires no special external programming capability.

The sensor field interface should be able to accommodate a wide variety of sensor polling arrangements. This includes both serial and parallel configurations. Capability for direct sensor coupling and video switching and logging will be provided as required.

Serial arrangements can be configured as either a single or double loop. Although a multiplexed format such as EIA RS422 is preferred, compatibility with almost any other serial format can be achieved through custom programming. Parallel polling formats, such as repetitive singular addressing and interrogation, can also be accommodated with custom programming to enable utilizing communication systems already in place. Individual sensors which are not now part of a polled system can be hard wired to an additional "junction box" unit. This unit will handle multiplexing into the interface processor's serial loop.

Sufficient asynchronous serial and parallel I/O lines should be provided for communication between the multi-layer processing interface, alarm station peripheral devices such as printers and CRT's, and perimeter sensor segments. The signal levels should conform to EIA-RS-232C.

Circuitry should have built-in redundancy so as to minimize the effects of single component failures on the system's performance. Such redundancy should also serve to accommodate future growth and expansion of the system.

The configuration should include a back-up noninterruptable battery power supply and be suitable for mounting in a standard EIA 19 inch rack. The chassis should be enclosed and provided with tamper indicating devices. The system should be designed for an inside building environment. Cooling means should be built in if required, drawing on inside building air.

Benefits and features of the multi-layer processing interface are summarized following:

- Combines diverse detector signals sensitive to different intruder and nuisance manifestations.
- Reduces nuisance alarms by "ANDing" two or more sensors with time integration of alarm sources.
- Increases detection probability as the combined probability of two or more diverse layers responding to the same alarm source.
- Accepts conditioned and filtered signals from sensor preprocessors or communication transducers.
- Communicates with sensor to provide:
  --Threshold settings and self-test command
  --Failure state and alarm contact state identification
  --Automatic reset after alarm source time setting
  --Line supervision
  --Power mode indication and backup power switch in the event of power failure
  --Sensor layer and segment identification code
  --Alarm signal priority
  --Output keying of annunciators, video scene, and recorder

5.5.8 LIGHTING ELEMENT

The isolation zone should be illuminated to a minimum of 2.0 foot candle with an uniformity ratio of 3:1. The light source should be either High Pressure Sodium (HPS) or Low Pressure Sodium (LPS). Pole height should be between 40 and 50 feet; pole spacing should be about 80 feet. Depending on the light source chosen, poles should have one or two luminaires. Power should be delivered to the poles with buried wiring which may share the trenching for perimeter sensors and video surveillance. In case of power failure, luminaires should be capable of quick re-strike (within 10 seconds with a 90% probability). At present many nuclear power plants have perimeter lighting that provides a minimum of 0.2 f.c. illumination, some by means of high rise area lighting, others by means of road lighting. Either type of lighting may be upgraded by the replacement of luminaires, using two luminaires in place of one or possibly by increasing the number of

poles. The objective for retrofit should be to add on to what already may be there to provide 2.0 f.c. illumination. Lighting requirements and trade-offs are given in Appendix A.

5.5.9 ALARM ASSESSMENT ELEMENT

The perimeter sensor status should be presented through the interface processor to the alarm monitor operators by means of one or a combination of the following display/control modes, in conjunction with audio signal, access/secure controls, alarm acknowledge and reset provisions.

- Map boards or annunciator panels with lights to display the status of each alarm circuit.
- Alphanumeric readouts which use a single digital display to report alarm information from each alarm circuit, usually one at a time.
- Computer-driven cathode ray tube (CRT) displays which can simultaneously present alarm circuit history.
- Alarm keyed closed circuit television (CCTV) comprising the following:
  --Fixed video cameras viewing the isolation zone and capable of "seeing" in illumination levels from bright sunlight to one footcandle.
  --Video monitors in CAS and SAS keyed by alarms to show segment or segments intruded upon to an operator.
  --Video recording and playback equipment capable of recalling an alarm scene as an assessment aid.

The perimeter alarm assessment element should be integrated in the central and secondary alarm stations with those equipments selected for interior security. Computer driven or stand-alone reporting and logging devices may be shared by both interior and exterior alarm functions. However, if each function has its own dedicated equipment, that equipment should be compatible, uniform and standardized.

Selection of security alarm assessment equipment for new plants should coordinate both interior and perimeter requirements using NUREG-0320

"Interior Intrusion Alarm Systems" Chapter 4, "Annunciator Units" as a guide.

Exterior video assessment cameras should be housed in suitable moisture sealed environmental enclosures complete with sun shields. Cameras should incorporate 2/3 in. or 1 in. silicon vidicon or "ultricon" type sensing elements capable of full video in illumination levels 1 foot-candle and above. The lens should have a focal length of 75 mm and should be equipped with an auto-iris to control the amount of light entering the camera. Viewing range should be 200 meters for new installations but may be less if already installed at a lesser spacing in existing CCTV installations. Height of mounting should be between 35 and 40 feet.

If video motion detection is contemplated either for initial installation or eventual retrofit, cameras should be rigidly mounted on structures not subject to large deflections in the normally expected winds at the site.

The video signal from each camera should be transmitted to the CAS and to the SAS separately by means of baseband video on coaxial cable or alternatively by means of cable TV (CATV, two way RF carrier channelized video transmission). If CATV is chosen, a modulator, demodulator and line amplifiers should be provided for each channel, together with provision in the cable for synchronizing horizontal and vertical camera sweeps to the VMD master clock. All cameras should be synchronized to enable roll-free scene switching. Power should be supplied at 115 VAC. from the utility's mains and uninterruptable power source. Power and signal lines should be buried. A common trench may be used to accomodate power, video and intrusion sensor signal lines to avoid indiscriminate excavation.

Video monitors should be provided in the CAS and SAS equipped with external sync capability. The monitor screen size should not be less than 12 inches (0.3 meters) on the diagonal.

Four monitors should be provided with controls to command any camera scene to appear on any monitor. An alarm should automatically key the

first monitor to show the alarmed segment and its address or location. As other segments alarm, they should show up on the other three monitors in time sequence. A fifth monitor can be used for playback of selected alarm events. The keying alarm signal should be either of two levels: a single layer "nuisance" alarm indication or a "true" alarm, either from a time integrated single sensor layer or a time integrated "ANDed" signal combining at least two layers. Only the true alarm should annunciate its presence to the operator.

A time lapse video recorder should be provided. The recorder should be equipped to go to full speed within 1 second upon alarm and have the ability to play in reverse. The recorder should use the VHS tape format or alternatively, whatever format exists that allows the most economical storage of time lapse video. Video tapes should comprise a record of alarms issuing from the multi-layer alarm processor. Additional alarm source identification, event time and alarm disposition logging should be keyed to the CAS and SAS CPU.

Replay should be enabled through the multi-layer alarm interface event counter, which will identify an event by time and address on the video tape and in memory. An identification command entered by the operator should recall any selected event on a particular tape or from a particular camera without requiring manual search.

For purposes of archives storage and potential referral, tapes should be retained for three months, then erased and reused.

Figure 5-4 shows CCTV cameras in the isolation zone with VMD incorporated as an example 3rd layer to supplement existing fence and isolation zone sensors.

5.5.10 PRIORITIES IN ASSESSMENT

The following list summarizes the approach to forwarding alarms to the CAS/SAS.

- Any one sensor element disturbance will activate corresponding alert location on annunciator board at CAS, SAS.

- Any one sensor persisting through a set time window will alarm CAS,SAS.
- Any two sensor elements signaling through processor will alarm CAS, SAS.

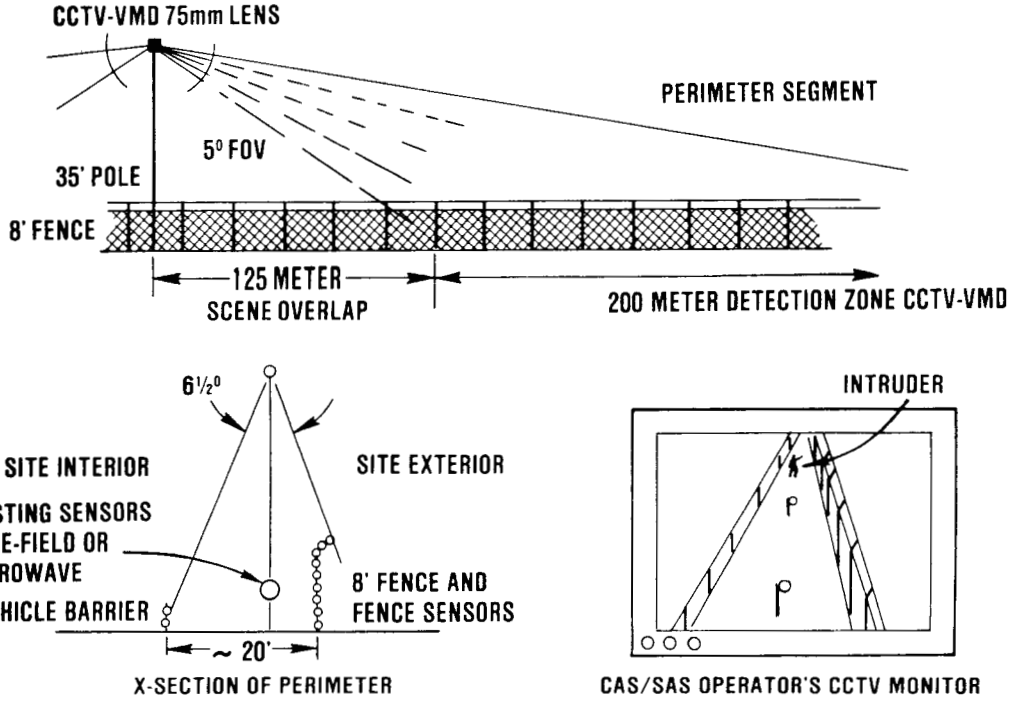


Figure 5-4. CCTV In Isolation Zone

- Location will automatically appear on monitor for immediate assessment.
- Guard force will be dispatched upon CCTV assessment, or if CCTV is down.
- Guard force will be provided with protective aids and denial agents.

The processing interface may permit assessment of single sensor or nuisance alarm signals as well as hierarchical assessment of genuine alarms. Consider, for example, a 16 segment system with 4 monitors. Primary attention should be devoted to genuine alarms, i.e. a segment where 2 or more sensors have detected something. Therefore, alarmed segments should have the highest priority in terms of display. With 4 monitors, 4 alarmed segments could be displayed simultaneously.

For example, the priority of display could be:

1. Alarmed segments: 3 sensors detecting
2. Alarmed segments: 2 sensors detecting
3. Alarmed segments: 1 sensor detecting
4. Non-alarmed segments: 1 sensor detecting
5. Routine displays

The monitor displays working with this priority would be assessing the most likely threats first. Within a given priority, if more than 4 segments were alarmed at once, the monitors would be switched automatically after a short but sufficient time period for assessment. The switching would take place until all alarms were evaluated. If more than 4 segments were alarmed, the non-alarmed segments with detection would not be displayed.

With fewer than 4 alarms at once, the displays not required for alarms would respond to detections by a single sensor on a segment. These displays could be switched in rotation if necessary.

The operator should be given a forceful audible annunciation on an alarm and the segment number displayed or indicated. A mild audible reminder with a segment number displayed or indicated should be sufficient for detections which do not result in alarms.

While it would be possible to overload such an assessment system and its operators, the display overload itself should be sufficient to indicate a coordinated penetration effort. Also, to create such an overload would require precision timing and detailed knowledge of the security system.

5.5.11 INTERIOR CLEAR ZONE

A clear space interior to the perimeter fence and isolation zone, combined with hardened outer building and vital area walls, doors, and grids can impose transit delay time on the intruder. Additionally it can provide a lighted region for video surveillance (utilizing high mast sodium luminaires) and a tactical maneuver space for response force confrontation. Plans for new plants should allow at least 30 meters between the inner fence and any buildings housing vital areas.

5.6 DESIGN AND CONSTRUCTION

Perimeter security elements should be manufactured and installed in accordance with best accepted commercial design standards in cognizance of site and terrain, local, state and federal construction regulations. Some suppliers have designed rugged, reliable, long life items especially for the nuclear power plant perimeter role - and such attention to the ultimate application is to be encouraged.

The perimeter intrusion alarm layers and other perimeter security elements should be interfaced and integrated together as one overall system; and construction activities should be integrated and coordinated to accomplish such things as earth moving, pier and footing pouring, cable trenching, wiring, etc., common to each segmented perimeter layer.

It is not recommended to put up one intrusion detection layer at a time because of cost for reexcavation and rewiring for subsequent layers.

Intrusion detector candidates should be commercially available, off-the-shelf systems that have been performance level tested by SANDIA to one of their sensor type-specifications. Upon tentative selection among perimeter security elements, sensor layer options, combined processing and assessment alternatives, it is recommended to discuss their acceptability with NRC.

5.6.1 MATERIALS, PROCESSES AND PARTS

Parts made to commercial standard should be used wherever possible. Screw threads should be American standard. Wire gages should be AWG. Fence mesh and barbed wire should be double galvanized. All other externally used metal parts should be treated for corrosion resistance. Plastic parts should not be subject to breakdown from moisture, atmospheric or dust components nor from sun exposure. Plastic parts and paints should be fungus resistant.

Wiring and cabling should be of good commercial quality. Rodent resistant insulation should be used.

5.6.2 ELECTROMAGNETIC RADIATION

The overall installed system should reject electromagnetic interference among the three sensor layers, energized simultaneously. Microwave systems should reject commercial and military aircraft radars within a distance of 3 km. All systems should be operable under or adjacent to 60 Hz high voltage power lines within a distance of 10 meters.

All wiring and TV cables should be housed in metal conduit. Surge protection devices and appropriate grounding should be provided on power and signal lines and on conduit to clamp component input voltage to prevent damage from nearby lightning strikes. Sensors should not alarm from lightning generated electromagnetic fields within a distance of 3 km.

5.6.3 SAFETY

All sensor components, electronic processing equipment, power supplies, and alarm monitors should be capable of meeting the typical design requirments for fire safety of nationally recognized testing laboratories such as Underwriters Laboratory (UL) or Factory Mutual (FM). All electrical systems should be grounded. IEEE standard 308-1974 (15) as endorsed by Regulatory Guide 1.32, "Criteria for Safety-Related Electrical Power Systems for Nuclear Power Plants" (15), should be used as a guide. System design, methods of construction and operation and environmental exposure should not create the potential for injury of personnel.

5.6.4 ELECTRICAL INTERFACES

In the event primary power is interrupted, the system should provide for automatic switchover to emergency battery power without causing an intrusion alarm. Primary power should be 115 VAC from mains, with a backup uninterruptable power supply (UPS).

5.6.4.1 Uninterruptable Power Supply (UPS)

The UPS should consist of battery charger, inverter, automatic bypass switch, circuit breakers and necessary control elements. The UPS should provide 1 KVA of continuous power at 120 volts AC, single phase, 2-wire, 60 Hz output for critical loads during normal operation and during a utility power failure. The UPS also should provide DC charging current to the battery, and a DC supply to the UPS inverter.

The automatic bypass switch should transfer the critical load back to the input line in case of an UPS failure. Circuit breakers should be

the fast acting type which can be tripped by systems malfunction signals, thereby eliminating the need for power fusing.

Batteries alone should sustain the above load for 10 minutes (sufficient time for the utility's auxiliary generators to come on line).

Emergency power should be capable of sustaining operation for a minimum of 24 hours without replacing or recharging batteries or refueling generators. Batteries (including stored batteries) should be maintained at full charge by automatic battery-charging circuitry. Batteries should be checked in accordance with IEEE Standard 450-1975 (16) as endorsed by Regulatory Guide 1.129, "Maintenance Testing and Replacement of Large Lead Storage Batteries for Nuclear Power Plants" (16), and IEEE Standard 308-1974 (15) as endorsed by Regulatory Guide 1.32, "Criteria for Safety-Related Electric Power Systems for Nuclear Power Plants" (15).

5.6.4.2 Communication Modes

Existing communication lines which may directly connect each alarm segment to the CAS/SAS should input parallel ports in the multi-layer alarm interface. New plants, or existing plants utilizing serial bus communication, should employ compatible serial ports in the multi-layer alarm interface. Serial digital communications should be full duplex and dual loop to provide redundancy. Baseband video should be transmitted on coaxial cables from each camera to the interface processor. Alarm processing using both parallel and serial I/O should be internal to the multi-layer alarm interface and should not require special additional terminals or multiplexers to be installed at the perimeter.

5.6.4.3 Line Supervision

All signal lines connecting alarm relays with alarm monitors should be supervised. Signal lines linking the sensors to the processing electronics should also be supervised. Signal line supervision should

preferably be by means of time domain reflectometry, in which a reflected pulse time of arrival is compared to known system characteristics. Special supervision should not be required for video signals.

5.6.4.4 Tamper Indication

All enclosures for equipment should be equipped with tamper switches or triggering mechanisms compatible with the alarm systems. The electronics should be designed so that tamper-indicating devices remain in operation even though the system itself may be placed in the access mode. (Access mode means the condition that maintains security over the signal lines between the detector and annunciator and over the tamper switch in the detector but allows access into the protected area without generating an alarm.)

Power switches and all controls that affect the sensitivity of the alarm system should be located within tamper-resistant enclosures. All key locks or key-operated switches used to protect equipment and control should have UL-listed locking cylinders (see Regulatory Guide 5.12, "General Use of Locks in the Protection and Control of Facilities and Special Nuclear Materials", (28)).

5.7 RELIABILITY

Life cycle cost is a strong function of component and system reliability. Equipment failures can impose operational maintenance penalties, and by definition of failure-in-the-alarm-state, will contribute to the nuisance alarm budget. Individual segment intrusion detection layers, as well as the other perimeter security elements should have as a goal, mean-time-between failure (MTBF) of at least 30,000 hours. Parts such as TV camera tubes and luminaires which exhibit active wearout mechanisms are exceptions, but such items should be placed in a scheduled replacement operation and costed over the plant life cycle. Electronic processors should show a MTBF of at least 8760 hours (1 year).

High system MTBF is achieved by a parts count of high individual reliability and/or redundancy. Redundancy provides protection against single failures. Phenomenological diversity of layers protects against nuisance alarms and common mode failures.

5.8 MAINTAINABILITY

5.8.1 MAINTENANCE PHILOSOPHY FOR A LAYERED SYSTEM

The recommended maintenance and replacement philosophy is based on the following system considerations.

- Coping with system failures becomes manpower intensive and expensive. Therefore, overall system reliability should be optimized. High reliability parts should be used and piece part or subsystem redundancy incorporated in design to economically optimize system MTBF.
- Maintaining high system alarm detectability will minimize the statistical probability of power plant outage due to sabotage, and thus associated costs.
- System P_D should be optimized by layering to keep system testing at an economically realistic level.
- Security system hardware and software capability is rapidly evolving. Initial spares inventory may become obsolescent over the depreciation time of the security equipment. Therefore specific replacement parts should be ordered when required upon failure.
- Preventive maintenance or scheduled replacement should be made for wear-out items.
- Layers are taken as representative of sensors now in use at nuclear plants; and for a three layered system, a Video Motion Detector (VMD) is taken as an example third sensor supplementing Closed Circuit Television (CCTV) used primarily for assessment purposes.

The following analysis shows how these operational and maintenance considerations can affect the choice of a system.

For a single layer system the guards must not only respond to a failure but also remain on patrol at the failed segment to maintain security. This can prove expensive to the plant operator and have a negative effect on the morale of the guard force particularly in inclement weather.

For a double layer system the guards will need to respond to a failure and will need to patrol the segment more frequently, monitor it remotely or remain at the segment to assure security.

The triple layer system still requires guards to respond to a failure if assessment by CCTV or other remote means is not possible or is inconclusive. But the depth and performance of a 3 layer system will allow the guards to return to their base if the failure is not caused by an intruder.

However, for this operating philosophy to be viable, double failures or two or more sequential failures within a short period of time must be shown to be very rare statistically.

To examine the risk of double failures in more detail, the following are assumed.

- Failures in the various layers and equipments are independent.
- Downtime for a layer which has failed will average 96 hours or less. This is taken to be the time that a replacement LRU can be ordered and delivered from the equipment contractor.
- The video motion detector is assumed to have an overall MTBF of 8000 hours. This is apportioned to be a 30,000 hour MTBF in the common equipment channel and 174,545 hour MTBF in each of the 16 independent video processing channels.
- From a fully working state, 4 types of failures can occur.
  --VMD single channel - MTBF = 174,545 hours
  --VMD all 16 channels - MTBF = 30,000 hours

--Sensor A in a segment - MTBF = 30,000 hours
--Sensor B in a segment - MTBF = 30,000 hours

The expected number of failures for each type over 6 years is tabulated following:

	NUMBER	TOTAL OPERATING HOURS	MTBF	EXPECTED NUMBER OF FAILURES
VMD Single Channel	16	841,536	174,545	4.82
VMD Common	1	52,596	30,000	1.75
Sensor A	16	841,536	30,000	28.05
Sensor B	16	841,536	30,000	28.05

Treating each of the predicted failures as being "a first failure" will be slightly pessimistic but computation is simplified.

In the first case, it is assumed the video motion detector fails in a single channel. The system would be rendered deficient if sensor A or sensor B failed on the same segment. Considered together, sensors A & B in one segment will have a MTBF of 15,000 hours. Thus the probability that one would fail in 96 hours is 0.0064. Since there are 4.82 single channel VMD failures expected, the total expected number of system failures in this mode is 0.0308 over six years.

In the second case, the Video Motion Detector is assumed to have failed in all 16 channels. Now a single failure in either layer A or layer B would result in the system being deficient. The MTBF for 32 sensors in series is 937.5 hours. The probability that any one would fail in 96 hours is 0.0973. With 1.75 common video motion detector failures expected, the expected number of system failures in this mode is 0.1706 over 6 years.

In the third case it is assumed that sensor A on a segment has failed. Then, a failure in the common portion of the VMD, that channel of the VMD, or that segment's sensor B will cause a system deficiency. The resulting subsystem has a MTBF of 13,812 hours with a probability of failing in 96 hours of 0.0069. Since there are 28.05 failures of

sensor A expected over 6 years, 0.1943 system failures can be expected from this mode. The calculations for the fourth case, a sensor B failure, are identical.

Totalling these results in 0.59 cases of 2 layers failing before repair is completed in a period of 6 years, or 3 events during the 30 years life of the plant.

At each of these events, 2 guards would be required at the segment for an expected time of 48 hours. At a cost of $20 per guard per hour, the expected cost for each event for guards would be $1,920.

Since so few such double failure events are expected over the plant lifetime in a layered system, the low cost risk justifies the concept of procuring replacement parts when needed instead of maintaining a large spares inventory. Furthermore the layered system permits repair of failures to be scheduled generally to normal shift work.

Further improvements in reliability may be achieved by providing standby modules in place for any equipments of decidedly poorer MTBF than the rest, e.g., the VMD processor. Tradeoff must justify the cost of such standby equipment vs. the cost of temporarily manning the expected number of events derived from the single equipment reliability figures.

5.8.2 MAINTENANCE IMPLEMENTATION

Maintenance of the perimeter security system encompasses normal wear and tear on the non-electronic systems such as fences, poles and fixtures.

Scheduled replacement should be performed as preventive maintenance for low MTBF components such as luminaires and camera vidicons. Spares should be allocated from inventory and periodically replaced as scheculed over the plant life cycle. Such spares should be considered as part of operating costs.

Repair of perimeter sensor and processor components should be effected by the change out of line-replaceable units (LRU). By definition, a LRU is a complete sensor assembly or box or, at the minimum, a printed circuit board which can be quickly replaced in the field by unplugging and by reinsertion of a spare in its place.

Location, replacement and electrical checkout of a LRU should require no more than one hour of elapsed time, after which continuity of perimeter detection can be restored. Spares for this type of repair should be allocated on the basis of no more than 20% of initial equipment cost. Alternatively, with one layer down in a 3 layer system, the other two layers may be expected to maintain security until replacement parts can be obtained expeditiously from the supplier, thus minimizing spares inventory.

As recognized in paragraph 5.8.2 preceding, computer and processor obsolescence is a continuing concern; and improvement in performance in both hardware and software may give a particular intrusion detection concept an entirely new appearance in just a few years. Therefore, it is not intended to freeze an initial design and supply the plant with original spares for its life cycle. Rather, as major replacements are required, the improved design existing at the time should be procured. This imposes on suppliers the requirement that subsequent versions be upward compatible and interchangeable with, but not identical with the original equipment.

Maintenance should be accomplished by trained utility personnel on a one shift basis. As shown in paragraph 5.8.2, except under extraordinary circumstances, off shift failures statistically should leave two out of the three intrusion detection layers active and thus permit repair to be scheduled for a routine time.

5.9 ENVIRONMENTAL CONDITIONS AND PROVISIONS

5.9.1 GENERAL

Perimeter intrusion alarm systems should be capable of operating throughout the climatic extreme of the environs in which they are

used; as a minimum, the outdoor systems should be capable of effective operation between -40°C and +71°C. Components that necessarily must be located out of doors should be protected from moisture damage by such methods as hermetic sealing, potting in an epoxy compound, conformal coating, or watertight enclosures. Video and IR systems, if used, should incorporate environmental enclosures and features to prevent both moisture condensation and icing on optical parts and windows.

External installations should be able to withstand winds of 160 km/hr without damage and winds and gusts up to 48 km/hr without alarming.

Equipment for installation inside buildings (e.g., at CAS and SAS) should be able to function in surroundings between 10°C and 40°C and 10% to 90% R.H. with no condensation.

5.9.2 SITE SPECIFIC CONSIDERATIONS

Sensor systems should be carefully analyzed for compatibility with their intended site and environment. The basis for their selection should be a site survey and local environment history.

It is repeated here as a truism that no single sensor is capable of detecting all intrusions in any environment. Vulnerability to defeat is site variable depending on such things as terrain, snowfall and drifts permitting bridging of barriers or tunneling past free standing sensors. Certain sensors become insensitive in frozen ground or in soils which become conductive when wet. Likewise some sensors can be damaged by ice and by corrosive atmospheres. IR detection and video surveillance can be degraded by ice, heavy fog or driving snow storms.

It must be accepted that there will be times when both detection and assessment may not be dependable due to weather. Appropriate selection of diverse layers will minimize but not eliminate these cases. Therefore, contingency procedures should call for adoption of a manned security mode (continuous perimeter patrol) until the disturbance subsides or can be cleared away.

Terrain features, hills and gulleys and natural obstacles along the perimeter can not always be avoided or filled in to make a level surface. Such conditions would eliminate consideration of line-of-sight sensors such as free standing microwave or IR in favor of sensors that follow the terrain.

It will be necessary to gauge EMI background sources which may affect electronic sensors. EMI may originate from local communication links and radars as well as from nearby power lines. If seismic sensors are contemplated, then measurements will be necessary of the microseismic background noise.

Therefore, site environmental and weather histories should be compiled and site soil and terrain surveys performed to enable compatible equipment selection. In addition, verification testing of selected systems should be performed on site in cooperation with suppliers and contractors prior to committing to procurement.

Section 6

6.0 MANNING IMPLICATIONS

Using closed circuit television surveillance may enable guard force reduction by five men over manning two watch towers on a three shift basis.

The provision of three detection layers at the perimeter allows for one shift scheduled maintenance. By not requiring round-the-clock on-call maintenance, the maintenance force can be reduced by an estimated 6 men. Automatic keying of an alarmed segment onto a TV monitor for assessment, automatic reset of nuisance signals and the achievement of processed reliable alarms should enable minimal manning of the CAS and SAS and thus a work force reduction of about five people.

Dedication of personnel strictly to the continual perimeter performance testing suggested by Regulatory Guide 5.44 has not yet been made. If the 5.44 test sequences were to be followed, many full time test personnel would be required for a non-layered system. On the other hand, a three layered perimeter test program as recommended in Appendix B may be accomplished with the present number of guards in normal duty times. The implications of layering to man hours required for performance verification are explored in Appendix B.

Section 7

7.0 PROCUREMENT

7.1 SECURITY SYSTEM CONTRACTOR

It is recommended that a security system contractor be retained to interpret the requirements of the NRC and interface among NRC, the utility, the construction contractor and equipment vendors. The responsibilities of a security system contractor would include the following:

- Site-specific requirements analysis and specification
- Pre-procurement site specific sensor testing
- Selection of all perimeter security elements
- Choice of supplemental sensors (tested by Sandia)
- Integration with existing elements through a multi-layer processing interface
- Spares for wearout items
- Operational and maintenance training
- Documentation
- Post installation acceptance testing
- One year warranty

7.2 SPARES

Spares should be minimized consistent with the maintenance philosophy of pararaph 5.8. Spares for replaceable equipment should be provided as a function of MTBF and on the basis of no more than 20% of the initial equipment cost.

7.3 DOCUMENTATION

Detailed specifications, performance data, schematics, assembly and installation drawings and instructions, test plans and procedures, parts lists, training manuals and maintenance manuals should be provided with each security element subsystem.

This documentation should be kept current by each supplier as subsystem designs change and evolve.

This documentation should provide all information needed to enable plant personnel to perform all adjustment, maintenance, repair and replacement of installed subsystems.

7.4 PERSONNEL AND TRAINING

The number of maintenance personnel required should be determined by a parts count and conditional probabilities of failure based on parts MTBF and upon a mean time to repair (MTTR) of one hour. Skills should be compatible with the operational characteristics and failure modes of electrical, electronic and optical equipment.

The maintenance duty cycle should be one shift daily, 7 days a week with provision for occasional emergency overtime. Approximately half the duty should be allocated to preventive maintenance.

Necessary checkout and test equipment should be provided by the contractor or subsystem supplier. The contractor should provide system personnel training for operation and maintenance including necessary training equipment, training facility and training manuals.

7.5 SYSTEM CERTIFICATION

MTBF claims should be supported by test documentation, operational experience, or by analogy to similar parts and systems in a similar environment.

Site survey and evaluation, including on-site verification testing, should be accomplished to define performance limits and capabilities prior to subsystem procurement.

Installation testing and check-out should be made of the individual subsystems and of the whole perimeter alarm system completely interfaced with all its elements.

Formal acceptance test verification of performance characteristics to demonstrate that system requirements of section 3 have been met should be the responsibility of the perimeter security system contractor and should take place during the first three months of utility operation (or construction) after completion of the perimeter installation.

Delivery of the system to the utility should occur upon NRC acceptance of the installation and test results.

The perimeter security system contractor should warrant that the installed system will meet or exceed the performance and materials quality requirements of the perimeter security specification for a period of one year.

7.6 EQUIPMENT SUPPLIERS

Perimeter security vendors are listed following who are known through SANDIA (9) and the INMM Workshop held in Charleston, S.C., March 1981 or who supplied cost and performance data in response to the minispec of section 9.1. Most of those listed supply just the perimeter detection sensor equipment and not a layered system complete from perimeter to alarm station. Most also depend on the plant construction contractor or plant owner to handle installation tasks. A few suppliers do provide several phenomenologically different sensor types, signal processing, and alarm terminals but are only at the threshold of providing the diverse sensor layering logic processing, microcomputer programming, and integrated systems engineering recommended in section 5.0 herein. As of this writing, some of the listed sensors are still being proven in the field or in test and should be considered only upon demonstration of performance and compliance with the

criteria of section 4.0. This listing should not be considered definitive or complete since there may be applicable systems unknown to us and since new and improved sensors and processors continue to be introduced.

7.6.1 MICROWAVE SYSTEMS

A. Polarized bi-static radar

- PRS 2100 Polarized bi-static radar
  1) National Security Systems
     P.O. Box 22665
     Tampa, Fla. 33622
     (813) 885-2136

B. Standing line bi-static radar

- Southwest Microwave Model 300
  2) Southwest Microwave, Inc.
     (formerly Omnispectra)
     707 W. Geneva Dr.
     Tempe, Ariz. 85282
     (602) 968-5995

- RACON Microwave
  3) RACON Inc.
     8490 Perimeter Rd., So.
     Seattle, Wash. 98108
     (206) 762-6011

- RACAL Microwave
  4) RACAL Security
     1151 Seven Locks Rd.
     Rockville, Md. 20854
     (301) 251-0279
     representing

5) RACAL-MESL Security, Ltd
Lochend Industrial Estate
Newbridge
Midlothian EH28 8LP
Scotland
Phone Edinburgh (031) 333 2000

- SERPE Mercure 300

6) Safeguards Technology Inc.
2222 Richmond Ave
Staten Island, N.Y.10314
(212) 698-0266
representing the manufacturer:

7) Mercure
4, rue Pierre-Mael
56100 Lorient
France
Phone (97) 215 444

- Microwave Fence Model 33

8) Shorrock Inc.
A subsidiary of the Greyhound Corp.
Parkway Industrial Center
7235 Standard Drive
Hanover, Md. 21076
(301) 796-8520
representing the manufacturer:
Shorrock Security Systems, Ltd.

9) Shadsworth Road
Blackburn BB1 2PR,
Lancashire, England
Phone (0254) 63644

C. Polystatic radar, fence mounted.

- Southwest Microwave Model 700
Address no. 2.

D. Ported Coax.

- Guidar

10) Computing Devices Company a division of Control Data
P.O. Box 8508
Ottawa Ontario, Canada, Ltd
Canada K1G3M9
(613) 596-3810

- H. Field

11) Stellar Systems
3020 Olcott Street
Santa Clara, Ca. 95051
(408) 244-8161

- MAGBELT

Address No. 6
representing the manufacturer
12) Magal
Israel Aircraft Industries, Ltd
Ben Gurion International Airport 70100
Phone 973906

7.6.2 ELECTROMAGNETIC FIELD, E-FIELD

A. E-Field: Three or four wire fence mounted or free standing.

- E-FIELD

13) Stellar Systems
231 Charcot Avenue
San Jose, CA. 9513
(408) 946-6460

B. Differential Field

- Stellar Systems Differential E-Field
address no. 13

- Shorrock Differential T-Line
  address no. 8
- Magal Magstaf
  address no. 6 and no. 12

7.6.3 MAGNETIC

A. Magnetic Buried Line

- Honeywell BLS 1000
  14) Honeywell Inc.
  Tactical Support Center
  Defense Systems Div.
  13350 U.S. Highway 19
  P.O. Box 11568
  St. Petersburg, Fl. 33733
  (813) 531-4611

7.4.4 PRESSURE/STRAIN

A. Pressure/Strain Buried Line.

- Teledyne Geotech BLID
  15) Teledyne Geotech
  P.O. Box 28277
  Dallas, Tx. 75228
  (214) 271-2561

7.6.5 INFRA-RED

A. Bi-Static IR

- Bird Eye
  16) Bird-Eye Security International, Inc
  1 Bergen Turnpike
  Little Ferry, N.J. 07643
  (201) 488-1440

- S5700 Outdoor Photoelectric Intrusion Detector

  17) Arrowhead Enterprises, Inc.
  Anderson Avenue
  New Milford, Conn. 06776
  (203) 354-9381

- Active I.R. Perimeter System

  18) Del Norte Technology, Inc.
  1100 Pamela Dr.
  P.O. Box 696
  Euless, Tx. 76039
  (817) 267-3541

7.6.6 FENCE DISTURBANCE SENSORS

A. Switch and Counter

- Inertiaguard

  19) Morse Product Manufacturing
  P.O. Box 4128
  Sylmar, Ca. 91342
  (213) 367-5951

- Perim Alert II

  20) Air Space Devices
  Division of Norton Company
  P.O. Box 197
  Paramount, Ca. 90723
  (213) 774-4905

- MAGILINE
  address no. 6 and no. 12

- FDS

  22) Fourdee, Inc.
  Division of Emerson Electric Co.
  440 Plumosa Avenue
  Casselberry, Fla. 32707
  (305) 831-2800

- Shorrock SID Latch Fence Vilration Sensor
  address no. 8 and no. 9

B. Electrostatic or Tribo-electirc

- Sylvania FPS Electret

  22) GTE Products Corp.
  Western Division
  P. O. Box 188
  Mountain View, Ca. 94042
  (415) 966-2210

- Stellar E-Flex
  address no. 13

C. Seismic

- Del Norte Seismic Fence System
  address no. 19

- Litton F.I.D.S.

  23) Litton Security Products
  1213 North Main Street
  Blacksburg, Va. 20406
  (703) 552-3011

D. Tension Wire

- DTR 90 Taut-Wire Fence
  address no. 6

7.6.7 VIDEO MOTION DETECTORS

- WISCO Teleguard

  24) Wood Ivey Systems Corp.
  3535 Forsyth Road
  Orlando, Fl. 32807
  (305) 678-6116

- Video Tek Visigard

  25) Video Tek, Inc.
  8 Morris Ave.
  Mountain Lakes, N.J. 07046
  (201) 335-1678

7.6.8 CLOSED CIRCUIT TELEVISION

- G.E. CCTV

  26) General Electric CCTV
  Owensboro, Ky. 42301
  (502) 926-8600

- COHU

  27) Cohu Electronics Division
  Box 623
  San Diego, Ca. 92112
  (714) 277-6700

- RCA

  28) RCA Closed Circuit Video Equipment
  New Holland Ave.
  Lancaster, Pa. 17604
  (717) 397-7661

- DAGE

  29) DAGE-MTI, Inc.
  208 Wabash St
  Michigan City, Ind 46360
  (219) 872-5514

7.6.9 LIGHTING

- HUBBELL

30) Lighting Division
Harvey Hubbell Incorporated
Electric Way
Christianburg, Va. 24073
(703) 382-6111
represented by:

31) Adra-Carnell
2302 Parkside Drive
Irving, Tx. 75061
(214) 254-4114

- G.E.

32) General Electric Company
Lighting Systems Department
Hendersonville, N.C. 28739
represented by:
General Electric Company
8101 Stemmons Freeway
Dallas, Tx. 75247
(214) 688-6231

- NORELCO (Low Pressure Sodium)

33) North America Philips Lighting Corp.
Bank Street
Hightstown, N.J. 08520
(609) 448-4000

7.6.10 FENCE

- Fence and Cable Guard

34) McKay Fence and Awning
Rt. 1, Box 52
Wolfe City, Tx. 75496
(214) 496-2343

7.6.11 SITE SURVEY AND INSTALLATION

- VITRO

  35) Automation Industries, Inc.
  Vitro Services Division
  Industrial Park
  Fort Walton Beach, Fla. 32548
  (904) 244-7711

7.6.12 STAND-ALONE ALARM MONITORING SYSTEMS

- Vindicator SMS-2000M

  36) Vindicator Corporation
  1092 Stewart Drive
  Sunnyvale, Ca. 94086
  (408) 739-2500

- Stellar Systems MARS-1000
  and Model 2450 "AND" Gate
  address no. 11

- MAGAL MAGAMUX
  address no. 6

- KELTRON SIRS700 and DM-701

  37) Keltron Corporation
  225 Crescent Street
  Waltham, Mass. 02154
  (617) 894-8700

- RECEPTORS CP 8400

  38) Receptors, Inc.
  4203 Spencer Street
  Torrance, Ca. 90503
  (213) 542-0501

- VIDEO-TEK VISIGARD SLS-100
  address no. 24

ICI CHIPMUX

- ICI Systems, Ltd.

  39) 43B Inverness Dr. East
  Inglewood, Co. 80112
  (303) 779-8528

- ADT CENTRASCAN

  40) American District Telegraph Company
  One World Trade Center
  92nd Floor
  New York, N.Y. 10048
  (212) 558-1100

- OMEGALARM

  41) Radionics, Inc.
  228 Reindollar
  Marina, Ca. 93933
  (408) 384-8877

- CMP-1 Central Multiplex Processor

  42) Wells Fargo
  4910 W. Rosecrans Ave.
  Hawthorne, Ca. 90250

Section 8

8.0 USER DETECTABILITY TESTING

After installation and throughout the lifetime of utility operations, perimeter detectability should be continuously checked. Procedures suggested to be followed are repeated here from NRC Regulatory Guide 5.44, Revision 2, May 1980.

All tests and test results should be documented to establish the performance history of each perimeter alarm system and each segment of the isolation zone. The test results should be available for inspection and analysis.

8.1 OPERABILITY TESTING

Perimeter intrusion alarm systems should be tested on all segments of the isolation zone at least once each 7 days. Testing may be conducted during routine patrols by the members of the licensee security force. The testing should be conducted by crossing the segment of the isolation zone where the alarm system is located or by climbing the fence to which the system is attached to provide the required alarm stimulus. Where appropriate, a specific test procedure should be followed. Prior to making the test, the individual making the test should notify the central alarm station that a test is about to be conducted. The area under test should be maintained under visual observation by a member of the security organization.

