AVAILABILITY NOTICE

Availability of Reference Materials Cited in NRC Publications

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

1. The NRC Public Document Room, 2120 L Street, NW., Lower Level, Washington, DC 20555
2. The Superintendent of Documents, U.S. Government Printing Office, P.O. Box 37082, Washington, DC 20013-7082
3. The National Technical Information Service, Springfield, VA 22161

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

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

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

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

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

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

Single copies of NRC draft reports are available free, to the extent of supply, upon written request to the Office of Administration, Distribution and Mail Services Section, U.S. Nuclear Regulatory Commission, Washington, DC 20555.

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

DISCLAIMER NOTICE

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

NUREG/CR--5723

TI92 000596

Security System Signal Supervision

Manuscript Completed: September 1991

Date Published: September 1991

Prepared by
M. R. Chritton, BE Inc.
J. C. Matter, Sandia National Laboratories

BE Inc.
P.O. Box 381
Hwy. 278, Airport Industrial Park
Barnwell, SC 29812

Under Contract to:
Sandia National Laboratories
Albuquerque, NM 87185

Prepared for
Division of Safeguards and Transportation
Office of Nuclear Material Safety and Safeguards
U.S. Nuclear Regulatory Commission
Washington, DC 20555
NRC FIN L1387

MASTER

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

ABSTRACT

The purpose of this NUREG is to present technical information that should be useful to NRC licensees for understanding and applying line supervision techniques to security communication links. A review of security communication links is followed by detailed discussions of link physical protection and DC/AC static supervision and dynamic supervision techniques. Material is also presented on security for atmospheric transmission and video line supervision. A glossary of security communication line supervision terms is appended.

CONTENTS

SECTION	Page
ABSTRACT	iii
INTRODUCTION	1
1 LINE SUPERVISION AND PHYSICAL PROTECTION	2
2 SECURITY COMMUNICATION LINKS	3
2.1 Types of Links	3
2.1.1 Direct Wire	3
2.1.2 Leased Line	4
2.1.3 Multiplexing	4
2.1.4 Fiber Optic	6
2.1.5 Microwave Frequency Transmission	7
2.2 Typical Communication Link Segments	7
2.2.1 Sensor to Multiplexer	8
2.2.2 Multiplexer to Controller	8
2.2.3 Controller to Computer	8
2.2.4 Computer to Display	9
2.3 Communication Link Monitoring	9
2.3.1 Passive Communication Links	9
2.3.2 Active Communication Links	10
3 COMMUNICATION LINK VULNERABILITIES	11
3.1 Monitoring of Sensor Status	11
3.2 Loss of Communication Link	11
3.3 Shunting of the Sensor Signals	11
3.4 Substitution of Sensor Signals	11
3.5 Substitution of Similar Equipment	12
4 PHYSICAL PROTECTION OF THE LINK	13
4.1 Conduits	13
4.2 Burial	13
4.3 Access Restrictions	13
4.4 Tamper Switches	13
5 STATIC SUPERVISION TECHNIQUES	14
5.1 DC Supervision	14
5.1.1 End-of-Line Resistors	14
5.1.2 Tamper Alarms	14
5.1.3 Alarm/Access Mode	14
5.2 AC Supervision	15
5.2.1 Amplitude Monitoring	16

5.2.2 AC Phase Monitoring	16
5.2.3 Combined Waveform Monitoring	17
5.3 Multiplexing	17
5.3.1 Inherent Security	18
5.3.2 Multiplex Polling	20
5.4 Fiber Optics	20
5.4.1 Inherent Security	20
5.4.2 dB Level Monitoring	20
5.4.3 Microbending Detection	21
6 DYNAMIC SUPERVISION TECHNIQUES	22
6.1 DC-Randomized Voltage	22
6.2 Multiplexing	22
6.2.1 Randomized Polling	22
6.2.2 Signal Encryption	22
6.3 Fiber Optic Encoding	23
7 ATMOSPHERIC TRANSMITTED SIGNALS	24
8 CCTV LINE SUPERVISION	25
8.1 Video Presence Detection	25
8.2 Scene Dynamics	25
8.3 Tamper Detection	25
9 SYSTEM CONSIDERATIONS	27
GLOSSARY	28

FIGURES

2-1. Radial (star) transmission system	3
2-2. Series multiplexed system	5
2-3. McCulloh multiplexed system	5
2-4. Typical fiber optic link	6
2-5. Typical dual-loop multiplex configuration	7
2-6. Typical sensor-to-MUX link	8
2-7. Typical MUX-to-controller link configuration	9
2-8. Unsupervised alarm circuit	10
5-1. End-of-line resistor wiring	15
5-2. Tamper switch wiring	16
5-3. Dual-window supervision	17
5-4. AC amplitude monitoring	18
5-5. AC phase monitoring	19
5-6. Combined waveform monitoring	19
5-7. Effects of microbending in optic fiber	21
8-1. Typical fixed camera installation	26

INTRODUCTION

U.S. Nuclear Regulatory Commission (NRC) regulations under Part 73 "Physical Protection of Plants and Material" of Title 10, Code of Federal Regulations, specify performance requirements for the physical protection of special nuclear materials and associated facilities. For fuel cycle facilities using or possessing a formula quantity of strategic special nuclear material, paragraph 73.45(c)(1)(iii) calls for the use of detection and surveillance subsystems and procedures to discover and assess unauthorized activities and conditions and communicate them so that response can stop the activity or correct the conditions. For these facilities, an example reference system is outlined in paragraph 73.46. Paragraph 73.46(e)(7), in part, states that all alarm devices including transmission lines to annunciators shall be tamper-indicating and self-checking, e.g., an automatic indication shall be provided when a failure of the alarm system or a component occurs, when there is an attempt to compromise the system or when the system is on standby power.

Power reactor licensees are subject to the provisions of paragraph 73.55. Paragraph 73.55(e)(2) contains a requirement similar to the aforementioned fuel cycle facility requirement. This paragraph, in part, states that 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 purpose of this NUREG is to present technical information that may be of use to a licensee in developing a system to provide security of sensor signal communication links. By virtue of the nature of a NUREG document, the discussion of equipment or systems, herein, does not constitute acceptance or endorsement by the NRC.

1 LINE SUPERVISION AND PHYSICAL PROTECTION

The objective of this document is to explain the role and application of alarm communication link supervision in a security system. The vulnerabilities of the various types of alarm communication links will be analyzed, and methods of protecting against those vulnerabilities will be presented. Throughout the document, an effort has been made to describe only those technologies commercially available and to avoid speculative theoretical solutions.

An effective security system should have a proper balance of three basic elements: detection, delay, and response. The overall effectiveness is only as good as the weakest element.

- An adversary can set off alarms in the system and still take as long as needed to complete the intended task if the response is inadequate to counter the adversary's efforts.
- Superb detection and response capability are of little value if the adversary can trip a sensor, complete the job, and leave before the response arrives.
- An adversary can spend days defeating protective barriers with no fear of response if there is no detection.

The detection function consists of three components:

- Intrusion detection sensors generate alarm signals at the time of the disturbance.
- Alarm signals are transmitted back to a central monitoring station where they are annunciated/ displayed to system operators.
- Means are provided for rapid assessment of the alarm stimulus to determine if an actual intrusion is underway.

There are two parts to protecting communication links between sensors and the central monitoring station:

- Link physical protection. This involves physical protection such as cable conduit and tamper-protected junction boxes.
- Signal integrity monitoring. Electrical/electronic protection is provided by monitoring some signal characteristic, such as voltage level or digital-bitstream integrity.

2 SECURITY COMMUNICATION LINKS

To assure proper application of line supervision, it is necessary to first be aware of the different types of links available and the typical functions of each portion of the overall communication path.

2.1 Types of Links

Today's technology provides a multitude of options for transmitting data. Each type of link has some advantages, and many present-day systems employ several different transmission media along any given path from the sensor to the central station.

2.1.1 Direct Wire

Nearly every system uses direct wiring on at least one segment of its alarm communication link. Usually the link from the sensor back to an intermediate alarm collection point is direct wired. Systems which utilize a separate annunciator for each sensor or alarm zone are normally direct wired with dedicated wires from the annunciator to the device. Typically, a twisted wire pair ranging in size from #18 AWG to #22 AWG is employed. To reduce electromagnetic interference, the cables normally have a foil shield surrounding the wire pair. The radial, or star, transmission system is common for direct-wired applications (see Figure 2-1).

The advantages of direct-wired systems are the relative ease of installation and maintenance in terms of technical competence required. Also, failure of a wire results in the loss of only one alarm in a radial, or star, transmission system. Disadvantages include potentially high initial material and installation costs if long distances are traversed with a large number of cables. For a large system if each sensor is wired to its own annunciator and if a multiple alarm situation should occur, then operator confusion can be a concern. Future expansion can also be costly if new wires are installed from the device to the alarm station. Other disadvantages of wire communications include their susceptibility to electromechanical interference that can create nuisance alarms and radiation of information which could be detected and interpreted.

Figure 2-1. Radial (star) transmission system

2.1.2 Leased Line

One alternative to installing dedicated wire pairs from alarm device to alarm station is to use transmission lines that may be available from existing phone company installations. If long distances are to be covered, particularly if the data transmission is in the form of audible tones, then dedicated lease lines may be an acceptable cost-effective solution. Attacks against the link along the line will be difficult if the leased line is part of a large cable bundle. Precautions include ensuring that the lines used for communicating alarm data are not uniquely identified at any terminal boxes along the route and that the lines are not connected to any phone switchgear.

2.1.3 Multiplexing

A multiplexed system transmits signals from many sensors on a single communication link, so multiplexing is cost-effective for many different layouts. Another advantage of multiplexing is increased security since it is more difficult for an attacker to determine the status of a particular sensor and to defeat it. On the other hand, multiplexed systems can be complicated and may require a greater amount of technical expertise and test equipment for repair and maintenance than radial transmission. The advantages and disadvantages of some common multiplexing methods are described in this section.

2.1.3.1 Party-Line Multiplexing

A party-line multiplexed system transmits no signal as long as none of the sensors is alarming. When an alarm occurs, the signal is transmitted on the shared party line. An advantage of the party-line system is that any sensor can transmit an alarm signal at any time.

Sensors are connected in series in the simplest party-line system (Figure 2-2). One disadvantage of a series line is the inability to determine which sensor transmitted an alarm. Also, failure of one component disables the entire system.

In a McCulloch party-line system (Figure 2-3), each sensor transmits a unique identification so the receiver can determine which sensor is alarming. Sensors employing simple contact closure are unsuitable in this system without incorporating some means to transmit identification information. If two or more sensors alarm at the same time, the receiver may not be able to decode the resulting signal. This disadvantage may be insignificant if alarms are infrequent, making clashes unlikely. McCulloch multiplexing has been used successfully for many years; however, it is based on electromechanical devices that are becoming obsolete.

2.1.3.2 Time Division Multiplexing

Sensors transmit signals over a common link at predetermined time intervals in time division multiplexing (TDM). TDM solves clashing and identification problems by dedicating a unique period of time to each sensor. Failure of individual sensors is thus easily identified. The scan period, which is the time required for a transmission from every sensor, is constrained by the number of sensors and the speed by which the transmission line responds to changes.

The main disadvantages of a TDM system are that 1) a sensor cannot transmit an alarm signal at the instant it occurs but waits for its time slot and 2) clock synchronization is difficult to maintain.

Dead time is the length of time between two successive uses of the line by a particular sensor. The status of the sensor is unavailable during dead time, and, if an alarm lasts less than the span of dead time, it may not be transmitted to the central station. Dead time can be reduced by reducing the scan period, but the possible amount of reduction is limited. To solve this problem, the multiplexer can be designed to remember that an alarm has occurred, or the alarm sensor may incorporate a latching mechanism that ensures the alarm signal is present long enough to be reported. The number of sensors on the time division multiplexed line should be limited so that the dead time is shorter than an adversary's transit time through the sensor zone so that an intrusion is not missed by the assessment system.