All segments of the isolation zone should be tested in a different, preferably random, order every 7 days and the testing should be conducted throughout the week, not all tests in one day. The operability testing should result in 100% detection on all segments each 7 days. If the perimeter alarm system fails to detect an intrusion on one or

more segments, corrective actions should be taken and documented. A sample method for determining the testing order for the segments and a suggested method for determining if the detection rate of the perimeter alarm system has decreased to below 90% is given in Appendix A to Regulatory Guide 5.44.

8.2 PERFORMANCE TESTING

At least quarterly, after each inoperative state, and after any repairs, the perimeter intrusion alarm system should be tested against its manufacturer's design specifications and for proper detection probability. An inoperative state for an alarm system or component exists when (1) the power is disconnected to perform maintenance or for any other reason, (2) both primary and backup power sources fail to provide power, and (3) when power is applied and one or more components fail to perform their intended function. Placing a properly operating alarm system in the access mode would not constitute an inoperative state unless accompanying or followed by any of the above three conditions.

8.2.1 SPECIFICATION TESTING

The test procedure recommended by the manufacturer should be followed. While the test is being conducted, the area under test should be maintained under visual observation by a member of the security organization. For all perimeter systems, tests should be conducted to verify that no obvious dead spots exist in the segment of protection. As a minimum, the tests should include line supervision and tamper proofing when testing in both the access and secure modes. If the perimeter alarm system does not meet the manufacturer's specifications, corrective actions should be taken and documented.

8.2.2 DETECTION PROBABILITY TESTING

Proper detection probability is defined as the ability to detect an intruder with at least 90% confidence, under the conditions stated in

the Performance Criteria of each type of alarm system. While the detection probability testing is being conducted, the area under test should be maintained under visual observation by a member of the security organization.

8.2.3 PROBABILITY DEFINITIONS

1. Acceptance Criterion Minimum acceptable P_D, within a confidence interval, (P_D = .9 with 95% confidence)
2. 95% Confidence Interval The true P_D will be a value between .9 and 1.0 95% of the time. (See figure 8-1)
3. True P_D, Inherent P_D: $0.9 \leq P_D \leq 1.0$
4. P_D Point Estimate Number of successes in a limited number of tests divided by the total number of tests
5. Type II Error False acceptance of sensors that do not satisfy the acceptance criterion.
   (Consumer's Risk)
   - Limited to 5% or less by the 95% confidence requirement
6. Type I Error False rejection of sensors that satisfy the P_D requirement.
   - A function of P_D point estimate and lower bound of confidence interval
   - A function of the number of test trials per test sequence

8.2.4 TESTING METHODS

Appendix A to Regulatory Guide 5.44 should be used as a guide for testing perimeter intrusion alarm systems.

8.2.4.1 Performance Testing of a Multilayer Perimeter Intrusion Alarm Segment

Probability testing should be performed per Regulatory Guide 5.44 except that the test segment will be layered, and alarms combined to define detection of a complete isolation zone penetration.

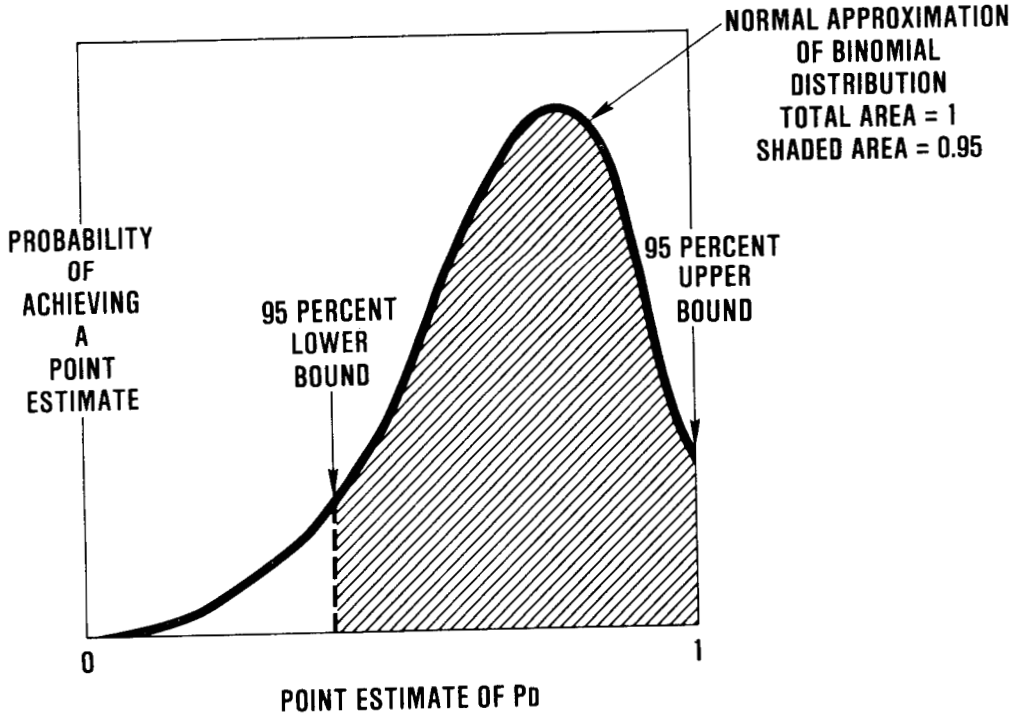


Figure 8-1 Confidence Interval

See appendix B for the test rationale and expected number of trials for a layered system.

If a single layer perimeter intrusion alarm system has a 95% confidence lower bound equal to 90% (P_D), then the probability that this P_D be equaled or exceeded in the NRC recommended test sequence of 50 trials is only about 14%. The probability of obtaining the expected number (0.9) decreases with an increase in the number of trials. This is characteristic of the the binomial cumulative probability of success in that many independent trials.

Therefore the probability of rejecting single layer sensor segments satisfying the 0.9 P_D requirement (Type I error) is expected to be about 86% for the NRC recommended test sequence. However, the Type I error probability greatly decreases as the probability of detection rises with a multi-layered perimeter segment. A layered P_D = 0.99 for instance would be expected to yield only 1.22% Type I errors in the NRC test sequence.

In terms of the number of test trials versus numbers of layers, a two layer perimeter reduces the cumulative probability of a Type I error from 86 percent to 43 percent and thus reduces the average number of test trials per segment from over 200 to 68. A 3 layer perimeter reduces the cumulative probability of a Type I error from 86 percent to less than 2 percent and thus reduces the average number of test trials per segment from over 200 to 34. A comparison of one, two and three layer effects is shown in Table 8-1.

8.2.4.2 Vendor Qualification Testing

Layered testing can also avoid the problem of Type I errors in vendor qualification testing and at the same time realistically verify sensor performance. A vendor testing approach is recommended following.

- Perform the testing of a production segment at the designated nuclear power plant site, or on a site which has been determined to have similar terrain, soil and environmental conditions.

- P_D is expected to vary with environmental changes. Therefore, any one sequence of tests should be completed under identical conditions. On the other hand, to evaluate seasonal, weather, and day-night effects on P_D, several test sequences should be made, separated in time as such conditions dictate.
- Ascertain the most likely vulnerable penetrating mode e.g., walking, running, crawling, jumping, or rolling, and standardize it using a test subject complying with the required intruder characteristics and the segment location most vulnerable to defeat.
- Rather than using diverse sensor layers (since nuisance alarms or defeat vulnerability is not an issue here), evaluate probability of detection as the combined or contingent probability of penetrating two layers of the same sensor. That is, a segment will comprise two layers for this test, both of which must be penetrated. Thus if a single layer has a P_D of .9, two layers should realize a P_D of .99 and consequently an expected Type I error of only about 1%.

  The measure of P_D thus will be the number of Type I errors experienced in the NRC (0.9, 95% confidence) test sequence considering the layered segment as a single sensor of inherently greater P_D. This greater P_D is the ORed product of the individual layer P_D.
- Document the test and test results including environmental conditions, troubleshooting and adjustments required, equipment failures and replacements, defeat modes and conditions.

Table 8-1

PERIMETER SEGMENT TESTING

EXPECTED TYPE I ERRORS VS. TRUE P_D

	SINGLE LAYER 0.90 P_D	TWO LAYER 0.95 P_D	THREE LAYER 0.99 P_D
•PER SEGMENT			
--Successful Test Percentage In One Test Cycle	13.84	57.42	98.78
--Tests/Cycle	35.03	39.63	33.10
--Test Cycles	7.22	1.74	1.01
--Total Tests	254.00	69.00	34.00
--Service Calls	6.22	0.74	0.01
•FOR SIXTEEN SEGMENTS			
--Total Tests	4220.00	1105.00	536.00
--Expected Type I Errors	3636.00	471.00	6.60
--Service Calls	100.00	12.00	0.20

Section 9

9.0 COSTS

There is no consistent set of cost data which has been correlated with performance of perimeter intrusion alarm equipment; and it has been found very difficult to obtain meaningful information from equipment vendors. In an attempt to obtain figures which can be compared, the following mini-spec was circulated to the principal vendors of security equipment.

9.1 MINI-SPEC FOR ALARM SYSTEM COSTING COMPARISONS

Initial costs and annual costs for operating and maintenance are required for several perimeter lengths and alarm segment lengths which may be typical of nuclear power plants. Costs are required for each perimeter element candidate listed below. Costs should include alarm processors if applicable. Initial costs should include site preparation, equipment installation and buried wiring, to both central and secondary alarm stations assuming a typical rolling terrain with no deep gulleys or streams and no rock removal. Operating and maintenance costs should include an estimate of power expenses, training, spares and replacement, and scheduled upgrading if applicable, for a life cycle of thirty years. Assume constant 1982 dollars.

It is understood that some suppliers do not do their own installation work. Nevertheless your knowledge and experience of costs in this area are solicited as best estimates.

- It is requested that you provide five tabulations of costs for the following four perimeters and two segment lengths as applicable to your specific perimeter element.
  --1600 Meters, 100 Meter Alarm Segments

--3200 Meters, 100 Meter & 200 Meter Alarm Segments
--4800 Meters, 200 Meter Alarm Segments
--6400 Meters, 200 Meter Alarm Segments

- Environment: Clay soil, withstand 90 KT wind; -35°C to +50°C, 3 ft. snow, occasional standing water.
- Perimeter element candidates
  --Single Fence
  --Vehicle Barrier
  --Fence Disturbance Sensor
  --E-Field 3 Wire Free Standing
  --Differential Field
  --E-Field On Fence Standoffs
  --Polarized Bi-Static Radar
  --Bi-Static Radar
  --Polystatic Radar
  --Magnetic Buried Line
  --Pressure Buried Line
  --Ported Coax
  --Lighting (LPS, HPS)
  --Alarm Processing Interface
  --CCTV
  --VMD

Equipment sources and trade names are listed in Section 7-6.

- Features desired for perimeter sensors.
  --Threshold adjustment capability
  --Self checking
  --Tamper indicating
  --Failure indicating
  --Switchover to secondary power source
  --Loss of power indicating
- Performance desired for perimeter sensors.
  --90% detection probability with 95% confidence (ref. NRC Regulatory Guide 5.44, May 1980)
  --False alarm and nuisance alarm rates one per day each, maximum.

--Performance should be determined for the designated segment length assuming a human target having the following features: 35 KG, moving at 0.15 m/sec. and at 5 m/sec., having a low contrast, 1 $Ft.^2$ minimum cross section presented to the sensor when rolling or crawling. Walking, running and jumping comprise the other test modes.

- Fence. 8 ft. total height including 3 strands of barbed wire on extension arms. #11 AWG chain link, to be anchored in reinforced concrete curb or pier with 4 in. above ground, 18 in. below ground level. Curb to be 8 in. wide.
- Vehicle Barrier. Forms the inside boundary of 6 meter wide isolation zone. Consists of steel S beams or I beams anchored vertically in cylindrical concrete footings spaced 12 ft. apart. Two continuous 3/4 in. diameter steel cables are attached at each beam. The object is to stop or disable a 3/4 ton pick-up truck or heavy automobile.
- Lighting. 1 footcandle min. illumination with illumination ratio 3:1, 40 ft. poles, footings, buried wiring, luminaires of 3 types: HPS, LPS, Mercury Street Lamps. Suggested pole spacing - 140 to 160 ft., 2 luminaires per pole. Poles to light perimeter isolation zone 6 meters wide.
- Closed circuit television for alarm assessment. Fixed cameras looking down perimeter fence line and 6 meter wide isolation zone, auto iris, 1 footcandle min. illumination. Mountings and environmental enclosure. 35 ft. rigid pole, tower or pipe shaft to be provided complete with concrete footings. Multiplexed CATV cabling in buried conduit. One monitor for each four cameras.
- Video motion detection. Add-on to CCTV, with appropriate sync, controls, masking, hit and contrast adjustment. Each processor to accomodate 4 video channels. Motion alarm to command alarm scene to appear on video monitor for assessment. Provide capability to cassette record alarm scene (requires time coding and fast reaction to

attain recording speed: within 1 sec. approximately); alternatively a delay line or video disc could be used as a buffer for the tape recorder to cover the initial alarm event while the tape recorder gets up to speed. Camera pole stiffness to be augmented (pole within a pole, concrete filled sewer pipe, guy cables) so that camera movement does not cause video motion detector to alarm because of apparent scene motion in wind gusts up to 35 KTS.

9.2 EQUIPMENT COST TABULATIONS

Response to the mini-spec was mixed and incomplete. Nevertheless, security element cost inputs have been tabulated for a 1600 meter perimeter. They should be used with caution as rough order of magnitude numbers. Site specific requirements relating to perimeter length, terrain and climate could cause these figures to increase by large factors.

Table 9-1 shows values for the barrier, lighting and assessment elements. Table 9-2 shows costs for above grade line sensors. Table 9-3 compares costs of fence disturbance sensors, and Table 9-4 shows costs of buried line sensors.

9.3 THE IMPACT OF LAYERING ON SYSTEMS COST

If meaningful performance testing as advocated by NRC Guide 5.44 becomes a requirement, a single layer perimeter will not be economically viable as demonstrated in table 9-5. However, a two or preferably three layered system will pay for itself in terms of testing cost savings. The table 9-5 cost comparison of one, two and three layers was derived in Appendix B.

Considerable annual savings will also accrue from work force reductions associated with CCTV, single shift maintenance and achievement of reliable (high P_D, low NAR) alarms. The latter of these manpower

savings are the result of layering. Potential labor cost savings are shown in Table 9-6.

Table 9-1
COMPARATIVE ELEMENT COSTS BARRIERS/LIGHTING/ASSESSMENT
1600 METER PERIMETER

ELEMENT	QUANTITY	INITIAL TOTAL $(000)	HARDWARE $(000)	INSTALLATION $(000)	ANNUAL UPKEEP $(000)
Chain Link Fence	1 Lot	93	38	55	8
Cable Guard	1 Lot	24	No Data	No Data	2
HPS Lighting (Incl. Poles)	66	41	20	21	6
CCTV (Incl. Poles)	16	147	97	50	No Data
VMD Add-On	16	90	82	8	No Data
Watch Tower (Hardened)	2	150	No Data	No Data	8

Table 9-2
COMPARATIVE COSTS ABOVE GRADE LINE SENSORS
1600 METER PERIMETER

ELEMENT	QUANTITY	INITIAL TOTAL $(000)	HARDWARE $(000)	INSTALLATION $(000)	ANNUAL UPKEEP $(000)
Bistatic Microwave	16	64	40	24	1
Polystatic Radar	16	67	51	16	1.6
Differential T-Line	16	193	129	64	2
Infrared	19	233	152	81	6
4-Wire E-Field					
Free Standing	16	110	73	37	17
Fence Mounted	16	116	85	31	18

Table 9-3
COMPARATIVE COSTS PASSIVE FENCE SENSORS
1600 METER PERIMETER

ELEMENT	QUANTITY	INITIAL TOTAL $(000)	HARDWARE $(000)	INSTALLATION $(000)	ANNUAL UPKEEP $(000)
FPS Electret	16	48	42	6	5.2
Perim Alert II	528	22	17	5	2.5
Taut Line	32	130	50	80	Incl.
Inertia Guard	16	53	28	25	2.5
E-Flex	16	57	48	9	3

Table 9-4
COMPARATIVE COSTS BURIED LINE SENSORS
1600 METER PERIMETER

ELEMENT	QUANTITY	INITIAL TOTAL $(000)	HARDWARE $(000)	INSTALLATION $(000)	ANNUAL UPKEEP $k(000)
Guidar (Microwave)	1 Lot	135	92	43	10
H-Field (Microwave)	16	149	114	35	22
BLID (Pressure)	16	81	52	29	3
BLS-1000 (Magnetic)	16	238	No Data	No Data	No Data

Table 9-5

LAYERING IMPACT ON SYSTEM COST

	ONE LAYER	TWO LAYER	THREE LAYER
Initial Investment	171,000	194,200	292,000
Annual O & M Cost	17,300	24,500	27,500
Annual Testing Cost	334,700	89,800	51,000
Present Value of Total Cost*	1,805,000	736,700	664,500

*6 year amortization schedule, 12 percent inflation, 20 percent interest.

Table 9-6

POTENTIAL WORKFORCE REDUCTIONS

	WORK FORCE REDUCTION (MEN)	ANNUAL SAVINGS* $(000)
CCTV Surveillance vs. Two Watch Towers	5	200
Single Shift Scheduled Maintenance For Three Layer Perimeter System	6	240
Automated Alarm Keying Logging And Reset Dispatch Only On Combined Alarms	5	200

*Assumes $40000 Per Man, Including Overhead

Section 10

REFERENCES

1. Regulatory Guide 5.44. Rev. 2, Perimeter Intrusion Alarm Systems. U.S. Nuclear Regulatory Commission, Office of Standards Development, May 1980.

2. Part 73, Title 10, Code of Federal Regulations. Physical Protection of Plants and Materials. U.S. Government Printing Office.

3. P. De Leon, B. Jenkins, K. Kellen, J. Krofcheck. Attributes of Potential Criminal Adversaries of U.S. Nuclear Programs. R-2225-SL. Santa Monica: RAND, February 1978.

4. Army Field Manual. Physical Security, FM19-30. Hq. Department of the Army. Washington, D.C., 1 March 1979.

5. Nuclear Security Systems 1700. Barrier Technology Handbook. SAND 77-077 Sandia National Laboratories, April 1978.

6. J. J. Cadwell. Reactor Facility Threat Analysis and Tactical Response Procedure. Brookhaven National Laboratory, ANS Workshop on Power Plant Security. Oakbrook, Ill, Oct 5-8, 1980.

7. Security World Magazine. Security Retrofit and Review Survey. Chicago: Cahners Publishing Co., Feb. 1981.

8. J. L. Darby, F. L. Crane. Physical Protection Technology for Nuclear Power Plants. SAND 80-1046, Sandia National Laboratories, April 1981.

9. Nuclear Security Systems 1700. Intrusion Detection Systems Handbook. SAND 76-0554, Vol. I, Vol. II. Sandia National Laboratories, July 1980.

10. NUREG/CR-0484 (MH-7814). Vehicle Access and Control Planning Document. U.S. Nuclear Regulatory Commission Office of Standards Development, Oct. 1979.

11. Regulatory Guide 5.61. Intent and Scope of the Physical Protection Upgrade Rule Requirements for Fixed Sites. U.S. Nuclear Regulatory Commission Office of Standards Development, June 1980.

12. NUREG/CR-0509 (Y/DA-7678). Emergency Power Supplies for Physical Security Systems. U.S. Nuclear Regulatory Commission Office of Standards Development, Nov. 1981.

13. NUREG/CR-0543 (MHSM-SD-7816). Central Alarm Station and Secondary Alarm Station Planning Document. U.S. Nuclear Regulatory Commission Office of Standards Development, June 1980.

14. NUREG/CR-1327 (MHSM-SD-7911). Security Lighting Planning Document for Nuclear Fixed Site Facilities. U.S. Nuclear Regulatory Commission Office of Standards Development, April 1980.

15. Criteria for Safety-Related Electric Power Systems for Nuclear Power Plants. IEEE Standard 308-1974 as endorsed by Regulatory Guide 1.32.

16. Maintenance Testing and Replacement of Large Lead Storage Batteries for Nuclear Power Plants. IEEE Standard 450-1975 as endorsed by Regulatory Guide 1.129.

17. ANSI Standard Keyboard. American National Standards Institute (ANSI) X4.14-1971.

18. Electrical Performance Standards for Monochrome Television Studio Facilities. EIA RS-170. Electronics Industries Association (EIA).

19. Interface between Data Terminal Equipment and Data Communication Equipment Employing Serial Binary Data Interchange. EIA RS-232-C. Electronics Industries Association (EIA).

20. Electrical Performance Standards for Closed Circuit Television Camera 525/60 Interlaced 2:1. EIA RS-330. Electronics Industries Association (EIA).

21. Electrical Performance Standards for Direct View Monochrome Closed Circuit Television Monitors 525/60 Interlaced 2:1. EIA RS-375-A. Electronics Industries Association (EIA).

22. Part 15 Sub. "F", Title 47-76-605, Paragraph 12. Federal Communications Commission (FCC).

23. Interim Federal Specification GSA-FSS W-A-00450B.

24. Class 1, Class 2 and Class 3 Remote-Control, Signaling, and Power-limited Circuits. Article 725. National Electrical Code (NEC) NFPA #70-1981.

25. National Electric Manufacturers Association (NEMA).

26. Grounding Methods for Electrical Supply and Communication Facilities. Section 9. National Electrical Safety Code (ANSI-C2), 1981.

27. Underwriter's Laboratory, Inc. UL-198 Fuses, UL-512 Fuse-holders, UL-796V Printed Circuit Boards.

28. Regulatory Guide 5.12. General Use of Locks in the Protection and Control of Facilities and Special Nuclear Materials. U.S. Nuclear Regulatory Commission Office of Standard Development.

APPENDIX A
CCTV AND VMD IN NUCLEAR PLANT SECURITY

APPENDIX A

CONTENTS

APPENDIX A
CCTV AND VMD IN NUCLEAR PLANT SECURITY

A perimeter security system can be augmented by the addition of closed circuit television (CCTV). This section discusses requirements for CCTV systems and various Video Motion Detection (VMD) systems in perimeter security applications for alarm assessment and for intrusion detection. The first section below lists requirements for a CCTV system covering perimeters up to a 1-mile square. A baseline system is established from these requirements. The second section addresses VMD for intrusion detection in a perimeter security system. Later sections deal with the addition of VMD to existing CCTV systems and to other types of intrusion detectors.

A.1 CCTV SYSTEMS

Complete coverage of the secure area's perimeter and adequate resolution for the eye to detect human or larger-sized intruders are requirements placed on a CCTV system for perimeter security. These requirements are used to specify TV camera parameters required for coverage of the perimeter.

A.1.1 TV CAMERA SELECTION

Selection of a TV camera should be based on features of available TV cameras corresponding to application needs. Such considerations are listed below:

- Availability of low-light level (LLL) vidicons.
- Availability/Interchangeability of different types of lenses, including auto-iris lenses.
- Compatibility with other equipment to be used.
- External sync. (EIA RS-170 or compatible sync. interface).

- Ruggedness, reliability and repairability.
- Performance: Light level sensitivity and resolution.
- Low initial cost and maintenance.

Types of imaging detectors used for closed circuit television (CCTV) cameras include:

- Conventional Vidicons
- Silicon Vidicons
- Intensified Vidicons
- Charge Coupled Devices

These types of imaging detectors are shown in Table A-1 with their characteristics listed below. For exterior CCTV systems where artificial lighting can be employed, the silicon-vidicon camera type is preferred. Silicon vidicons have moderately high resolution; high resistance to burn in from viewing bright scene areas; a long Mean Time To Failure (MTTF); a relatively high signal-to-noise ratio (S/N); adequate light sensitivity and dynamic range for artifically lit exteriors; and low cost in terms of initial purchase and maintenance.

Several different manufacturers have silicon vidicon cameras which are particularly suited for exterior perimeter CCTV use. For the purpose of this report, we consider the use of the RCA TC-2000® series cameras. They are compact, lightweight, have reasonably high resolution and are available with many accessories. The TC-2000® cameras also cost much less than most other CCTV camera types.

Other cameras which are recommended if increased TV camera resolution is necessary are the RCA TC-1005 series, the COHU 2850C, Dage RGS-60 and similar 1" silicon vidicon cameras. Whereas a typical 2/3" silicon will give about 300-400 TV lines per picture height horizontal resolution, the 1" silicon vidicons will give a horizontal resolution of about 500 to 700 lines.

Table A-1

CCTV CAMERA TYPE COMPARISON SHOWING TYPICAL VALUES

Type of Camera / Characteristic	Conventional Vidicons	Silicon Vidicons (or Newvicon or Ultricon)	Intensified Vidicons (Typical ISIT)	Charge-Coupled Devices ("Solid State" Camera)
Resolution TV Lines Picture Height	TVL 800 PH	TVL 600 PH	TVL 500 PH	TVL 200 PH
Resistance to Burn in	Poor	Good	Poor	Good
MTBF	10,000 hr.	15,000 hr.	6,000 hr.	20,000 hr.
Signal to Noise Ratio (S/N)	44 dB	43 dB	10-42 dB	48 dB
Light Sensitivity (Min. Illumination Level)	2 fc.	0.5 fc.	8×10^{-5} fc.	2 fc.
Light Level Dynamic Range	10^4	10^6	10^9	10^4
Initial Purchase Price	$800	$1300	$8000	$3500
Average Annual Owning Cost for 5 Years	$1,200	$1,650	$12,000	$2,000

Camera enclosures are necessary for any exterior TV camera usage. Requirements for the camera enclosures include:

- Protection from dust and foreign material.
- Protection against humidity and water.
- Preservation of TV camera temperature range.
- Prevention of obscuration of line of sight for TV camera.

Additional requirements (e.g. aerodynamic considerations) may further constrain TV camera enclosure selection.

A.1.2 LIGHT LEVEL - F/# REQUIREMENTS

Lighting requirements for a CCTV system are calculated from the minimum faceplate illumination level for the vidicon used, lens F/number, and scene reflectance values as shown in Eq. A-1.:

$$L_s = \frac{4L_f(F/\#)^2}{r\,\tau} \qquad \text{(A-1)}$$

where L_s = Scene minimum illumination,
L_f = Minimum full video faceplate illumination level,
F/# = TV camera lens F/number,
r = Scene reflectance, and
τ = Lens transmission.

Another equation useful in CCTV system design is used when the minimum scene light level is fixed and the lens F/Number must be selected:

$$F/\# = \frac{1}{2}\sqrt{\frac{\tau\, r L_s}{L_f}} \qquad \text{(A-2)}$$

where F/# = Maximum TV camera lens F/# and
L_s = Existing minimum scene illumination.

As a sample calculation, a silicon vidicon-type TV camera (say an RCA TC-2011/u) having a minimum faceplate illumination requirement of 0.006 foot candles, an F/1.4 lens with a transmittance of 0.6, and whose typically viewed scene has a reflectance of 0.75 (reflectance of snow) will require a scene illumination level of:

$$L_S = \frac{4\ (0.006)\ (1.4)^2}{(0.75)\ (0.6)} \qquad fc = 0.105 \text{ footcandles}$$

This can be compared to the NRC lighting requirement for nuclear power plant peripheries, 0.2 footcandles. Table A-2 below shows typical scenes and their reflectivities:

Table A-2
TYPICAL GROUND COVER SCENES AND THEIR REFLECTIVITIES

Scene (Ground Cover)	Reflectivity
Plowed field	0.1-0.15
Sand	0.5
Grassy field	0.3-0.4
Gravel	0.5
Caliche	0.6
Compacted earth	0.3
Asphalt	0.1
Snow	0.75

Given TV camera types, measured illumination levels or lens F/No. availability, Eq. A-1 and A-2 can be used to specify requirements for satisfactory CCTV operation.

A.1.3 CAMERA COVERAGE AND NUMBER OF CAMERAS REQUIRED

Perimeter coverage per TV camera is calculated from projecting 2 cycles (1) of system resolution across an intruder's minimum dimension (body width) at the maximum range from the camera. This figure, 2.0 cycles, is the number of cycles needed to insure a probability of detection (P_D) nearly equal to 1. The maximum range of the camera (based on vertical resolution) is:

$$D_{max} = \frac{D_m\ F(_2\ (0.7\ (\text{Kell factor})))}{(2 \text{ cycles})\ S_V} \qquad (A\text{-}3)$$

where D_{max} = The maximum range in feet the camera will detect an object having a minimum dimension D_m with probability almost 1.

D_m = Minimum dimension in feet presented by an object to the TV camera.

F = TV camera focal length in mm.

ℓ = Number of TV scan lines vertically, (here ℓ = 525).

Kell factor = A factor (usually 0.7) included to normalize scanned scene's resolution to that of continuous scenes (2). (A factor of 2 is included due to Nyquist sampling.)

2 cycles = Used since 2 cycles or line pairs subtended by an object gives a probability of detection of 1 for the CCTV system.

S_v = The vidicon vertical format dimension in mm (for a 2/3" vidicon, S_v = 6.4 mm).

The vertical field of view of the TV camera is found by the relation:

$$\theta = 2 \tan^{-1} \left(\frac{S_v}{2F}\right) \qquad \text{(A-4)}$$

where θ = TV camera vertical field of view.

S_v = Vertical format division of vidicon (6.4mm for a 2/3 inch vidicon).

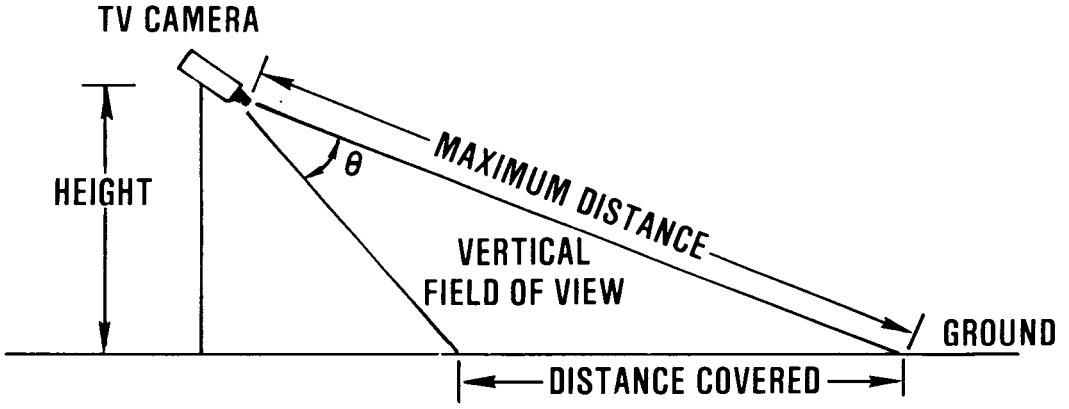
The length of the camera coverage can then be determined by this maximum range, the camera height, and the field-of-view of the camera as shown below:

$$D_{cov} = \sqrt{D^2_{max} - h^2} - h \tan \left(90^o - \sin^{-1} \left(\frac{h}{D_{max}}\right) - \theta\right) \qquad \text{(A-5)}$$

where D_{cov} = Coverage range in feet as shown in Figure A-1.

θ = TV camera vertical field of view.

h = TV camera height above terrain



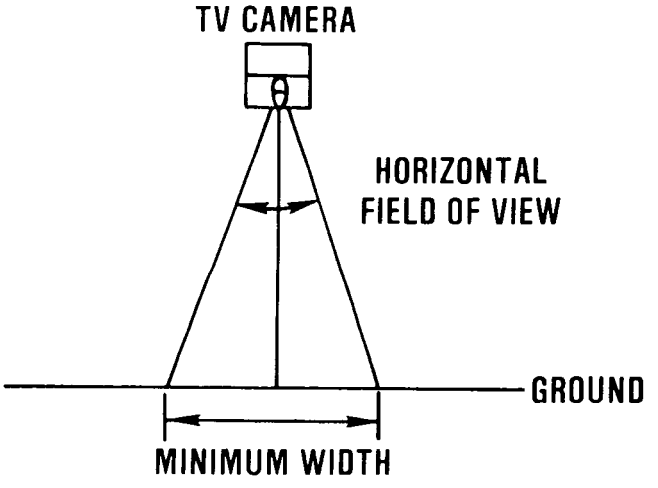


Figure A-1. Dimensions For Coverage Distance

Width covered by the TV camera field of view is calculated here to show whether the perimeter zone is adequately covered. The minimum width coverage will occur where the bottom of the TV camera's field of view intersects the ground. This minimum width should be wider than the perimeter zone, which at most plants is 20 feet. Thus:

$$W_{min} \geq 20 \text{ feet} \qquad \text{(A-6)}$$

where W_{min} = The minimum ground width coverage by the TV camera.

The range at which the bottom of the TV camera's field of view intersects the ground is:

$$D_{min} = h\sqrt{1 + \tan\left(90° - \sin^{-1}\left(\frac{h}{D_{max}}\right) - \theta\right)^2} \qquad \text{(A-7)}$$

where D_{min} = The closest range from the TV camera to where the TV camera field-of-view intersects the ground.

The minimum ground coverage is then:

$$W_{min} = D_{min}\ \frac{S_h}{F} \qquad \text{(A-8)}$$

where S_h = the vidicon horizontal format dimension (for 2/3 inch vidicon S_h = 8.5333...mm).

If W min fails to satisfy inequality (A-6), the field-of-view of each camera will be inadequate to fully cover the perimeter zone. Thus, either the height of the TV camera or the TV camera lens's focal length would need adjustment to assure full coverage.

The total number of TV cameras needed can be estimated from the length of coverage for each camera and the total length of the perimeter to be covered:

$$N = \frac{D_{peri}}{D_{cov}} \qquad \text{(A-9)}$$

where N = Number of TV cameras

D_{peri} = Total length of perimeter in feet.

Figure A-2 depicts the relationship between TV camera focal length and estimated number of TV cameras required for coverage of perimeters from 1 mi. (1600m) to 4 mi. (6400m).

A.1.4 MONITOR SIZE REQUIREMENT

Selection of an adequate-sized monitor is based on the size of an intruder's image on the CCTV monitor screen. A human's minimum dimension at maximum range from the TV camera should subtend a minimum of 4 to 7 1/2 arc-minutes in the viewer's eye when viewed on the monitor from the normal operator's eye position (1, 2). If we assume an eye-to-monitor screen distance of 30 inches, an image subtense of 7 1/2 arc-minutes would correspond to a height of 0.6545 inches. Using the TV camera resolution requirement definition of minimum resolvable distance at a maximum range, the image height compared to the vertical field height (VFH) is:

$$VFH\left\{\frac{2 \text{ cycles}\left(\frac{\text{lp}}{2 \text{ scan lines}}\right)}{525 \text{ scan lines (0.7 Kell Factor)}}\right\} = \text{Image height} \qquad \text{(A-10)}$$

$$\frac{VFH}{91.875} = \text{Image height}$$

thus from image height = 0.6545 inches, VFH = 6.01 inches.

From the ratio of vertical field height to horizontal field width (HFW).

$$\frac{VFH}{HFW} = \frac{3}{4} \qquad \text{(A-11)}$$

or diagonal size of screen, DS = 8.02 inches.

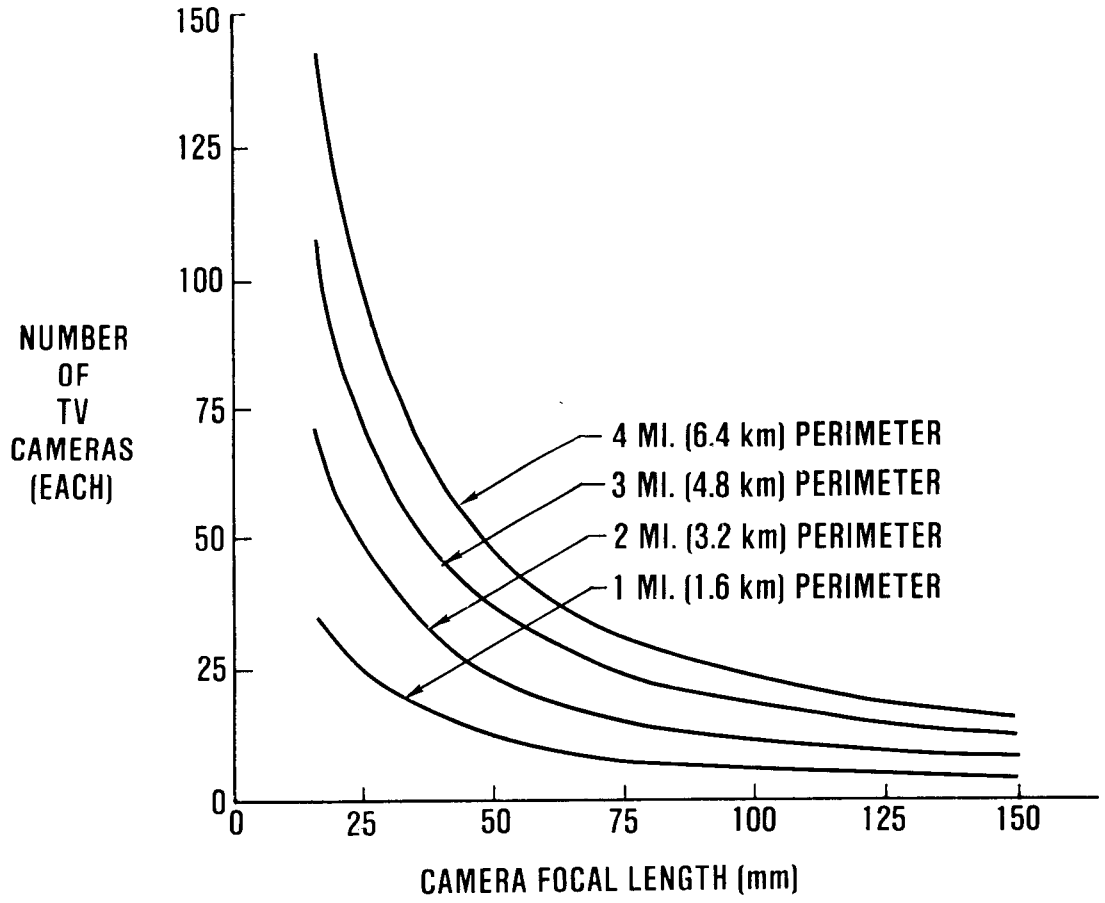


Figure A-2. Relationship Between TV Camera Focal Length and Estimated Number of TV Cameras Required for Coverage of Perimeters From 1 mi. (1600m) to 4 mi. (6400m)

The TV monitor diagonal size for this application should be a minimum of 10 inches. It would be advantageous to use a 12 inch diagonal monitor to allow viewing by persons with subnormal vision and viewing from longer than normal operating distances.

A.1.5 VIDEO SIGNAL TRANSMISSION

Due to the requirement to transmit a number of video signals with bandwidths of 5-6 MHz to a centrally located security center over distances up to 2 miles, consideration needs to be given to the means by which these video signals are transmitted. Four approaches and two generic types of cable are dealt with below. The approaches considered are:

1. Baseband video
2. Radio Frequency (RF) carrier channelized video
3. Digitally coded video
4. "Cable-less" optical video

and the types of cable considered are:

1. Electrical coax
2. Fiber Optic Cable

Several approaches and cable types are discussed following:

A.1.5.1 Baseband Video Over Electrical Coax

The simplest approach to video signal transmission is to transmit the video over a conventional electrical coaxial cable. This is most effective for short distances up to 50-100 feet. For transmission distances greater than 100 feet, frequency response equalization and amplification may become necessary. Distances of up to 1-2 miles (1.6-3.2 km) can be covered in this manner. One disadvantage of baseband video transmission is that each video channel requires a dedicated cable. Thus, expenses for cabling rise proportionally with the number of video channels. Figure A-3 shows a block diagram of a medium-distance baseband video transmission system.

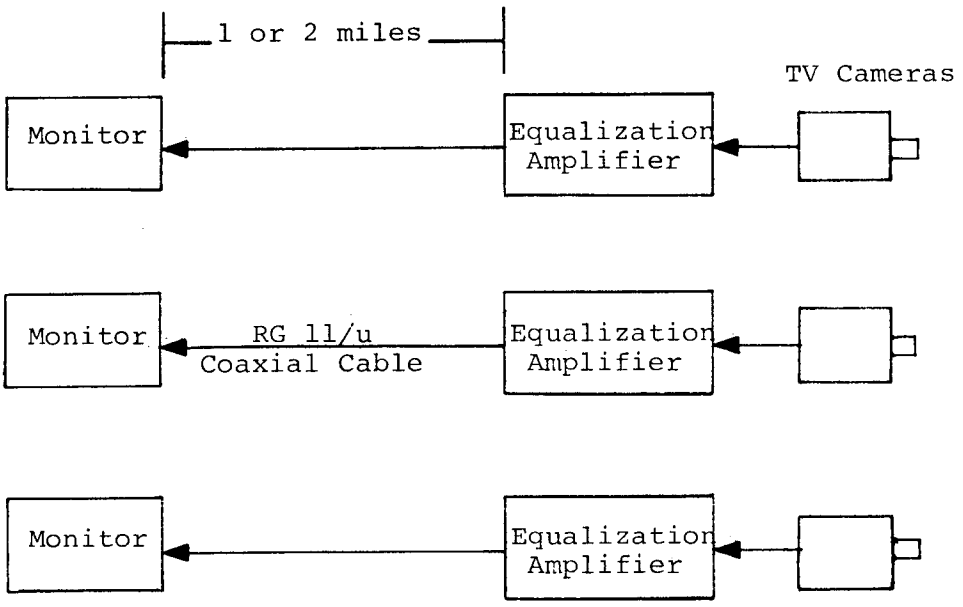


Figure A-3. Medium Distance Baseband Video Transmission System

Table A-3 shows parts costs of a 24-channel baseband video transmission system for a 3 mile perimeter.

Table A-3
PARTS COSTS OF A 24-CHANNEL BASEBAND VIDEO TRANSMISSION SYSTEM FOR A 3 MILE PERIMETER

Item	Unit Cost	Quantity	Number	Total Cost
Equalization Amplifier	$119.00	---	24	$2856.00
RG 11/u Coaxial Cable	$0.25/ft	105,600 ft	--	$26,400.00
			Total Cost	$29,256.00

The baseband video transmission system may suffer from ground-loop problems, induced EMI and lack of electrical isolation.

However, through careful routing of signal lines, The use of coaxial or triaxial cable, line amplifiers and noise-bucking isolation transformers, most of these problems can be overcome. Most CCTV systems currently in use have baseband video distribution systems, due to the familiarity, low cost and mature technology of the baseband video transmission approach.

Baseband video transmission is recommended for most CCTV applications in power plant perimeter security because of its low cost and its small number of active devices relative to other transmission approaches.

A.1.5.2 RF Carrier (Channelized) Video Transmission Systems

Since the electrical noise environment in power plants is worse (mostly at 60 Hz) at low frequencies, a video signal on a radio frequency (RF) carrier would be less affected by this noise. Also, frequency response equalization is usually unnecessary and several RF carriers can be placed on each coaxial cable, allowing several channels of video to be transmitted. Figure A-4 shows a block diagram of a channelized RF carrier video transmission system.

Table A-4 shows parts costs for 24-channel RF carrier video transmission system for a 3 mile perimeter.

Notice in Figure A-4 that instead of video monitors, television receivers are utilized. If conventional TV receivers are used, the cost differential between receivers and monitors will be slight; on the order of roughly $50.00. If video motion detectors (VMD) are to be used, outboard demodulators will be required. The cost of a typical CATV multi-channel demodulator is $650.00. Each demodulator is placed with its output feeding both the video motion detector input and the monitor console input. The input to each of the demodulators is an RF split-off from the CATV cable.

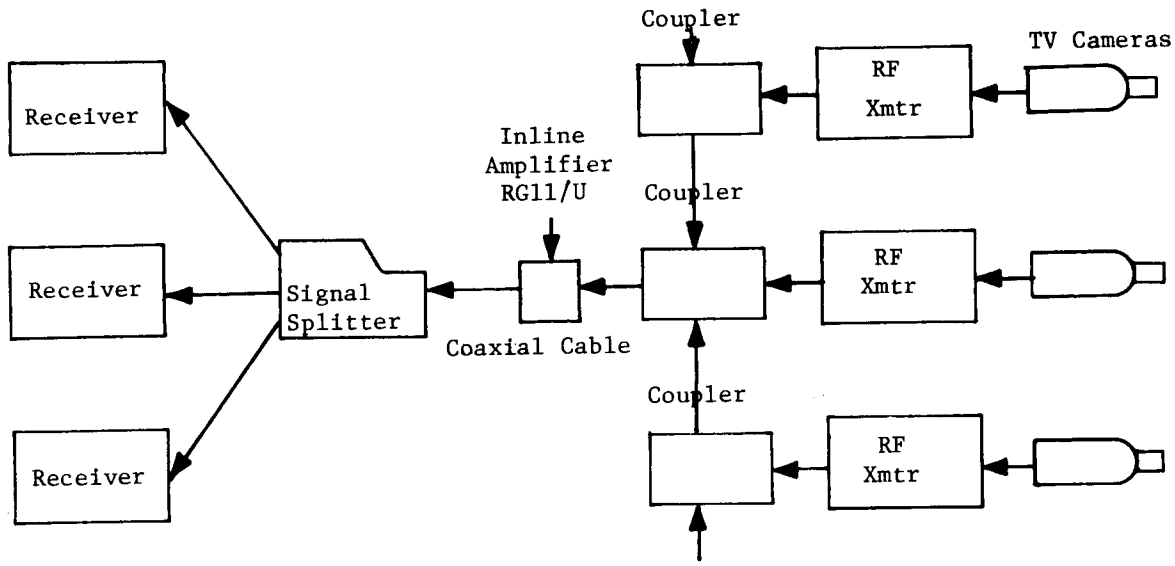


Figure A-4. RF Carrier Video Transmission System

Table A-4.a

CATV VIDEO TRANSMISSION SYSTEM PARTS COSTS

ITEM	QUANTITY	NUMBER	UNIT COST	TOTAL COST
RG 11/u Coax	31,680 ft		$ 0.25/foot	$ 7,920
CATV Modulator		24	$1500	$36,000
CATV Amplifier		16	$1000	$16,000
CATV Amp Power Supply		16	$ 360	$ 5,760
Cost Differential Between Receiver and Monitor		6	$ 50	$ 300
			TOTAL COST	$65,980

Table A-4.b

CATV VIDEO TRANSMISSION SYSTEM FOR VMD PARTS COST

ITEM	QUANTITY/NUMBER	UNIT COST	TOTAL COST
RG 11/u Coax	31,680 feet	$0.25/foot	$ 7,920
CATV Modulator	24	$1,500	$ 36,000
CATV Amplifier	16	$1,000	$ 16,000
CATV Amp Power Supply	16	$ 360	$ 5,760
CATV Demodulator	24	$ 650	$ 15,600
External Sync Coax Line	42,240 feet	$ 0.25/foot	$ 10,560
		TOTAL COST	$ 91,840

Distances that can be covered by the RF carrier video transmission system can be extended to several miles by using inline amplifiers. Limiting factors on RF carrier system distances arise from induced noise on the cable and amplifier noise.

The RF carrier video transmission system is an alternative to the baseband video transmission system for high EMI situations, longer transmission distances than several hundred feet, and for multi-camera applications.

A.1.5.3 Baseband Video on Fiber Optic Cable

Fiber optic cable can be used to overcome the EMI susceptibility of the baseband video on coax cable. Fiber optic cable is totally resistant to all forms of EMI, can be made totally non-conductive and has inherently wide bandwidth. Fiber optic cable is now available which has comparable ruggedness to electrical coaxial cable.

Also, the cost of telecommunications grade fiber optic cable is becoming comparable to the cost of electrical coax.

Analog baseband video transmission on fiber optic cable is possible with relatively good signal-to-noise (S/N) ratios, but like baseband

video on coax cables, it requires a dedicated cable for each video channel. Thus, baseband video transmission on fiber optic cables is most suited to CCTV systems with few TV cameras. A block diagram of a baseband video fiber optic transmission system is shown in Figure A-5.

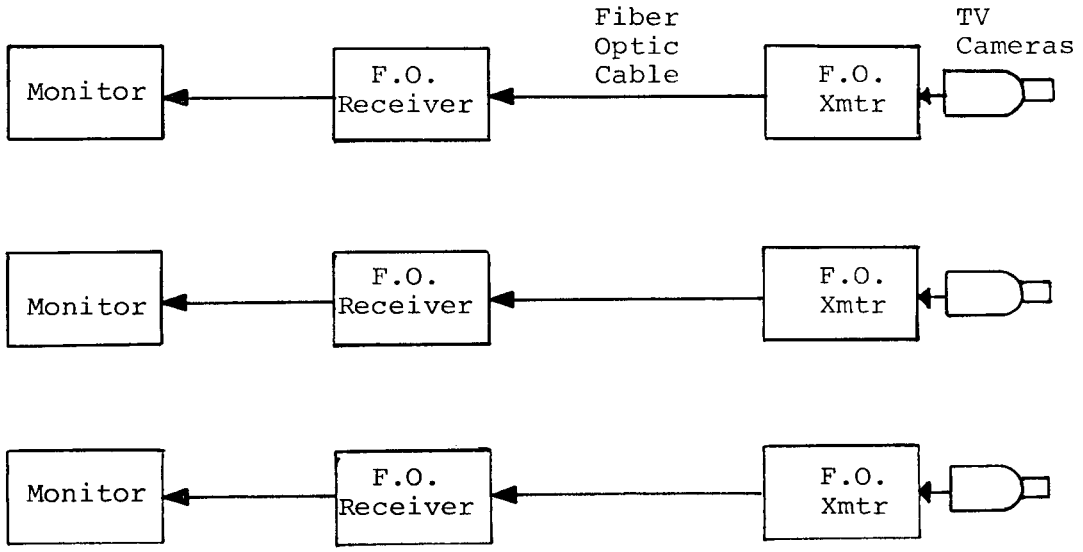


Figure A-5. A Baseband Video Fiber Optic Transmission System

In the similar manner to the RF carrier video transmission system, the transmission distance of the fiber optic system can be increased by inline repeaters which receive and retransmit optical signals. The transmission distance is then limited by the nonlinearities and receiver noise level which can be tolerated by the CCTV system. Like the baseband video on coax, however, the baseband video fiber optic system cost increases linearly with the number of channels in the CCTV system.

A.1.5.4 Digitally Coded Video on Fiber Optical Cable

To allow multiple channels on each fiber optical cable, to improve linearity and to decrease CCTV system sensitivity to noise, video

Table A-5

PARTS COST OF BASEBAND VIDEO FIBER OPTIC TRANSMISSION SYSTEM

ITEM	QUANTITY	NUMBER	UNIT COST	TOTAL COST
Fiber Optic Cable	32 kM		$ 1.30/m	$41,600
Fiber Optic Xmtr		24	494.00	11,856
Fiber Optic Rcvr		24	380.00	9,120
Fiber Optic Rcvr Power Supply		4	750.00	3,000
Assorted Connectors		100	62.50	6,250
Inline Receptacles		50	25.00	1,250
External Sync Coax	42.240 ft		0.25 ft	$10,560
			TOTAL COST	$83,636

signals can be digitally encoded prior to transmission. Presently available digital fiber optic links are limited to 150 Mbit/sec data rates; and a video signal having sufficient resolution and gray-scale quantization for security purposes, requires around 50 Mbit/sec. Thus, about 3 channels can be transmitted over each fiber optic cable.

Figure A-6 depicts a digital video fiber optic transmission system. Video signals from the TV cameras are first digitized and transmitted via fiber optic cable to a nearby multiplexer which encodes all its video inputs into a data stream. This multiplexed data stream is then transmitted via fiber optic cable to the security facility where the data is demultiplexed and converted back to video signals which are then viewed on the monitors. Table A-6 shows the cost of the digital video fiber optic transmission system.

The digital video fiber optic system would be very EMI-resistant, free from nonlinearities and capable of spanning almost unlimited distances by using in-line repeaters. Due to their high cost, multiplexed digital fiber optic video links are not recommended for this application. For a large number to TV cameras and extremely long coverage distances, the multiplexed digital video fiber optic system could attain a lower cost than the baseband video fiber optic system. However, for smaller

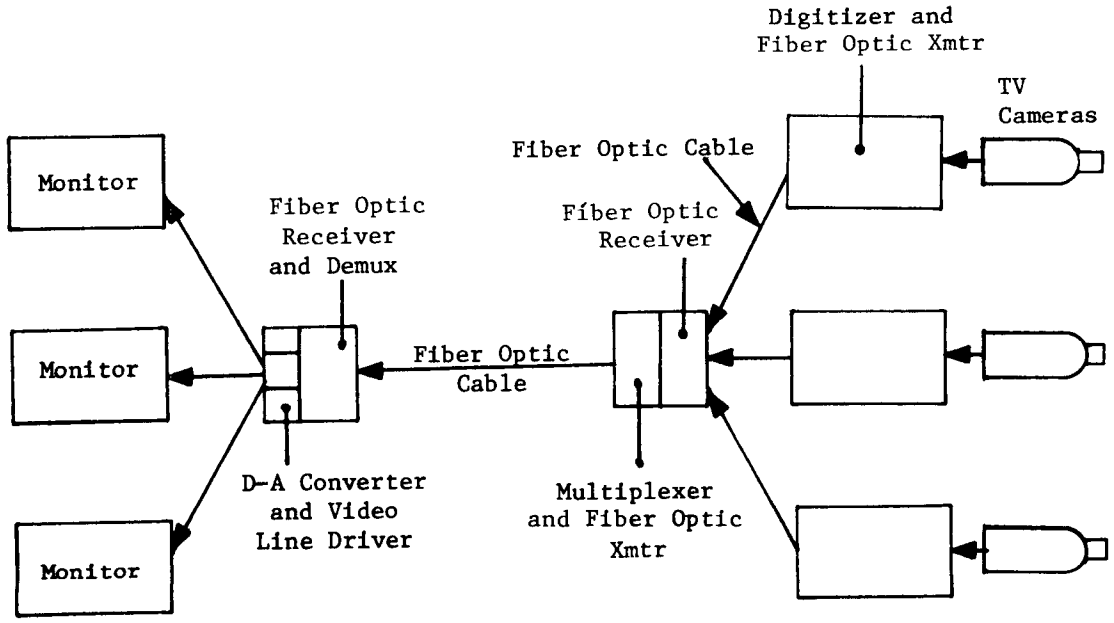


Figure A-6. A Digital Video Fiber Optic Transmission System

Table A-6

PARTS COST OF MULTIPLEXED DIGITAL VIDEO

FIBER OPTIC TRANSMISSION SYSTEM

ITEM	QUANTITY	NUMBER	UNIT COST	TOTAL COST
F.O. Cable	16 KM	24	$ 1.30/M	$ 20,800
50 MBit/sec FO Xmtr		24	1200	28,800
50 MBit/sec FO Rcvr		8	600	4,800
150 MBit/sec FO Xmtr		8	1750	14,000
150 MBit/sec FO Rcvr		8	850	6,800
8 ESY designed & built		8	4000	32,000
3-1 SP and Demux		Development	60,000	60,000
connectors, etc.				
External Sync Coax	42,240		$ 0.25/ft	$ 10,560
Line				
			TOTAL COST	$185,260

systems, a non-multiplexed fiber optic link would have lower costs as shown in Table A-7.

Table A-7
PARTS COST OF NON-MULTIPLEXED DIGITAL VIDEO FIBER OPTIC TRANSMISSION SYSTEM

ITEM	QUANTITY	NUMBER	UNIT COST	TOTAL COST
F.O. Cable	32 KM		$130/M	$41,600
50 MBit/Sec F.O. Xmtr		24	1200	28,800
50 MBit/Sec F.O. Rcvr		24	600	4,800
Connectors, etc.				14,400
External Sync Coax Line	42,240 ft		0.25/ft.	$10,560
			TOTAL COST	$102,860

The non-multiplexed digital F.O. approach would have a slightly greater cost than the analog F.O. approach but could feasibly be extended to greater distances than the analog system.

A.1.5.5 Optical Video Link

To eliminate the need for cables, video signals can be carried by an optical beam. Optical video links have become available which operate in the near-infrared spectrum and are designed for video transmission. Optical video links do not require FCC licensing, but may require safety approval as an eye hazard because of their near-infrared radiation. Figure A-7 shows the block diagram of an optical video link.

Typical optical video links have a maximum transmission distance of 2000 ft. in clear weather, which would make necessary the use of an additional transmitter-receiver pair as a repeater for each TV camera. Also, all transmission is strictly line of sight. The number of repeaters is limited to four in any one channel, as signal degradation becomes intolerable because of poor frequency response equalization,

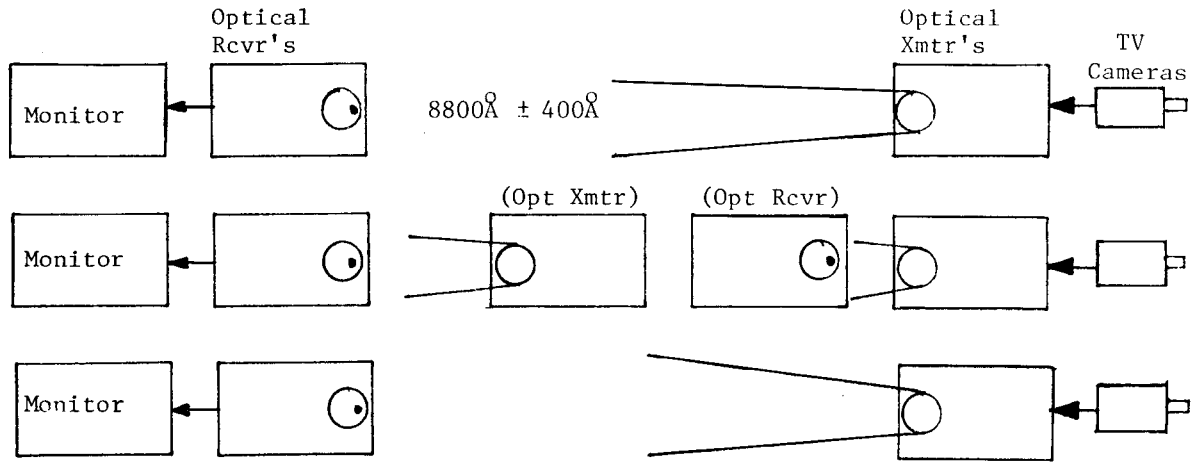


Figure A-7. Optical Video Links

noise and non-linearities. Inclement weather reduces feasible optical link distances to shorter distances (e.g. link range in heavy fog = 450 feet). However, since exterior TV cameras are ineffective in inclement weather, link distance for clear weather is the most applicable to outdoor CCTV and VMD systems. Table A-8 shows costs for an optical video link.

The expense of this optical video link approach could be much reduced if greater distances could be spanned between transmitter and receiver. To accomplish this, a higher transmitter power level is required. However, increased infrared radiant power might be hazardous from an eye safety viewpoint. The cost of optical links may be reduced from the amount listed in Table A-8 if the links were ordered in the quantities needed for this application. However, unless prices are reduced, optical links are not recommended due to high cost.

A.1.6 CONCLUSIONS

For typical power plant CCTV applications, we recommend baseband video transmission using coaxial or triaxial cables, due to the low cost and minimum number of active devices inherent in this appproach.

Table A-8
COSTS FOR AN OPTICAL VIDEO LINK

ITEM	QUANTITY/ NUMBER	UNIT COST	TOTAL COST
Optical Link Xmtr	48	$1950	$ 93,600
Optical Link Rcvr	48	$1950	$ 93,600
External Sync Coax Line	$42,240 ft.	$0.25/ft.	$ 10,560
		TOTAL COST	$197,760

Techniques for reducing induced noise are well known among CCTV system engineers and are very effective in high-EMI environments such as generating stations. A few situations could arise in which the alternative approaches listed above may be less expensive and more reliable alternatives to video transmission than baseband video transmission. However, most CCTV systems currently operating in generating stations use baseband video transmission with few problems.

A.1.7 PERIMETER LIGHTING EQUIPMENT OPTIONS

As discussed in the Light Level - F/# Requirements section previously, a certain ambient light level must be present to assure proper CCTV system operation. When natural light levels fall below that minimum illumination level, artificial lighting must be employed to maintain perimeter illumination levels of at least 2 footcandles assuming a luminance of 0.7 footlamberts against a compacted earth background.

A.1.7.1 Lamp Types

Several different types of lamps are presented in Table A-9 with their characteristics.

From Table A-9 it is seen that the sodium vapor lamps are preferable to the other lamp types in terms of luminous efficacy. Whereas high

Table A-9

LAMP TYPES AND CHARACTERISTICS

Characteristic	Incandescent	Hg Vapor	Metal Halide	High Pressure Na	Low Pressure Na
Luminous Efficacy lm/watt	12-23	40-65	80-100	95-130	131-183
Spectral Distribution	Broad with maximum in infrared	Blue - Green	Broad Visible	Orange - Yellow	Yellow
Restrike Time	Immediate	3-6 Min.	10-20 Min.	$\leq$ 2 Min.	Immediate to 2 Min.
Time from Strike to Full Output	Immediate	3-7 Min.	3-5 Min.	3-4 Min.	8-15 Min. Initial 5 min. Restrike
Lamp Life (wattage)	750 H. Conv. (100W) 2000H. I/Sio2	24000 H. 100 W.	15000 H 400 W.	20000 H 400 W.	18000 H. 180 W.
Supply Range Voltage	5-5000 V.	175-3000 V.	175-1500 V.	50-1000 V.	35-180 V.

Source: SAND80-1046 Report

pressure sodium is somewhat more similar to existing mercury-vapor lamps and has superior time to full output when compared to low pressure sodium, the low pressure sodium generally has a high (75%-95%) probability of immediate restrike from power interruption and has greater luminous efficacy. In this section, high pressure sodium and low pressure sodium lamps will be considered as candidate lighting systems.

Incandescent lighting is being recommended for perimeter lighting by one of the video motion detection (VMD) processor manufacturers. They point out that, for equal visual lighting levels, incandescent

lighting provides much more near-infrared scene radiance at wavelengths near the peak response of silicon-vidicon TV cameras.

It still remains a matter of discussion whether the incandescent lighting is more efficacious than sodium vapor lighting in terms of TV camera response versus lighting power input.

A.1.7.2 Light Levels and Distribution

Light levels and their spatial distributions are determined by several factors:

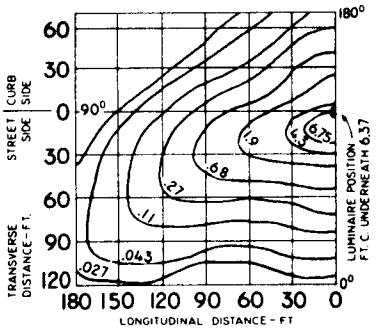
- Lamp type
- Lamp wattage
- Luminaire type
- Lamp spacing
- Lamp height
- Light depreciation factors

Parameters addressed for light levels and their distribution are:

- Minimum light level
- Uniformity (maximum-to-minimum light level ratio)
- Installation costs
- Life cycle costs and power consumption costs
- Peculiar lamp characteristics

Lighting systems can be designed by using the luminaire iso-footcandle graphs shown in manufacturer's data sheets. As an example, Figure A-8 shows an iso-footcandle graph for a General Electric M-400A Luminaire. Iso-footcandle graphs are shown as maps of footcandle (or lux) levels measured with a detector at a height of 6 inches viewing a hemisphere whose center is directly over the detector. For these measurements, the luminaire is set at a specified height; and distance from the luminaire is given in units of the luminaire mounting height. For applications where the luminaire is mounted at other than the specified height, a height factor is given (usually it is the square of the ratio

of the specified height to the actual height). This height factor is multiplied by the graph's footcandle (or lux) values to give the actual light level values of the distribution for the other-than-specified mounting height. A lamp light depreciation factor for worst case life-cycle illumination is also sometimes specified. If it is not specified, values must be assumed (Ref: 12 IES Handbook).



Curve Reference: 35-174486
Luminaire: M-400A
Distribution: M-S-III
Lamp: 400-watt Lucalox
Luminaire height: 30 feet

Figure A-8. Iso-footcandle Graph for GE M-400A Luminaire

The high pressure sodium vapor lighting system is considerably less expensive to install than the low pressure sodium vapor lighting system. This is mainly due to two factors; the higher cost of low pressure sodium components relative to high pressure sodium components, and the fact that the roadway luminaire used for the high pressure sodium lamp is better suited for lighting the narrow perimeter area than the floodlight luminaire of the low pressure sodium.

To estimate quantities of lamps for a perimeter, a map of a section of the perimeter is compared with the luminaire's spatial light distribution. The footcandle (or lux) values are multiplied by the proposed height factor and the lamp light depreciation factor to give realistic worst-case lighting information. Lighting patterns from several lamps are superimposed and light levels are calculated from the sum of the light patterns of the individual lamps. Lamp locations are arranged and superimposed using as many lighting patterns as necessary to meet

the average, minimum, and maximum light levels and uniformity criteria. Other criteria peculiar to the installation regarding lamp placement must also be carefully observed. Algorithms have been written which compute lamp quantities and placements from required light levels within an area, using luminaire iso-footcandle graph information. Quantities and placement of lamps can also be determined graphically in simple systems such as those presented in Figures A-9 and A-10.

Placement of luminaires in actual lighting systems require careful consideration of factors such as perimeter terrain, avoiding immediate proximity between luminaires and TV cameras, and avoiding placement of luminaires in TV camera fields of view.

The following paragraphs discuss several different systems for use in lighting secure area peripheries for CCTV and Video Motion Detector applications.

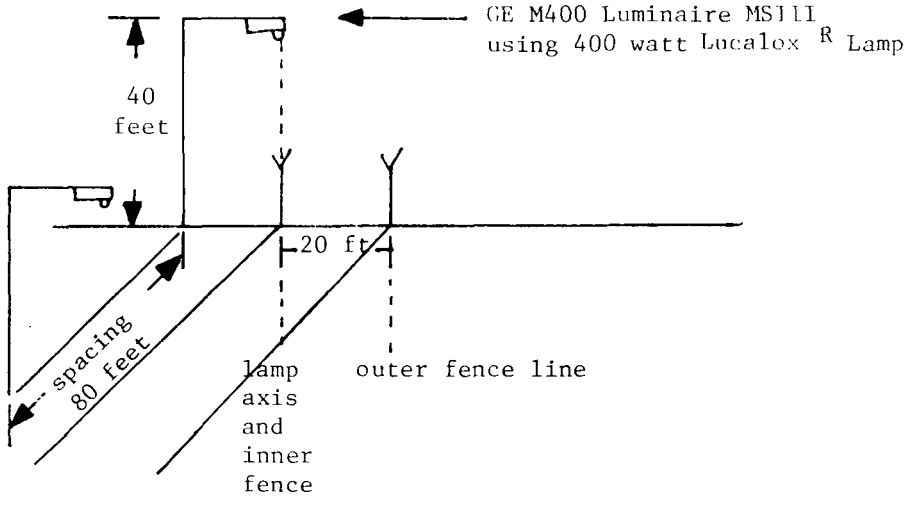


Figure A-9. High Pressure Sodium Vapor Lighting System For 20 Foot-Wide Strip

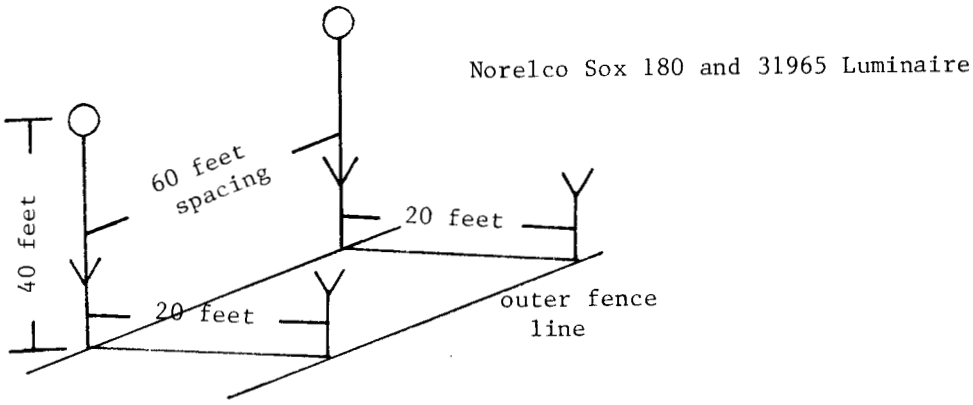


Figure A-10. Low Pressure Sodium Vapor Lighting System For 20 Foot-Wide Strip

A.1.7.3 Low and High Pressure Sodium Vapor Lighting Systems

If it is desired to light only a twenty foot wide zone to a minimum level of about 2.0 foot candles with a uniformity ration of 2:1 $\frac{\text{maximum}}{\text{minimum}}$, the arrangement in Figures A-9 or A-10 can be used.

In spite of its higher installation costs, low pressure sodium has slightly lower operating costs, due to the greater luminous efficacy of the low pressure sodium lamps relative to the high pressure sodium lamps. Two considerations may make low pressure sodium lighting preferable to high pressure sodium lighting. First, if a broad area is to be lit to a high illumination level as discussed below, floodlight illumination patterns no longer suffer a disadvantage relative to roadway lighting as in the examples above. Second, if energy costs rise excessively above the present day rates (which is likely) the operating cost of the lighting system would rise in importance as a basis for determining the type of lighting system to be installed.

NUREG/CR1327 specifies a 60 foot-wide strip as an isolation zone requiring at least 0.2 foot candles (2.15 lux) with maximum to minimum light ratios not to exceed 8 to 1. To accommodate reliable, readily available LLLTV camera tubes, it may be preferable to light this entire zone to a level of 2 footcandles with maximum to minimum light ratios not to exceed 4 to 1, to allow video assessment in the entire isolation zone as well as the immediate 20 foot-wide zone mentioned above. This would also reduce the possibility of disability glare resulting from uneven light distribution on the 60 foot-wide isolation zone.

Figure A-11 shows a high-pressure sodium vapor lighting system using roadway luminaires to light the 60 foot-wide isolation zone. The minimum light level in the isolation zone is 2.0 foot candles (21.5 lux), and the uniformity ratio (maximum to minimum illumination ratio) is 1.95.

Figure A-12 shows a similar lighting system using low-pressure sodium lamps.

Light levels are calculated for these arrangements shown in Figures A-11 and A-12, taking into account degradation from decreases in lamp lumen output and luminaire transmission.

A.1.7.4 Lighting System Costs

Costs of lighting the perimeter are separated into two categories, initial cost and operating cost. The initial cost calculated here is the cost (we exclude labor costs) of the components needed to construct the lighting system. The operating cost (again excluding labor cost) is the sum of the power consumption cost and re-lamping cost on an annual basis. The initial cost is:

$$C_i = \left[(P + W) + M\,(L + B)\right]\ (N)\ (D) \qquad \text{(A-12)}$$

where C_i = Initial lighting system cost
P = Pole cost

M = Number of luminaires per pole
L = Luminaire cost
B = Bulb cost
W = wiring cost (to pole)

N = Number of light standards per mile
D = Perimeter length in miles

and the operating cost is

$$C_O = \left\{ \frac{W_L \; H \; C_P}{1000} + \frac{HB}{L_L} \right\} (M) \; (N) \; (D) \qquad \text{(A-13)}$$

where C_O = lighting system cost per year
W_L = lamp wattage
H = number of hours per year operation
C_P = cost of electrical energy per kilowatt hour
L_L = bulb life

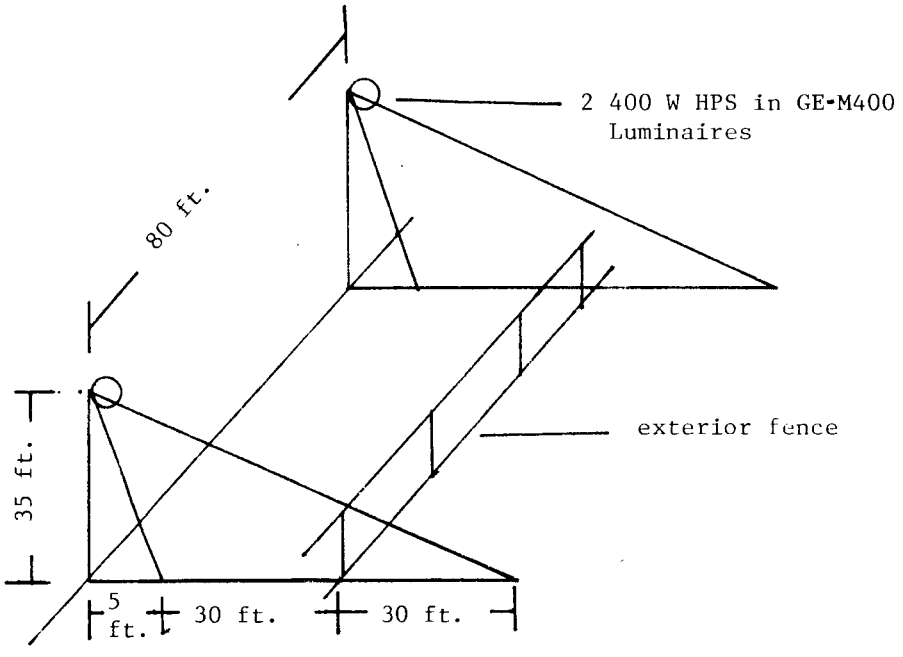


Figure A-11. High Pressure Sodium Vapor Isolation Zone Lighting System
Source: NuReg/CR1327

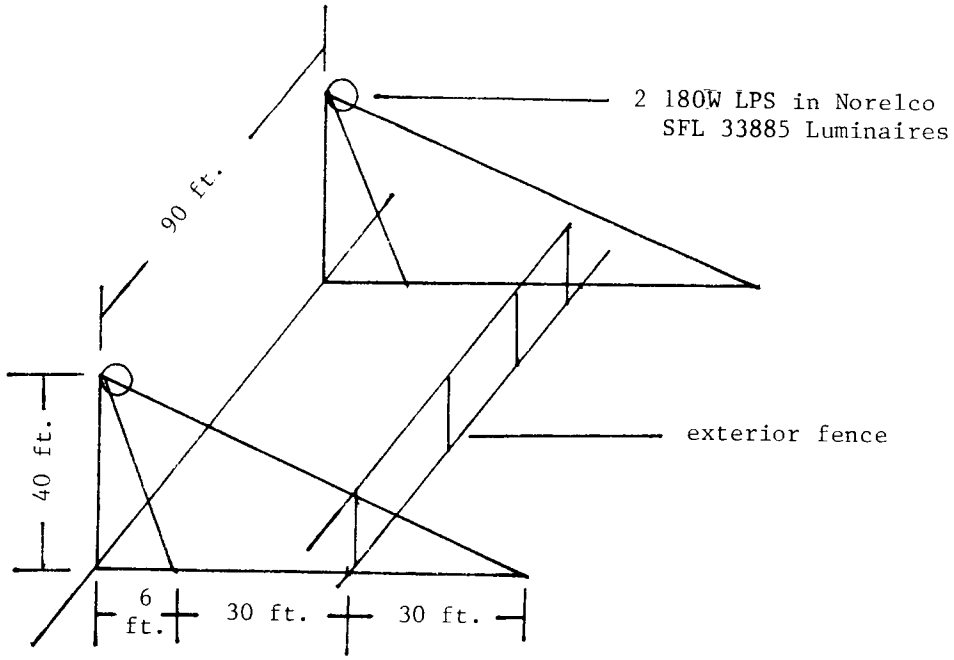


Figure A-12. Low Pressure Sodium Vapor Isolation Zone Lighting System
Source: NuReg /CR1327

The first system in this section is analyzed for initial and ongoing costs for a 1 mile perimeter as follows:

Pole cost: $165.00 per pole
Number of luminaires per pole: 1
Luminaire cost: $250.00
Bulk cost: $50.00
Wiring Cost: $200.00
Number of standards per mile: 66
Perimeter length in miles: 1 mile
Initial Cost = [($165.00 + $200.00) + 1 ($250.00 + $50.00)]
(66)(1)
Initial Cost = $ 42,230.00/mile
= $ 86,460.00/2 miles
= $128.690.00/3 miles
= $172.920.00/4 miles
Lamp wattage: 480 watts
Operating hours per year: 3500 hours

Cost of electrical energy per KWH: $0.05/KWH

Bulb life: 24,000 hours

$$\text{Operating cost} = \left\{\frac{(480)(3500)(\$0.05)}{1000} + \frac{(3500)(\$50.00)}{42000}\right\}(1)(1)(66)$$

Operating cost/yr = $ 5,819.00/mile
= $11,638.00/2 miles
= $17,457.00/3 miles
= $23,276.00/4 miles

In a similiar manner the costs for the low pressure sodium vapor lighting system are as follows:

LPS	Pole Cost	$100.00	Initial Cost
	#Lum/Pole	1	$ 70,840.00 1 mile
	Lum. Cost	$350.00	$141,680.00/2 miles
	Bulk Cost	$ 90.00	$212,520.00/3 miles
	Wiring Cost	$200.00	$283,360.00/4 miles
	#Poles/Mi.	88	Operating Cost
	Peri. Length/Mi.	1 mile	$ 5,390.00/yr/1 mile
	Wattage/Bulb	250 W.	$ 10,780.00/2 miles
	Operating Hours	3500 Hr/Yr	$ 16,170.00/3 miles
	Energy Cost	$ 0.05/KWH	$ 21,560.00/4 miles
	Bulb Life	14,000 hrs	

The two broad area coverage systems' cost are as follows:

HPS	Pole Cost	$100.00	Initial Cost
	# Lum/Pole	2	$ 63,690.00/1 mile
	Lum Cost	$250.00	$127,380.00/2 miles
	Bulk Cost	$ 50.00	$191,070.00/3 miles
	Wiring Cost	$200.00	$254,760.00/4 miles
	#Poles/Mi.	66	Operating Cost
	Peri. length/Mi.	1 mile	$ 12,050.50/1 mile
	Wattage/Bulb	480 watts	$ 24,101.00/2 miles
	Operating Hours	3500 hours	$ 36,151.50/3 miles
	Energy Cost	$ 0.05/KWH	$ 48,202.00/4 miles
	Bulb life	24,000 hours	

LPS	Same except:		Initial Cost
	Lum Cost	$350.00	$ 73,455.00/1 mile
	Bulb Cost	$ 90.00	$146,910.00/2 miles
	#Poles/Mi.	59	$220,365.00/3 miles
	Wattage/Bulb	250 watts	$293,820.00/4 miles
	Bulb Life	18,000 hrs	Operating Cost
			$ 7,227.50/1 mile
			$14,455.00/2 miles
			$21,682.50/3 miles
			$28,910.00/4 miles

As can be seen, the narrow-strip lighting system lends itself to the high pressure sodium, where the broad area lighting system favors the low pressure sodium, especially if energy costs escalate.

This cost evaluation approach is confirmed by vendor budgetary price information given in Section 9 of this report.

A.1.8 RELIABILITY AND LIFE CYCLE COSTS

To illustrate typical MTBF and life cycle cost considerations, an example is made using the RCA 2000/U, a typical economy CCTV camera.

The stated MTBF of the RCA TC-2000/u 2/3 inch vidicon camera is 15,000 hours, with the principle failure mechanism being failure of the vidicon. Simple calculations based on uniformly random failures as a function of time would indicate that a 24-camera system would have an MTBF of

$$MTBF_{sys} = \frac{\text{MTBF Camera}}{N} \qquad \text{(A-14)}$$

$$= \frac{15{,}000 \text{ hr}}{24}$$

$$= 625 \text{ hours (or nearly 4 weeks)}$$

where $MTBF_{sys}$ = Mean Time Between Failures of the entire CCTV system based on camera failures

N = Number of cameras

MTBF camera = Mean Time Between Failures of the individual cameras.

The prospect of a camera failure once every four weeks seems bleak and is also somewhat unrealistic. TV cameras exhibit a cumulative failure probability curve as shown in Figure A-13. Few cameras fail in the first 10,000 hours, but nearly half fail by 15,000 hours and nearly all have failed by 20,000 hours. If the vidicons (the principal failure items) are replaced in a 9,000 hour (yearly) cycle, the overall failure rate becomes negligible. It is advisable to retain spare cameras and vidicons as replacements to components which fail between replacement cycles.

In a VMD system, camera failures would produce a false alarm which could not be distinguished from TV camera sabotage. Therefore, the minimization of false alarms from TV camera failures is very important.