Figure 2-2. Series multiplexed system

Figure 2-3. McCulloh multiplexed system

2.1.3.3 Frequency Division Multiplexing

Frequency division multiplexing (FDM) allows several sensor signal transmitters to share a communication link by assigning each transmitter to a specific frequency band. Thus, each sensor alarm is uniquely identified by the frequency band in which it transmits an alarm. FDM does not experience the disadvantages associated with dead time and synchronization inherent in TDM. However, FDM is usually more costly to implement than TDM.

2.1.3.4 Polling (Interrogation)

In polling multiplexed systems, a centrally located device manages the use of the shared communication line by interrogating the sensors. Each sensor inputs its status (e.g., secure, access, alarm, or tamper) to the line in response to an interrogation from the control processor. If each sensor is interrogated in a sequential order, the system resembles a TDM system. If the interrogation requests a response from any sensor with an alarm, the system is similar to a McCulloch system. Polling systems are commonly used in modern computer-based and microprocessor-based alarm communication and display systems. Factors to be considered in selecting a polling multiplexed system are the polling rate of the sensors, the delay time in reporting an alarm, and the number of sensors that can be managed by the system.

2.1.4 Fiber Optic

The use of fiber optic communication links in physical security systems is relatively new but rapidly gaining widespread application due to large bandwidths suitable for both high alarm data transmission rates and video transmission and immunity from electromagnetic interference. The basic components required for a fiber optic link are

- electro-optical transmitter
- electro-optical receiver
- fiber optic cable

The transmitter and receiver each have a power supply to convert electrical signals to light impulses and vice versa (see Figure 2-4). The fiber optic cable consists of a very thin strand of ultrapure glass or plastic surrounded by a thin cladding layer of glass or plastic. For single fiber cables, the fiber is surrounded by a cushioning buffer material and some type of fiberglass, Kevlar™, or steel-strength member, all contained in an outer jacket formed typically of high density polyethylene (HDPE) or polyvinyl chloride (PVC). Multifiber cables are manufactured in a variety of configurations with differing quantities of fibers. Cables for exterior direct burial applications have an extremely tough outer jacket of HDPE or PVC with internal strength members consisting of braided, thick strands of steel, fiberglass, or Kevlar™.

Because of the non-conductive nature of the fiber cables, they are immune to electromagnetic interference and cross talk between fibers and have relatively low path length attenuation compared to wire cable. Installation calls for relatively sophisticated equipment and specially trained personnel that, when combined with the cost of transmitters, receivers, and power supplies, make the use of fiber optics less practical for transmission of individual alarms and better suited for transmitting multiplexed communications.

Figure 2-4. Typical fiber optic link

2.1.5 Microwave Frequency Transmission

Microwave frequency transmission systems are line-of-sight systems employing transmitters and receivers to communicate alarm signals. They are useful where installation of cables is difficult or when the distances involved make the cost of installing cables prohibitive. Microwave transmission can easily be employed for distances of several miles as long as the transmitter and receiver antennas maintain a line-of-sight. This mode of data transmission is susceptible to interference from climatic events, and the equipment costs make it more cost-effective for transmission of a group of alarms from a remote location back to the central station.

2.2 Typical Communication Link Segments

A typical modern alarm communication system has several path segments along any given sensor-to-central station communication path. Each segment serves a slightly different role, requiring the use of different technologies for optimal performance. Today's systems frequently have sensors communicating in a star configuration with a nearby alarm monitor in the form of a multiplexer (MUX), which is one of several multiplexers all communicating in a loop configuration with a controller. The controller is communicating with a central alarm station computer, which is taking the information and presenting it via some type of display to the alarm station operator. Figure 2-5 shows a typical dual loop multiplexed system. One advantage of a dual loop system is its ability to sustain multiple line breaks with minimal loss of desired data. This particular configuration can incur a single break anywhere in the controller to MUX link with no loss of sensor status information.

Figure 2-5. Typical dual-loop multiplex configuration

2.2.1 Sensor to Multiplexer

A typical system will have four, eight, or sixteen separate sensors wired to a MUX located relatively nearby. If the alarm device does not have an internal end-of-line resistor, then it is wired to a terminal box where the resistors are installed, and this box is wired to the multiplexer. Twisted, shielded wire pairs are the standard medium used. Normally the MUX continuously monitors the status of all sensors connected to it, and reports that status when its turn arises depending on the type of multiplexing used. (See Figure 2-6.)

2.2.2 Multiplexer to Controller

A typical system will have several multiplexers reporting to one or two controllers. This multiplexed communication is typically sent over a single, twisted pair, although fiber optic or RF transmission may be used in lieu of wire, or even intermixed depending upon distances and other environmental considerations. Loop communications are often used to provide redundancy and protect against single-point failures. (See Figure 2-7.) The dual-loop system shown can sustain two line breaks anywhere in the two loops with no loss of sensor status information.

2.2.3 Controller to Computer

The controllers pass the information they receive from the multiplexers to the system computer. Advanced systems have backup computers, which are either fully redundant with the primary, or at least capable of maintaining essential communications flow.

Standard serial asynchronous communication is typically used, and the nature of the communication is the reporting of the status of all alarms. Evaluation of the messages sent to the computer is performed, with the computer requesting clarification of any data that appear to contain errors.

Figure 2-6. Typical sensor-to-MUX link

Figure 2-7. Typical MUX-to-controller link configuration

2.2.4 Computer to Display

The computer interprets the raw data arriving from the controllers and, through its software programming, translates it to presentable information which is then communicated to some type of display device. Possible displays include annunciator panels, map boards, and video display terminals. The specific type of cable used varies with the type of display utilized, but wire is most commonly used.

2.3 Communication Link Monitoring

Sensor communications links can be divided into two categories:

- passive links
- active links

Passive links are characterized by the fact that a signal is sent over the link only when a change in status occurs. Active communication links are characterized by a continuous or repeated status signal being transmitted between alarm devices and alarm stations. Note that in general throughout this discussion, sensor status conditions include secure, access, alarm, tamper, power failure, and communication failure, not just "alarms."