A.1.9 CCTV FOR VISUAL ASSESSMENT - OPTIONS AND COST FIGURES

If VMD is not proposed as an application for the CCTV system, the number of TV cameras and video channels can be reduced to half the number estimated above by the use of pan-tilt-zoom (PTZ) controls. Alarms from perimeter intrusion sensors can be used to train the TV cameras to the area of the alarmed sensor and the history of the intrusion can be recorded on videotape for a thorough assessment. Hierarchies of alarms would enable the CCTV system to give efficacious response to multiple alarms. Cost figures are drawn up for both staring and PTZ CCTV systems.

Though CCTV systems' costs decrease with increasing TV camera lens focal length and increasing coverage per TV camera, it may be advantageous, for assessment purposes, to let the coverage of each TV camera coincide with sectors of other sensors. A "reasonable" length of coverage, 200 meters per TV camera, has been selected as coinciding with 2 microwave and 2 fence sensors, so that alarms from sensors in any given sector can be assessed unambiguously. Thus, three approaches are mentioned in the cost totals: a CCTV system using 24 cameras to view

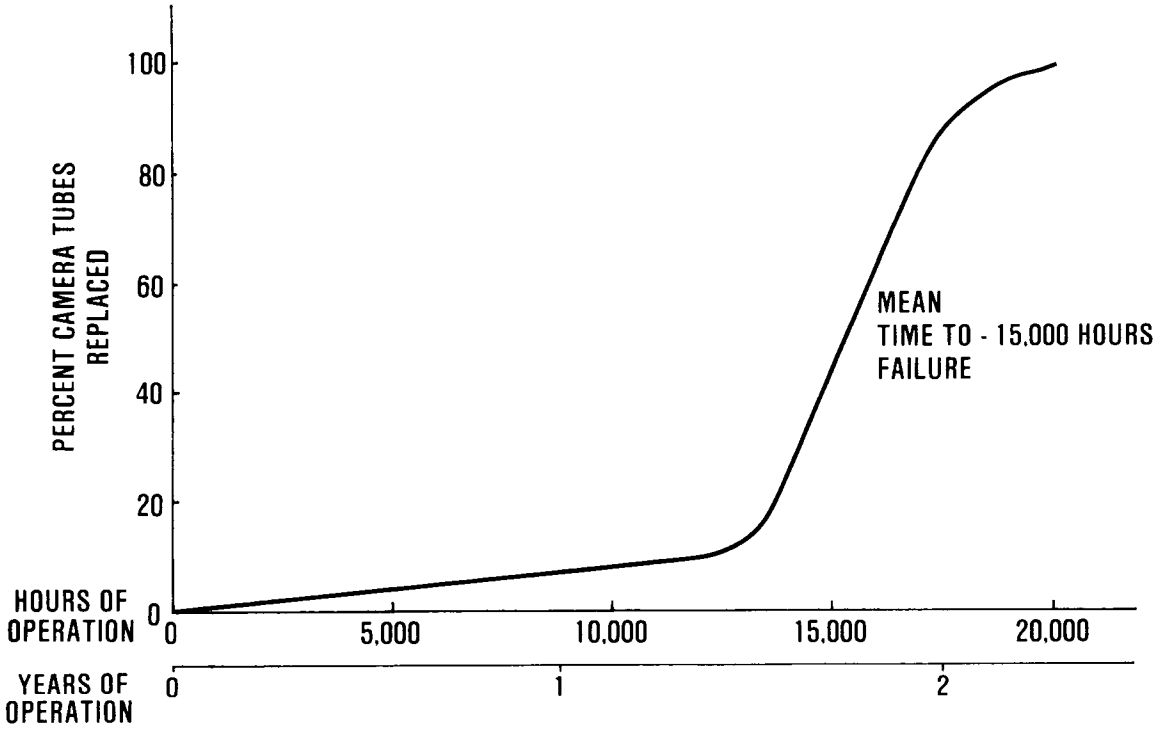


Figure A-13. CCTV Vidicon Life and Reliability

a 4800 meter (2.98 mi) perimeter in 200 meter segments; another CCTV system using 16 cameras to view a 4 mile (6437 meter) perimeter, to illustrate the cost advantage inherent with longer focal length TV camera lenses; and a PTZ CCTV system using available hardware to cover either the 4 mile or 4800 meter perimeter.

A.1.9.1 Shot Boxes for PTZ Operation

A shot box is a microprocessor-controlled pan-tilt-zoom (PTZ) control which, when given a command, trains the camera to any one of several preprogrammed locations. This enables an alarm from a perimeter sensor to command the appropriate camera to view the neighborhood of that sensor. The shot box gives commands to the camera automatically at the time of the alarm, thus reducing the time needed for a human operator to locate the neighborhood of the sensor and assess the scene.

A.1.9.2 Video Tape Recording

Video tape recording during the time of the alarm with instant replay capability would allow operators to have a historical record of the alarm event, and make a thorough assessment of the event, thus minimizing the false dispatch rate. Channel number and time code generation would assist later assessment efforts.

One weakness of videotape recorders is that they take about 1 to 5 seconds to begin recording after a command to record.

Time lapse video tape recorders are available which record up to 200 hours (or 8 days) on a cassette. These recorders also can record at actual speed when commanded from an alarm. Thus a time lapse history of the past plus a full speed record of alarms is recorded for assessment.

Video disk recorders have virtually instantaneous response to a record command, in contrast to video tape recorders. However, the video disk can store only about 10 to 20 seconds of video, and its cost is in the neighborhood of $30,000 each. A video disk could be used with a video

tape recorder to provide a complete video record for alarm assessment. For perimeter security applications, however, a time-lapse video tape recorder will provide sufficient coverage for assessment.

A.1.9.3 Response to Multiple Alarms for PTZ Operations

Multiple alarms from several points on the perimeter would require that priorities be assigned to sensor types and order of alarms. Redundancy in perimeter coverage by the CCTV system would allow better response to multiple alarms. Widely separated alarms would require coverage by separate video cameras, thus multiple TV monitors and some form of multiplexing of videotape recording (split-screen or time sequential) during alarms would enhance the completeness of the video history.

A.1.9.4 Cost of CCTV for Visual Assessment

CCTV visual assessment system costs are broken down for two cases. Full-time staring coverage may require more video channels but is mechanically less complex and more reliable. PTZ control CCTV systems allow a high degree of interaction with operators and may require fewer video channels. Table A-10 shows cost breakdowns and totals for each case. Figure A-14 shows a block diagram of the two CCTV systems.

Central Alarm Station (CAS) costs are given here. Inclusion of video monitors at a Secondary Alarm Station (SAS) requires duplication of the video monitor console, and duplication of controls and their cabling. If SAS and CAS are separated by some distance, additional video distribution cabling and line amplifiers will be necessary.

A.2 VIDEO MOTION DETECTION AS AN INTRUSION SENSOR

Video Motion Detection (VMD) is a means whereby a CCTV system can be used as an intrusion detector without the need for constant viewing. A VMD channel samples the video signal from a TV camera so that the light levels in several areas of the TV camera's field-of-view are monitored.

Table A-10

CCTV ASSESSMENT COST BREAKDOWN

(a) 4800M (2.983 mi.) perimeter, 24 Cameras

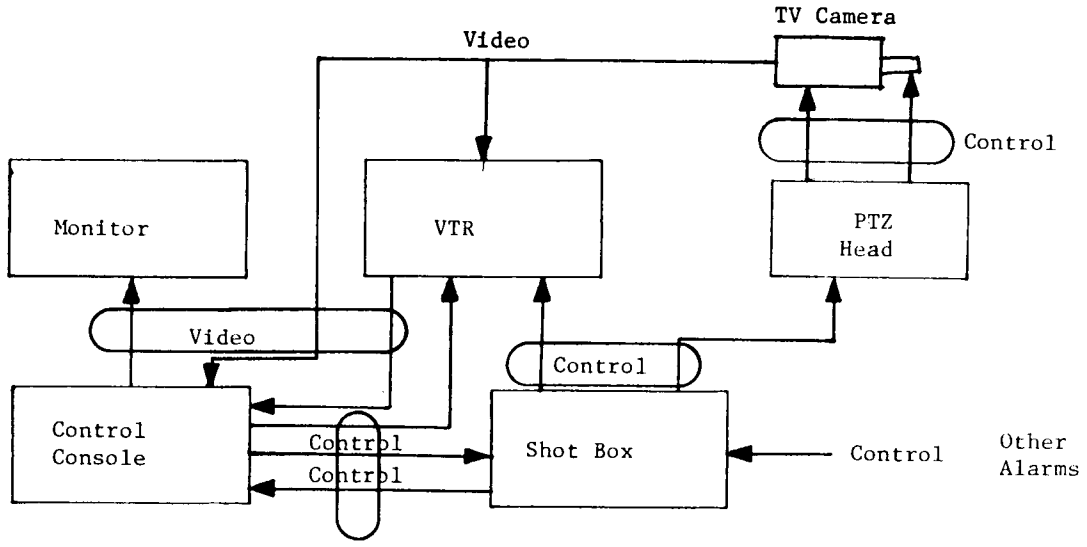
ORDER OF COST	ITEM	QTY/NO.	UNIT COST	TOTAL COST
1	Video Transmission Sys.			$29,256.00
2	35' Poles	24	$1,000 ea.	24,000.00
3	RCA TC2011/u75	24	775 ea.	18,600.00
4	External Sync Coax Line	8 miles	0.25/foot	10,560.00
5	Environmental Enclosures	24	220 ea.	5,280.00
6	6 Monitor Switching Console			3,500.00
7	Video Tape Recorder	1	1,000 ea.	1,000.00
			Grand Total	$92,196.00
			Cost Per Channel	$ 3,841.50

(b) 4 mi. (6437M) Perimeter, 16 Cameras

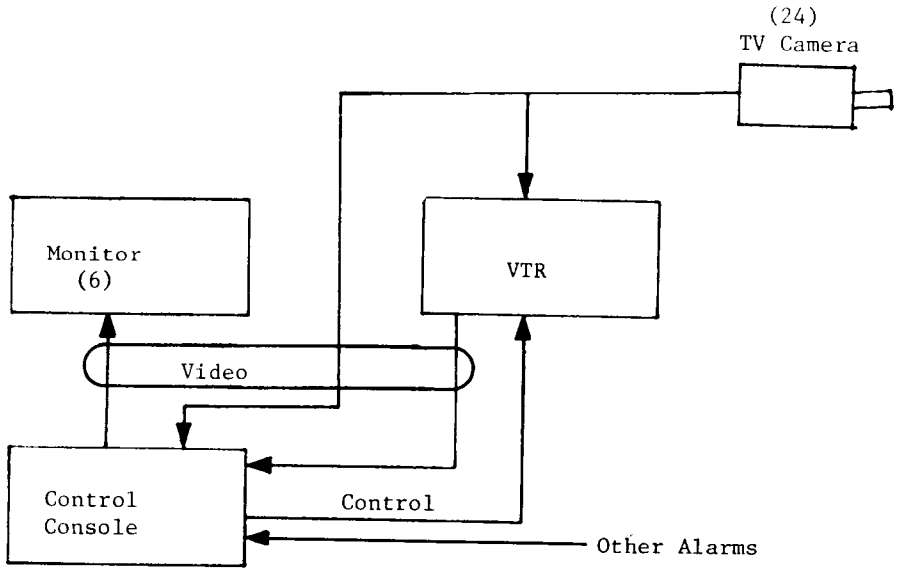
1	Video Transmission Sys.			$19,504.00
2	35' Poles	16	$1,000 ea.	16,000.00
3	External Sync Coax Line	8 miles	0.25/foot	10,560.00
4	RCA TC2011/u Body	16	570 ea.	9,120.00
5	Lenzar 150mm AI lens	16	489 ea.	7,824.00
6	Environmental Enclosures	16	220 ea.	3,520.00
7	6 Monitor Switching Console			3,500.00
8	Video Tape Recorder	1	1,000 ea.	1,000.00
			Grand Total	$71,028.00
			Cost Per Channel	$ 4,439.25

(c) 4 mi. (6437M) or 4800M (2.983 mi.) Perimeter, 24 PTZ Cameras

1	RCA TC 2011/uZ0	24	$1,500 ea.	$36,000.00
2	Video Transmission Sys	24		29,256.00
3	Shot Boxes	24	1,020 ea.	24,480.00
4	35' Poles	24	1,000 ea.	24,000.00
5	TV Control Cable	20 miles	0.219/foot	23,126.40
6	PTZ Head	24	540 ea.	12,960.00
7	External Sync Coax Line	8 miles	0.25/foot	10,560.00
8	Twin Joy Stick Controls	3 pair	1,850/pair	5,550.00
9	Environmental Enclosures	24	220 ea.	5,280.00
10	6 Monitor Switching Console			3,500.00
11	Video Tape Recorder	1	1,000 ea.	1,000.00
			Grand Total	$175,712.40
			Cost Per Channel	7,321.35



(a) PTZ Video Assessment Block Diagram



(b) Staring Video Assessment Block Diagram

Figure A-14. CCTV Schemes for Video Assessment of Alarms

In digital VMD systems, the video signal from each area is digitized and stored for comparison with future signals from the same area as they are repeatedly sampled. When the light level in the sample area changes, the signal from the TV camera will also change. If the signal changes enough, the newly digitized signal will disagree with the previously stored signal. This disagreement is then noted by a central processing unit (CPU) which sounds an alarm when the number of disagreements exceeds a preset number.

VMD systems are available with a great variety of features, numbers of sample areas and levels of complexity. The following subsections give a rationale showing the desirability of a large number of sample areas and a degree of programmability for detection in exterior perimeter security surveillance. Interior security using VMD over short distances can be accomplished using a small number of areas in the observed scene, but as distances to potential intruders increase, a greater number of sampling areas are needed to enhance the VMD system's contrast sensitivity and its probability of intercept of an intruder. Also, video tape or disk recording with "instant replay" capability and "trace map" features highlighting disturbed scene areas will aid assessment of alarms and reduce the false dispatch rate of the security system.

A.2.1 RELATION OF SAMPLING AREA NUMBER TO VMD PERFORMANCE

This subsection deals with the relation between the VMD system's number of sampling areas and the contrast sensitivity and probability of intercept for the system.

A.2.1.1 Size of Sampling Area Versus Size of Detected Object

VMD systems rely on detecting a scene brightness change from the original level to a disturbed level. To assure a conditional probability of detection near unity, this change must exceed a certain threshold depending on the number of bits to which the brightness level is digitized. (See Figure A-15.) If the area of the brightness disturbance

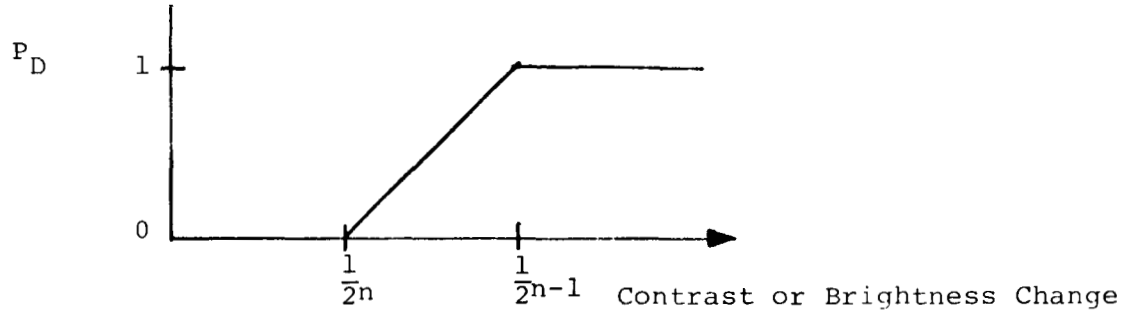


Figure A-15. Conditional Probability of Detection vs Contrast Change

is the same size or larger than the field-of-view of the VMD system's sample, the brightness change of the disturbance will cause a proportional change in the sample channel's signal level. If the disturbed area is smaller than the sample area's field-of-view, the change in channel signal level will also depend on the ratio of the areas as shown in Eq. A-15.

$$C \propto \begin{cases} \dfrac{(B_d - B_b)}{Bb}, & A_d \geq A_{samp} \\ \dfrac{(B_d - B_b)\, A_d}{Bb\; A_{samp}}, & A_{samp} \geq A_d \end{cases} \qquad \text{(A-15)}$$

Where C = Change in signal level
Bd = Brightness of disturbance
Bb = Original scene brightness
Ad = Area of disturbance
Asamp = Area of sample FOV

Thus, if the sample area is large compared to the disturbance area, the VMD system will be insensitive to brightness changes in the disturbance, as shown in Figure A-16.

A.2.1.2 Sample Area Spacing

The spacing of sample areas has a direct impact on the VMD system probability of detection. In an exterior VMD system with long distances between the intruder and the TV camera, an intrusion would be characterized by a small, point-like object in the TV camera's field-of-view.

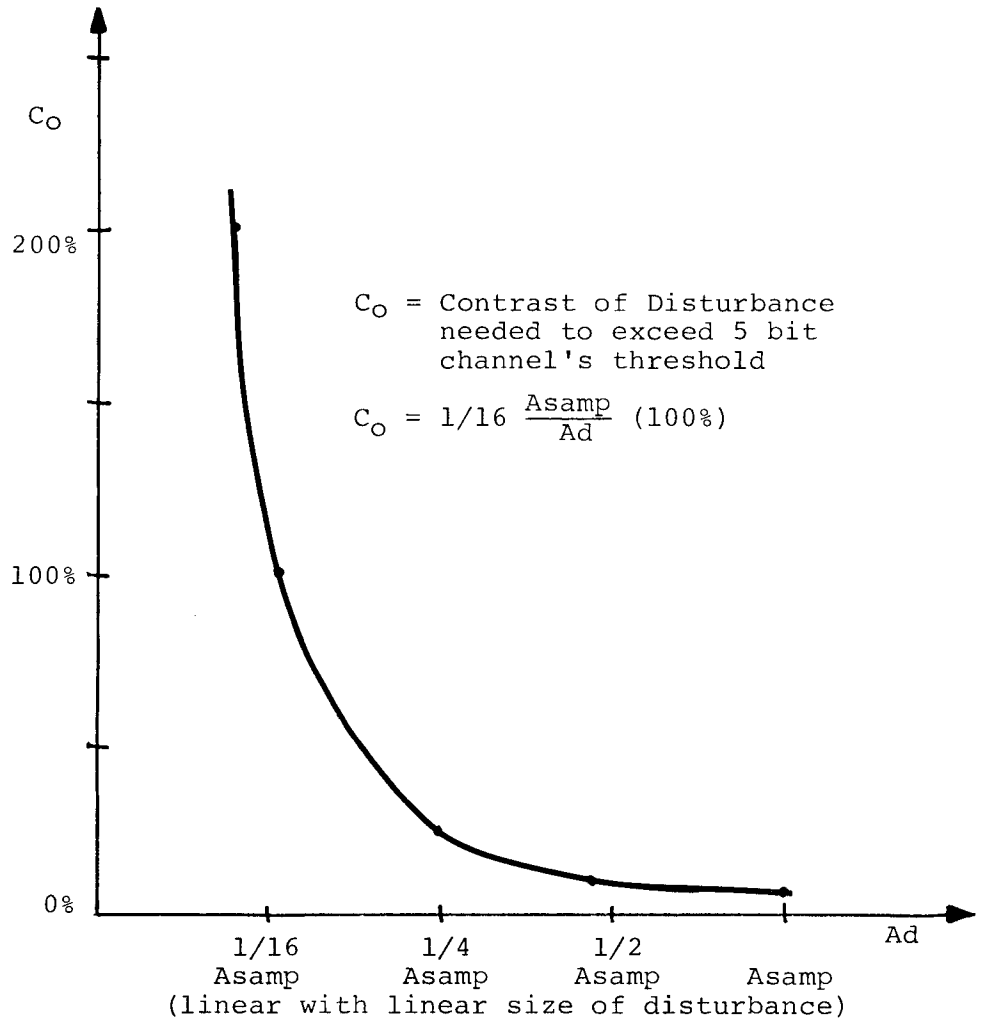


Figure A-16. Contrast Level of Disturbance with Area A_d Needed to Trigger a 5 Bit VMD Sample Channel

The probability of the small, point-like object occupying a VMD sample area is:

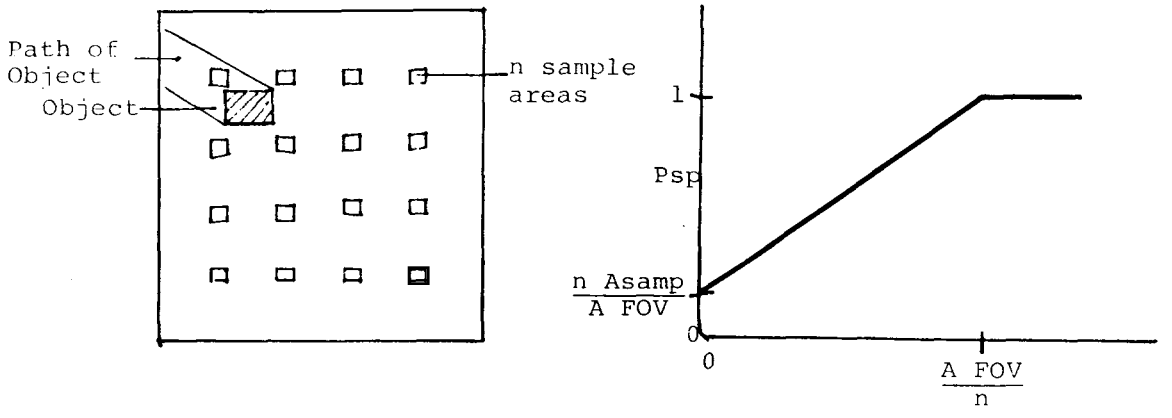
$$P_{sp} = \frac{n\ A_{samp}}{A_{fov}} \qquad \text{(A-16)}$$

where P_{sp} = Probability that the disturbance occupies a sample area

n = Total number of sample points (uniformly distributed

A_{fov} = Total field-of-view area of TV camera

A large object has a probability approaching 1 of occupying a sample area if the object's size approaches the average spacing of the sample points. Figure A-17 shows this scenario and a plot of the probability of encountering a sample area versus object area for a square object.



(a) Video Display of Sample Windows and Object

(b) Plot of Psp Versus Object Area

Figure A-17. Probability of an Object Encountering a VMD sample Area

The probability of occupying a sample area is one of the conditional probabilities affecting the overall probability of detection for the VMD system. Thus, the overall probability of detection of the VMD system is proportional to the combined probabilities of occupying sample areas for the disturbances in question. The small point-like disturbance is more characteristic of an exterior perimeter intrusion whereas the large disturbance is more typical of an indoor intrusion, with short ranges between the intruder and the TV camera.

To get a realistic idea of the effect the number of sample areas has on a VMD system's probability of detection, a model is proposed. Failure to detect an intrusion for the VMD system is defined as failure to detect a 10% penetration of the TV camera's field-of-view. The intruder is defined as a 1 foot square at maximum camera range with sufficient contrast to trigger the VMD sample area channel when it occupies that area. The sample areas are assumed to have zero

area, and are distributed in the TV camera field-of-view as a uniform rectangular matrix of $\sqrt{n}$ x $\sqrt{n}$ where n is the total number of sample areas. If the intruder enters the edge of the TV camera's field-of-view as shown in Figure A-17(a) and travels on a path towards the center of the field-of-view, its path will enter the neighborhood of $\frac{\sqrt{n}}{10}$ samples. Thus the probability of triggering one of the sample areas is:

$$P_t = 1-(1-P_{sp1})(1-P_{sp2})(1-P_{sp3})\ldots(1-P_{sp\frac{\sqrt{n}}{10}}) \qquad \text{(A-17)}$$

where P_t = Probability that at least one of the sample areas will be triggered

P_{sp} = Probability that the intruder will trigger a particular sample area when the intruder is near that sample area

n = Total number of sample areas

If the path of the square is a random straight line, the probability that it intercepts a sample area is described by

$$Psp = \frac{A_{path}}{A_{rect}} \qquad \text{(A-18)}$$

where P_{sp} = Probability of path intercepting the sample area

A_{rect} = Area of the rectangles whose vertices are adjacent sample areas

A_{path} = Area of path in rectangle

The rectangle area A_{rect} is the total area in the TV camera field-of-view projected at maximum range divided by n, the total number of sample areas. The path area is the product of the average intruder path width and the width of the rectangle (sample rectangle) described above. The average intruder path width is the expected value of the 1 foot square's projection at a uniformly distributed random angle, a value of 1.27324 feet.

Thus, the area of the sample rectangle is

$$A_{rect} = \frac{A_{fov}}{n} = \frac{(91.875)(122.5)\,ft^2}{n} = \frac{11254.69\ ft^2}{n} \qquad (A\text{-}19)$$

where A_{fov} = total projected area of field-of-view at maximum range

and the path is then

$$A_{path} = \frac{A_{fov}}{n}(W_p) = \frac{(106.09)}{n}(1.27324)ft^2 = \frac{135.076\ ft^2}{n} \qquad (A\text{-}20)$$

where W_p = average intruder path width

Plugging these values into equation 17 gives us

$$P_t = 1 - (1 - \frac{n}{83.32})^{\frac{\sqrt{n}}{10}} \qquad (A\text{-}21)$$

A graph of this probability as a function of n is shown in Figure A-18. From the graph, it can be seen that a VMD system having 5000 samples will have nearly a 100% probability of detection (P_D). For example, the 4000 sample Teleguard unit's predicted probability of detection (P_D) = 99.9% for the 1-foot square intruder at maximum range.

A.2.1.3 Temporal Effects on Probability of Detection

In addition to spatial considerations and contrast requirements, temporal constraints also affect the probability of detection of moving objects. As VMD processors only sense each sample area at discrete times, fast moving small objects may escape detection by sample areas in their path. For example, as shown in Figure A-19, a rectangular object of length D, passing a sample area sampled at intervals, t_s, at velocity, v, has a conditional probability of detection.

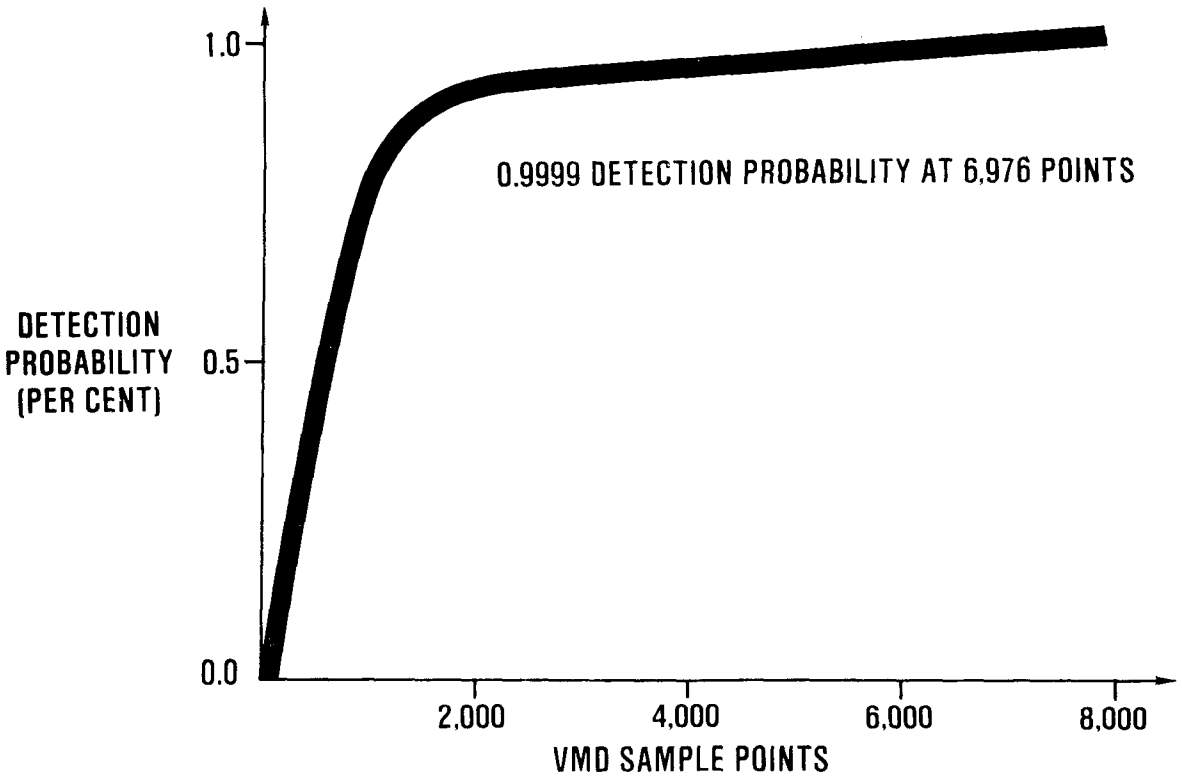


Figure A-18. Probability of Detection of a 1-Foot Square Object at Maximum Range During a 10% Intrusion Into the Field-of-View

$$P = \begin{cases} \dfrac{D}{vt_s} & \text{for } t_s > \dfrac{D}{v} \\ 1 & \text{for } t_s \leq \dfrac{D}{v} \end{cases} \qquad \text{(A-22)}$$

Where the conditional probability of detection reflects the length of time the object intersects the sample area. This probability is the temporal conditional probability of detection which must be multiplied by other conditional probabilities of detection for the sample area, and then combined with other sample areas' detection probabilities. Another consideration arises when more than one alarm point or trace point is required to produce a system alarm. If the hit counter (or error rate counter) is set for a given amount of alarms ($n_e > 1$), an object must trigger that number, n_e to alarm the system. Since a VMD processor also updates (or resets or refreshes) the memories the reference pixel values at refresh intervals, t_r, an intruder could escape

detection by triggering fewer than n_e alarms during each time, t_r. Hence, the motion detector requires a minimum speed to assure detection:

$$V_{min} = \frac{(V_{fov})(H_{fov})\ n_e}{2n\ (W_o)\ t_r} \qquad \text{(A-23)}$$

where V_{min} = the minimum speed needed to produce a VMD system alarm
V_{fov} = the vertical field-of-view of the TV camera
H_{fov} = the horizontal field-of-view of the TV camera
n = total number of sample points of VMD system per camera
W_o = width of object's leading edge

A factor of 2 is included because both the object's leading and trailing edges cause contrast changes in the sample areas (see Figure A-20).

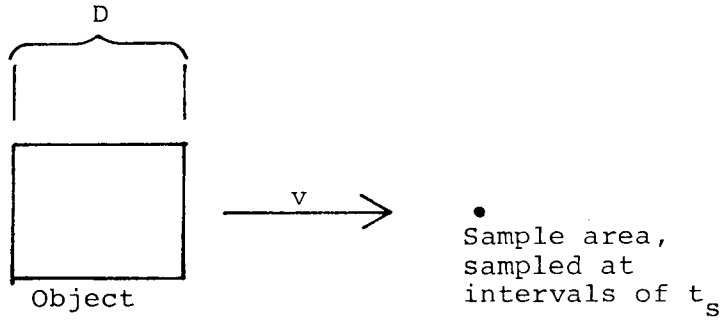


Figure A-19. Scenario for Probability of Detection of Fast Moving Object.

The velocities at which objects of interest begin to evade detection are usually fairly high. For example, with a VMD processor having a 30 frame per second sample rate, an object a foot long travelling 30 feet per second (20.5 mph) still has a temporal conditional probability of detection of 1.

On the other hand, speeds needed to produce VMD system alarms are in the range of 0.5 to 1.6 feet/second for a typical VMD system and a rolling or crawling intruder. (System parameters in this calculation: 2/3" vidicon, 75mm lens, VMD processor hit counter = 8, refresh time = 8 seconds; intruder minimum dimension = 1 foot, 4000 sample points). It is noted that while it is simple for an intruder to crawl at lower speeds than 1.6 feet per second, it is nearly impossible to crawl or roll smoothly over the terrain with no jerky motions having much greater speeds.

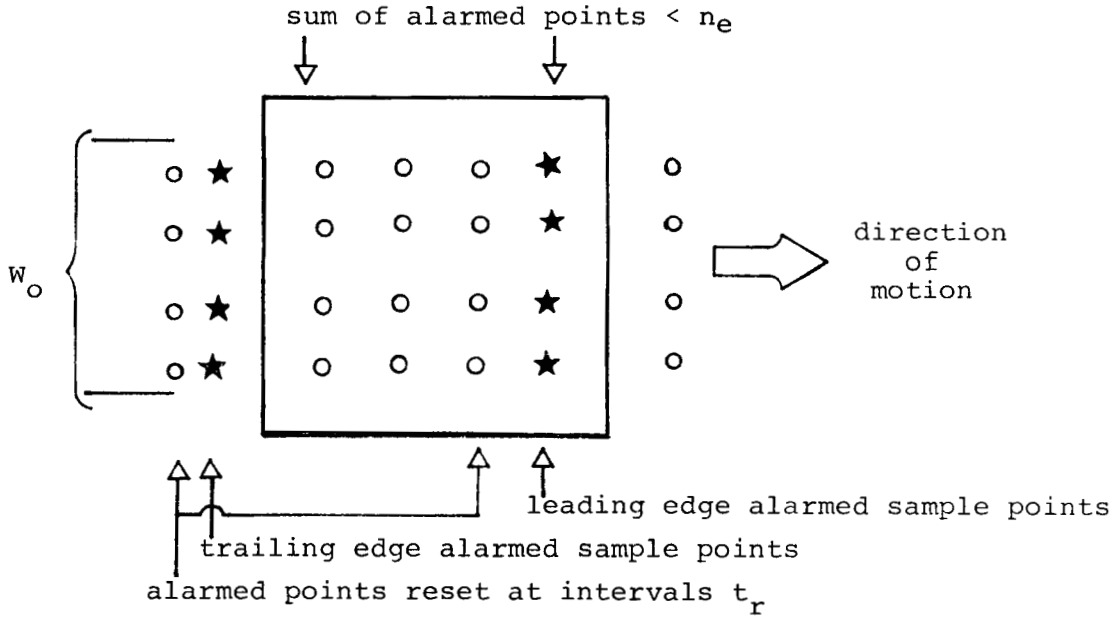


Figure A-20. Slow Moving Object Escaping Detection Scenario

A.2.2 NUISANCE AND FALSE ALARMS

Video motion detection systems for exterior perimeter security are prone to the following nuisance and false alarms:

- Nuisance alarms from authorized personnel and equipment movement in TV camera field-of-view,
- Nuisance alarms from inclement meteorological conditions,
- Nuisance alarms from glare, reflections from objects in field-of-view,

- Nuisance alarms from blowing litter in field-of-view,
- Nuisance alarms from fauna intrusion to field-of-view (birds, rabbits, insects, etc.),
- Nuisance alarms from TV camera support movement,
- False alarms from VMD system equipment failure,
- Nuisance alarms from natural and artificial lighting changes,
- False alarms from power line and video transmission system EMI, and
- False alarms from unknown causes (other).

Nuisance and false alarm information is being compiled by personnel at several facilities having newly-installed VMD systems. The test program appearing in Appendix AA also gave information which appears in Appendix AB on nuisance and false alarm mechanisms.

A.2.3 POLE DEFLECTIONS

A problem closely related to the nuisance alarm rate for a VMD system is pole deflection caused by wind. Pole movement has an effect on the scene viewed by the TV camera characterized by angular displacement of the camera from its original orientation. The following discussion describes the action of wind on the tower and the TV camera's angle.

A.2.3.1 Effect of Pole Displacement on Field-of-View

When the pole upon which a TV camera is mounted vibrates or is deflected, three effects may occur. Displacement in the direction of the line-of-sight will cause an up and down (vertical) change. Tower twisting movement will cause horizontal motion in the field-of-view, and tower movement perpendicular to the line of sight will cause a small rotation of the field-of-view plus a small displacement horizontally. Video Tek has compiled a table of field-of-view displacement for tower top deflections of various heights of towers, but no calculation for twisting deflections (5).

A.2.3.1.1 Deflection Levels Defined. Deflections of the camera field-of-view may approach several different levels of seriousness. The first level can be described from the dimension of the sample area relative to the TV camera field-of-view. To be reasonably assured of no nuisance alarms from a 100% contrast boundary, the deflection would have to be less than $\frac{1}{2^{n-1}}$ of the angle of the sample area field-of-view, where n is the number of bits to which the sample's light level is quantized.

The second level of deflection can be defined as the field-of-view angle of the VMD sample area.

The third level can be defined as the angle of the sample-to-sample spacing of the VMD sample areas.

The fourth level is defined from CCTV parameters, independently of VMD specifications, and specifies that display motion be less than 1/2 the angle of the period of the vertical maximum resolved spatial frequency on the CCTV monitor. Figure A-21 shows these definitions pictorially.

As a representative system to illustrate the range of these numbers, we consider a 525 line scan, 4000 sample point system. Its levels are described in Table A-11.

Table A-11
Deflection Levels for a Representative VMD System in Terms of Field-of-View

Deflection Level 1 = VFOV/1600 (5 bit algorithm)
Deflection Level 2 = VFOV/100
Deflection Level 3 = VFOV/65
Deflection Level 4 = VFOV/367.5

If a long focal length lens, say a 150mm lens, on a 2/3" vidicon is used, the deflection levels to be met are very small as shown below.

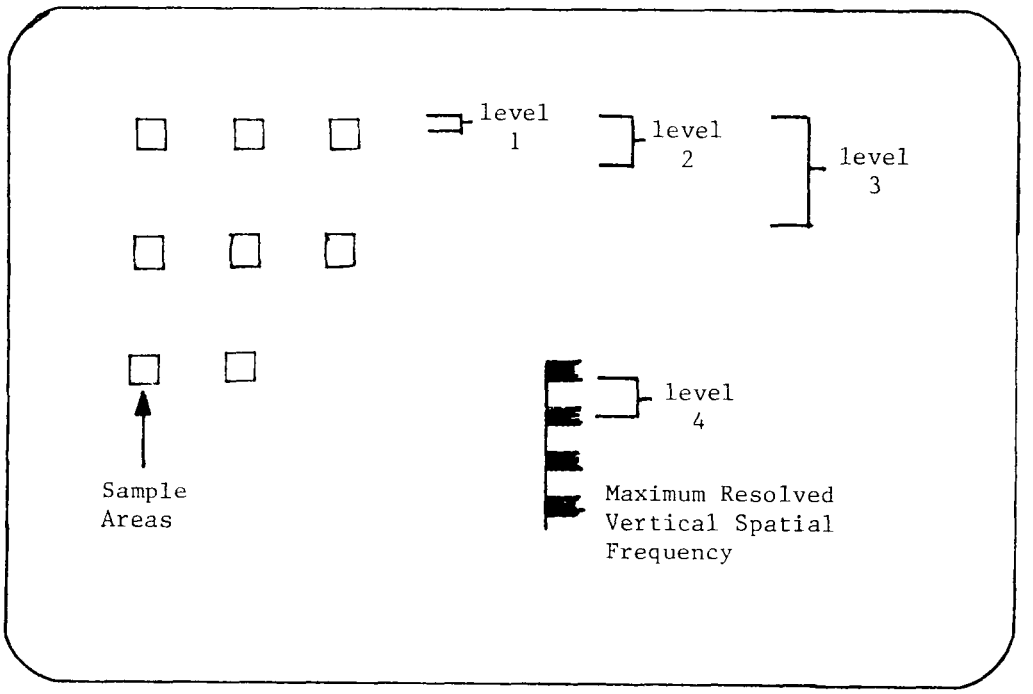


Figure A-21. Depiction of Definitions of Levels of Deflection of Field-of-View

The vertical field-of-view is 2.44425° for this combination, giving the set of levels below:

Deflection Level 1 = 0.001527655° = 5.5 arc seconds
Deflection Level 2 = 0.0244425° = 1.46655 arc minutes
Deflection Level 3 = 0.037604° = 2.25623 arc minutes
Deflection Level 4 = 0.006651° = 23.944 arc seconds

To gain a feeling for how these figures compare with actual tower deflections, a calculation of deflection for a flagpole-type cylindrical tower is shown below.

A.2.3.2 Calculation of Tower Angular Deflection

The following calculations deal with the angular deflection at the top of a 35-foot tall, 6" diameter, 1/2" wall, cylindrical steel pole fixed from angular or translational motion at the ground and either guyed or unguyed at the top. A steady wind velocity of 50 mph is

assumed. No mechanical resonance effects are assumed to occur, since at this velocity, the wind vortex-shedding frequency (7) is much lower than mechanical resonant frequencies.