2.3.1 Passive Communication Links

Early alarm communication systems consisted of a relatively simple circuit with no communications occurring between the alarm station and the alarm devices until an alarm occurred. Figure 2-8 shows a basic version; no current flows until the alarm contact is closed, which completes the circuit and causes the annunciator to sound. The disadvantage of this system is that a line break will go unnoticed until the alarm is tested. Depending upon the frequency of that testing, an adversary could have a large amount of time to complete a task undetected once the line was cut anywhere in the circuit.

Figure 2-8. Unsupervised alarm circuit

2.3.2 Active Communication Links

Active links maintain a continuous signal between the alarm device and the alarm monitor. This allows for immediate detection of simple breaks in the link. Typical configurations have one signal representing the no-alarm (secure) condition, another signal for alarms, and an absence of signal (open or short circuit) to indicate failure or tampering. Depending on the mode of transmission, different techniques are available to supervise the lines. These techniques are defined as being either static or dynamic, and are discussed in detail in Section 5.

3 COMMUNICATION LINK VULNERABILITIES

Alarm signals are often transmitted over a relatively long distance from the sensor to the central station. An adversary who chooses to defeat a security system by attacking that communication link has several options available.

3.1 Monitoring of Sensor Status

In some scenarios, an adversary may not be sophisticated enough or may simply not have the need to intercept messages or substitute bogus signals into the communications link. It may be sufficient to merely monitor the status of the sensor system. Knowledge that a sensor has or has not initiated an alarm can provide information with which to make crucial decisions. If an adversary knows detection has not occurred, the adversary may proceed deliberately and continue use of stealth tactics to avoid detection. If an adversary is aware that an alarm has been initiated, several options become available. The adversary may attempt to avoid the subsequent assessment and thereby not be detected, resort immediately to use of force tactics to continue the task while minimizing delay, or opt to abandon the mission and escape before the response arrives. While this last option may be deemed a successful operation of the security system for this one instance, the adversary is free to formulate a new plan armed with the knowledge and experience gained on the initial attempt.

Depending on the type of communication link, alarm status information can be obtained without making a physical break in the link. Radio transmissions can easily be intercepted and monitored at great distances from the transmitter and its intended receiver. Even wire transmissions can be monitored by a knowledgeable adversary without disturbing the wire or its insulation.

3.2 Loss of Communication Link

A simple method of attacking a communications link is merely to interrupt it. Cutting a conduit and the wires contained within will certainly prevent an alarm signal from being transmitted over those wires. In systems which do not check the integrity of the signal path, such a line break could go undetected until the next time the system is tested. In systems which do monitor continuity of the signal link, a break will probably be detected, although a deliberate break or series of breaks might be intended to blind the alarm station by severing it from many sensor points. This could make it difficult for the central station to know which specific area was being attacked unless adequate compensatory measures have been planned and rehearsed.

Another way of causing a loss of communication link is to flood the signal stream with noise. Naturally occurring environmental phenomena or intentionally induced disruptive signals could block the intelligible transmission of sensor status and effectively create a loss of communication link.

3.3 Shunting of the Sensor Signals

A different category of attacks on the communications link are efforts made to spoof the alarm communication system into believing it is communicating normally with all sensors when in actuality it is not. The simplest method in this category is to shunt the sensor signal, thereby preventing its transmission to the central station. If allowed undetected access to alarm communication wiring at critical locations, an adversary with a basic knowledge of electrical systems could install a simple jumper to accomplish this task.

3.4 Substitution of Sensor Signals

Shunting, as discussed in Section 3.3, is the simplest form of substitution of the no-sensor signal to prevent an alarm response. More sophisticated attacks can be made if the adversary has sufficient additional technical expertise and equipment. If the normal (secure) sensor signals can be determined, an adversary could potentially substitute a bogus secure signal. Once again, undetected access to the link needs to be obtained to accomplish this task.

3.5 Substitution of Similar Equipment

Another method of attacking the detection system is to substitute a sensor emulating device for one of the monitored sensors. The substituted device could be preset to prevent it from generating an alarm, yet it would respond to the sensor system monitoring and testing in the same manner as the original. As in the two previous methods, denying undetected access to the link will successfully defeat an adversary's efforts to spoof the system into believing it is communicating with its sensors.

4 PHYSICAL PROTECTION OF THE LINK

Even a highly skilled adversary needs to gain undetected access to the link and have time to analyze the supervision in order to defeat it. The best way to assure the integrity of the sensor communication link is to achieve a successful balance of denying the adversary easy access to the system using various physical protection techniques, coupled with selection of a supervisory method appropriate to the perceived threat and type of link. This section will discuss various physical protection techniques which should be employed as appropriate.

4.1 Conduits

All signal cables, whether metallic wire or fiber optic, should be encased in a rigid-metal conduit. Where joints, pull boxes and other access points exist, it is advisable to tack-weld them shut to prevent access. Placing the cables in conduits reduces electromagnetic interference, which could cause nuisance alarms and makes it more difficult for an adversary to inductively monitor communications along the cable. Access which would allow shunting of the signal or substitution of a bogus signal is also made more difficult.

4.2 Burial

Where cabling runs outside buildings, underground burial is preferred, and encasement in concrete further enhances security of the link. Asphalt or concrete paving above the buried line also increases the difficulty for an adversary to gain access. It is advisable to install several spare cables to minimize the cost of future expansion or to allow reconnection of equipment should a line failure occur.

4.3 Access Restrictions

Consideration should be given to the placement of access points and routing of sensor communication lines. Whenever possible, lines should be routed through areas under protection and access points located within areas. When access to signal wiring is necessary for maintenance or other reasons, use of a two-person rule while the wires are accessible, followed by a test of associated circuit signals upon completion of work, is the recommended administrative control.

4.4 Tamper Switches

When signal wiring passes through an enclosure that allows access to the wiring, installation of a tamper switch should be considered. If the wiring is exposed and passes through a terminal strip, or if the enclosure is outside the area under protection, the enclosure should have a tamper-indicating device installed. Even if the signal wiring passes uninterrupted through an accessible enclosure inside the area under protection, a tamper device is still advisable. When feasible, enclosure tamper switches should be wired as a separate tamper circuit independent of any intrusion sensor circuits passing through the enclosure. This allows the system to discriminate between attempts to open the enclosure and attempts to tamper with the external sensor wiring. Although less desirable, in those instances where the enclosure is located at the same location as the sensor, the tamper switch may be wired in series with the sensor as described in Section 5.1.2.

5 STATIC SUPERVISION TECHNIQUES

Supervisory systems can be static or dynamic. Static systems represent the secure condition by an unchanging signal. The secure signal is more easily discovered and characterized by an adversary. Consequently the static system can be defeated by substituting a counterfeit signal. Dynamic systems generate a continually changing signal to represent the secure condition. Such systems are more difficult to defeat. The goal of a static supervisory system is to detect unauthorized access to the protected line or to prevent successful substitution of a counterfeit signal.

5.1 DC Supervision

Static DC supervision maintains a constant DC voltage across the protected circuit and, through the use of resistors, monitors the sensor status by measuring the current through the circuit. Specific techniques employed with static DC supervision are described below.

5.1.1 End-of-Line Resistors

Through the selection and use of resistors on (or near) the sensor output terminals, the status of both the sensor and its communication link can be determined. Figure 5-1 shows a typical configuration for end-of-line resistors in a DC-supervised system. The normal secure condition will have a specific current flow which is a function of the DC voltage applied to the circuit and the value of the end-of-line resistor, R_{EOL} .

In this example, a change in the sensor status that causes opening or closing of the switch contacts will result in a circuit resistance increase or decrease of 15 percent, which will generate an alarm. Ideally, the end-of-line resistors would be located inside the alarm device itself. The nearer the resistors are to the alarm output terminals, the fewer places are vulnerable to use of a simple jumper to shunt the alarm contact as described in Section 3.3.

5.1.2 Tamper Alarms

As described in Section 4.4, tamper switches on enclosures should ideally be wired as a separate alarm point. If it is necessary to wire the switches in series with the sensor alarm, the tamper devices should be wired as shown in Figure 5-2. Whereas an alarm will cause a change in current of ± 15 percent, operation of the tamper switch will result in overall circuit resistance, R_C , being infinite (open circuit), as in Figure 5-2A, or R_C will equal zero if wired per Figure 5-2B. The disadvantage of wiring the tamper switch in series with the sensor alarm circuit is that it makes it impossible to discriminate between activation of the tamper switch and attempts to short or cut the sensor circuit wiring somewhere along the communication link segment. Additionally, if the tamper switch is not near the sensor, assessment of both locations is necessary if a tamper indication is received at the central station.

5.1.3 Alarm/Access Mode

Certain alarm zones require that they be placed in an access mode for periods of time. In this mode of operation, the central alarm station computer still monitors the sensor status, but sensor intrusion alarms are not annunciated to the system operator. An example is an office area occupied during the day shift only, which is equipped with a detection system to protect the area during off shifts. It is desirable that the security system ignore the alarm signals generated by the motion detectors in the office on the day shift, yet still monitor the tamper devices to detect unauthorized insider access to the sensor circuits. Systems which utilize a single alarm circuit to accomplish both intrusion alarm and tamper alarm monitoring are referred to as dual-window. Figure 5-3 shows typical dual-window values. The current corresponding to the nominal end-of-line resistance value, R_{EOL} , results in communication of a secure condition. To minimize nuisance alarms caused by environmentally induced resistance changes, an alarm will not be generated unless the overall circuit resistance changes more than some predetermined percentage, in this example 10 percent. If the overall resistance changes too much, in this example more than 20 percent of R_{EOL} , it is reported as an indication of tampering. Therefore, operation of the sensor contacts shown in Figure 5-2A would cause a change of +15 percent in the overall circuit resistance, which

A. Closed Contact = No Alarm

B. Open Contact = No Alarm

R_C = Overall Circuit Resistance

R_{EOL} = End-of-line Resistor Value

Figure 5-1. End-of-line resistor wiring

falls in the range which generates communication of an alarm indication. Cutting the wires or opening the terminal box would create an open circuit, $R = \infty$, which would cause a tamper indication to be reported. Placing the sensor in access tells the monitor to ignore changes of less than 20 percent and report changes greater than that.

5.2 AC Supervision

Static AC supervision is similar to static DC supervision in that a steady-state AC voltage is applied to the sensor circuit, with the resistors replaced by complex impedance.

A. Closed Contact = No Alarm

B. Open Contact = No Alarm

R_C = Overall Circuit Resistance

R_{EOL} = End-of-line Resistor Value

Figure 5-2. Tamper switch wiring

5.2.1 Amplitude Monitoring

Systems which employ amplitude monitoring impose an AC signal on the sensor communication link and monitor the amplitude of the returning signal (see Figure 5-4). Changes in the alarm or tamper contact status will cause a change in the impedance, which will alter the amplitude of the returning AC signal.

The difficulty of defeating this type system is greater than for the DC system because of the need for more advanced equipment and increased electrical expertise.

5.2.2 AC Phase Monitoring

Systems which employ AC phase monitoring impose an AC signal on the sensor alarm lines and monitor the phase shift of the returning signal (see Figure 5-5). This method makes it more difficult to merely

Figure 5-3. Dual-window supervision

substitute end-of-line impedance; an adversary would need to use some form of more advanced waveform monitoring to assure the returning signal experiences no discernible phase shift.

5.2.3 Combined Waveform Monitoring

Some supervisory systems use a complex waveform generated by combining different AC waveforms and monitor the returning signal for changes. Multiple AC signals may be superimposed on a standard DC supervisory circuit, and the monitoring circuit observes the returning complex waveform for changes greater than the preset threshold levels (see Figure 5-6). An adversary would have to not only compromise their balanced current supervision, but would also have to successfully duplicate and superimpose the multiple AC signals.

5.3 Multiplexing

Types of multiplexing methods were described in Section 2.1.3. Most state-of-the-art systems use some form of multiplexing on one or more of their communication link path segments. It offers the ability to communicate more information in the form of digitized information on a smaller number of signal lines. A static system uses the same sequence and method of digitizing information each time it cycles through its associated sensors.