The wind force loading the pole as described above is (6).

$$F = \tfrac{1}{2} \rho \quad V^2 A \qquad \text{(A-24)}$$

where F = Total force on pole (lb.)
ρ = density of air $(\frac{\text{lb}}{(g)\ \text{ft}^3})$
V = Velocity of wind (ft/sec)
A = Frontal area of pole (ft^2)

In this case

$$F = \tfrac{1}{2} \left\{ \frac{0.076\ \frac{\text{lb}}{\text{ft}^3}}{32.2\ \frac{\text{ft}}{\text{sec}^2}} \right\} \quad (73.3\ \tfrac{\text{ft}}{\text{sec}})^2 \quad (35\ (\tfrac{1}{2})\ \text{ft}^2)$$

$$= 111.26 \text{ lb.}$$

The deflection of the top of an unguyed pole fixed at the bottom having this evenly distributed loading will be described by

$$\delta = F \frac{\ell^3}{8EI} \qquad \text{(A-25)}$$

where δ = The deflection of the pole's top (in.)
F = The evenly distributed total force (lb.)
ℓ = The height of the pole (in.)
E = The elastic modulus of the pole material $(\frac{\text{lb}}{\text{in}^2})$
I = Moment of inertia of pole cross section (in^4)

The angular displacement of the pole top from vertical is described by

$$\theta = F \frac{\ell^2}{6EI} \text{ (radians)} \qquad \text{(A-26)}$$

where θ = angle of tower top from vertical in radians.

In this case, the deflection at the top is:

$$= 111.26 \text{ lb} \left\{ \frac{((35 \text{ ft.})(12 \frac{\text{in.}}{\text{ft.}}))^3}{8(30X10^6 \frac{\text{lb}}{\text{in}^2})(18.7 \text{ in}^4)} \right\} = 1.836 \text{ in.}$$

The angular displacement is then:

$$= 111.26 \left\{ \frac{(35 \text{ ft } (12 \frac{\text{in}}{\text{ft}}))^2}{6(30X10^6 \frac{\text{lb}}{\text{in}^2})(18.7 \text{ in}^4)} \right\} 0.005831 \text{ rad}$$

$$= 0.334 \text{ deg} = 20.045 \text{ arc minutes}$$

If we are to constrain the top of the tower (with prestressed guy wires) to prevent translation, leaving only angular deflection, the angular motion would then be described by

$$\theta = \frac{F \ell^2}{48 \text{ EI}} \quad \text{(radians)} \qquad \text{(A-27)}$$

or merely 1/8 of the quantity calculated in Eq A-26. In this case, the angular change is

$$\theta = 0.00073 \text{ radians}$$
$$= 0.0418 \text{ degrees}$$
$$= 2.51 \text{ arc minutes}$$

Even this amount of deflection exceeds all the levels mentioned for a 150mm lens focal length, 2/3 inch vidicon TV camera and the representative VMD unit as described in the preceding subsection. Obviously a stiffer tower is needed for TV camera support if 50 mile/hour winds are expected.

A.2.3.3 Types of Towers

Several types of TV camera support towers are available. Their unique features, cost per tower, and expected performance are mentioned in the following paragraphs.

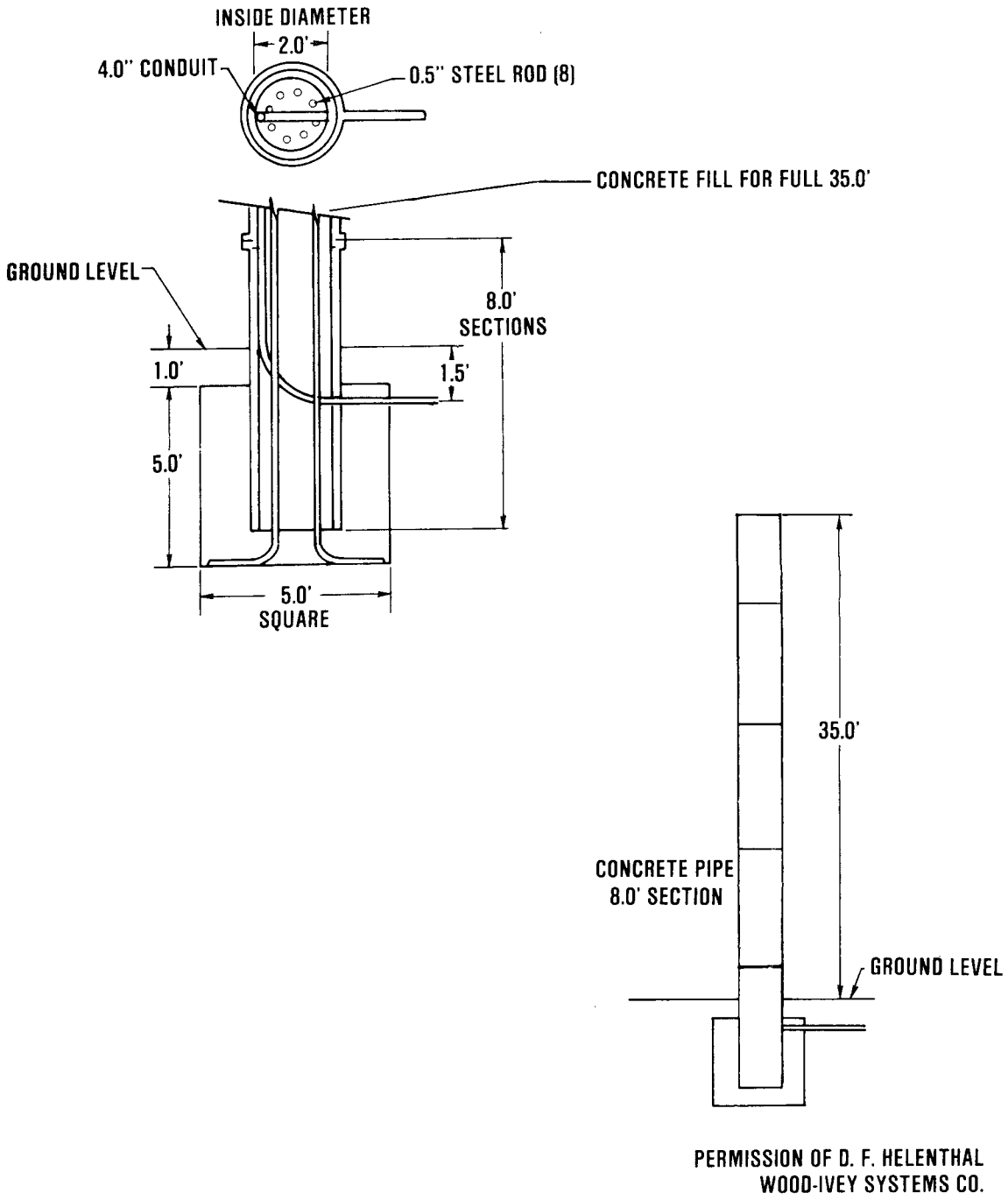


Figure A-22. 2 Foot Diameter Concrete Pier Tower

A.2.3.3.1 6 Inch Diameter Cylindrical Steel Pole. One approach to TV camera mounting is the 6 inch diameter steel pipe mentioned above. The previous subsection dealt with an analysis of this material, where calculations showed that the top of a pole having a height of 35 ft. in a 50 mph wind would exhibit a deflection of 20 arc minutes unguyed, or 2.5 arc minutes guyed. The cost of this tower is approximately $1450.

A.2.3.3.2 Rohn 45® Fold-Over Tower. A fold-over tower would solve much of the serviceability problem inherent with other types of poles. The fold-over feature allows one service person to lower the TV camera to the proper working height for replacement or adjustment.

This commercially-made tower, however, may have poorer stability than the steel pole. No quantitative data has been found relating tower top deflection to wind velocity, however. The cost of the Rohn 45® fold-over tower in a 48-foot height is approximately $1000.

A.2.3.3.3 Tinawa Pole. The Tinawa Pole is a tapered steel pole having an octagonal cross section and a cost of $1000 and is in use at the Canadian White Shell NR Station. No quantitative stability data has been found.

A.2.3.3.4 Double Walled Pole. A double-walled steel pole like those in use at Ontario Hydro, Pickering Station, has a cost of $4000. The inner pole is shielded by an outer pole. No quantitative stability data has been found.

A.2.3.3.5 Concrete Pier. A lower-cost alternative to the double-walled pole is the concrete pier shown in Figure A-22. The pier is made from concrete and reinforcement rods poured into a sewer pipe or Sonotube® form with an inside diameter of 2 feet. Towers from 20 to 40 feet made in this manner are stiff and highly damped from vibration, but present a large frontal area to wind. The cost

of the concrete pier tower in quantity is roughly $1800 for materials. No quantitative stability data has been found.

A.2.3.3.6 Servicing. Use of any above-mentioned towers besides the Rohn tower as a support for the TV camera presents servicing difficulties, since they are not foldable. A cherry-picker is probably the most practical means of gaining access to a top-mounted TV camera on the non-foldable towers.

A.2.3.3.7 High Voltage Area Constraints. In some high electric field environments encountered at many power plants, guy wires are not recommended for tower stabilization. The hazard of contact with high-voltage lines and possibility of corona discharges make guy wires and fold-over towers undesirable in close quarters with HV equipment.

A.2.3.3.8 Live Test. To test for the effects of vibration on VMD system performance, a test plan has been formulated. The test plan in Appendix AA allowed testing for nuisance alarms due to tower deflection. The results of the tests outlined in Appendix AA are discussed in Appendix AB.

A.2.4 VMD FOR SMOKE AND FIRE DETECTIONS

Video Motion Detection (VMD) could conceivably be used as an adjunct to already-existing fire and smoke alarms by sensing light-level changes due to fire and smoke in the TV camera's field-of-view in the perimeter area. This section discusses this possibility and considers the feasibility of such an approach.

A.2.4.1 Probability of Detection Considerations

Video Motion Detectors are triggered by light level changes exceeding a minimum threshold within a given time. Smoke can be detected when it obscures a TV camera's field-of-view, or when it blocks the illumination source for the area in view. Both of these effects are dependent upon the extinction coefficient and depth dimension of the smoke. Smoke can also be detected when it reflects light to a TV camera. This effect is dependent on the scattering coefficient of the smoke and the intensity of the light incident upon the smoke. Figure A-23 shows a scenario where smoke is detected in the latter case.

The requirement for detecting smoke is that passage of smoke results in at least the following minimum change in scene brightness:

$$\% \text{ Change} = 100\% \left(\frac{1}{2^n}\right) \qquad \text{(A-28)}$$

where % Change = Percent change in scene brightness
n = number of bits in Video Motion Detector channel

This change must occur in the maximum time set by the refresh cycle of the VMD channel.

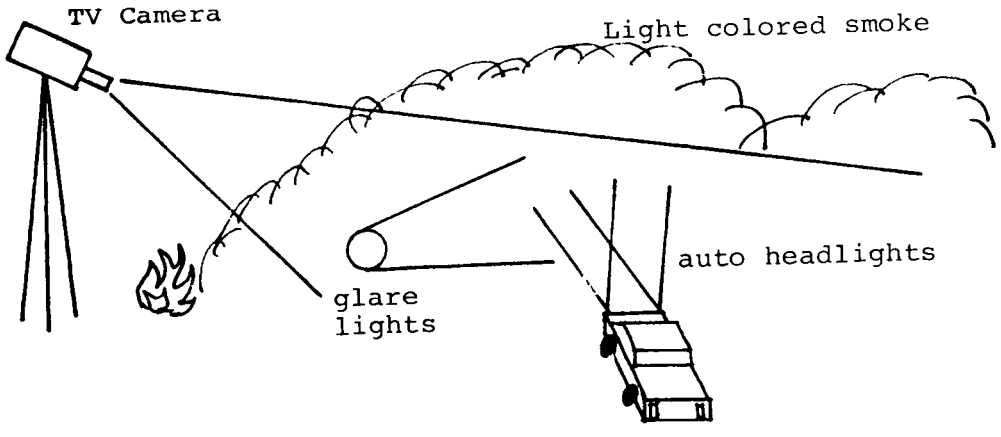


Figure A-23. Smoke Detection by Reflection Scenario

Fire detection can be accomplished by VMD in the following ways:

- Fire in TV camera field-of-view
- Smoke (from fire) detected as above
- Reflection of fire brightness by objects in TV camera's field-of-view

Here, the presence of fire or reflections from fire must be at least as large and result in the same brightness changes as described in Section A.2.1.1 to be detected. The brightness change must occur within the maximum time set by the refresh rate cycle of the VMD channel.

A.2.4.2 Nuisance Alarm Rate for Plant Viewing TV Cameras

Plant-viewing TV cameras are susceptible to the same nuisance and false alarms sources as perimeter-viewing sensors, except that nuisance alarms from the following sources become especially troublesome:

- Authorized personnel and equipment movement in TV camera field-of-view
- Glare and reflections from objects in field-of-view
- Steam movement from cooling towers
- Litter blowing into field-of-view

Techniques used to reduce nuisance alarms for plant viewing TV cameras will also have the effect of concealing fire and smoke in high-movement areas. Form this standpoint, plant viewing as compared to perimeter viewing TV cameras for fire and smoke are considered of little use and are not recommended.

A.2.5 VMD SYSTEM USING PAN-TILT-ZOOM FEATURES

For a moderate increase in system cost, Pan-Tilt-Zoom (PTZ) features can be added to a VMD system. PTZ capabilities might add to the capabilities of the VMD system's use as an assessment tool, and would allow the CCTV system a means to partially compensate for gaps in perimeter coverage in case of component failures. Operator-system interaction capability would be increased as well. The main disadvantage of PTZ

units is that operators tend to lose orientation with the field-of-view when panning, due to the telephoto lenses on the TV cameras and the excessively fast pan rates of most PTZ units. Increased cost and decreased mean time between failures (MTBF) are other disadvantages.

A.2.5.1 VMD/Assessment Modes

During times of PTZ operation, scene motion will take place, and the VMD channel connected to the TV camera being adjusted will alarm unless it is disabled during PTZ operation. Therefore, the system would be aided by having two modes of operation; an assessment mode during PTZ operation, and a VMD mode when staring along the perimeter to be protected. During the assessment mode, the VMD unit is disabled and the desired TV cameras' outputs are displayed on the monitors. During VMD mode the PTZ controls are disabled, the TV cameras are positioned by shot boxes and the VMD unit is enabled. This prevents simultaneous PTZ operation and VMD alarming.

A.2.5.2 Hardware for VMD Assessment

The following items would be added to a staring VMD system to convert it to a VMD/Assessment system utilizing PTZ capability:

- Zoom lenses
- Pan Tilt head
- Wiring appropriate for PTZ operation
- Shot boxes
- Console controls
- Mode controller for VMD unit/PTZ controls/shot boxes

A.2.5.2.1 Zoom lenses - RCA Auto Iris 11-110mm or similar lenses. These are the longest practical focal length zoom lens for 2/3" vidicon format.

A.2.5.2.2 Pan-Tilt Head - Must be capable of 360° rotation az, 180° el or as close as possible to this, with controllable slow or fast rates.

A.2.5.2.3 PTZ Wiring - Multi-wire cable for driving PTZ head to be pulled with video signal coax.

A.2.5.2.4 Shot boxes - These allow setting the TV camera positions to looking down the perimeter for the primary VMD task when the system is in VMD mode.

A.2.5.2.5 Console controls - PTZ joysticks and paddles to allow operation of several TV cameras from each control by switching between cameras.

A.2.5.2.6 Mode Controller - To be built to disable/enable VMD unit/ PTZ controls and to trigger the shot boxes appropriately for either VMD or assessment mode.

A.2.6 COST OF VMD SYSTEM

The following trade-offs are based on the RCA TC 2011/u camera with its associated accessories and a representative 4000 sample motion detector. Cameras are fixed or staring.

- Focal length/field-of-view versus cost of VMD system
- Assumed intruder minimum dimension versus cost of VMD system
- VMD sample area number versus cost of VMD channel

Finally a cost breakdown table is given for a staring VMD and a PTZ VMD system.

A.2.6.1 Focal Length/Field-of-View Versus Cost of VMD System

For a representative 2/3 inch vidicon, the RCA TC-2011/u, and square perimeters of 1, 2, 3 and 4 miles, Figure A-24 shows the dependence of hardware costs on the TV camera lens focal length for a staring VMD system and a staring CCTV surveillance system. These graphs indicate that using the longest possible TV camera lens focal lengths would be the most cost-effective approach to VMD perimeter security surveil lance. To interface with other possible sensors, however, a focal

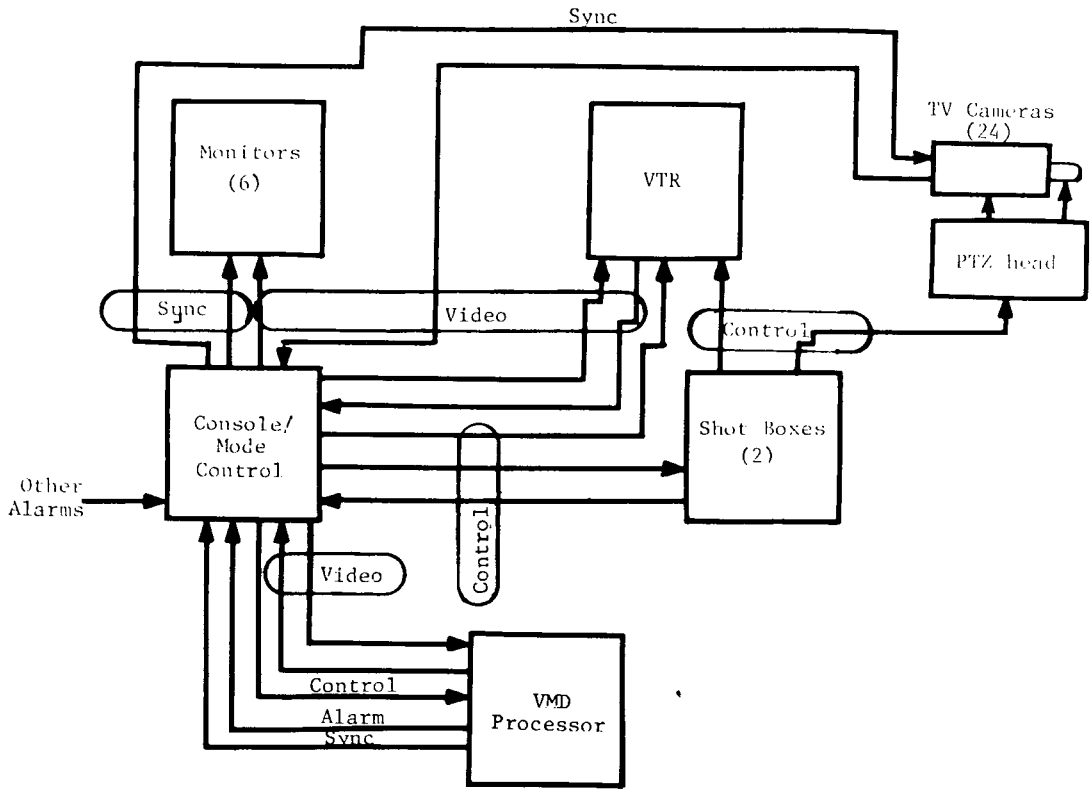


Figure A-24(a). Block Diagram of a PTZ VMD/Assessment System

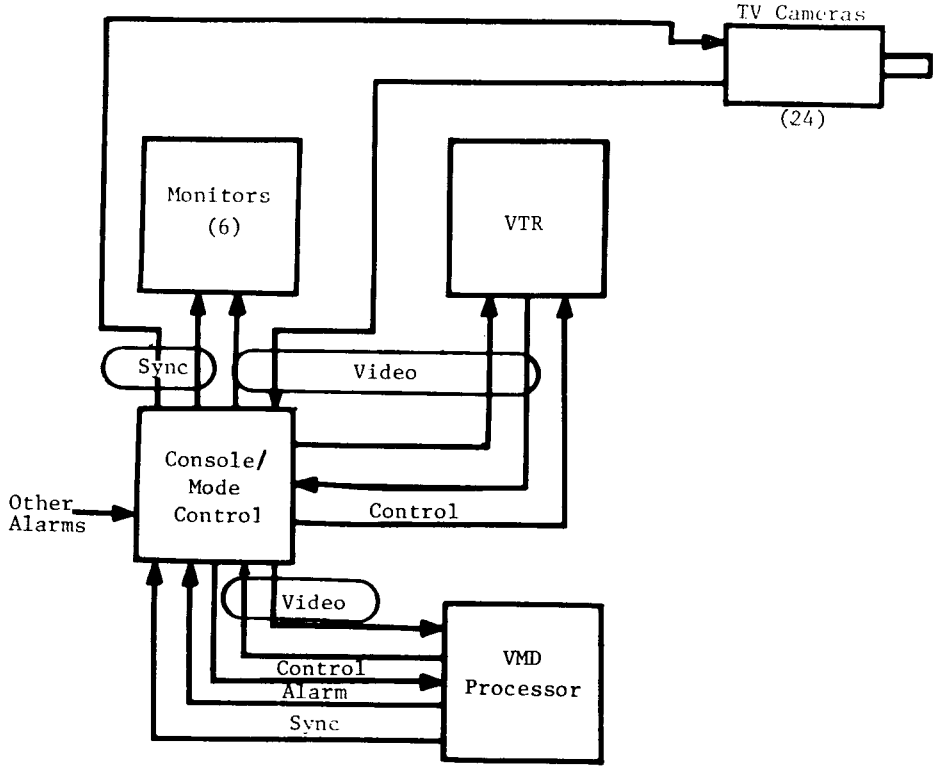


Figure A-24(b). Block Diagram of a Staring VMD/Assessment System

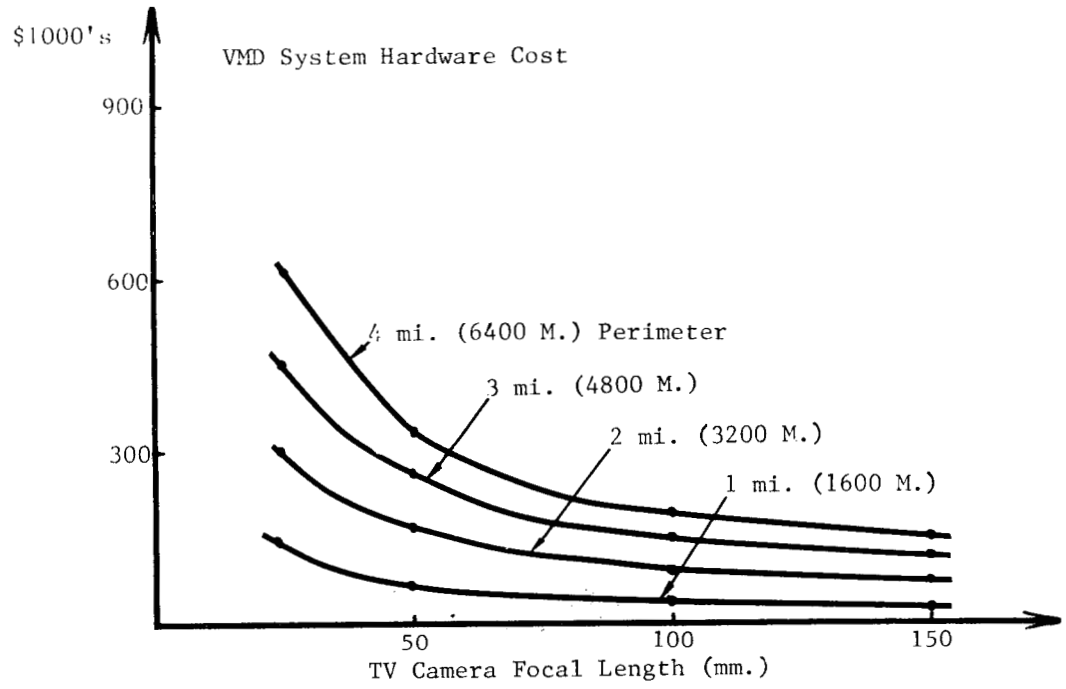


Figure A-25(a). VMD System Cost Versus TV Camera Focal Length

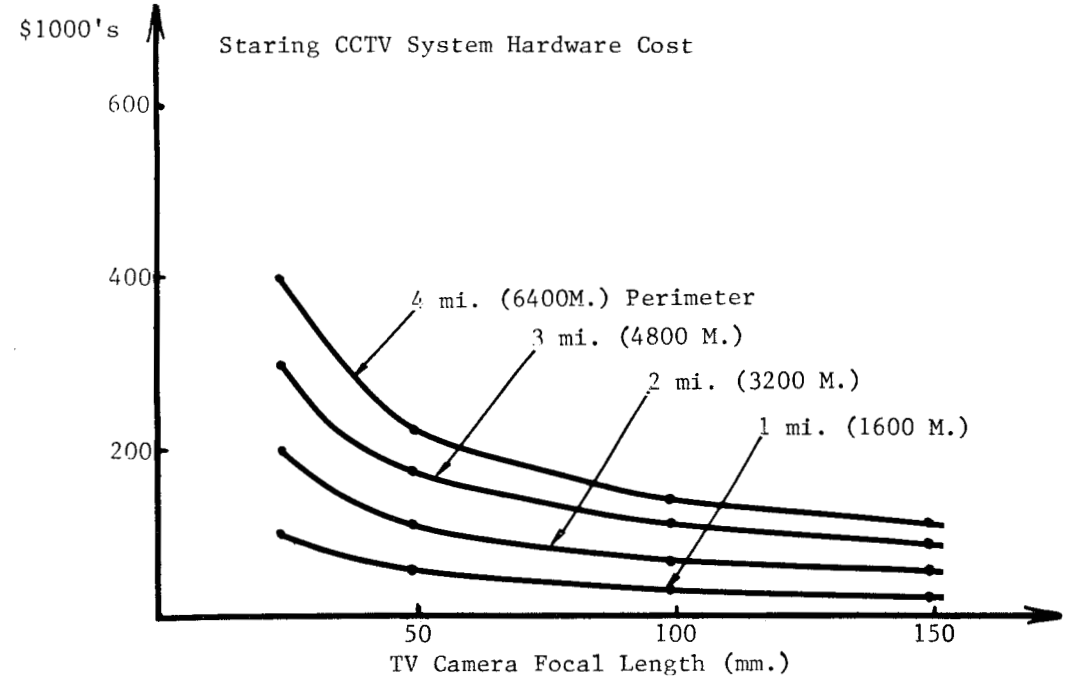


Figure A-25(b). CCTV System Cost Versus TV Camera Focal Length

length may be selected to give a distance coverage coinciding with the sector covered by the other sensors thus simplifying alarm processing. Here the minimum dimension for unity probability of detection (P_D) is 1 foot.

A.2.6.2 Assumed Intruder Minimum Dimension Versus Cost of VMD System

For staring VMD systems, Figure A-25 shows the CCTV system conditional probability of detection curves for representative size classes of objects. Costs for otherwise similar VMD systems with different Assumed Intruder Minimum Dimensions (AIMD) are shown in Figure A-26. Two perimeter lengths are given, and two different design philosophies of camera coverage are assumed. The impact of having a smaller AIMD will include higher systems costs, greater need for tower/camera stabilization, decreased width of perimeter coverage, and greater probability of false alarm from small objects. On the other hand, assessment capability will be enhanced, as will intruder recognition, though this will be somewhat offset by the narrower fields-of-view in smaller AIMD systems.

A.2.6.3 VMD Sample Area Number Versus Cost of VMD Channel

As discussed earlier, a vital parameter of VMD systems is the number of sample areas per camera channel. A scatter plot (Figure A-27) shows a general trend of sample point number versus VMD cost per channel. Model numbers and manufacturers are shown in Table A-12.

A.2.6.4 Cost Breakdown Figures For Staring and PTZ VMD/Assessment Systems

Table A-13 shows cost breakdowns for the two different types of VMD systems as described earlier, the staring mode VMD system and the Pan Tilt Zoom (PTZ) VMD/Assessment system, again, for a Central Alarm Station (CAS) facility only. Secondary Alarm Station (SAS) video motion detection capability will require duplication of the monitor

Table A-12
REPRESENTATIVE VMD SYSTEMS

POINT	TYPE OF VMD SYSTEM	SAMPLE AREAS	COST PER CHANNEL
A	Wisco Visiguard	338	$ 600
B	Wisco Visiguard	676	$ 800
C	32-channel Videotek MDU4	1024	$1,000
D	16-channel Videotek MDU4	1024	$1,250
E	Wisco Teleguard	4000	$2,500
F	Videotek MDU5 8-camera sequential	16384	$3,000
G	Videotek MDU3	16384	$6,250

console, the VMD channels, and TV camera controls. Added cabling and video signal line amplifiers will be necessary if the central and secondary alarm stations are widely separated.

Though CCTV Motion Detection systems' costs decrease with increasing TV camera lens focal length and increasing coverage per TV camera, it may be advantageous, for assessment purposes, to let the coverage of each TV camera coincide with sectors of other sensors. A "reasonable" value of coverage, 200 meters per TV camera, has been selected as coinciding with 2 microwave lengths and 2 fence sensors, so that alarms from sensors in any given sector can be assessed unambiguously. Thus, three approaches are mentioned in the cost totals: 1) a CCTV-VMD system using 24 cameras to view up to a 4800 meter (2.98 mi.) perimeter in 200 meter segments; 2) another CCTV-VMD system using 16 cameras to view a 4 mile (6437 meter) perimeter, to illustrate the cost advantage inherent with longer focal length TV camera lenses; 3) a PTZ CCTV-VMD system using available hardware to cover either the 4 mile or up to 4800 meter perimeter.

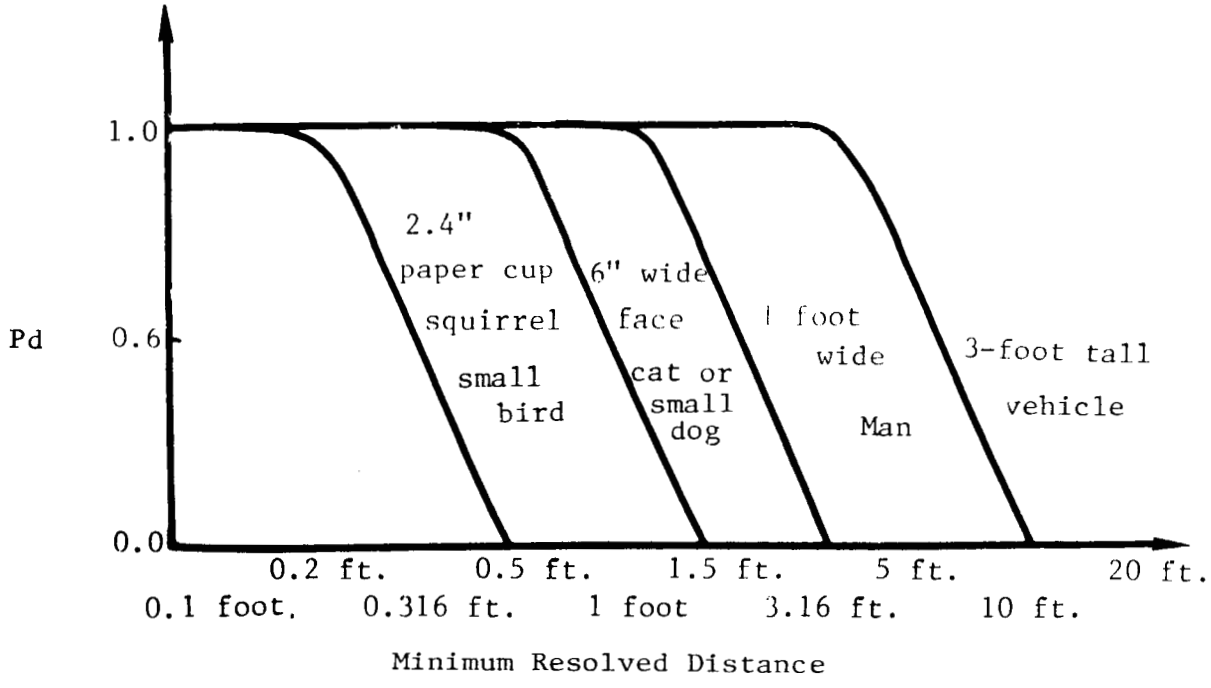


Figure A-26. Video Camera Probability of Detection Versus Minimum Resolved Distance (for 2 cycles)

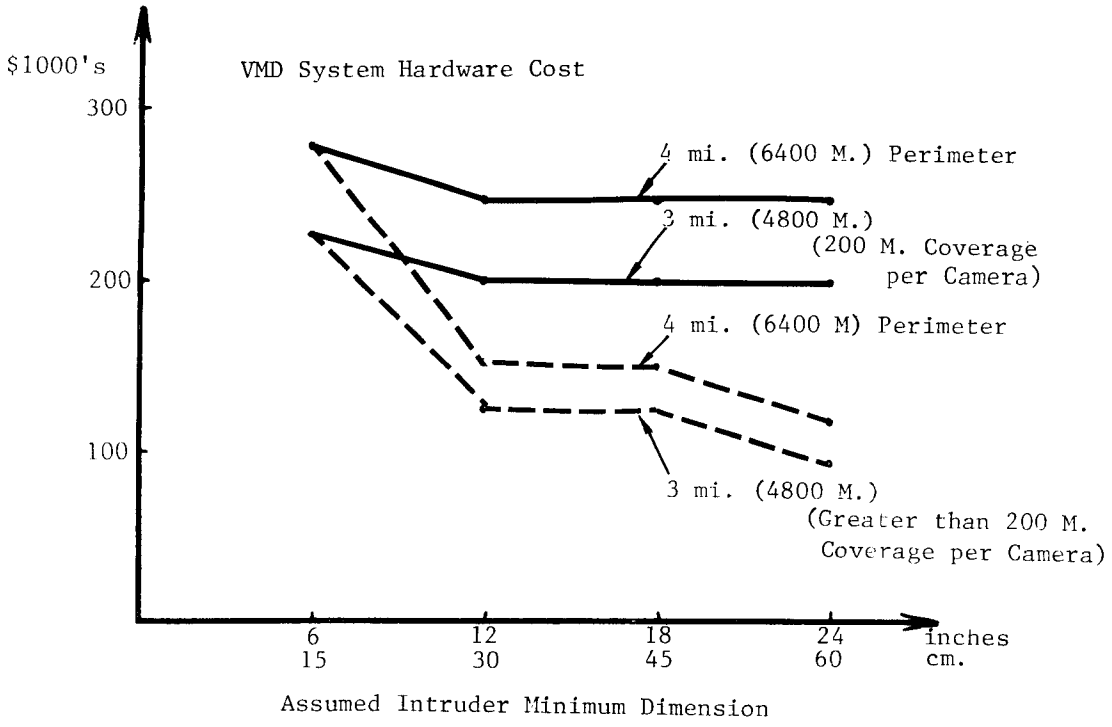


Figure A-27. VMD System Hardware Cost Versus Assumed Intruder Minimum Dimension

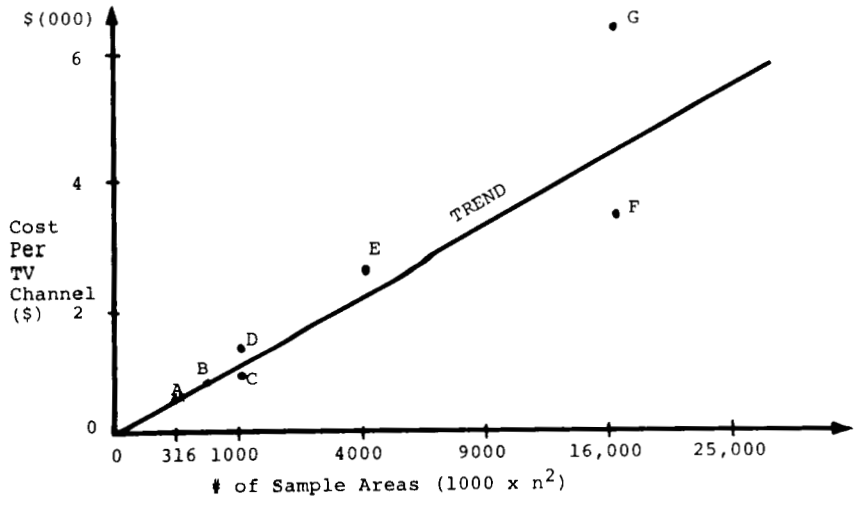


Figure A-28. Scatter Plot of Various Available VMD Systems Cost Versus Number of Sample Areas

A.3 USING EXISTING CCTV SYSTEMS FOR VMD

For less cost than a VMD system with all new parts, existing CCTV system components can be integrated into the proposed VMD systems.

A.3.1 EVALUATION OF EXISTING SYSTEM

Before the final design of the proposed VMD system, a thorough evaluation of the existing CCTV system should be made. All directly applicable already existing equipment should be retained for the proposed VMD system. Design goals of the VMD system should include making the maximum use of the already existing equipment, to minimize cost without compromising the system's performance. In most cases, incompatibility between existing equipment and the proposed VMD systems can be overcome by retrofitting and modification, but sometimes incompatible equipment will need to be replaced by new equipment.

A.3.2 EXAMPLE COST CALCULATION FOR VMD RETROFIT

For example, consider a hypothetical CCTV installation with the following characteristics. VMD will be added to the system, whose

Table A-13

VMD SYSTEM COST BREAKDOWN

ORDER OF COST	ITEM	QTY/NO.	UNIT COST	TOTAL COST
(a) 4800M (2.983 mi.) Perimeter, 24 Cameras				
1	Wisco Teleguard 400-4000	24 channels	$2500/chan.	$60,000
2	35' Poles	24	$1000 ea.	24,000
3	Video Transmission System			22,656
4	RCA TC-2011/u75	24	$ 775 ea.	18,600
5	External Sync Coax Line	8 miles	$0.25 ft.	10,560
6	Environmental Enclosures	24	$ 220 ea.	5,280
7	6-Monitor Switching Console			3,500
8	Video Tape Recorder	1	$1000 ea.	1,000
			Grand Total	$145,596
			Cost per Channel	$ 6,066.50
(b) 4 Mile (6437M) Perimeter, 16-Channel				
1	Wisco Teleguard 400-4000	16 channels	$2500/chan.	$40,000
2	Video Transmission System			19,504
3	35' Poles	16	$1000 ea.	16,000
4	External Sync Coax Line	8 miles	$0.25/ft.	10,560
5	RCA TC2011/u	16	$ 570 ea.	9,120
6	Lenzar 150mm AI lens	16	$ 489 ea.	7,824
7	Environmental Enclosures	16	$ 220 ea.	3,520
8	6-Monitor Switching Console			3,500
9	Video Tape Recorder	1	$1000 ea.	1,000
			Grand Total	$111,028
			Cost per Channel	$6,939.25
(c) 4 Mile (6437M) or 4800M (2.983 mi.) Perimeter, 24 PTZ Cameras 100% Redundancy in Coverage				
1	Wisco Teleguard 400-4000	24 channels	$2500/chan.	$60,000
2	RCA TC2011/uZ0	24	$1500 ea.	36,000
3	Shot Boxes	24	$1020 ea.	24,480
4	35' Poles	24	$1000 ea.	24,000
5	TV Control Cable	20 miles	$0.219/ft.	23,126.40

Table A-13

VMD SYSTEM COST BREAKDOWN (Continued)

ORDER OF COST	ITEM	QTY/NO.	UNIT COST	TOTAL COST
6	Video Transmission Sys.			22,656
7	PTZ Heads	24	$ 540 ea.	12,960
8	External Sync Coax Line	8 miles	$0.25/ft.	10,560
9	Twin Joystick Controls	3 pair	$1850 pair	5,550
10	Environmental Enclosures	24	$ 220 ea.	5,280
11	6-Monitor Switching Console			3,500
12	Video Tape Recorder	1	$1000 ea.	1,000
			Grand Total	$229,112.40
			Cost per Channel	$ 9,546.35

(d) 2 Mile (3218M) Perimeter, 16 Cameras

1	Wisco Teleguard 400-4000	16 channels	$2500/chan.	$40,000
2	35' Poles	16	$1000 ea.	16,000
3	RCA TC-2011/u75	16	$ 775 ea.	12,400
4	Video Transmission Sys.			10,704
5	External Sync Coax Line	5 miles	$0.25/ft.	6,600
6	Environmental Enclosures	16	$ 220 ea.	3,520
7	4-Monitor Switching Console			2,400
8	Video Tape Recorder	1	$1000 ea.	1,000
			Grand Total	$92,624
			Cost per Channel	$ 5,789.00

(e) 1 Mile (1609M) Perimeter, 8 Cameras

1	Wisco Teleguard 400-4000	8 channels	$2500/chan.	$20,000
2	35' Poles	8	$1000 ea.	8,000
3	RCA TC-2011/u/75	8	$ 775 ea.	6,200
4	External Sync Coax Line	3 miles	$0.25/ft.	3,960
5	Video Transmission Sys.			3,152
6	4-monitor Switching Console			2,400
7	Environmental Enclosures	8	$ 220 ea.	1,760
8	Video Tape Recorder	1	$1000 ea.	1,000
			Grand Total	$46,472
			Cost per Channel	$ 5,809

alarms will then be processed with alarms from other sensors. The present system has the following characteristics:

- 4800 Meter perimeter, 24 cameras
- 200 meter coverage per camera with adequate resolution
- Baseband video transmission on coaxial cable from TV cameras to monitor control panel. Some channels have visible 60 Hz modulation in the form of "hum bars" which roll slowly up the screen.
- Adequate tower stability in up to 40 mph winds.
- 2 cameras view entrance/exit gates where authorized vehicle, equipment and personnel movement is prevalent.
- Light level is adequate for entire perimeter. Sodium vapor lights are turned on from dusk to dawn by a photo-cell relay.
- All cameras mounted on fixed platforms in appropriate environmental enclosures.
- Chain link fence with barbed wire outrigger surrounds outside perimeter. Fence moves in wind over 30 mph.