Figure 5-4. AC amplitude monitoring

5.3.1 Inherent Security

In a typical multiplex system, the status output from the sensor is connected via an AC- or DC-supervised link to a MUX that converts the status of the sensor into a digital format. Each MUX may have several sensor inputs, which it multiplexes and transmits to a central station. Frequently, several MUX units may be using the same transmission line to communicate with the central station.

An adversary with access to that transmission line would have a difficult time determining the status of any particular sensor. Knowledge of the exact multiplexing format being used and the corresponding equipment for that format are required to extract useful information. Substitution of a bogus signal for any one sensor status signal would be extremely difficult. Substitution of similar equipment would likewise be of little use unless the specific number and digitized addresses of all sensors connected to that MUX are known. Because a static multiplex system uses the same sequence and translation of information each time it cycles through its associated sensors, enhanced protection can be obtained by introducing some degree of randomness in the polling sequence.

During the design phase, cycle time for reporting of signals should be analyzed to assure an acceptable dead time period between sensor messages. If the dead time between successive reports for any sensor is of sufficient duration, an alarm signal may return to secure by the time it is reported again. Most systems use a latched alarm signal that does not return to secure status until the alarm has been reported. If a long cycle time is unavoidable, some systems allow critical sensors to be polled more than once per complete cycle, thereby reducing the dead time for those sensors.

Figure 5-5. AC phase monitoring

Figure 5-6. Combined waveform monitoring

5.3.2 Multiplex Polling

Most present-day security systems use a polling system that consists of an interrogation/response method of communicating. Some systems install a transponder at each sensor while others handle many sensors with a single multiplexer. The transponder is receiving communications from the central station at all times, but any particular transponder responds with its status only when it receives its own digitized address in the incoming message stream.

Thus, an attempt to substitute a no alarm signal for a particular sensor will generate an alarm unless the bogus signal is synchronized with the polling message. Substitution of similar equipment is likewise made difficult if the digital addresses for each sensor were assigned randomly.

5.4 Fiber Optics

As explained in Section 2.1.4, fiber optics transmission sends modulated light through a glass fiber. The most frequent application of fiber optics in alarm communications involves the transmission of multiplexed information or transmission through high or noisy electromagnetic fields.

5.4.1 Inherent Security

Because the information traveling through the optical fiber is digitized, the same advantages of multiplexed communications described in Section 5.3 exist. As a result of the unique nature of light transmissions, several additional benefits exist.

The information carried on a fiber optic link is sent as modulated light, which makes normal methods of electronic eavesdropping ineffective. Even given access to the fiber, special knowledge and equipment are required to interpret the information. Attempts to penetrate the cable sheathing carry the inherent risk that the relatively delicate fiber inside will be broken. Just damaging the fiber cladding can also cause the communication link to fail.

The physical size of the fiber makes it possible to group many fibers into small, tightly packed bundles. Determining which specific fiber needs to be attacked, and then locating that fiber within the bundle can be extremely difficult.

Techniques for eavesdropping on fiber optics communications are improving, causing fiber optic links to no longer be considered as inherently self-protecting as before.

Substitution of a bogus signal is still very difficult. An adversary will need to determine the information being transmitted without disturbing the data flow, then inject the bogus signal without disruption, which also requires removal of the original signal. In addition to the inherent difficulties in accomplishing these tasks, the following steps may be taken to deliberately defeat an adversary.

5.4.2 dB Level Monitoring

One static supervisory technique available for use with fiber optics involves monitoring the light intensity being received. The transmitter sends a test pulse periodically, or a constant light with a frequency different than the message traffic, which is monitored for signal strength in decibels. Attempts to tap into the fiber, which create even a slight leakage of transmitted light may then be detected as a dB loss. Injection of a bogus signal should then not only match this desired message content, but the strength should be precisely matched also.

5.4.3 Microbending Detection

Another supervisory technique utilizes a receiver that detects even minute deflections of the fiber. As light travels through an optical fiber, it is reflected internally as shown in Figure 5-7. As light exits the fiber, it creates a speckle pattern. This speckle pattern will change with even minute deflections of the cable, or microbending. Any movement of the fiber that alters the speckle pattern beyond preset limits will be detected.

Figure 5-7. Effects of microbending in optic fiber

6 DYNAMIC SUPERVISION TECHNIQUES

Dynamic supervision varies the sensor status signals over time. An adversary experiences great difficulty in learning the nature of the sensor status signals and then substituting a counterfeit signal. The ideal dynamic supervisory technique uses a random number sequence or key to encode each bit of data. The major problems associated with such an encoding scheme are the generation and the storage of the large number of random keys required. Security is reduced when the data rate is reduced and when one random key is used for several bits of data. Vulnerability and cost are increased by storing only enough random numbers to last for a specified time and then periodically supplying new number sequences.

A dedicated internal microprocessor or memory chip may be used to generate sequences of pseudorandom binary digits for encoding data. The encoding disguises both the data and the random number. If an intruder has access to the unencoded data or if a string of all ones or all zeros is sent, the intruder can determine the random sequence with only a few observations. The use of nonlinear feedback logic is more secure, but it does not make the system undefeatable.

6.1 DC-Randomized Voltage

A recent development useful in retrofitting an existing DC supervisory system utilizes a randomized DC voltage. By varying the voltage in a random fashion over time, successful injection of a false signal is improbable unless the random key is known.

A major advantage of this technique is that it may easily be installed to enhance existing static DC-supervised systems.

6.2 Multiplexing

The inherent security benefits of a multiplexed system can be enhanced if combined with a dynamic supervisory technique.

6.2.1 Randomized Polling

Use of the interrogation/response method of multiplexing was described in Section 5.3.2. The vulnerabilities of a static system, which polls all circuits in the same sequence each time, can be overcome by changing the sequence in a random fashion for each cycle. While changing the entire sequence each time is an option, a simple yet effective method is to merely change the starting address randomly each cycle. This allows the polling order to remain the same, but the interrogation will arrive at a different time each cycle. Attempts to substitute a prerecorded response will thus be detected. Attention should be given to the maximum possible dead time. If that time is too great, then the same start point can be used each cycle, but at the end of each cycle, one or more randomly selected sensors are polled. This will prevent simple substitution of a prerecorded signal.

6.2.2 Signal Encryption

Encryption involves changing the representation of message data as it is transmitted along the link. Most multiplexing involves the transmission of binary bits of data, meaning that each piece of data is represented as either being on or off, or a logic one versus a logic zero. These logic ones and logic zeros may be represented as different voltage levels, different tones, or different pulse lengths. By randomly varying this voltage, tone, or pulse duration for the logic ones and logic zeros, it becomes very difficult for an adversary to determine the status of a sensor or substitute a signal for that sensor.

Data authentication is a term used to describe a supervised communication mode in which the sensor status information is transmitted in the clear (unencrypted), but an encrypted data authentication word is attached to the message. The primary advantage of this mode is that permits easier troubleshooting of the communication system by maintenance technicians than fully encrypted messages.

New commercially available transponders have been developed that allow digitized encrypted message traffic beginning at the sensor itself. These transponders are sized small enough to be placed inside most sensor enclosures and function with interrogation/response multiplexing.

6.2.2.1 DES Communications

Most encryption devices used in general computer communications use the Data Encryption Standard developed in 1975 by the National Bureau of Standards. The transmitter sends out a parcel of information containing encrypted data. The receiver uses the proper decryption key to decode the data message and present it as an intelligible message to the central station operator. The DES algorithm provides more than 72 quadrillion (72×10^{15}) codes when a 56-bit key is used. Most security systems in use employ proprietary algorithms developed by or for the manufacturer.

A different key should be used each time a reset occurs to prevent playback of a prerecorded message stream following a system reset. The key should be changed periodically so that sufficient time is not available for an adversary to decipher the key and then determine and inject the no-alarm message before the next key changes the encryption for that message.

6.3 Fiber Optic Encoding

Many of the encrypting techniques that apply to multiplex systems apply to the fiber optic portions of a communications link. Additional techniques which are being developed specific to fiber optics include

- superimposing a randomly changing light frequency on the message pulse (Attempts to substitute message pulses will be detected when the superimposed light fails to correspond to the appropriate frequency.)
- applying DES encryption techniques to randomly shift the pulse duration representing the binary logic ones and zeros

7 ATMOSPHERIC TRANSMITTED SIGNALS

In applications where alarm communications use radio, microwave, infrared, or laser transmission, many of the previously described supervisory techniques apply.

By their very nature, atmospheric transmissions are more susceptible to undetected eavesdropping than cabled links. Signals sent from a transmitter to a receiver may be monitored at any point between them or at distances of up to several miles beyond the receiver. Very narrow beam, short range transmission makes eavesdropping more difficult for an adversary.

Atmospheric transmissions are also susceptible to electromagnetic interference. Ambient electromagnetic energy or jamming equipment can either mask or distort messages beyond the point of recognition or generate spurious signals.

Since detection of monitoring by an adversary is nearly impossible, protection of the information is needed. DES encryption has successfully been widely employed in radio transmission security for several years. Properly applied, it is adequate to prevent an adversary from extracting usable information or substituting a bogus signal. By itself, it does not prevent the use of jamming to block transmission of an alarm signal. To counter this, periodic, expected state-of-health messages should be utilized to verify that all sensors have reported their status.

While not truly supervisory in nature, most steps taken to reduce the atmospherically transmitted signal's susceptibility to natural interference will also enhance the ability to withstand jamming attempts. Examples include dual frequency transmissions, frequency hopping, spread spectrum transmission, repeated transmissions, and reduction of signal-to-noise ratio through the use of narrowband filters.

8 CCTV LINE SUPERVISION

Timely assessment of a received alarm is essential to accurate detection of intrusion attempts. Closed-circuit television (CCTV) systems provide one important method for accomplishing this assessment capability. Since the role of line supervision is to increase the probability of accurate detection by making the alarm system less susceptible to an adversary's attempts to defeat it, supervision of the CCTV assessment communications is strongly advisable.

8.1 Video Presence Detection

Large security system installations frequently have many more remote video cameras used for assessment purposes than central alarm station video monitors. This implies that at any given moment there is no way for an alarm station operator to visually verify the functionality of all cameras. Commercially available video loss detectors are a good method of supervising the CCTV signal line to detect loss of the video sync signal that occurs with camera or video transmission line failure or sabotage. Attempts to interrupt power to the camera or cut the video transmission lines will be detected and an alarm generated by the video loss detector.

8.2 Scene Dynamics

While video loss detectors work well at detecting a complete loss of the video signal from any given camera, it does not provide protection against fogging of the lens or other masking of the camera. Detectors are available which monitor the overall scene dynamics and will alarm on a change which exceeds preset limits. Some of these detectors monitor the average gray level of the fixed camera's field of view, and attempts to cover the lens will alter that ratio. Newer digital systems monitor specific pixels in various locations on the camera's imaging device and will generate an alarm based upon changes in those locations.

8.3 Tamper Detection

As with sensor signal lines, CCTV lines should be physically protected as described in Section 4 to prevent unauthorized access to the lines. If fiber optics are used to transmit the video signal, then the techniques described in Section 5.4 and 6.3 may be employed. No technology is currently available to allow real-time encryption of the video signal. Where coaxial cable is employed, it is impractical to attempt to connect access point enclosure, tamper-indicating devices in series with the video signal. Providing tamper alarms will normally require the use of a separate tamper alarm circuit wired into the alarm communication system. This, however, increases the costs with the addition of a dedicated wire pair and new alarm circuit. Figure 8-1 shows a typical fixed camera installation and the types of communication links employed.

Figure 8-1. Typical fixed camera installation

9 SYSTEM CONSIDERATIONS

As has been described, there is a variety of commercially available methods of supervising security communication links. As the level of protection offered increases, the cost typically increases also. The less expensive techniques are more susceptible to environmental constraints. For example, AC and DC line supervisory systems experience a high false alarm rate when the lines are exposed to large temperature fluctuations that vary line impedance or to high electromagnetic interference such as that caused by thunderstorms, power line fluctuations, electrical generators, or power transformers.

In a large security system, each communication link will likely travel through different types of transmission media and experience format changes between the sensor in the field and the display at the central alarm station. Each segment of that path needs to be evaluated to determine which supervisory method should be used for that portion of the path.