This system requires the following action for the above mentioned items.

- 24 cameras will need 24 channels of VMD
- No action needed
- Channels with "hum bars" should be equipped with noise-bucking isolation transformers to prevent ground loop potentials from modulating video signals and to eliminate induced noise. Some channels will require amplification in the coax line and/or triaxial cable.
- If tower instability is troublesome, additional bracing can be added; otherwise, VMD alarms can be ignored on extremely windy days.
- Opaque barriers can be installed shielding the TV camera field of view motion from the camera's view. Alternatively, a programmable VMD unit can be programmed to disregard movement in authorized areas.
- No action needed except perhaps setting photocells to turn lights on and off in fairly bright conditions.

- No action needed.
- Fence may require painting in a dull black or dark gray color to avoid glare from shiny surfaces. A programmable VMD unit could be programmed to disregard fence movement.

Table A-14 shows parts costs of this conversion for typical quantities of items needed for retrofit with VMD.

Table A-14

PARTS COST OF TYPICAL CCTV RETROFIT WITH VMD SYSTEM

Item	Qua./No.	Unit Cost	Total Cost
Video Motion Detector	24 channel	$2500/chan	$60,000
Video Noise Bucking Isolation Transformers and Triaxial Cable	6	$ 500/chan	3,000
Opaque Barriers	4	$1000 ea.	4,000
Flat Black Paint	200 gal.	$ 10/gal.	2,000
		Grand Total	$69,000

A.4 STARING VMD SYSTEM USING EXISTING PTZ CCTV SYSTEM AS AN EVENT KEYED ASSESSMENT SYSTEM

Where an existing Pan-Tilt-Zoom (PTZ) CCTV system is installed and operational, a staring VMD system could be added to the system as an alarming sensor system, directing the existing CCTV system to observe the area of the alarm for assessment. The only advantage of this approach is redundance in the assessment coverage of the perimeter. This approach has the disadvantage of yielding no cost reduction from employing existing equipment as in the last section. Maintenance and life cycle costs are increased over that of the assessment-only or VMD-only system due to the greater number of components. The VMD system itself is an alarming sensor which gives assessment capability as well as an alarm. Therefore, it is probably wiser to retrofit the existing CCTV system as discussed in the previous section if VMD is contemplated. Cost Tables A-14 and A-15 should be compared when considering the addition of a VMD system to an existing CCTV system.

Table A-15

COST FOR VMD/CCTV ASSESSMENT SYSTEM FOR 4800M, 24-CAMERA SYSTEM FOR VMD AND 24 CAMERA CCTV SYSTEM

Item	Number	Unit Cost	Total Cost
VMD System	1	$145,596	$145,596
Shot Boxes (Optional)	24	1,020	24,480
		Grand Total	$170,076

A.4.1 DESCRIPTION OF SYSTEM

A staring VMD system using the existing CCTV system as assessment would employ the existing CCTV system and the VMD processor in parallel, except that the CCTV system can be triggered by VMD and other alarms to view alarmed areas. A block diagram appears in Figure A-28.

Interaction between the VMD and CCTV systems would be facilitated by the shot box control which allows PTZ response to alarms as well as response to console control.

Staring CCTV systems could incorporate a logical interface from a VMD system to view the alarmed area. This would probably be unnecessary, since the VMD unit would automatically display the alarmed scene.

A.4.2 SAMPLE COST CALCULATIONS

Since the VMD system is unchanged from the staring approach listed in Section A.2, the cost for the VMD with CCTV assessment will be the total of the staring VMD cost total added to the total listed in Table A-15.

A.5 VMD SYSTEM COMBINED WITH OTHER SENSORS

To increase the probability of detection and decrease the false alarm rate of the perimeter security system, a staring CCTV in the VMD mode can be added as an intrusion sensor whose alarms are logically combined with other intrusion sensors. Additionally, the CCTV would fill the assessment function, if not already installed for that purpose.

Description/Examples: Logical combinations of alarms could include AND, OR, time-sequenced layered, or more complex logic to apply to alarms form various sensor types. Here, the VMD system is the basic staring VMD system developed in Section A.2, and the other sensors could include E-field, microwave, fence sensors, etc. For an example, a block diagram of a layered sensor logic sensor array with microwave and VMD is shown in Figure A-29.

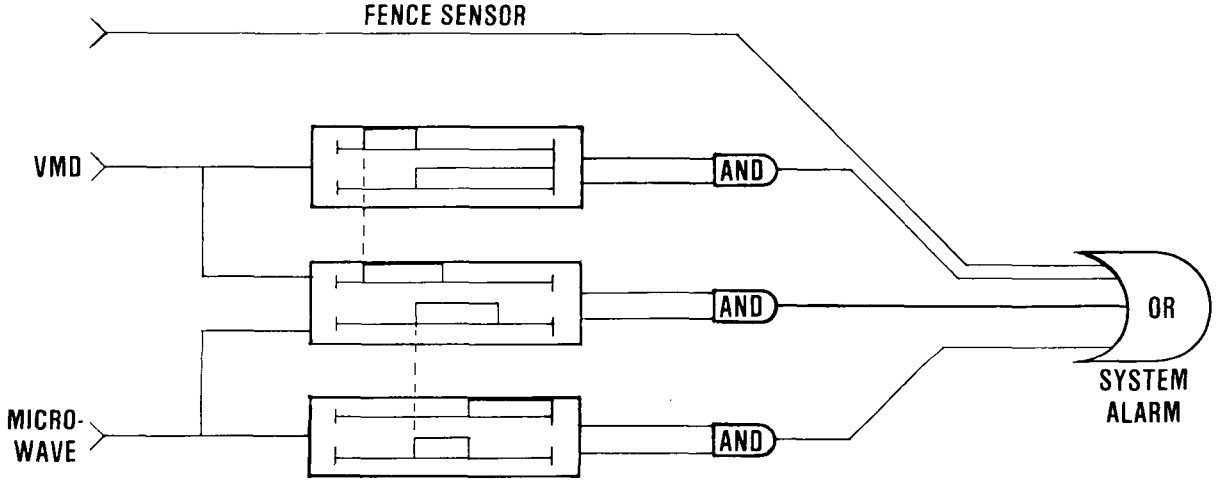


Figure A-29. Layered Sensor Logic for Tautline, VMD, and Microwave Sensors

If the taut line type fence sensor is tripped, the system alarm will be triggered. If either the VMD or microwave sensors are triggered exclusively of the other, no alarm will be triggered unless they are triggered again in 10 to 60 seconds. If the VMD and microwave sensors

are both triggered within 20 seconds of each other, the system alarm will be triggered. If either the VMD or the microwave sensors are exclusively triggered twice within a 10 second period, no alarm will be triggered. This scheme works well with high probability of detection, high nuisance or false alarm rate sensors such as microwave and VMD, and yet allows inclusion of other low false alarm rate sensors such as taut line fence sensors.

Where a CCTV system is already present and coverage is adequate, the addition of a VMD system layered with other already existing sensors may be the most cost-effective means of improving intrusion detection system effectiveness.

In view of upgrade plans (for many nuclear power plants) to incorporate CCTV for alarm assessment, VMD as a sensor layer add-on is therefore recommended for consideration as a retrofit.

A.6 CCTV SYSTEM COMPARISON

To give a quick comparison of the different characteristics and costs of each CCTV system approach mentioned, Table A-16 presents the CCTV system approaches mentioned in this report together with their salient characteristics. Most categories in this chart are self-explanatory. However, the MTBF is qualified on the basis that it is calculated from vidicon failure rates assuming yearly (9000 hr.) scheduled replacement. Difficulty of interfacing is based on 3 items:

- Does CCTV system coverage fail to coincide with other sensor coverage sectors?
- Does the CCTV system employ the Pan-Zoom-Tilt feature?
- Is the CCTV system a video motion detector (VMD) whose alarms must be processed with those from other sensors?

If all answers are negative, the CCTV system is considered trivially difficult to interface with other sensor systems. One affirmative to these questions places the CCTV system in the "moderately difficult" category. Two or three affirmatives class the system as difficult to interface with other sensor systems. If the design criteria in this

Table A-16

CCTV System Approach Comparison

System Type	Perimeter Length	Number of Cameras	Coincide with other Sectors?	Assessment or Alarming Sensor?	Redundancy in Coverage %	Parts Cost $(000)	Requires Existing CCTV System?	Vidicon Probable MTBF (Hr)	Difficulty to interface with other sensors?
Staring CCTV	4800 m. (2.98 mi)	24	yes	assess only	0%	222.6	no	3125	Trivial
Staring CCTV	4 mi. (6437 m.)	16	no	assess only	0%	246.1	no	4690	Moderate
PTZ CCTV	4800 m.	24	yes	assess only	Pan Tilt Zoom 100%	305.1	no	3125	Moderate
Staring VMD	4800 m.	24	yes	assess and alarm	0%	275.3	no	3125	Moderate
Staring VMD	4 mi.	16	no	assess and alarm	0%	283.9	no	4690	Difficult
PTZ VMD	4800 m.	24	yes	assess and alarm	Pan Tilt Zoom 100%	358.8	no	3125	Difficult
Staring VMD Retrofit on existing CCTV System	4800 m.	24	yes	assess and alarm	0%	69.0	yes	3125	Moderate
Staring VMD Adjunct to Existing CCTV System	4800 m.	24	yes	assess and alarm	Full Time 100%	170.4	yes	3125	Moderate

appendix are followed, probability of detection for all alarming systems here can be considered to be 99%. Correctly installed VMD systems typically can be adjusted to give false or nuisance alarm rates of 1 every 2-3 hours.

A.6.1 RECOMMENDATION

Where an existing CCTV system is installed, it is recommended that VMD be retrofitted to the CCTV system as described in Section A.3. If a CCTV system has not already been installed, the staring VMD system covering the perimeter in 200 m. sectors is recommended. In both cases the CCTV system is used for assessment as well as for motion detection.

REFERENCES

1. RCA Electro-Optics Handbook, 1974, p. 202.

2. Luxemberg, H. R. and Kuehn, Rudolf L., Display Systems Engineering, 1968, McGraw-Hill Book Company, pp. 157-158.

3. Intrusion Detection Systems Handbook, Volume 1, Sandia Laboratories, November 1976, Revised October 1977.

4. Video Tek Notes, Video Tek Inc.

5. Video Tek Report, "Pole Stability Considerations".

6. Roark, Raymond J., Formulas for Stress and Strain, 1965, McGraw-Hill, pp. 104-109.

7. Hoerner, Aerodynamic Drag - Priv. Pub.

8. Sand 79-0984C The Engineering and Economics of Lighting for Closed Circuit Television (CCTV) Security Alarm Assessment, R. E. Faucett and F. L. Schow, October 1979.

9. NUREG/CR1327, Nuclear Regulatory Commission.

10. Basic Considerations for Assembling a Closed Circuit Television System, Nuclear Regulatory Commission, May 1977.

11. Wood-Ivey Systems Company 400-4000-4 Operation and Maintenance Manual.

12. IES Lighting Handbook (two volumes) Illuminating Engineering Society of North America, 1981.

APPENDIX AA

CONTENTS

APPENDIX AA

AA.1 FIELD TESTING AND EVALUATION

It is proposed to demonstrate that the processor will be able to reliably perform its functions in a real environment, and over a period of time in which a perimeter sector may experience environmental changes, nuisance alarms, and genuine intrusion events.

The E-Systems Multi-Sensor Test Facility and sensor test bed will be utilized to evaluate the processor in conjunction with the following sensors:

- E-Field standing line
- Taut Wire Fence
- Buried Line Intrusion Detector (BLID)
- Video Motion Detection (VMD)

AA.2 FALSE ALARM CORRELATION

In order to have a video correlation (assessment) of alarm events, it is proposed to utilize a CCTV camera and recording console. VMD evaluation, planned for accomplishment in 1981 as an uncombined sensor layer, is proposed to be repeated as part of the processor evaluation whereby its outputs would be combined with two other layers in the above list.

Recording of weather data from the on site weather station is also proposed for correlating with alarm events. This will provide another time annotated basis for explaining false or nuisance alarms with the objective of setting thresholds or modifying the sensor field to minimize them.

The recording system will enable both low level and high level alarm counts to be time annotated and accumulated to permit final analysis of overall intrusion system performance.

AA.3 INTRUSION TRIALS

Activities to exercise the processor are listed below. These should be considered as representative test procedures which may be modified as required by results of the system analysis and design phases.

1. Adjust sensor layers to vendor specifications. Connect to alarm processor. Include VMD unit, TV camera, video tape recorder, TV monitor. TV camera should be fitted with a 75mm fixed lens on a tower approximately 35 feet high. Observe the maximum range (1075 ft.). First test VMD performance as a single sensor layer.
2. With Man/Bar target at maximum range, observe monitor to see relative size of target. Have a subject walk around the neighborhood of the target in highly conspicuous clothing and again with camouflaged clothing. Note presence or absence of alarm, and the illumination level and quality (direct or diffuse). Perform this step with hit counter set on minimum number of hits required for an alarm, then set switch in next higher level and repeat until this step has been performed for each position of the switch. In further repetitions of this step, only test for a minimum, a maximum and an intermediate amount of hits.
3. Perform step 2 in ambient light levels for diffuse (cloudy day) illumination and direct illumination (clear day) as thoroughly as meteorological conditions and schedules permit. Record these tests on videotape and catalog carefully.
4. Devise a litter simulation by using a paper cup on a fishing line. Cast the cup and draw it across the middle of the TV camera field of view at ranges of 800 feet, and about 400 feet. Note presence of

alarm with and without VMD processing aids. Perform this step for 4 cases of illumination from clear bright to diffuse dark. Record all test on video and catalog carefully.

5. Using all processing aids necessary to optimize P_D/ False Alarm Rates, arrange video camera for a range of 300 feet to 1075 feet from 35 feet height with the Man/Bar Target at very top of the FOV. Record all alarms over a 24 hour period. Also include video tape of subject with camouflaged and noncamouflaged clothing during this period.
6. As weather permits, record step 2 for inclement meteorological conditions such as rain, fog, high winds, etc.
7. Complete connection of all layers to processor and complete post processor recording instrumentation.
8. Deliver the intruder threat to the multi-layered perimeter detection system with the objective of determining whether or not detection probabilities will have been degraded by the establishment of the necessary processor time windows for each layer.

Human subjects should be employed to introduce elements of randomness and surprise likely to be found in deliberate intruders. For the following tests, the human subject should not exceed 45 kg in weight and should be clean of ferrous metal including nails in shoes. A string or rope should be laid on the ground to indicate buried sensor locations. The following examples of Human Testing have been used by Sandia Laboratories.

AA.3.1 WALK TEST

Test personnel should walk at a normal rate perpendicular to the sensor line. Walk tests should be repeated at intervals of approximately 1 meter segment.

AA.3.2 RUN TEST

Run tests should be repeated at intervals of approximately 3 meters or less for a minimum of 33 runs over each 100-meter segment. Running speed should approximate 5 M/sec.

AA.3.3 ROLL TEST

Roll tests (very slowly roll across the transducer with the body parallel to the transducer, arms held close to the body, and feet together) should be repeated at intervals of approximately 3 meters or less. At least 50 roll tests must be included over every hardtop surface crossing the transducer. If failure occurs on the hardtop surface, additional roll tests should be conducted to determine performance at these locations.

AA.3.4 SHUFFLE WALK TEST

This test is performed by very slowly shuffling toward the sensor with arms held motionless at the side. Both feet must remain on the ground during the shuffle walk, and steps should be limited to about 5cm in length. Shuffle walks, 50 each, should be directed toward the transducer whose location will be identified by small surveyor's flags. Each walk shall start at maximum range, proceed to and over the sensor, to an equal distance on the other side.

AA.3.5 SIMULATED CRAWL TEST

To eliminate actual human crawl tests and to obtain more repeatable results, the crawl test can be performed by dragging a 30cm diameter aluminum sphere across the detection zone. A metal sphere can be successfully utilized to simulate the various modes of human locomotion. This is true because movements along any given path cause rather sinusoidal phase variations that are independent of the target shape. The sphere is ideally unique because it is not aspect sensi-

tive. The sphere is mounted to a thin non-metallic platform such as plywood, and pulled across the zone with a small rope which is long enough for the person pulling the rope to be located outside the microwave field. Drag tests should be performed at 1-M intervals over the full detection zone.

A.3.6 MULTIPLE TARGET BEHAVIOR

Response of the sensors to multiple targets should be assessed. Two targets should be programmed or coordinated to approach the sensor array from opposite corners of the test bed and to arrive there simultaneously. Target velocities should be .5 meters per second and 5 meters per second. Five trials should be recorded at each velocity.

A.3.7 BRIDGING

Bridging trials test the vulnerability to defeat of the fence and surface sensors. Bridging paraphenalia should include two 4 meter long two-by-fours for laying on the ground over buried sensors. Alternatively, the two-by-fours can be used in conjunction with two 3 meter tall A-frames to form an adjustable aerial bridge. Twenty attempts should be made in each defeat mode for each layered system.

A.3.8 SPOOFING

A competition might be considered among those who think they can defeat the sensor systems and a reward offered to any that succeed. This should uncover sensor and system vulnerabilities and shortcomings and thus contribute to credible countermeasure schemes. For instance, one might wish to mimic an animal gait or a drunkard's walk, or shuffle on skis. Additionally, it will be interesting to view the response of the system to a squad in lockstep, or to a mock march of demonstrators out of step.

APPENDIX AB

CONTENTS

APPENDIX AB
Video Motion Detector Test Reports

AB.1 INTRODUCTION

As part of the IR&D efort to investigate a variety of intrusion detection sensors, a digital video motion detection (VMD) system was assembled with its TV camera on a rigid metal support structure overlooking the E-Systems intrusion detection sensor test range. Probability of detection measurements and false alarm experiments were then performed. After testing at the intrusion detection test range, the VMD system was reassembled with the TV camera mounted on a wooden telephone pole for the tower vibration test. This report describes the procedures used, results of, and conclusions drawn from these tests.

AB.2 DESCRIPTION OF THE WOOD-IVEY SYSTEMS COMPANY 400-4000 VMD PROCESSOR

The VMD unit tested here is a Wisco Teleguard 400-4000-4 (Ref: Sec. 4.3, Wisco O&M Manual) digital VMD processor which accepts video signals from up to 4 TV cameras. The video signals are sampled at times corresponding to picture elements (pixels) at 4000 locations within the scene. Each sample is digitized, assigned a number and stored in memory. Samples from subsequent frames are compared to the stored samples for brightness deviations. The deviations are also stored so that when a definite pattern of these deviations (corresponding to an expected intruder's signature) occurs, an alarm is generated. During an alarm, those pixels activated by the intruder are displayed as trace signals on a video monitor, tracing the intruder's path. To generate an alarm, at least one of the pixels must have a brightness level change of $\pm 6\%$ of the full scale brightness. This level of change generates an alert point. The

number of alert points required to generate an alarm (from 1-15) is set by the error rate counter switch. The error rate counter helps the VMD processor to ignore false alarms caused by electrical noise, as well as some nuisance alarms caused by very small disturbances in the TV camera field of view. The error rate counter is referred to elsewhere as the "hit counter". To reduce false alarms due to slow brightness changes in the TV camera field of view, the pixel samples in memory are updated at time intervals of a few seconds.

The VMD processor has video outputs for two TV monitors and a video tape recorder for assessment purposes. The Sequencer monitor output is sequenced through the TV cameras' channels while the Motion Detector (or Alarm) monitor remains blank during non-alarm conditions. When one channel is alarmed, the previously blank Motion Detector monitor displays the alarmed scene. If another channel is alarmed, it is displayed on the Sequencer monitor, while subsequent alarms are sequenced through the Sequencer monitor. The VMD processor also has a set of relay contacts to activate a video recorder during alarms and/or allow alarm status to be recorded or combined logically with other alarms.

The next section deals with the setup and probability of detection testing of the VMD processor.

AB.3 PROBABILITY OF DETECTION TESTS

The purpose of the probability of detection testing was to establish whether the video motion detector attained at least a 90% probability of detection with a 95% confidence level. Several different approaches were tried in attempts to traverse a 20 foot-wide area without being detected, by walking, crawling and rolling. Walking trials were performed in various light levels to demonstrate VMD system performance in low light levels.

AB.3.1 PROBABILITY OF DETECTION AND CONFIDENCE LEVELS

An estimate of the VMD processor's probability of detection (P_D) is made by performing experiments (attempted intrusions) which result in either successes (detections of the intrusions) or failures (evasion of detection). The proportion of successes in the number of experiments is then called a point estimate or a sample estimate of the probability of success of detection, and has an accuracy bound that is determined by the number of tests performed.

For additional trials, the probability of detection may or may not match the original point estimate but will fall within upper and lower limits of confidence. The width of the confidence interval is a function of the number of trials and is a binomial distribution centered around the point estimate as the mode for the same number of trials.

The Nuclear Regulatory Commission (NRC) has stated that sensors for perimeter security at nuclear power plants should have a probability of detection of 0.9 with a 95% confidence level. In this they are stating that testing of the sensors should establish the lower 95% confidence limit at a proportion of success or probability of detection (P_D) estimate of 0.9. Table AB-1 shows the number of experiments (tests) needed to establish this.

AB.3.2 PROCEDURE

The VMD system was configured as shown in the block diagram in Figure AB-1. The video tape recorder was used to log the action in the scene and record time and date information. Figure AB-1 shows the geometry of the intrusion detector with respect to the VMD system TV camera.

Man and bar targets were set at ranges of 500 feet and 1000 feet from the TV camera. The TV camera was a 2/3" Ultricon vidicon camera having a 12.5-75.0 mm zoom lens with a remote zoom and focus control. The camera mounting height was approximately 43 feet from ground

Table AB-1

Lower 95% Confidence Limits for P_D

Total No. of Tests (sample size)	Minimum Number of Successful Detections	Maximum Number of Detection Failures	Minimum Acceptable Point Estimate of P_D
30	30	0	30/30 = 1.0
40	39	1	39/40
50	48	2	48/50
60	57	3	57/60
80	76	4	76/80
90	85	5	85/90
110	104	6	104/110

level, and was aimed so that both sets of man and bar targets were included in the field of view. Two walk paths for the test trials were established at roughly 550 feet from the camera, one inside and one outside the intrusion detector test range fence. Another walk path was established at a range of 1000 feet, immediately in front of the man and bar targets at that range. During the tests, the following items were logged: time, subject,presence of VMD alarm, illumination level and quality, VMD processor control settings, remarks, and electrodynamic transducer setting (not used on probability of detection tests). The test procedure originally involved having the test subject dress in camouflaged clothing. Later this was dropped, since the camouflage had a high contrast with the background vegetation. The test subject was directed via 2 way radio to proceed back and forth across a 20 foot length of the walk path. Alarms generated by the test subject were noted on videotape and in the logbook, and appear in Table AB-1.

AB.3.3 WALKING TESTS

The first attempt at a walk test was made at a range of 550 feet with the video motion detector set at a 5 bit algorithm (6.25% contrast

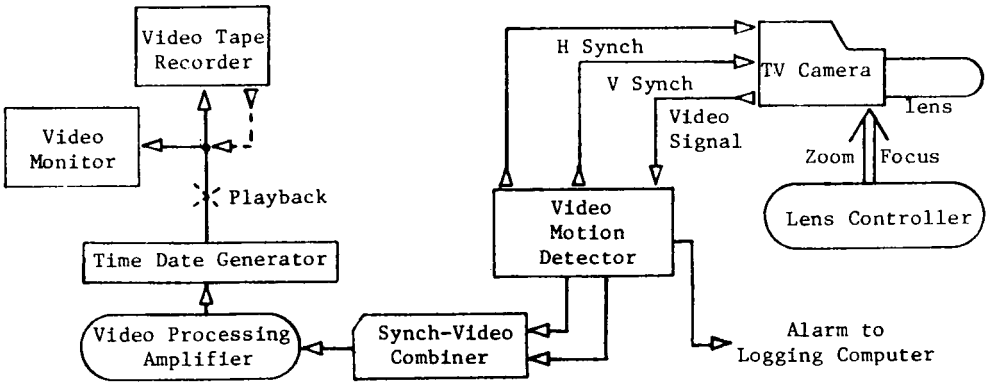


Figure AB-1. Block Diagram of Video Motion Detection (VMD) System

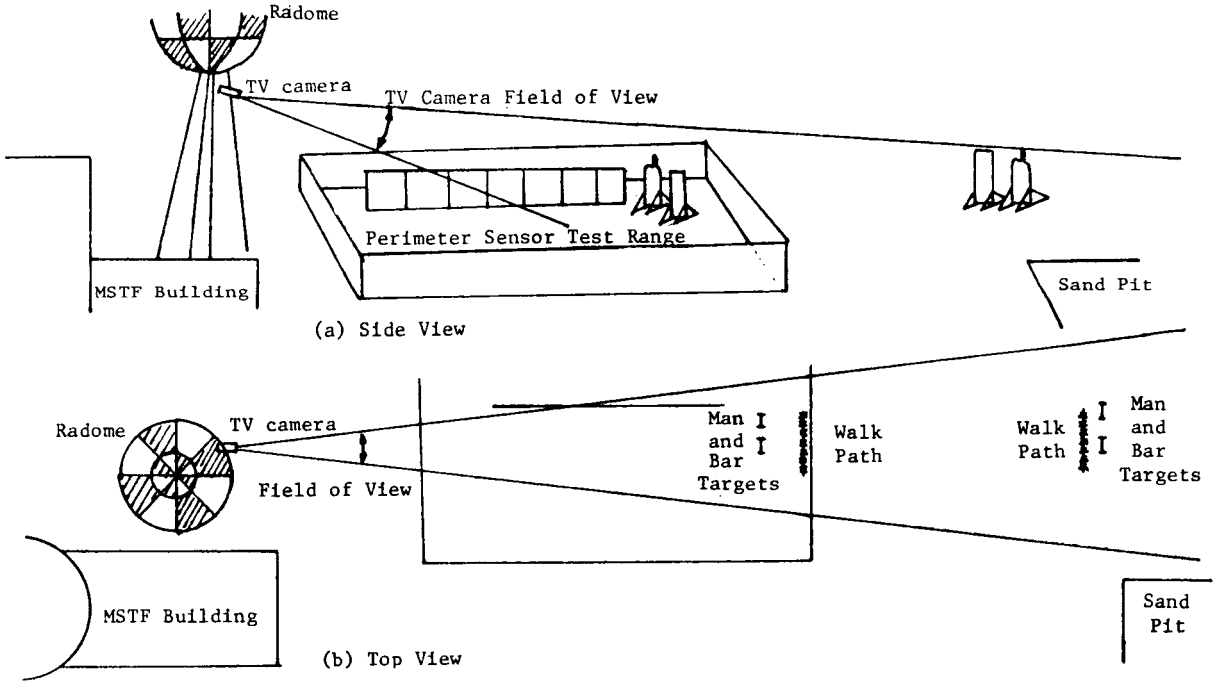


Figure AB-2. Geometry of TV Cameras Field of View

sensitivity) which alarmed only after 12 exceedances or "hits". It was found at this setting that by walking very slowly an intruder could traverse the 20 foot path undetected. With the hit counter set at 8 hits, a series of 30 traversals were all detected by the video motion detector. All further walk tests were then made at this same setting.

Walk tests were made in various light levels, under nominal light levels of 10^4 footcandles, 10^3 footcandles, 10^2 footcandles, 10 footcandles, 1 footcandle and 0.2 footcandle. All levels except 1 footcandle and 0.2 footcandle afforded at least a 90% P_D with a 95% confidence level. This series of experiments specifically applied to the Ultricon camera used in the test, but established a relationship between light level and probability of detection for a representative VMD system.

Walking trials were also performed with the subject at a range of 1000 feet (305 meters) from the TV camera. Thirty (30) of these trials were attempted, with 30 detections, thus giving a 90% P_D with a 95% confidence level at this distant range.

AB.3.4 CRAWLING TEST

Crawling tests were performed together with the walking test at 12 hits to show results for a relatively more surreptitious intruder's technique. The first position taken by the crawling subject was crouching on hands and knees with the head towards the camera, and keeping the body down as much as possible. The motion of the crawling subject was to one side, constantly maintaining a minimum frontal area to the TV camera. Whereas the VMD unit, when set at 12 hits, could be spoofed by a walker covering 20 feet in 8 minutes, the crawling subject was able to cover the 20 feet in 3 minutes while evading detection. When the VMD unit was set down to 8 hits, the subject could no longer evade detection. Two more crawling techniques were tried, both of which involved the subject lying in a prone position on the ground. In the second technique, the subject lay broadside to the TV camera and crawled forward across the 20 foot

Algorithm / Category	5 bit 16 hits	5 bit 12 hits	5 bit 8 hits	5 bit 4 hits	5 bit 2 hits	5 bit 1 hit	4 bit 1 hit
WALKING							
550 feet from TV camera Light Level nominally ≈							
10^4 fc		2 spoofs	30/30				
10^3 fc			30/30				
10^2 fc			30/30				
10 fc			30/30				
1 fc			2 spoofs				
0.2 fc			2 spoofs				
1000 feet							
$5X10^3$ fc			40/40				
CRAWLING							
550 feet		2 spoofs	30/30				
ROLLING			39/40 1 spoof				
LITTER DEMO	0/10	0/10	0/10	0/10	0/10	0/10	0/10
NUISANCE ALARM/min. (Vegetation motion in 10 mph wind to 20 mph wind)	1/min	0/min	0/min	0/min	0/min	1(?)	≈15/min
POLE VIBRATION >1/10"							15/min
POLE VIBRATION <1/10"							0/min
INCLEMENT WEATHER			see tape				
WIND MOTION			see tape				
FAST CLOUDS			see tape				
BIRDS			see tape				

Table AB-2. Results of Video Motion Detector Trials

path. In the third technique, the subject faced the TV camera and crawled sideways across the 20 foot path. None of these techniques allowed the subject to evade detection. Thirty (30) trials were performed, of which all were detected, giving a 90% probability of detection with a 95% confidence level.

AB.3.5 ROLLING TEST

The rolling test was performed after the walking and crawling tests, and proved to be the most nearly successful means of crossing the 20 foot path while evading detection. The subject began the rolling test lying prone on the ground facing the TV camera, then began slowly rolling to one side along the path. On the first series of trials with the VMD unit set on the 5 bit algorithm and 8 hits, the subject managed to evade detection twice in 20 trials. However, it was discovered that the VMD unit was adjusted incorrectly, making the contrast change required to exceed the detection threshold about 40% too high. With the VMD unit correctly adjusted, the subject evaded detection only once out of 40 trials, giving a 90% probability of detection with a 95% confidence level for a rolling subject.

AB.4 NUISANCE ALARM TESTING

Although the test range used was not representative of an actual perimeter segment, especially from a nuisance alarm rate basis, tests were conducted on some specific nuisance alarm sources. A litter demonstration and a camera support vibration test were performed. Naturally occurring nuisance alarm sources included moving cloud shadows, birds, lens dewing, wind motion, inclement weather, etc. These phenomena were recorded on video tape for inspection and evaluation. Although no procedure for separating nuisance alarms from false alarms was followed, actual false alarms due to system internal noise were never noticed during the entire test. All alarms noted could be correlated to actual scene changes as viewed by the TV camera.

AB.4.1 LITTER DEMONSTRATION

To simulate litter movement across the TV camera field of view, a fishing rod was used to cast a light-colored "brick" of foam rubber, 3" X 3" X 5" in size, into the field of view. The foam rubber brick was then drawn across the field of view at rates of 2 to 5 feet per second, and presence or absence of alarms was noted for various settings of the video motion detector. Results are shown in Table AB-2. At most normal settings of the video motion detector (5 bits, 2-15 hits) no alarms were generated by the foam rubber brick, indicating good immunity from false alarms caused by single objects having sizes and velocities typical of wind-blown litter.

AB.4.2 SUPPORT VIBRATION TESTING

To simulate wind loading motion of TV camera support towers, the TV camera was mounted as shown in Figure AB-2 at a height of 38 feet on a 12 inch diameter, 40 foot tall wooden telephone pole overlooking roof tops and taxiways in front of aircraft hangars. The TV camera's field of view was 4.9 degrees vertically by 6.5 degrees horizontally. An electrodynamic transducer capable of delivering 50 lbs. of force at frequencies from 1.4 Hz to 20,000 Hz was attached to the wooden telephone pole at its center of percussion (the point at which an applied force transfers only angular momemtum and no translation to the base) to drive the top of the telephone pole into an angular and/or translatory oscillation. The oscillation's amplitude was then measured by noting the excursions taken by vertical and horizontal boundaries as seen on the TV monitor. Two main resonant frequencies were noted in the telephone pole, one at 4 Hz and another at 16 Hz. At 4 Hz it was possible to drive the amplitude of the angular excursion to about 0.34 degrees or 5.9 milliradians, at which point the drastic jerking of the field of view made it apparent that other frequencies besides 4 Hz were being coupled into the oscillations. The 16 Hz oscillation maximum amplitude was 0.18° or 3.2 milliradians. All amplitudes above a perceived 0.042° or 0.74 mr produced alarms from boundaries between light and dark areas. This corresponds roughly to the height of one of the VMD sample areas. The frequency of vibration can be correlated

to a wind velocity for a pole of this geometry by the expression for the vortex shedding frequency of a cylindrical pole in moving air.

$$F = 0.21 \qquad \text{(AB-1)}$$

where F = frequency in hertz
v = wind velocity in ft/sec
d = diameter of pole in feet

Thus a frequency of 4 Hz for this pole corresponds to a wind velocity of approximately 13 mph. However, at this velocity the wind force would be insufficient to excite large deflections. The second frequency, 16 Hz, coresponds to a wind speed of 52 mph, which is equalled or exceeded less than 0.5% of the time and has sufficient force to excite resonance and the large deflections exhibited.

AB.4.3 NATURAL SOURCES OF NUISANCE ALARMS

Nuisance alarm sources which were observed during the VMD System testing included the following:

- birds
- cloud shadows
- dew on the lens and/or the enclosure window
- inclement weather, and
- vegetation movement in wind.

Birds in flight usually did not cause nuisance alarms when they flew through the field of view. However, the radome structure supporting the TV camera was a gathering place for birds. They were often seen flying at close range in front of the camera, causing many nuisance alarms. These alarms may be minimized by TV camera supports and enclosures designed to give no surfaces on which birds could roost.

Cloud shadows from fast moving small cumulus clouds often were of sufficient contrast to cause large scale nuisance alarms from the scene being viewed. Light level measurements in cloud shadows revealed as much as a 60 percent contrast between the shadow and the sur-

rounding lighted area. Cloud speeds ranged from nearly stationary to 20 to 30 feet/second. It is conceivable that weather patterns causing a partial cover of dense, fast-moving clouds could produce an intolerable number of nuisance alarms. To minimize nuisance alarms from cloud shadows, the area covered by the field of view of the TV camera should be kept as small as possible and the auto iris lens on the TV camera should have a very rapid response so as to track sudden light level changes accurately.

Dew on the TV camera lens and the environmental enclosure window became a problem first as scene contrast was washed out, reducing the VMD system's sensitivity to scene motion. Later as the droplets increased in size, nuisance alarms were generated as droplets coalesced in front of the lens. The resulting subtle brightness changes were not easily seen on the monitor screen but readily triggered the VMD unit. The best remedy for the dewing problem is to seal moisture completely out of the environmental enclosure, and to use dessicant in the enclosure to insure that moisture inside the enclosure will not collect on the optical surfaces.

Inclement weather such as rain, hail, blowing dust, etc. produced nuisance alarms by its motion and by obscuring the field of view. Lightning caused sudden light level changes resulting in nuisance alarms. No preventive measures are known for lightning induced alarms, but precipitation's effect on the nuisance alarm rate can be reduced by reducing the range covered from each TV camera.

Vegetation movement caused by wind was a major source of nuisance alarms during VMD system testing. Wind velocities in excess of 10 miles per hour caused enough motion to result in a steady rate of nuisance alarms. During testing, the vegetation motion was ignored in scene areas not of interest by using the diode pins supplied with the VMD unit for masking purposes. This eliminated all but a few nuisance alarms. The site used for testing is not representative of anticipated perimeters, however. While the site used had a large amount of low, brushy vegetation, it is recommended that perimeters be surfaced with gravel, asphalt, tamped earth or closely mowed grass, to reduce the number of nuisance alarms from vegetation movement.

AB.5 CONCLUSIONS

The VMD system as tested represents an intrusion detection sensor with at least a 0.9 probability of detection, but also a nuisance alarm rate around 1 alarm per 2-3 hours; higher rates occur due to clouds, wind, etc. Our testing with various types of intrusion techniques supports at least a 90% probability of detection with a 95% confidence level for human intruders. Specific mechanisms causing nuisance alarms were investigated, the most thoroughly investigated of which was camera support motion. The VMD system was able to tolerate a level of 0.04 degrees or 0.75 milliradians peak to peak angular motion of the TV camera without suffering an incapacitating number of nuisance alarms. This amount was 0.82% of the vertical field of view of the TV camera, and corresponded to the height of one VMD processor sample area. The field of view of the TV camera was 4.9 degrees vertically by 6.5 degrees horizontally. Other nuisance alarm sources, most of them natural sources, combined to make the VMD system alarm as frequently as 10 times a minute, or as infrequently as once every 2-3 hours. Since our test range was not typical of a secure area perimeter, the nuisance alarm rate of a real perimeter would be much lower, probably averaging one alarm every 2-3 hours, except under extreme weather conditions.

AB.6 VIDEO TEK MDU-5 VIDEO MOTION DETECTOR TEST REPORT

A Video Tek MDU-5 Video Motion Detection (VMD) System was assembled with its TV camera on a rigid metal support structure overlooking the E-Systems intrusion detection sensor test range. Probability of detection measurements and false alarm experiments were then performed. This report describes the procedures used, results of, and conclusions drawn from these tests.

AB.7 DESCRIPTION OF THE VMD PROCESSOR

The VMD Unit tested here is a Video Tek MDU-5 digital VMD processor which accepts video signals from up to 16 TV cameras. The video

signals are sampled at times corresponding to 16,384 locations within the scene. Each sample is digitized, and its value is either stored in memory or compared with previously stored sample values already in memory. Scene areas with brightness deviations of a sufficient magnitude will cause sample values to disagree with previously stored values, causing alarms at these points. The MDU-5 processor uses four memories for every eight TV channels for detection of short and long term scene changes. One part (the "fast algorithm") of the processor's algorithm monitors any given channel at intervals of up to 1.87 seconds to detect quick scene changes. Longer-term changes are detected by comparing selected frames with stored values by another part (the "slow algorithm") of the processor's algorithm which revisits each channel at intervals of 3.74, 7.46, 14.92 or 22.4 seconds.

To generate an alarm, a scene brightness deviation from 6% to 12% of the full scale brightness must occur at one of the scene locations sampled by the processor. Deviations must occur in a sufficient number of locations to exceed the alarm counter threshold (or the hit counter) to cause the processor to alarm. The alarm counter threshold is adjustable independently for each algorithm from 1 to 255 alarm points required for a processor alarm. The threshold number is set by connections on a wire-wrap board inside the processor, and should correspond to the number of sensitive areas the smallest expected intruder would encounter in the TV cameras' field of view. Smaller intruders, tiny nuisance alarm sources and electrical noise are discriminated against by the setting of the alarm counter.