GLOSSARY

access mode means the operational state of an intrusion sensor in which only line-tamper alarms are displayed at the operator's console; intrusion alarms are not displayed, thus permitting traffic through the normally alarm-covered area. (See also secure mode.)

adversary means a person performing hostile acts against the interests of a facility; an adversary may be an insider or an outsider.

alarm status means the state of an intrusion detection sensor, usually expressed as alarm, no-alarm. Some systems also report a third category of alarm status, trouble, to indicate an open or short circuit.

annunciator means an alarm display device usually consisting of a lamp and audible alert.

assessment means the determination of the validity and priority of an alarm signal.

bogus signal means a false signal created by an adversary.

central alarm station means that location at which alarms are displayed for assessment and subsequent action.

closed-circuit television (CCTV) means a television system in which the signal distribution is limited or restricted, usually by cable.

closed contact means a switch, usually in a relay through which current may flow.

communication means the function of transmitting or interchanging information, including both transmission of sensor signals to a central processing station and transmission of response information to security personnel.

communication link means the physical equipment or medium used to carry signals from a transmitting device to the receiving device.

conduit means a hollow tube, usually metal, used to route and protect enclosed wiring.

controller means a device which manages the communications between several multiplexers and a central computer.

cross talk means 1) undesired transfer of signals between systems or between parts of a system. 2) undesired energy appearing in one signal path as a result of coupling from other signal paths; such signal paths may be wires, waveguides, or other localized or constrained transmission systems.

delay means the element of physical protection system designed to impede adversary penetration into or exit from the area under protection.

DES (data encryption standard) means an algorithm, established in 1975 by what was then the National Bureau of Standards, which provides more than 72 quadrillion codes (72×10^{15}).

detection means the function of a physical protection system designed to discover and to verify that an unauthorized act has occurred or is occurring, including sensing the action, communicating the alarm to a control center, and assessing the alarm.

electromagnetic interference (EMI) means disruptive signals caused by external sources such as lighting, electrical motors, power transmission lines, etc.

end-of-line (EOL) resistor means a resistor placed in or near the intrusion detection sensor alarm contact, used to allow DC supervision of the alarm circuit. Complex impedances are used for AC supervision.

FDM (frequency division multiplexing) means a method of multiplexing whereby each transmitter is assigned a unique frequency.

fiber optics means a method of transmitting information using a thin strand of glass or plastic and modulated light.

force means a tactic whereby an adversary attempts to penetrate a physical protection system by minimizing delay. (See also stealth.)

infrared (IR) means the region of the electromagnetic spectrum between the long-wavelength extreme of the visible spectrum, about 700 nm, and the shortest microwaves, about 1 mm.

insider means a person having authorized access to facility premises and information and who thereby has the opportunity to carry out or to aid others to carry out malevolent acts which could adversely affect the safety, security, or operational capability of the facility.

intrusion detection system (IDS) means a subsystem of a physical protection system which combines sensing, controlling, and annunciating functions such that intrusion attempts into the area under protection are detected and reported with a minimum of direct human observation.

intrusion sensor means a device which detects an unauthorized entry or attempted entry into an area under protection in response to an event or stimulus within its detection zone resulting from the intrusion; also called an intrusion detector.

laser means light amplification by stimulated emission of radiation, refers to a device which produces an intense, coherent directional beam of ultraviolet, visible, or infrared light by stimulating electronic, ionic, or molecular transitions to lower energy levels.

line supervision means capability of detecting tampering and/or circuit interruption, usually provided by digital modulation over circuit lines accompanied by interrogation and reply schemes.

microwave means extremely short electromagnetic wave, 1 GHz or higher in frequency, especially one shorter than 30 cm in wavelength.

multiplexing means the transmission of several independent signals on one communication link.

MUX (multiplexer) means a device which manages the communications between several sensors downstream and a single communication link upstream.

open circuit means an electrical term describing an incomplete circuit, caused by an open switch, a break in the line, or some other means of introducing infinite resistance in the circuit. (See also short circuit.)

open contact means a switch, usually in a relay, which has no current flow.

outsider means a person who does not have authorized access to facility premises and information.

physical protection system (PPS) means a security system concerned with physical measures designed to safeguard people and to prevent unauthorized access to equipment, facilities, nuclear material, and documents and safeguard them against damage and loss.

pixel (picture element) means the smallest resolvable detail that can be detected in a TV system, equivalent to one TV line of resolution.

polling means a multiplexing method whereby a particular sensor will only place its signal on the line in response to an interrogation from a controller.

radio frequency (RF) means an electromagnetic wave frequency intermediate between audio and infrared frequencies, named because of its application to radio communications, considered to be approximately 10 kHz to 100,000 MHz.

relay means an electrically operated switch which opens or closes contacts when voltage is applied or removed.

response means the act of alerting, transporting, and staging a security force to intercept the adversary and to stop him before his goal is achieved.

secure mode means the security state of a sensor during which no traffic is permitted through the area under protection and both intrusion and tamper alarms are displayed at the operator's console. (See also access mode.)

self test means a feature often available on sensors which allows them to be tested readily to determine whether they are functioning properly.

short circuit means an electrical term describing a circuit containing no resistance.

shunt means an electrical bypass of normal circuit wiring.

spoof means to defeat an intrusion sensor by means of any technique that allows an adversary to pass through the detection volume without generating an alarm.

stealth means a tactic whereby an adversary attempts to penetrate a physical protection system by avoiding detection. (See also force.)

tamper alarm means an equipment tamper alarm is generated by an attempt to modify or disable a piece of equipment; a line tamper alarm is generated by an attempt to modify the sensor in the communication path.

tamper switch means a device designed to produce an alarm when a piece of equipment is disturbed.

time division multiplexing (TDM) means a method of multiplexing which designates a unique period of time for each sensor's signal.

transducer means a device which converts one kind of energy into another kind of energy, typically when one is electrical, e.g., acoustic or mechanical energy to electrical energy.

wire pair means a set of two conductors, normally with separate and differently colored insulation, often twisted around each other and contained in an overall protective sheath.

END

**DATE
FILMED**

12126191