The video monitor output of the MDU-5 processor normally displays a blank raster during non-alarm conditions. A manual override switch for each channel allows the display of that channel during non-alarm and alarmed conditions. When an alarm occurs and no manual override is selected, the monitor will cycle through all alarmed channels. Under non-alarmed conditions using the manual override, the monitor will display sensitive areas with normal video, desensitized areas as darkened video and current alarm points as brightened, flickering video. Alarmed scenes show all alarm points that have accumulated since the time of the first alarm as brightened, flickering video, allowing an operator to trace areas of scene disturbances.

The next section deals with the setup and probability of detection testing of the VMD processor.

AB.8 PROBABILITY OF DETECTION TESTS

The purpose of the probability of detection testing was to establish whether the video motion detector attained at least a 90% probability of detection with a 95% confidence level for human intruders. Several different approaches were tried in attempts to traverse a 20 foot-wide area without being detected; running, walking, crawling and rolling.

AB.8.1 PROCEDURE

The VMD system was configured as shown in the block diagram in Figure AB-3. The video tape recorder was used to log the action in the scene and record time and date information. Figure AB-4 shows the geometry of the intrusion detector test range with respect to the VMD system TV camera.

Man and bar targets were set at ranges of 500 feet and 1000 feet from the TV camera. The TV camera was a Sony 2/3" vidicon camera having a 12.5-75.0 mm zoom lens. The camera mounting height was approximately 43 feet from ground level, and was aimed so that both sets of man and bar targets were included in the field of view. A walk path for the test trials was established at roughly 550 feet from the camera, inside the intrusion detector test range fence. Another walk path was established at a range of 1000 feet, immediately in front of the man and bar targets at that range. During the tests, the following items were logged: time, subject, presence of VMD alarm, illumination quality, VMD processor control settings, and remarks. The test subject was directed via 2 way radio to proceed back and forth across a 20 foot length of the walk path. Alarms generated by the test subject were noted on videotape and in the logbook, and appear in Table AB-3.

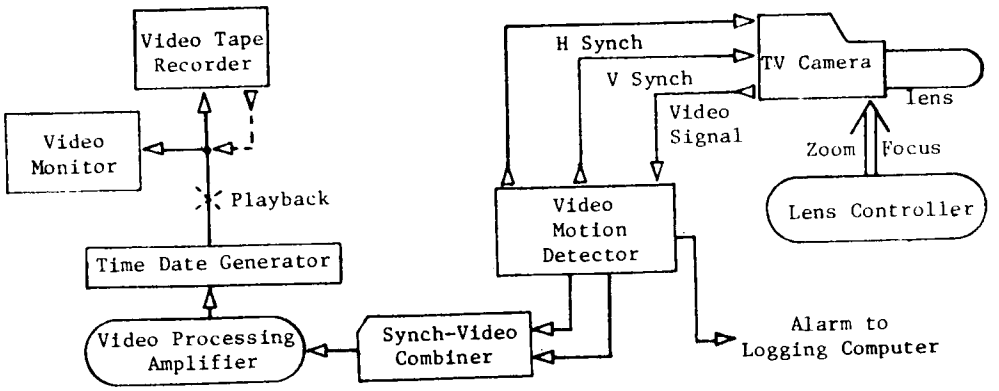


Figure AB-3. Block Diagram of Video Motion Detection (VMD) System

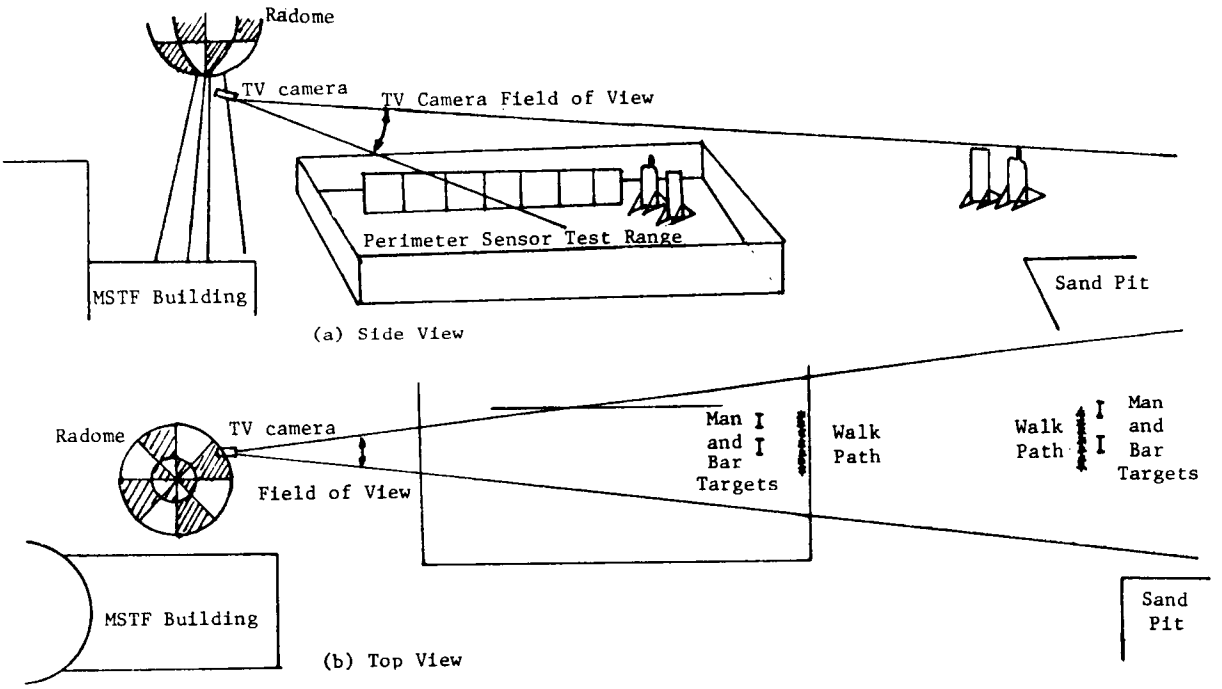


Figure AB-4. Geometry of TV Camera's Field of View

Cycle Time of Slow Algorithm	3.73 Sec.	7.47 Sec.	3.73 Sec.	7.47 Sec.
# Alarms Fast Algorithm	6	6	2	2
# Alarms Slow Algorithm	6	6	6	6
Category				
Walking 550 feet	30 detections/ 30 trials	30/30		
Walking 1000 feet			30/30	
Running 550 feet	22/24 2 evasions of detection		30/30	
Crawling 550 feet	30/30			
Rolling 550 feet			4/5 1 evasion of detection	30/30
Litter Demo 550 feet	0/10		30/30	
Cloud Shadows			see tape	see tape
Wind Motion			see tape	

Table AB-3. Results of Video Motion Detector Trials

AB.8.2 WALKING TESTS

The first walk test was made at a range of 550 feet with the VMD processor set to alarm after 6 alarm points occurred, and with a 3.73 second slow algorithm revisit time. At this setting, a series of 30 traversals were all detected by the video motion detector. Another walk test was made with the VMD processor set to alarm after 6 alarm points and with a 7.47 second slow algorithm revisit time, also yielding 30 detections of 30 traversal attempts.

Walking trials were also performed with the subject at a range of 1000 feet (305 meters) from the TV camera. The VMD processor was set to alarm after 6 alarm points on the slow algorithm or 2 alarm points on the fast algorithm; and a 3.73 second slow algorithm cycle time. Thirty (30) of these trials were attempted, with 30 detections, thus supporting at least a 90% P_D with a 95% confidence level for each of these three scenarios.

AB.8.3 CRAWLING TEST

Crawling tests were performed together with the walking test at the original 6 alarm setting with a 3.73 second slow algorithm cycle time to show results for a relatively more surreptitious intruder's technique. The position taken by the crawling subject was crouching on hands and knees with the head towards the casmera, and keeping the body down as much as possible. The motion of the crawling subject was to one side, constantly maintaining a minimum frontal area to the TV camera.

Thirty (30) trials were performed, of which all were detected, supporting a 90% probability of detection with a 95% confidence level.

AB.8.4 RUNNING TEST

Because of the relatively long period (1.83 seconds) between samples of a given channel, a running test was performed to try to exploit

this apparent deficiency of the MDU-5 processor. The slow algorithm cycle time was set to 7.47 seconds and the alarm counter was set so that 6 alarm points produced a processor alarm on both the fast and the slow algorithms. The first set of trials attempted resulted in 2 escapes of detection in 24 attempts of traversal. The slow algorithm cycle time was then set to 3.73 seconds and the alarm counter was set so that 6 alarm points produced a processor alarm from the slow (long-term) algorithm and only 2 alarm points produced a processor alarm from the fast (short-term) algorithm. With this setting, 30 out of 30 traversal attempts were detected, supporting a 90% probability of detection with a 95% confidence level.

AB.8.5 ROLLING TEST

The rolling test was performed after the walking, crawling, and running tests, and proved to be the most nearly successful means of crossing the 20 foot path while evading detection. The subject began the rolling test lying prone on the ground facing the TV camera, then began slowly rolling to one side along the path. On the first series of trials with the VMD unit set to alarm the slow algorithm on 6 alarm points and the fast algorithm on 2 alarm points, and with the fast refresh rate, the subject managed to evade detection once in 5 trials. However, with the VMD processor set on the slow refresh rate, the subject was detected 30 times out of 30 trials, supporting a 90% probability of detection with a 95% condifence level for a rolling subject.

AB.9 NUISANCE ALARM TESTING

Although the test range used was not representative of an actual perimeter segment, especially from a nuisance alarm rate basis, tests were conducted on some specific nuisance alarm sources. A litter demonstration was performed and naturally occurring nuisance alarm sources such as moving cloud shadows and wind motion were recorded on video tape for inspection and evaluation. Although no procedure for separating nuisance alarms from false alarms was followed, actual false alarms due to system internal noise were never noticed during

the entire test. All alarms noted could be correlated to actual scene changes as viewed by the TV camera.

AB.9.1 LITTER DEMONSTRATION

To simulate litter movement across the TV camera field of view, a fishing rod was used to cast a light-colored "brick" of foam rubber, 3" X 3" X 5" in size, into the field of view. The foam rubber brick was then drawn across the field of view at rates of 2 to 5 feet per second, and presence or absence of alarms was noted for two different settings of the video motion detector. Results are shown in Table AB-3. At a typical setting of the video motion detector (6 alarm points from either algorithm required for a processor alarm and a 3.73 second slow algorithm cycle time) no alarms were generated by the foam rubber brick during 10 trials, indicating good immunity from nuisance alarms caused by single objects having sizes and velocities typical of wind-blown litter. A more sensitive setting of the fast algorithm (2 alarm points for a processor alarm) gave 30 detections out of 30 trials. This indicates that while the processor easily detects litter-sized objects, it can be programmed to ignore litter, by setting the alarm counter to an appropriate number.

AB.9.2 NATURAL SOURCES OF NUISANCE ALARMS

Nuisance alarm sources which were observed during the VMD System testing included cloud shadows and vegetation movement in wind.

Cloud shadows from fast moving small cumulus clouds often were of sufficient contrast to cause large scale nuisance alarms from the scene being viewed. Light level measurements in cloud shadows have revealed as much as a 60 percent contrast between the shadow and the surrounding lighted area. Cloud speeds can range from nearly stationary to 20 to 30 feet/second. It is conceivable that weather patterns causing a partial cover of dense, fast-moving clouds could produce an intolerable number of nuisance alarms. To minimize nuisance alarms from cloud shadows, the area covered by the field of view of the TV

camera should be kept as small as possible and the auto iris lens on the TV camera should have a very rapid response so as to track sudden light level changes accurately.

Vegetation movement caused by wind was another source of nuisance alarms during VMD system testing. Wind velocities in excess of 10 miles per hour caused enough motion to result in a steady rate of nuisance alarms. During testing, the vegetation motion was ignored in scene areas not of interest by using the bias masking feature of the VMD unit. This eliminated all but a few nuisance alarms. The site used for testing is not representative of anticipated perimeters, however. While the site used had a large amount of low, brushy vegetation, it is recommended that perimeters be surfaced with gravel, asphalt, tamped earth or closely mowed grass, to reduce the number of nuisance alarms from vegetation movement.

AB.10 CONCLUSIONS

The Video Tek, Inc., MDU-5 VMD system as tested represents an intrusion detection sensor with at least a 0.9 probability of detection, but also a nuisance alarm rate around 1 alarm per 2-3 hours; higher rates occur due to clouds, wind, etc. Our testing with various types of intrusion techniques supports at least a 90% probability of detection with a 95% confidence level for human intruders. Nuisance alarms from small moving objects such as litter and small fauna can be "programmed out" by using the proper combination of algorithms. Though our test range was not typical of a secure area perimeter, we estimate that the nuisance alarm rate of a real perimeter would probably average one alarm every 2-3 hours except under extreme weather conditions. The masking features of the MDU-5 allow suppression of nuisance alarms in a versatile fashion, allowing an operator to minimize recurrent alarms cumulatively without adversely affecting the probability of detection in non-nuisance areas.

APPENDIX B

THE EFFECTS OF LAYERING ON PERFORMANCE TESTING

APPENDIX B

CONTENTS

APPENDIX B
THE EFFECTS OF LAYERING ON PERFORMANCE TESTING

B.1.0 APPROACH

Providing proper security and meeting the Nuclear Regulatory Commission Guidelines for security are serious concerns for nuclear power plant operators. To give guidance in selecting, operating and testing a suitable security system, 3 sensor arrangements are analyzed in terms of detection performance versus the cost of performance verification testing. The arrangements are a single sensor perimeter, and two layered perimeters bearing different inherent P_D values.

B.1.1 BASIC ASSUMPTIONS

The following system parameters have been chosen as a basis for comparison:

- The power plant perimeter is assumed to be 1600 meters which is broken into 16 - 100 meter segments.
- Guard cost (including overhead) is assumed to be $20.00/hour
- The cost of money is assumed to be 20% i.e., approximately the current prime rate.
- Although the nuclear plant's life expectancy is 30 years, the capital life of the security system is assumed to be 6 years.
- No attempt is made to consider the effects of taxes and investment credits, since these are significantly influenced by individual company situations and very subject to changes in Federal and State Tax Laws.
- The scrap value of equipment after 6 years is assumed to be equal to the cost of dismantling.
- Cost of Hardware, Cost of Installation and annual operating costs have been derived from vendors' estimates. These may differ from costs incurred in an actual system.

- Whenever the segment P_D falls below 0.90 with 95% confidence, 2 guards must be dispatched to patrol the segment.
- Although in many cases a vehicle will be required or proves to be very desirable for the "intruder" and "observer" to enable them to move about the site freely, and quickly respond to alarms, no vehicle costs have been included since this requirement is likely to be very site dependent.
- To perform testing, 2 people are assumed to be at the segment, an "observer" and an "intruder". Coordination with an operator at the Central Alarm Station and Secondary Alarm Station is required. During the test, data recording functions may be performed by the "observer" and central and secondary alarm station operators. Afterward, reporting and analysis time must be spent to put data and results into the form required by the Nuclear Regulatory Commission. The estimated time requirements for pertinent tasks on a per test basis where appropriate are outlined in Table B-1 and Table B-2.
- Inflation is assumed to be at 12% per year.

B.1.2 INITIAL VERIFICATION TESTING

The initial testing is assumed to consist of a preliminary specification test, an official specification test, a preliminary probability of detection test, and an official probability of detection test.

From NRC guidelines and their consequences, the manufacturer is expected to specify that P_D (probability of detection) for each sensor = 0.90. To specify it lower would be to say it does not meet NRC guidelines. To specify a higher P_D would cause their customer extra testing. The manufacturer is expected to perform acceptance testing under surveillance of the utility.

The preliminary specification test is to gain confidence that sensors are working correctly before proceeding with an official test. A test sequence of 10 intrusion tests is assumed with a passing score of at least 9 detections for each sensor.

Table B-1

ESTIMATED TIME REQUIREMENTS

	Time, Minutes Number of Layers		
	1	2	3
Pre Test Coordination			
"Intruder"	2	2	2
"Observer"	2	2	2
CAS Operator	1	1	1
SAS Operator	1	1	1
Test			
"Intruder"	3	4	5
"Observer"	3	4	5
CAS Operator	3	4	5
SAS Operator	3	4	5
Post Test Coordination			
"Intruder"	2	3	4
"Observer"	2	3	4
CAS Operator	1	1.5	2
SAS Operator	1	1.5	2
Rest			
"Intruder"	2	3	4
"Observer"	2	3	4
Reporting/Analysis	2	3	4
	30	40	50

Table B-2

ASSUMED PERSONNEL TIME FOR OTHER TASKS

	Time/Minutes
Travel to/and from Test Site	
"Intruder"	10
"Observer"	10
Repairman (On Duty)	10
Repairman (On Call)	60
Guard Answering Alarm	3
Investigating Alarm	15
System Checkout	
Repairman (1 layer)	30
(2 layers)	35
(3 layers)	40
Repair System (1, 2, or 3 layers)	60
Failure Report	15

The official specification test is assumed to consist of a test sequence of 30 intrusion tests with a passing score of at least 27 detections for each sensor. Note that for the specification tests, point estimates of P_D are deemed sufficient.

The preliminary probability of detection test is to gain confidence that the official test can be passed. This test should demonstrate that all individual sensors can make contributions adequate to give a segment $P_D \geq 0.90$. The required sensor P_D contributions are to be verified to a confidence level of 75%.

The official P_D test is to demonstrate a segment P_D of at least 0.90 with 95% confidence as per the NRC guidelines.

All initial testing is assumed to be done during regular working hours.

B.2.0 SINGLE LAYER SYSTEM

The single sensor example is a 3 wire free standing E-field fence.

B.2.1 PARAMETERS FOR ANALYSIS

The following cost and performance parameters are assumed.

1. Hardware for 16 segments cost $67,500.
2. Installation Cost $36,700.
3. Annual Operating Costs are $15,500.
4. The Probability of Detection P_D = 0.90 for each segment.
5. The unprocessed false alarm rate FAR = 10 per day.
6. Nuisance alarm duration t = 1/4 second.
7. Integration time = 1 second
8. Guards must respond to any segment failure and remain there until the segment has been restored to normal operation and tested.
9. Segment MTBF = 30,000 hours
10. Repairman must be on call 24 hours per day.

B.2.2 TEST TRIAL SEQUENCES

The system test flow is diagrammed in Figure B-1. For a single layer system the times required for preliminary and official specification test sequences, preliminary and official probability of detection test sequences, normal and emergency checkouts, normal and emergency repairs, operability test sequence, and quarterly test sequences are outlined in Tables B-3 through Table B-4. These data will be combined with other factors to give initial and annual costs.

B.2.2.1 PRELIMINARY PROBABILITY OF DETECTION TEST SEQUENCE

This preliminary test establishes that the one layer system has a P_D = 0.90 with 75% confidence.

Table B-3

PRELIMINARY SPECIFICATION TEST SEQUENCE

	NUMBER OF MEN	SINGLE LAYER NUMBER OF OF TESTS OR TRIPS	MAN MINUTES PER TEST (OR TRIP)	TOTAL MAN MINUTES
TESTING		10	30	300
TRAVEL	2	1	20	20
				320

Cost at 20.00/hour = $106.67

Table B-4

OFFICIAL SPECIFICATION TEST SEQUENCE

	NUMBER OF MEN	NUMBER OF TRIPS	NUMBER OF TESTS	MAN MINUTES PER TEST	TOTAL MAN MINUTES
TESTING			30	30	900
TRAVEL	2	1		20	20
					920

Cost at $20.00/hour = $306.67.

Table B-5

Preliminary Probability of Detection Test Sequence

	NUMBER OF TESTS	MAN MINUTES PER TEST	TOTAL MAN MINUTES
TESTING	23.3	30	700
TRAVEL			20
			720

Cost of a Preliminary P_D test sequence at $20.00/hr. = $240.00

Table B-6

Official Probability of Detection Test Sequence

	EXPECTED NUMBER OF TESTS	MINUTES PER TEST	TOTAL MAN MINUTES
Travel to/from Site			
"Intruder"		10	10
"Observer"		10	10
Testing	35.03	30	1051
			1071

The test sequence requires 17.85 man hours @ $20/hour

Test Sequence Cost = $357.00

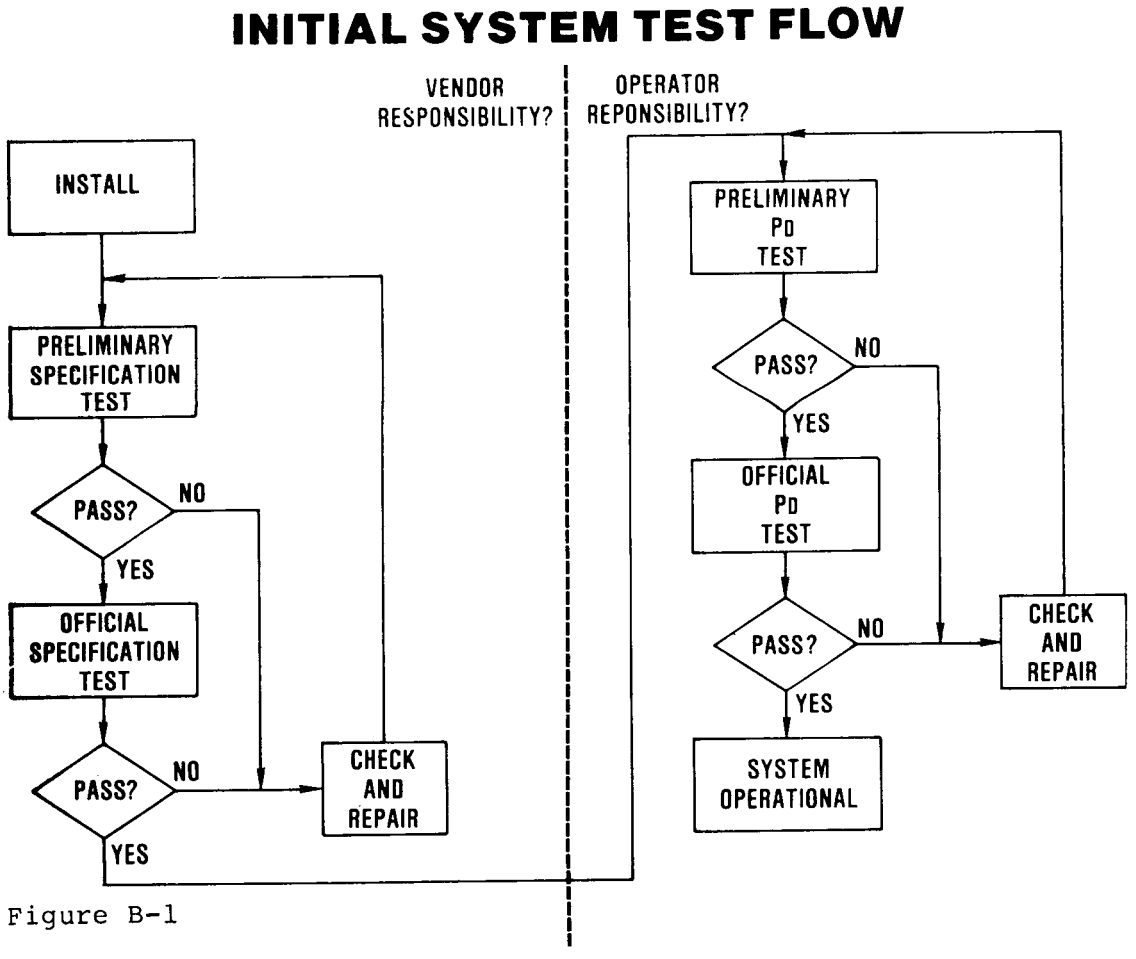


Figure B-1

The test sequence is patterned after the NRC Guide 5.44 test. First 13 tests are conducted; if all 13 are successful, the sensor passes; if less than 11 pass the sensor has failed. Otherwise 13 more tests are conducted. At this point, if 25 successes (out of 26 tests) have accumulated, the sensor passes. If 23 or fewer successes are recorded, the sensor fails. Otherwise 12 more tests are run. If the cumulative score is 36 successes out out of 38 tests, the sensor passes. If less than 36 successes are recorded, the sensor fails. Analysis shows that if $P_D = 0.90$ the expected number of tests/sequence is 23.3 and the expected cost is shown in Table B-5.

B.2.2.2 OFFICIAL PROBABILITY OF DETECTION SEQUENCE ($P_D = .90$)

The NRC probability of detection test sequence is analyzed assuming that the system is operating properly with a single layer and $P_D = 0.90$. If the NRC example is followed, 35.03 tests will be required per test sequence with an expected 0.1384 probability of passing. Time in man minutes for a test sequence is given in Table B-6.

B.2.3 INITIAL TEST COSTS

Test costs are summarized in Table B-7. Checkout and repair costs are listed in Table B-8 and Table B-9.

B.2.4 OPERABILITY TESTING SEQUENCES AND COSTS

Operability testing begins with 1 test per segment per week and follows the system flow of Figure B-2.

The cost of one week's testing is in Table B-10 and Table B-11.

Each week 10% or 1.6 segments will be expected to fail the initial test or 83.2 segments/year. Subsequently 9 more tests will be performed on each of these segments with the cost per segment shown in Table B-11.

Unit test sequences and costs are given in Table B-12.

Table B-7
INITIAL TEST COSTS
1 Layer

	PROBABILITY OF PASSING	EXPECTED SEQUENCES OR CALLS	COST PER SEQUENCE OR CALL	TOTAL
PRELIMINARY SPECIFICATION TESTING/CHECKOUT	.7361	1.3585	$106.67	$144.91
CALLS		.3585	45.00	16.13
OFFICIAL SPECIFICATION TESTING/CHECKOUT	.6474	1.5445	306.67	473.67
CALLS		.5445	45.00	24.50
PRELIMINARY P_D TEST CHECKOUT	.4032	2.4804	240.00	595.30
CALLS		1.4804	45.00	66.62
OFFICIAL P_D TESTING CHECKOUT	.1384	7.224	375.00	2578.99
CALLS		6.224	45.00	280.08
TOTAL COST/SEGMENT				$ 4180.20
COST FOR 16 SEGMENTS				$66,883.20

Table B-8

NORMAL CHECKOUT

	TIME MAN MINUTES
Checkout Time (1 Layer)	30
Guards (2)	60
Travel 3 Men	30
"Failure" Report	15
	135

Cost per Cycle at $20.00/Hour = $45.00

NORMAL REPAIR

Checkout Time (1 Layer)	30
Guards (2)	180
Repair	60
Travel	30
Failure Report	15
Cost at $20.00/Hour = $105.00	315
Parts Cost	200.00
Cost/Scheduled Repair Cycle	$305.00

Table B-9

EMERGENCY CHECKOUT

	NUMBER OF MEN	TIME MAN MINUTES
Response Time (for repairing)		60
Travel		10
Test Time (1 Layer)		30
Guard Time (2 x 100)	2	200
Report		15
		315

Emergency Checkout Cost @ $20.00/hour = $105.00

EMERGENCY REPAIR

Response Time	60
Travel	10
Test Time (1 Layer)	30
Repair Time	60
Guard Time (2 x 160)	320
Report	15
	495
Emergency Repair Time @ $20.00/hour	$165
Parts	$200

Total Emergency Repair Cost = $365.00

Table B-10
WEEKLY TESTING

		TIME MAN MINUTES
Transportation		
"Intruder"	10 min. x 16 segments	160
"Observer"	10 min. x 16 segments	160
Testing Time	30 min. x 16 segments	480
Total Time		800

13.33 manhours x $20/hour = $266.67 per week
For 52 weeks the operability testing will cost: $13,866.67

Table B-11
WEEKLY RETEST COST

		TIME MAN MINUTES
Travel/to/from		
"Observer"		10
"Intruder"		10
Test Time	30 x 9	270
		290

4.83 manhours @ $20/hour = $96.67 per segment
The cost for 83.2 segments/year is $8042.67

Table B-12

OPERABILITY TEST SEQUENCE (1st Test)

$P_D = 0.90$

Single Test

		TIME MAN MINUTES
TEST	30	30
TRAVEL	2 x 10	20
		50

Cost of One Test @ $20.00/hour = $16.67

OPERABILITY TEST (Following 9 Tests)

	NUMBER OF MEN	NUMBER OF TESTS	MINUTES PER TEST	TIME MAN MINUTES
TESTING		9	30	270
TRAVEL	2	10		20
				290

Cost of 9 Tests Sequence @ $20.00/hour = $96.67

QUARTERLY TEST SEQUENCE (10 Tests)

	NUMBER OF MEN	MINUTES PER TEST	NUMBER OF TESTS	TIME MAN MINUTES
TESTING		10	30	300
TRAVEL	2		10	20
				320

Cost of 10 test sequence @ $20.00/hour = $106.67

WEEKLY OPERABILITY TEST

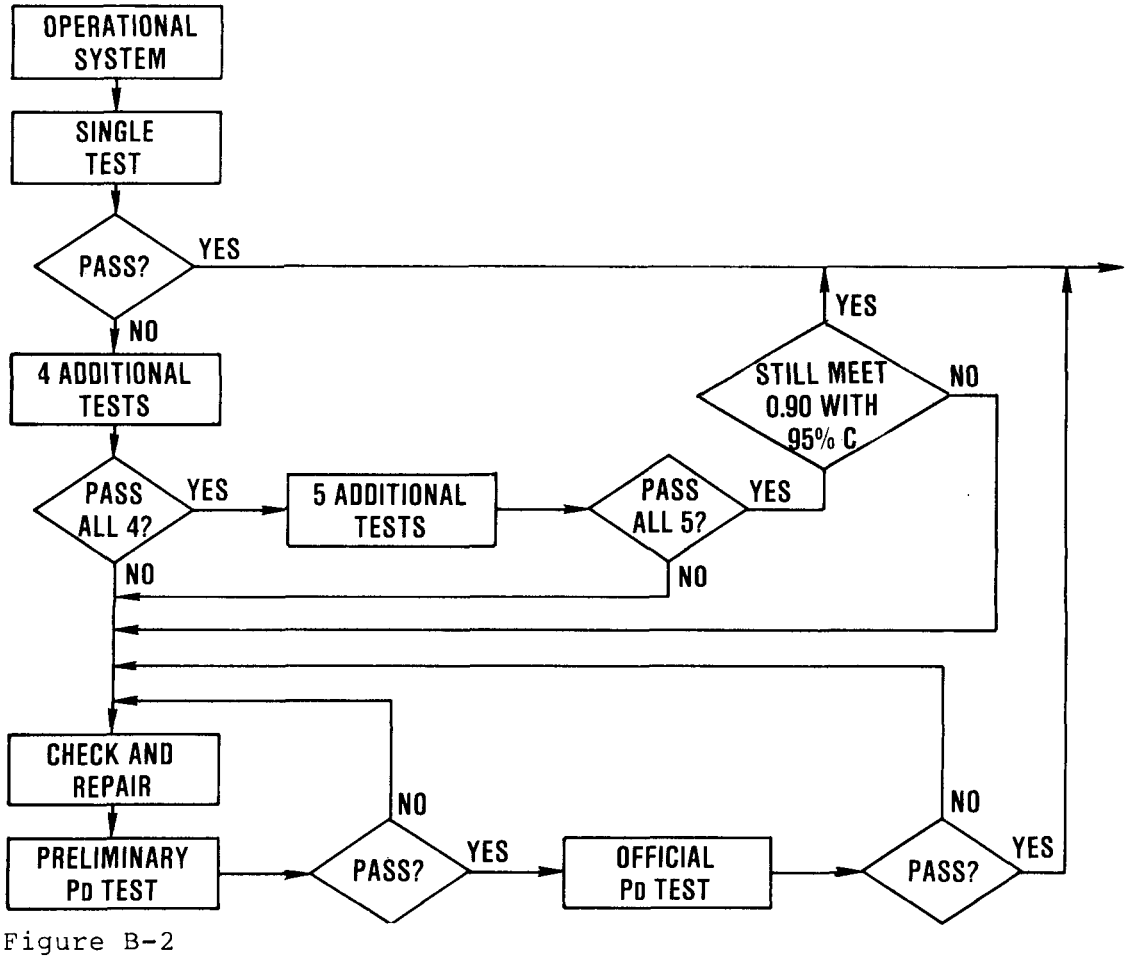


Figure B-2

After a 9 test sequence, it is expected that 9 successes would be scored in 38.74% of the cases. In two thirds of these cases of 9 out of 9, the segment will still be in compliance. In all other cases the repairman will be called out and the long test sequence will be performed again. Computation indicates that 25.83% of segments will be in compliance. This means that for 61.71 segments each year, requalification testing must be performed.

All that has been discussed so far have been initial and operability testing costs on a working system that meets (marginally) the recommendations of NRC Regulatory Guide 5.44 (P_D = 0.90 with 95% confidence). In a year's operation of 16 segments a total of 8766 x 16 or 140,256

hours of operation will be incurred. If each segment has an MTBF of 30,000 hours, 4.675 service calls per year would be expected. For simplicity 5 calls will be assumed of which 4 are emergency and 1 normal. System flow for the repair cycle is given in Figure B-3.

B.2.5 QUARTERLY TESTING

Normally the quarterly testing of 16 segments would require 64 tests. Since extensive testing is required only every 93 days, the testing performed because of equipment failures and type I errors should reduce the requirements for quarterly testing. The system flow for quarterly testing is shown in Figure B-4.

B.2.6 SINGLE LAYER COSTS

The failures will occur at random times which are uniformly distributed after a scheduled test. Thus the unscheduled testing would be expected to occur on an average half-way between scheduled tests. The unscheduled testing would initiate a new 93 day period. Therefore, it is assumed that one scheduled test will be dropped for every 2 unscheduled tests that occur. For 66 unscheduled tests, the reduction in required scheduled requalification tests would be from 64 to 31. Now total costs can be drawn as shown in Table B-13, Table B-14, Table B-15, and Table B-16.

B.3.0 TWO LAYER SYSTEM

The second system to be analyzed has two sensor layers. To the 3 wire free standing E-field fence is added an electret fence sensor.

B.3.1 PARAMETERS FOR ANALYSIS

The following cost and performance parameters are assumed:

1. Hardware for 16 segments cost $109,700.

2. Installation Cost $43,000.
3. Annual Operating Costs $20,700.
4. The Probability of Detection P_D = 0.95 if both layers are working, P_D = 0.90 for either layer by itself.
5. The unprocessed false alarm rate F_{AR} = 10 per day.
6. Nuisance alarm duration t = 1/4 second.
7. Integration time = 1 second.
8. Guards must respond to any single layer failure in any segment and remain there as guards or "intruder and observer" until the segment has been restored to normal operations and tested.
9. Segment MTBF = 15,000 hours (i.e. 30,000 hours for each layer.)
10. Repairman must be on call 24 hours per day.

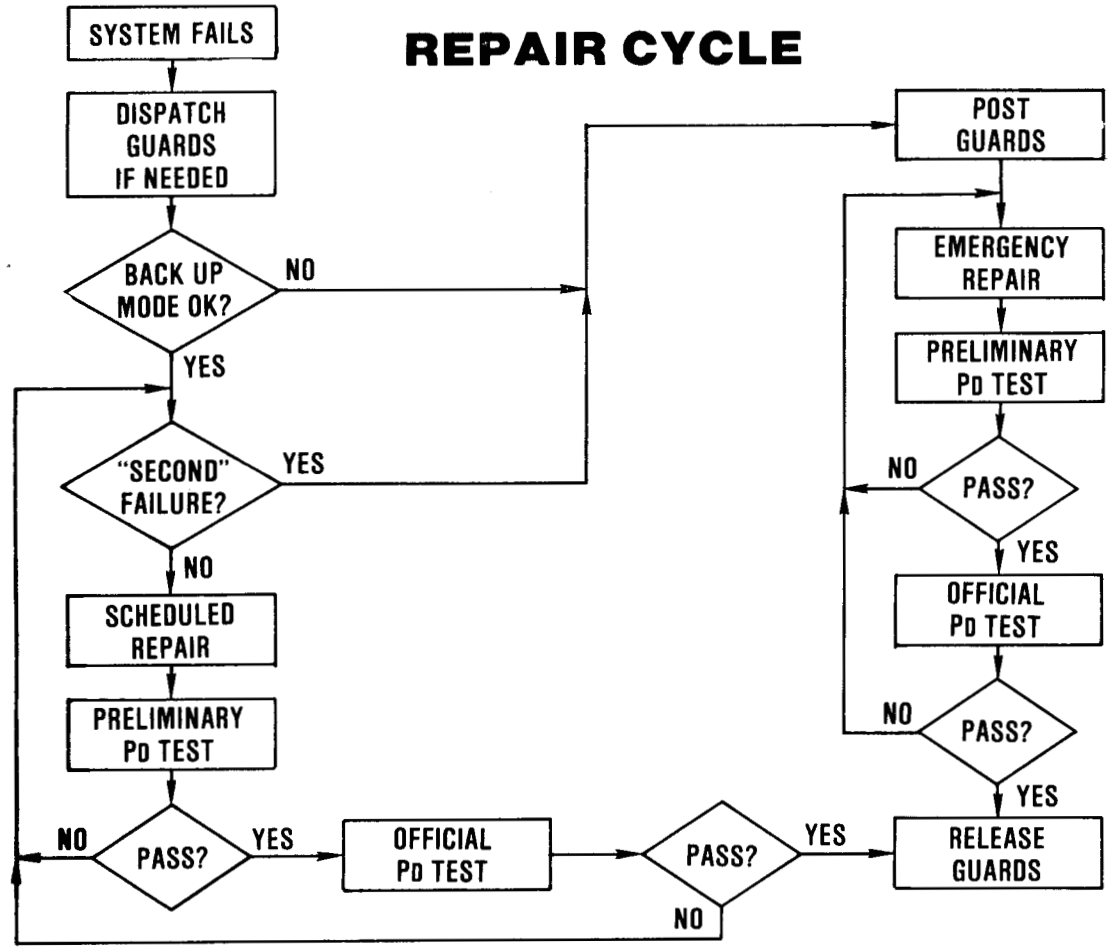


Figure B-3

QUARTERLY TEST

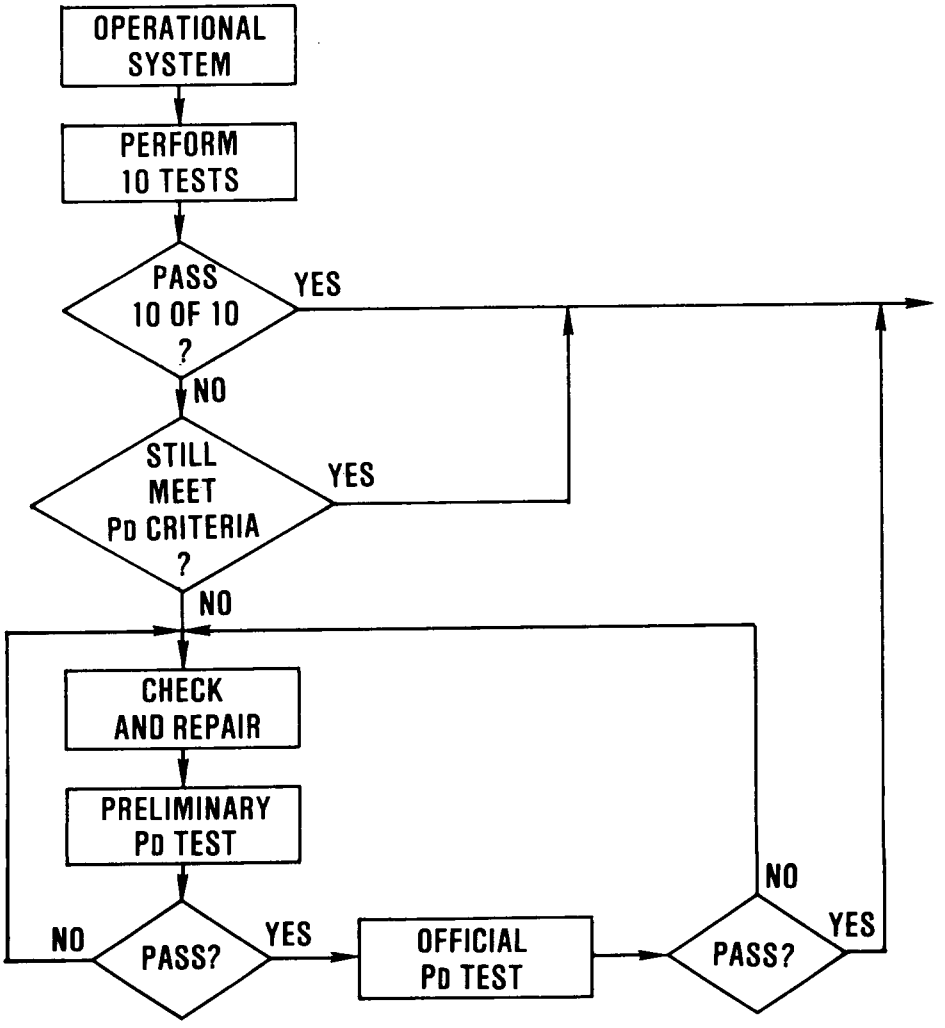


Figure B-4

Table B-13

OPERABILITY TESTING

	PROBABILITY OF TEST (OR CALL)	PROBABILITY OF PASSING	EXPECTED SEQUENCES OR CALLS	COST/ SEQUENCE OR CALL	TOTAL
Operability Testing					
First Test	1	.900	1	$16.67	$16.67
9 Test Follow Up	.1	.2583*	.1	96.67	9.67
Requalification Testing					
Preliminary P_D					
Testing	.07417	.4032	.1840	$240.00	$44.15
Normal Checkout	.01854		.04500	45.00	2.07
Emergency Checkout	.0556		.13798	100.00	13.79
Official P_D					
Testing	.07417	.1384	.53582	$357.00	$191.29
Normal Checkout	.01854		.11541	45.00	5.19
Emergency Checkout	.0556		.34623	100.00	34.62
Cost Per Segment Per Week					$317.45
Cost Per Segment Per Year					$ 16,507.40
Cost Per Year for 16 Segments					$264,118.40
Segments Requalified Per Year	61.71				

Table B-14

QUARTERLY TESTING COSTS

	PROBABILITY OF TEST OR CALL	PROBABILITY OF PASSING	EXPECTED NUMBER OF SEQUENCES	COST/ SEQUENCE	TOTAL
10 Test Sequence	1	.60696	1	106.67	106.67
Requalification Testing					
Preliminary P_D	.39304	.4032	.97491	240.00	233.98
Normal Checkout	.09826		.2437	45.00	10.97
Emergency Checkout	.29478		.7312	100.00	73.12
Offical P_D	.39304	.1384	2.8393	357.00	1013.64
Normal Checkout	.09826		.6116	45.00	27.52
Emergency Checkout	.29478		1.8347	100.00	183.47
1 Segment Test					1649.37
64 Segment Tests					105,559.68
31 Segment Tests*					51,130.47

*Since 66 unscheduled requalification tests performed only 31 of the 64 quarterly tests actually were required.

Table B-15

REPAIR RELATED COSTS

	NUMBER OF SEGMENTS	PROBABILITY OF PASSING	EXPECTED NUMBER SEQUENCES OR CALLS	COST/CALL OR SEQUENCE	TOTAL
Normal Repair	1			305.00	305.00
Emergency Repair	4		4	360.00	1440.00
Requalification Testing					
Preliminary P_D Testing	5	.4032	12.40	240.00	2976.50
Normal Checkout			.48	45.00	66.62
Emergency Checkout	4		5.92	100.00	592.17
Offical P_D Testing	5	.1384	36.12	357.00	12894.84
Normal Checkout	1		6.224	45.00	280.08
Emergency Checkout	4		24.896	100.00	2489.60
Repair Related Costs/Year for 16 Segments					21,044.81
Repair Related Costs/ Segments/Year					1,315.30

Table B-16

COST OF A SINGLE LAYER SECURITY SYSTEM

Initial Investment:

3 Wire E-Field Fence	
Hardware	67,500
Installation	36,700
Initial Testing	66,883
	171,083

Annual Costs:

Operating Cost	15,500
Repair Related Costs	21,045
Operability Testing	264,118
Quarterly Scheduled Testing	51,130
	351,793

B.3.2 TEST TRIAL SEQUENCES

For a two layer system the times required for preliminary and official specification test sequences, preliminary and official probability of detection test sequences, normal and emergency checkouts, normal and emergency repairs, operability test sequence, and quarterly test sequences are outlined below. These data will be combined with other factors to give initial and annual costs.

B.3.2.1 PRELIMINARY PROBABILITY OF DETECTION TEST SEQUENCE

This preliminary test establishes that each layer has a 0.80 probability of detection with 75% confidence. This is sufficient to support a system probability of detection of over 0.90 when the 2 sensors are connected in an "AND MOSTLY" configuration. However, it will be assumed that the individual sensors actually meet $P_D = 0.90$ and the two layers together actually meet 0.95.

This test sequence is also patterned after the NRC test. First 7 tests are conducted; if all 7 are successful on both sensors, both sensors pass. If at least 6 are successful on both sensors, six more tests are conducted on the sensor or sensors that have not yet passed. At the end of 13 tests, any sensor which has 12 successes, passes.

Testing continues if 11 successes have been recorded. The final 6 tests complete the sequence. At the end of 19 tests the probability that both sensors pass is 0.55658. The test sequences are summarized in Table B-17, Table B-18, and Table B-19.

B.3.2.2 OFFICIAL PROBABILITY OF DETECTION SEQUENCE

The NRC probability of detection test sequence is analyzed following, assuming that the system is operating properly with 2 layers and the actual two layer $P_D = 0.95$ after processing.

Table B-17

PRELIMINARY SPECIFICATION TEST SEQUENCE

	NUMBER OF MEN	NUMBER OF TESTS OR TRIPS	MAN MINUTES PER TEST OR TRIP	TOTAL MAN MINUTES
TESTING		10	40	400
TRAVEL	2	1	20	20
				420

Cost at 20.00/hour = $140.00

Following the NRC example, 38.59 tests will be required per test sequence with an expected 0.5742 probability of passing.

Time in minutes for a test sequence is shown in Table B-20.

Times for checkout and repair are shown in Table B-21 and Table B-22.

B.3.2.3 OPERABILITY TESTING SEQUENCE

Time and cost results are tabulated in Table B-23.

B.3.3 TWO LAYER COSTS

Initial and operability test sequence costs are summarized for two layer testing in Table B-24 and Table B-25.

Table B-18

OFFICIAL SPECIFICATION TEST SEQUENCES

	NUMBER OF MEN	NUMBER OF TRIPS OR TESTS	MAN MINUTES PER	TOTAL MAN MINUTES
TESTING		30	40	1200
TRAVEL	2	1	20	20
				1220

Cost at 20.00/hour = $406.67

Table B-19

PRELIMINARY PROBABILITY OF DETECTION TEST SEQUENCE

	NUMBER OF MEN	NUMBER OF TESTS	TIME PER TEST	TOTAL MAN MINUTES
TESTING		11.140	40	446
TRAVEL	2		10	20
				466

Cost of a preliminary P_D test sequence at $20.00/hour = $148.67.

In a year's operation of 16 segments with 2 layers, a total of 2 x 8766 x 16 or 280, 512 hours of operation will be incurred. If each layer of each segment has an MTBF of 30,000 hours, 9.35 service calls/year can be expected. For simplicity, 10 calls will be assumed.

Making the same assumptions as for a single layer the 10 tests following repairs and the 24 tests after type I errors should reduce the scheduled quarterly tests by 17. Only 47 tests will be required.

Table B-20

OFFICIAL PROBABILITY OF DETECTION SEQUENCE

	EXPECTED NUMBER OF TESTS	TIME PER TEST	TOTAL MAN MINUTES
Travel to/from site			
"Intruder"		10	10
"Observer"		10	10
Testing	38.59	40	1544
			1564

26.07 manhours @ $20/hour = $521.33

Table B-21

NORMAL CHECKOUT

(2 Layers)

Checkout Time	35
Guards (2)	70
Travel 3 Men	30
Report	15
	150 minutes

Cost of Normal Checkout @ 20.00/hour = $50.00

NORMAL REPAIR

(2 layers)

Checkout Time	35
Repair	60
Guards (2)	190
Travel	30
Failure Report	15
	330 minutes

Cost at 20.00/hour =	$110
Parts =	200
Costs of a Normal Repair =	$310

Table B-22

EMERGENCY CHECKOUT

(2 layers)

Response Time	60
Travel	10
Test Time 2 Layers	35
Guard Time (2)	210
Report	15
	330 minutes

Cost of Emergency Checkout @ 20.00/hour = $110

EMERGENCY REPAIR

(2 layers)

Response Time	60
Travel	10
Test Time	35
Repair Time	60
Guard Time	330
Report	15
Total Time	510 minutes

Emergency Repair Time @ 20.00/hour =	$170
Parts	200
Total Emergency Repair Cost	$370

Repair related costs are given in Table B-26 and quarterly testing costs in Table B-27. Cost of ownership of a two layer system is given in Table B-28.

Table B-23

OPERABILITY TEST SEQUENCE

First Test Time

(2 layers)

	NUMBER OF MEN	TIME PER TEST	MAN MINUTES
Test		40	40
Travel	2	10	20
Total Time			60

Cost of first test @ 20.00/hour = $20.00

9 Tests

	NUMBER OF MEN	NUMBER OF TESTS		TIME OF TESTS		MAN MINUTES
Test		9	x	40	=	360
Travel	2			10	=	20
						380

Cost of 9 Nine Tests @ 20.00/hour = $126.67

QUARTERLY TESTS

(2 layers)

Sequence 10 Tests

	NUMBER OF MEN	NUMBER OF TESTS		TIME OF TESTS		MAN MINUTES
Testing		10	x	40	=	400
Travel	2			10	=	20
Total Time						420

Cost of Quarterly Test @ 20.00/hour = $140.00

Table B-24

INITIAL TESTING 2 Layers

	PROBABILITY OR PASSING	EXPECTED SEQUENCES OR CALLS	COST/CALL OR SEQUENCE	TOTAL DOLLARS
Preliminary Specification				
Testing	.54184	1.8456	140.00	258.30
Checkout Calls		.8456	50.00	42.28
Official Specification				
Testing	.41918	2.3856	460.67	970.16
		1.3856	50.00	69.28
Preliminary P_D				
Each Layer P_D 0.80, 75% Conf.	.55658	1.7967	148.67	267.11
		.7967	50.00	42.28
Official P_D Test	.5742	1.7415	521.33	907.90
		.7415	50.00	37.08
Total Cost/Segment				$ 2,594.47
Cost for 16 Segments				$41,511.52

Table B-25

OPERABILITY TESTING

(2 Layers P^D = 0.95)

	PROBABILITY OF TEST OR CALL	PROBABILITY OF PASSING	EXPECTED NUMBER SEQUENCES OR CALLS	COST/SEQUENCE OR CALL	TOTAL
First Test	1	.950	1	20	20.00
9 test followings	.05	.4202*	.05	126.67	6.33
Requalification Testing					
Preliminary P_D Test					
Testing	.0290	.55658	.05209	148.67	8.26
Normal Checkout	.0072		.0130	50	.65
Emergency Checkout	.0217		.0390	110.	4.30
Offical P_D Test					
Testing	.0290	.4742	.05049	521.33	26.32
Normal Checkout	.0072		.0054	50.	.27
Emergency Checkout	.0217		.0161	110	1.77
Cost per segment per week					67.90
Cost per segment per year					$ 3530.80
Cost per year for 16 segments					$ 56492.80
Segments requalified per year	24.12				

Table B-26

REPAIR RELATED COSTS

	NUMBER OF SEGMENTS	PROBABILITY OF PASSING	EXPECTED NUMBER SEQUENCES OR CALLS	COST/CALL TOTAL OR SEQUENCES	
Normal Repair	2			310	620.00
Emergency Repair	8			370	2960.00
Requalification Testing					
Preliminary P_D Testing	10	.55658	17.967	148.67	2671.13
Normal Checkout	2		3.59	50	179.67
Emergency Checkout	8		14.373	110	1581.08
Offical P_D Testing	10	.5742	17.416	521.33	9079.24
Normal Checkout	2		1.483	50	74.16
Emergency Checkout	8		5.932	110	652.57
Repair Related Costs Per Year for 16 Segments					$ 17817.85
Repair Related Cost Per Year Per Segment					$ 1113.62

Table B-27

QUARTERLY TESTING COSTS

(2 Layers P_D = 0.95)

	PROBABILITY OF TEST	PROBABILITY OF PASSING	NUMBER OF TESTS	COST/ SEQUENCE	TOTAL
10 test sequences	1	.80882	1	140.00	140.00
Requalification Testing	.19118				
Preliminary P_D		.55658	.34349	148.67	51.07
Normal	.04780		.08587	50.00	4.29
Emergency	.14338		.25762	110.00	28.34
Offical P_D	.19118		.33295	521.33	173.58
Normal	.04780	.4742	.03545	50	1.77
Emergency	.14338		.10632	110	11.70
1 Segment Test					$ 410.75
64 Segment Tests					$ 26228.00
47 Segment Tests					$ 19305.25

Table B-28

COST OF A TWO LAYER SECURITY SYSTEM

Initial Investment:	
3 Wire E-Field Fence:	
Hardware	$67,500
Installation	36,700
Fence FPS Electret	
Hardware	42,200
Installation	6,300
Initial Testing	41,512
	$194,212
Annual Cost:	
Operating Cost E-Field	$ 15,500
Operating Cost Electret	5,200
Repair Related Costs	17,818
Operational Testing	56,493
Quarterly Scheduled Testing	19,305
Total Annual Cost:	$114,316

B.4.0 THREE LAYER SYSTEM

The third system to be analyzed is a three layer system. In addition to the 3 wire free standing E field fence and electret fence sensor, a video motion detector is added.

B.4.1 PARAMETERS FOR ANALYSIS

The following cost and performance parameters are assumed.

1. Hardware for 16 segment costs
2. Installation Cost
3. Annual Operating Cost
4. The Probability of Detection $P_D = 0.99$ if all three layers are working, $P_D = 0.95$ with 2 layers working.
5. The unprocessed false alarm rate $F_{AR} = 10$ per day.
6. Nuisance alarm duration $t = 1/4$ second.
7. Integration time = 1 second.
8. Guards must respond only to a double or triple layer failure. Since only about 11 failures are expected to occur during the year, or less than 1 failure per segment per year, it is assumed there are no double failures.
9. Segment MTBF's by layer
   30,000 hours for E field fence
   30,000 hours for electret fence sensor
10. Video motion detector for 16 channels
    MTBF = 8,000 hours
11. Repairs can be made during scheduled working hours. 24 hour on call repairman is not required.

B.4.2 PRELIMINARY SPECIFICATION TESTING AND OFFICIAL SPECIFICATION TESTING

For 3 layers an optimum testing scheme has not been derived yet. For simplicity the cost is taken as the sum of the Testing Costs for a single layer system plus the testing cost of a double layer system. A more efficient testing system can be devised which would cut the specifications testing costs for a 3 layer system but it would not affect the conclusions in this study.

For a three layer system the times required for preliminary and official specification test sequences, preliminary and official probability of detection test sequences, normal and emergency checkouts, normal and emergency repairs, operability test sequence, and quarterly test sequences, normal and emergency checkouts, normal and emergency repairs, operability test sequence, and quarterly test sequences are outlined in Tables B-29, B-30, and B-31. These data will be combined with other factors to give initial and annual costs.

The official P_D test sequence is analyzed assuming that the system is operating properly with three layers and $P_D = 0.99$. If the NRC example is followed, 33.07 tests will be required per test sequence with an expected 0.9878 probability of passing. Time in man minutes for a test sequence is given in Table B-31.

When test failure occurs, the repairman must be called to check out the equipment.

B.4.3 THREE LAYER COSTS

Initial test sequence costs are given in Table B-32; operability test costs are shown in Table B-33; quarterly test costs are shown in Table B-34; and, checkout and repair costs are given in Tables B-35 and B-36.

B.4.3.1 OPERABILITY TESTING

Operability testing begins with 1 test per segment per week.

Each week 1% or 0.16 segments will be expected to fail the initial test or 8.32 segments/year. Subsequently 9 more tests will be performed on each of these segments.

Table B-29

PRELIMINARY SPECIFICATION TESTING

(3 layers)

	MEN	NUMBER OF TESTS	TIME PER TEST	MAN MINUTES
TESTING		10	50	500
TRAVEL	2		10	20
TOTAL TIME				520

Cost at 20.00/hour = $173.33

Table B-30

OFFICIAL SPECIFICATION TEST SEQUENCE

(3 layers)

	MEN	NUMBER OF TESTS	TIME PER TEST	MAN MINUTES
TESTING		30	50	1500
TRAVEL	2		10	20
				1520

Cost at 20.00/hour = $506.67

Table B-31

OFFICIAL P_D TEST

(3 layers)

	MINUTES PER TEST	TOTAL MINUTES
Travel to/from Site		
"Intruder"	10	10
"Observer"	10	10
Testing	50	1654
Total		1674

The test sequence requires 27.9 man hours @ $20/hour

Test Sequence Cost = $558.00

Table B-32

INITIAL TESTS COSTS

3 Layers

	PROBABILITY OF PASSING	EXPECTED NUMBER SEQUENCES OR CALLS	COST/ SEQUENCE OR CALL	TOTAL
Preliminary Specification				
Testing (2 layers)	.54184	1.8456	140.00	258.38
Checkout Calls (2 layers)		.8456	50.00	42.28
Testing (1 layer)	.7361	1.3585	106.67	144.91
Checkout (1 layer)		.3585	45.00	16.13
Official Specification				
Testing (2 layers)	.41918	2.3856	406.67	970.16
Checkout Calls (2 layers)		1.3856	50.00	69.28
Testing (1 layer)	.6474	1.5445	306.67	473.67
Checkout (1 layer)		.5445	45.00	24.50
Preliminary P_D				
Testing	.4152	2.4083	196.00	472.03
Checkout Calls		1.4083	55.00	77.46
Official P_D				
Testing	.9878	1.0124	558.00	564.90
Checkout Calls		.0124	55.00	0.68
Total Cost per Segment				$ 3114.38
Total Cost for 16 Segments				$49830.08

Table B-33

OPERABILITY TEST SEQUENCE

(3 Layers)

	MEN	FIRST TEST	TIME/ TEST	MAN MINUTES
TEST			50	50
TRAVEL	2		10	20
TOTAL TIME				70

Cost of one Test @ 20.00/hour = 23.33

9 Follow-up Tests

	NUMBER OF MEN	NUMBER OF TESTS	TIME/ TEST	MAN MINUTES
TESTING		9	50	450
TRAVEL	2	10		20
				470

Cost of 9 Test Sequences @ 20.00/hour = 156.67

Table B-34

QUARTERLY TESTING SEQUENCE

(3 layers)

	MEN	TESTS	MINUTES PER TEST	MAN MINUTES
TESTING		10	50	500
TRAVEL	2		10	20
TOTAL TIME				520

Cost of 10 Test Sequence @ 20.00/hour = $173.33

Table B-35

NORMAL CHECKOUT
(3 layers)

	MAN MINUTES
Checkout Time (3 layers)	40
Guards (2)	80
Travel (3 men)	30
Report	15
Total Time	165

Cost of Normal Checkout @ 20.00/hour = $55.00

NORMAL REPAIR

	MAN MINUTES
Checkout Time (3 layers)	40
Repair	60
Guards (2)	200
Travel	30
Failure Report	15
Total Time	345

Cost of Repair Time @ 20.00/hour =	115.00
Parts	200.00
Costs of Normal Repair	$335.00

Table B-36

EMERGENCY CHECKOUT

	MAN MINUTES
Response Time	60
Travel	10
Checkout	40
Guards (2)	220
Report	15
Total Time	345

Cost of Emergency Checkout @ 20.00/hour = $115.00

EMERGENCY REPAIR

	MAN MINUTES
Response Time	60
Travel	10
Checkout Time	40
Repair	60
Guards (2)	340
Report	15
Total Time	525
Cost of Emergency Repair Time @ 20.00/hour	175
Parts	200
Cost of Emergency Repairs	$375

After the 9 test sequence it is expected that 9 successes would be scored in 91.35% of the cases. In at least two thirds of these cases of 9 out of 9 the segment will still be in compliance. In all other cases, the repairman will be called out and the long test sequence will be performed again. Computation indicates that 60.90% of segments will be in compliance. This means that for 3.25 segments requalification testing must be performed. Costs are shown in Table B-37.

All that has been discussed so far in this section have been initial and operability testing costs on a working system that meets the guidelines of NRC Regulatory Guide 5.44 (P_D = 0.90 with 95% confidence).

B.4.3.2 QUARTERLY TESTING

In a year's operation of 16 segments a total of 8766 x 16 x 2 or 280,512 hours of operation will be incurred. If each segment has an MTBF of 30,000 hours, 9.35 service calls per year would be expected. In addition, the video motion detector will operate 8,766 hours with an MTBF of 8,000 hours. This will add 1.1 failures per year. For simplicity, 11 calls will be assumed. Most repairs can now be performed on a normal i.e. first shift basis. Therefore, 10 of the 11 calls are assumed to be on a normal basis. Now 11 segments must be retested.

Normally the quarterly testing of 16 segments would require 64 tests. Since extensive testing is required only every 93 days, the testing performed because of equipment failures and type I errors should reduce the requirements of quarterly testing.

Repair related costs are shown in Table B-38. Quarterly test sequence costs are given in Table B-39 and the cost of ownership of a three layer system is given in Table B-40.

Table B-37

OPERABILITY TESTING

	PROBABILITY	PROBABILITY OF PASSING	EXPECTED NUMBER	COST	
First Test	1	.990		23.33	23.33
9 Test Followup	.01	.60901	.01	156.67	1.57
Requalification Testing					
Preliminary P_D					
Testing	.00391	.4152	.00942	196.00	1.85
Normal Checkout	.000978		.00235	55.00	0.13
Emergency Checkout	.002932		.00706	115.00	0.81
Official P_D					
Testing	.00391	.9878	.003958	558.00	2.21
Normal Checkout	.000978		.00001	55.00	.01
Emergency Checkout	.002932		.00003	115.00	.01
		Cost per segment per week.			29.92
		Cost per segment per year.			1555.84
		Cost for 16 segments/year.			24,893.44

Segments requalified/year=3.25

Table B-38

REPAIR RELATED COSTS

	NUMBER OF SEGMENTS	PROBABILITY OF PASSING	EXPECTED NUMBER SEQUENCES OR CALLS	COST/ CALL OR SEQUENCE	TOTAL
Normal Repair	10			310.00	3100.00
Emergency Repair	1			385.00	375.00
Requalification Freq.					
Preliminary PD Testing	11	.4152	26.493	196.00	5192.67
Normal Checkout	10		24.085	55.00	1324.66
Emergency Checkout	1		2.408	115.00	276.98
Official P_D Testing	11	.9878	11.1364	558.00	6214.11
Normal Checkout	10		.124	55.00	6.82
Emergency Checkout	1		.0124	115.00	1.43
Repair Related Costs/Year					16491.67
					1030.73

The failures will occur at uniformly distributed times after a scheduled test. Thus the unscheduled testing would be expected to occur halfway between scheduled tests. The unscheduled testing would initiate a new 93 day period. Therefore, it is assumed that one scheduled test will be dropped for every 2 unscheduled tests that occur. For 14 unscheduled tests, the reduction in required scheduled requalification tests would be from 64 to 57 per year.

Table B-39

QUARTERLY TESTING COSTS

3 Layers $P_D = 0.99$

	PROBABILITY OF TEST	PROBABILITY OF PASSING	NUMBER OF TESTS	COST PER SEQUENCE	TOTAL
10 Test Sequence	1	.965283	1	173.33	173.33
Requalification Testing					
Preliminary P_D Testing	.03472	.4152	.08361	196.00	16.39
Normal Checkout	.00868		.0290	55.00	1.15
Emergency Checkout	.02604		.06271	115.00	7.21
Official P_D	.03472	.9878	.03515	558.00	19.61
Normal Checkout	.00868		.00011	55.00	0.01
Emergency Checkout			.00032	115.00	0.04

Cost per year per test	$ 217.74
Cost per year for 57	$12411.18
Cost per year for 64	$13935.36

Table B-40

COST OF A THREE LAYER SECURITY SYSTEM

Initial Investment	
3 Wire E-Field Fence	
Hardware	$67,500
Installation	36,700
Fence FPS Electret	
Hardware	42,200
Installation	6,300
Video Motion Detector	
Hardware	81,500
Installation	8,000
Initial Testing	49,830
	$292,030
Annual Costs	
Operating Cost	
E-Field	$ 15,500
Fence Electret	5,200
Video Motion Detector	4,000
Repair Related Costs	16,492
Operability Testing	24,893
Quarterly Scheduled Testing	12,411
	$ 78,496

B.5.0 COST COMPARISON SUMMARY

Now that single, double and triple layer systems have been analyzed for cost, some conclusions may be drawn. Assuming a 12% inflation rate and 20% interest rate, present values, i.e., cost for systems with a six year life referred to present dollars, were computed for each system as follows:

	LAYERS		
	1	2	3
Initial Investment	171,083	194,212	292,030
Annual Cost (1st year)	351,793	114,316	78,496
Total Cost for 6 years	2,281,841	880,108	763,006
Present Value	$1,804,549	$736,709	$664,540

The study indicates that a single layer system is both uneconomical and operationally marginal. It should be noted that testing cost figures are very sensitive to the actual P_D of the system. If the P_D drops below 0.90 testing costs will become significantly larger. If the P_D increases above 0.90, testing costs will drop.

Although a 2 layer system appears viable the 3 layer system appears to be a better choice both from an operational standpoint and cost of ownership. This cost analysis has been developed assuming that meeting NRC 5.44 guidelines at a minimum cost is the primary objective. If penetration of the perimeter by hostile parties intent upon sabotage or plant shutdown is perceived as a real and significant threat, the case for a multilayer system becomes even stronger.

APPENDIX C
WORKSHOP SUMMARIES

APPENDIX C

WORKSHOP SUMMARIES

C.1.0 EPRI WORKSHOP

A Perimeter Intrusion Alarm System Workshop sponsored by the Electrical Power Research Institute (EPRI), was held at the E-Systems, Greenville Division plant, Majors Field, Greenville, Texas, Oct 6, 7, 1981. Presentations were made reflecting the survey of Nuclear Power Plant needs and wants and the NRC requirements to be met by a perimeter security system. The synthesis of a Baseline System was outlined as were the concepts of layering, signal processing and economical performance testing. An outline of the proceedings is given following in section C.2.0. Nuclear Utility attendees are listed in Section C.3.0.

C.2.0 AGENDA: EPRI WORKSHOP ON PERIMETER INTRUSION ALARM SYSTEMS

Tuesday, October 6

9:05 Opening Remarks, Cecil Byrom, Vice President Requirements

9:15 EPRI Introduction, Boyd Brooks, Project Manager Nuclear Engineering and Operations Department

9:35 Perimeter Security Requirements, Don Halsey

10:30 Summary of Proven Sensors, Dan Buehler

11:00 The Concept of Layering, Ray Houston
The concept of a Processing Interface, Don Gregg

12:30 Sensor Test and Evaluation, Brooks Nolan

1:00 Perimeter Security System Definition, Don Halsey

1:45 Workshops (Concurrent)
1. E-Field Experience, Rudi Stefancik
2. CCTV, VMD Experience, Wes Redus
3. Alarm Processing Systems, Dan Buehler

3:45 NRC Regulation Question and Answer Period - Jim Prell, NRC

Wednesday, October 7

8:30 CCTV, Lighting and VMD, Wes Redus
9:15 Workshops (Concurrent)
4. Probability Testing, Don Halsey
5. Specification Comments, Boyd Brooks
6. Sensor Test Bed Demonstration, Ray Walker
12:00 Performance and Cost Trade Offs - Paul Pritchard
12:30 Perimeter Security in the Sinai - Rudi Stefancik
1:00 Workshop Position Summaries by Workshop Chairmen

C.3.0 WORKSHOP ATTENDEES

Bass, Robert D.	Washington Public Power Supply Sys. 3000 Geo Washington Way Richland, WA 99352 (509) 372-5850
Bates, Greg	Public Service Company of Colorado 12015 E. 46th. Ave., Suite 440, Denver, Colo. 80239 (303) 571-6510 (Ft. St. Vrain Nuclear Plant)
Beach, Doug H.	Washington Public Power Supply Sys. P.O. Box 1223 Elma, WA 98541 (206) 482-4428
Bradley, Brian	Hoad Engineers, Inc. 1159 E. Michigan Ave. Ypsilanti, MI. 48197 (313) 482-0920
Conklin, Roland	Prairie Island Nuclear Plant Northern States Power (612) 388-1121

Davenport, David L.	Gulf States Utilities River End Nuclear Station P.O. Box 220 St. Francisville, LA 70775 (504) 635-4514
Faust, Robert	Hoad Engineers 854 Buhl Bldg. Detroit, Mich. 48226 (313) 964-3773
Flottmeyer, David	Dairyland Power Coop. P.O. Box 135 Genoa, Wisc. 54632 (608) 689-2331
Heady, Bill	Power Authority St. of New York P.O. Box 215 Buchanan, New York 10511 (914) 739-8200
Hollis, Horace L.	Ark. Power and Light Ark. Nuclear One P.O. Box 608 Russellville, Ark. 72801 (501) 964-3120
Kniskern, Kenneth L.	Yankee Atomic Electric Co. 1671 Worcester Rd. Framingham, MA 01701 (617) 872-8100 ext. 2373
Mayer, James P.	Commonwealth Edison Co. Dresden Nuclear Power Station RR #1 Morris, Ill. 60450 (815) 942-2920 ext. 530

Meehan, P. Michael	Northeast Utilities Service Co. P.O. Box 270 Hartford, CT 06101 (203) 666-6911
Michalka, Martin	Texas Utilities Generating Co. Comanche Peak S.E.S. P.O. Box 2300 Glen Rose, TX 76043 (817 897-4856
McMullen, Mark	Kansas Gas and Electric P.O. Box 208 Wichita, KS 67201 (316) 261-6653
Mcnaughton, David	Hoad Engineers 1159 E. Michigan Ypsilanti, MI 48197 (313) 482-0920
Nadeaul, E. J.	Washington Public Power Supply Sys. 3000 Geo Washington Way Richland, WA 99352 (509) 372-5850
Sedgwick, Richard H.	Yankee Atomic Electric Co. Star Route Rowe, Mass. 01367 (413) 652-6140
Simpson, J. K. (Ken)	Puget Sound Power and Light Puget Power Building Bellevue, WA 98009 (206) 453-6869

Rumsey, John	Texas Utilities Generating Co. P.O. Box 2300 Glen Rose, TX 76043 (817) 897-4856 (Comanche Peak Nuclear Plant)
Willaford, Felix D.	Commonwealth Edison Co. Braidwood Nuclear Power Station Route #1, Box 84 Braceville, Ill. 60407 (815) 458-2801 ext. 264
Wood, Robert E.	Rochester Gas and Electric Corp. 89 East Avenue Rochester, New York 14649 (315) 524-4446 ext. 257 R. E. Ginna Nuclear Power Plant
Harper, Hobert L.	Director of Security Duquesne Light Co. Beaver Valley Power Station P.O. Box 4 Shippingport, PA 15077 (412) 643-4121
Joseph, Gerald R.	Security Director La Crosse Boiling Water Reactor 2615 E. Ave. So. La Crosse, Wis 54601 (608) 788-4000
Roberts, Charles W.	Manager of Security Public Service Company of New Hampshire P.O. Box 300 Seabrook, NH 03874 (603) 474-9521

Brooks, Boyd
Electric Power Research Inst.
3412 Hillview Ave.
Pala Alto, CA 94303
(415) 855-2083

Prell, Jim
Office of Research
U.S. Nuclear Regulatory Comm.
Washington D. C. 20555
(301) 443-5976

C.4.0 WORKSHOP SUMMARY: E-FIELD EXPERIENCE RUDI STEFANCIK, CHAIRMAN

We had twelve people in attendance. Five have E-Field fences in operation. At least two were there to find out whether or not they wanted to put in an E-Field fence in the near future. Types of installations represented were: free standing in an isolation zone, stand-off from a chain link fence, standoff from a building. We had some over water installations; and of course the E-Systems Sinai Field Mission installation with barbed wire.

Most users appeared to be satisfied with E-Field performance. However, one user was experiencing problems in a salt environment. He was having high false alarm rates and extremely high maintenance costs similar to E-Systems' experience in the Sinai desert. In general, the older installations appeared to have the worst performance.

Over the past several years, however, equipment has evolved. Performance has improved and been proven in the right environments. The E-Field concept, consequently, is a leading candidate for non line of sight or terrain following installations and for use in layered systems. Selection of the proper type of E-Field and careful attention to installation and grounding details, will be specific to site and environment and of most importance to the ultimate success of the detector.

C.5.0 WORKSHOP SUMMARY: CCTV AND VMD EXPERIENCE - WES REDUS, CHAIRMAN

Video tapes of Video Motion Detector (VMD) testing done at E-Systems during 1981 were displayed and intrusion simulation methods were discribed. Both Video Tek and Wisco VMD processors exhibited at least a 90% probability of detection at a 95% confidence level in these tests.

Most of the workshop group held that there was still concern about the use of VMD as a sensor used by itself but they also agreed that it may be a good sensor to use together with other sensors to help process out nuisance alarms. There was still some concern that it might not have the high probability of detection in spite of the results of our tests.

CCTV and video motion detection are seen as an assessment tool affording detection, CCTV identification, alarm evaluation and then response in a very rapid sequence. There was, however, some concern whether probability of identification would be high enough to enable an operator to get a very quick evaluation of what was happening in the field. There was additional concern over nuisance alarm sources, discussion on what kind of clouds produced nuisance alarms and other inclement weather types which could conceivably cause high alarm rates. People who have worked in the closed circuit television area have reported that some of their cameras have had the searing of the image into the camera tube. Nobody reported scheduled maintenance plans for replacing vidicons every year or year and a half. However, a roughly two year life was reported for the Newvicon.

There were a few comments on video tape recording of alarms. Most of these were questions regarding whether a video tape recorder is sufficiently fast in response to an alarm in order to record a history of the intrusion as viewed by the CCTV system. We concluded that they're rather slow at present, but the new innovations in technology will soon allow video tape recording almost instantaneously. Another novel approach was mentioned, that is, a two-tube TV camera, a vidicon specifically for use at night and another one specifically for use in

daytime conditions; it was also mentioned that this type of camera should have a lot longer lifetime. Also human factors were mentioned; I believe Jim Prell suggested that research might be done into who would make a good observer of CCTV. I think that's something which probably should be investigated.

I'd say overall that CCTV was viewed favorably though requiring high maintenance and being a rather expensive approach to assessment. Weigh the alternatives, they're even more expensive.

C.6.0 WORKSHOP SUMMARY - ALARM PROCESSING SYSTEMS - DAN BUEHLER, CHAIRMAN

We had about 15 people in attendance, a good cross section of people having various processors in operation or who are bringing processors on line and some who are still in the design stage. Most everybody has a general purpose computer for their alarm processor and they use various manufacturers, various programs, various schemes. For example some utilities are using the computer to control the system, others are using it merely to provide a recording capability. Almost all had a dedicated computer, not dedicated necessarily to the perimeter security system but to the security function, so you have in it some other enrollment capability for access, and perhaps safety functions.

We had heard that software has been a problem and, in general, I think there's still a feeling that it is. In our workshop, we had people who developed their own in-house software, others had software developed by a computer company, and others who had changed the software that was given to them by the computer company. In essence, it was agreed, if there is expertise and experience available, software flows fairly readily; but, getting that experience, whether it's in house or it's from the supplier, becomes a fairly large problem.

Some utilities are using a computer in conjunction with a map display with perimeter sensors showing on a map, and with door sensors on a tallyboard and using the three light scheme. Some people had programs such that upon alarm, a map display would be brought up on a CRT. I

think the general agreement was that it was a good idea to have a constant indication of sensor state or sensor mode. This can be done with the map display and tallyboard. There's some concern, if you automatically brought a display up on a CRT, of what your sensor mode or sensor conditions would be and that it would distract the operator.

Most utilities felt very strongly that reset should be a positive action by the operator, not a gang reset and not an automatic reset. Line supervision and tampering indication should be a function that the processor furnishes. I was surprised that most people (even those who had it) did not feel that sensor selftest was an all important function. Most of them felt that the selftest function first, does not simulate an intruder and, second, does not test the entire sensor; and this is true.

As a rule of thumb, the utilities felt that one alarm per zone per day was more or less the acceptable threshold. Anything above that tended to be unacceptable and anything below that they could live with. This was with the guard forces going out for assessment, not necessarily with CCTV. One other thing that was mentioned by a participant was that when you get an alarm, bring that alarm indication up on a CRT but also give instructions to the guard pertaining to that particular zone. A few years ago this would have been out of the realm of being reasonable. With today's microprocessor technology, this is entirely feasible.

C.7.0 WORKSHOP SUMMARY: SPECIFICATION COMMENTS - BOYD BROOKS, CHAIRMAN

I would like to discuss the comments and proposed changes that we have developed as a result of our session on the specification that was given to you in the brochure handout. (Section 5 of this report presents the information contained in the "Workshop Specification".) In using the document the user should recognize several things. First off, the document itself imposes no requirements on anyone, but rather provides recommendations which are aimed at achieving a high probability of detection concurrent with a low false alarm rate and

a low nuisance alarm rate, for a site-perimeter security system. There is no intent in the document to confirm or justify any of the recommendations made in other sources, for example, the new Regulatory Guide 5.44. Additionally the user must recognize that the ultimate regulatory requirements may negate any of the recommendations that are now contained in it.

Multi-layer alarm processors as defined here and in the report are not currently off the shelf items. To support usage of the documents as a compilation of recommendations, we propose making some text changes. Where "shall" is used we would replace it with the word "should". Additionally we would emphasize that the report covers nuclear plant site-perimeter only and that the recommendations contained in it must be integrated with other plant requirements when they are implemented. Internal security certainly must also be considered when you implement any of the recommendations. Additionally, we would add the definitions of "and" logic, "or" logic and the "and or" time integration logic and the resulting effects on probability of detection and false alarm and nuisance alarm rates in multi-sensor systems.

C.8.0 WORKSHOP SUMMARY: SENSOR TEST BED DEMONSTRATION - RAY WALKER, CHAIRMAN

We were able to take observers up to the fourth floor of the MSTF test tower where our data collection and monitoring equipment is located and from that vantage point we were able to look out at the sensors under test. These included the Omni-guard 700 terrain following radar, the taut-wire fence, the BLID, the E-field fence, Stellar H-field, and the Omni-spectra 300 microwave link. I would like to stress that these sensors are on loan to us from the manufacturers. What we are doing is evaluating these sensors for our own use. Since we are systems integrators and not sensor developers, it behooves us to know what all the sensors will do and what they won't do so that, when we define a system for any specific site, we can call on our own background and knowledge and test evaluations and we don't have to rely on advertisements, words and phrases and so forth that are put forward by the sellers.

In addition to viewing the test bed you were given a short briefing and given a demonstration of an alarm processor which is currently under development by E-Systems. This unit is an alarm logic processor, it is not an alarm reporting system. It's not the processor that you would use in an alarm reporting system. What we're building is a experimental laboratory model to test the layering principle. It's not the final product you would put out to run your displays and alarms and so forth. It will interface eventually with the computer or alarm processor chosen to do the display. On the other hand, we may continue development to where we can do it all in one box...that hasn't been decided yet.

C.9.0 WORKSHOP SUMMARY: PROBABILITY TESTING - DON HALSEY, CHAIRMAN

I have a very short summary of our workshop on probability testing. Most of you would like to keep what you have in terms of equipment and operations. Most of you would like to keep the seven day test schedule that you have at the present time. Some of you have plans for layering not from the standpoint of saving on testing time but from the point of view of reducing nuisance alarms. You're really not interested in taking on the burden of the NRC 5.44 probability testing just for your own confidence that you have a system that has a high probability of detection. And it's doubtful whether you will be very happy to embrace the NRC guide if it ever becomes a regulation. You're really searching for some other way to prove that your system is in an up status and working and has a high performance. You would like to find some way of using the daily nuisance alarm manifestations for this purpose. I think that something like this is certainly worthy of looking at in some detail as an alternative to the probability testing that is suggested in the regulatory guide. We had about ten or twelve people involved in this workshop and most of them see Regulatory Guide 5.44 as unrealistic.