14. Alarm Communication and Display

Abstract. An alarm communication and display system (AC&D) transmits electronic signals from intrusion detection sensors, entry control devices, and video cameras and associated systems to a central alarm station and displays the information to a security operator for action. There are three key aspects and functions of an AC&D system. First is alarm communication which includes the functions of data collection and data communication. Second is alarm display which includes the functions of data processing and data presentation. Third is the operator function which includes data interpretation and action. State-of-the-art systems use computer technology and graphics to communicate information to the operator. The design of the system must consider the ability of the operator to monitor and maintain control of the AC&D system. The designer of an alarm display system must decide what information to display, how to present the information, how the operator will interact with the system, and how to arrange the equipment at the operator work station for optimum performance. Additional implementation considerations include reliability, availability and maintainability.

14.1 Introduction

Role of the Alarm Communication and Display (AC&D) System

An alarm communication and display (AC&D) system transmits alarm signals from electronic devices and systems to a monitoring station and displays the information to an operator for action.

More specifically, the alarm communication and display system is to:
- Collect and display data from the
  - Alarm (intrusion detection) system
  - Entry control (entry control) system
  - Video Management System (assessment and surveillance)
- Provide the human/machine interface
  - Provide overall status of site security system
  - Provide mechanism for operator input
- Support communication to others
  - To guards and response forces
  - To emergency personnel

14.2 Alarm Communication

14.2.1 Data Collection

Introduction

Data is collected from the alarm, entry control, video, and when applicable network, devices and systems that make up the physical protection systems (PPS) and is displayed at the alarm monitoring station.

Alarm System Data

Alarm system data includes signals from interior and exterior intrusion detection devices, from entry control devices, from devices that sense the integrity of the overall system and from duress devices.

Entry Control System Data

Entry control data also includes the data from the enrollment, or badging,
Define Physical Protection System Requirements

station where the credential is printed, the Personal Identification Number (PIN) is assigned and any biometric information is provided by the individual.

Video System Data
Video system data includes live video signals for live display, storage and recall. The data also includes signals associated with pan-tilt-zoom control.

14.2.2 Data Communication

Introduction
Data communication methods include wire, optical fiber and, when necessary, wireless links.

Wire Methods
Wire methods send signals using electrical (voltage) pulses. Wire methods include twisted pair wire (such as RS-232 cables or Category 6 cable) and coaxial cable.

The disadvantages of using wire is signal degradation due to line losses, signal impacts from lightning and improper grounding and signal impacts due to electromagnetic radiation.

Optical Fiber Methods
Optical fiber cables send signals using pulses of light. This method allows the signals to be sent over longer distances and at higher speeds.

- Optical fiber is 100 times faster than coaxial cable.
- Optical fiber is 1000 times faster than twisted pair.

There are two types of optical fiber: multimode and single mode. Multimode fiber uses an LED (or laser) that transmits light in several rays, or modes. Over long runs, the multiple rays become dispersed and may cause signal distortion.

Single mode fiber uses a laser source to transmit one light ray, or mode; and, can therefore, transmit the signals over a longer distance than multimode fiber.

Optical fiber is not affected by lightning, grounding problems or other sources of electromagnetic radiation. However, there are stringent installation requirements and, due to the equipment required, installation costs may be higher than installing wire. Single mode cable is more expensive than multimode cable. However, single mode fiber may be less expensive for longer runs since active repeaters are required when using multimode fiber over long distances. For data communication via optical fiber a transmitter and receiver is required to convert the electrical signal to light and back to an electrical signal. Each type of fiber has a minimum bend radius and some signal is lost at each connection or splice. In the nuclear industry, radiation darkening of the fiber is a consideration if the fiber runs through a radiation area.

Wireless Methods
Wireless communications use a radio or microwave frequency, or for very short distances infrared frequency, to transmit information. While this method of communications provides a useful solution when hard line communications are unavailable, wireless should not be considered as the main means of communications. Disadvantages of wireless links are signal loss due to jamming and susceptibility to interception.
Communication Network Topologies

Devices and systems may be connected directly to the alarm reporting system or the devices may be connected to field panels, which in turn are connected to the communications network. The network design should provide priority for alarm communication, especially when video signals use the same network. (Video signals use significant network bandwidth.)

Data communication networks have various types of topologies, or architectures, to transmit information from one device to another. Examples of communication network topologies include: star, bus, line, ring and tree networks.

Star Network

The star network uses a central computer to communicate with all other devices on the network. This is a common configuration, such as a hub or wireless router in a home network that connects a computer, printer and other devices. This is also the configuration used with RS-232 and RS422 point-to-point communications, for hardwired field and annunciator panels and older video systems.

Bus Network

The bus network is configured such that all devices are connected to a shared communications line. This configuration is commonly used with the motherboard in a computer and with RS-485 multi-drop communications.

Line Network

A topology similar to the bus network is a line network in which devices are “daisy-chained.” In this topology, the communication passes through each device and can be transmitted over a longer distance since each device acts as a repeater that keeps the signal strong between devices. Although this is the easiest way to add devices, implementation for large systems is very expensive.

Ring Network

A ring network configuration is a type of line network in which the devices at each end are connected forming a ring.
A second connection between devices in a ring network, called a “counter-rotating” ring, may be used to provide redundancy. However, a malfunctioning node can still be a single-point of failure; modifications to the ring can disrupt the network; and, the increasing the number of nodes on the network increases communication delays. A large number of nodes on redundant fiber loops may also result in an unstable network upon failure of one connection.

Ring topology has been used for over 20 years to provide continued communication in the event of a single cut. However, technology advancements now allow for configurations not constrained to a ring.

**Tree Network**

The tree network configuration is a hierarchical topology with a root node and branches. Note that unless there are at least three levels in the hierarchy or the network would be classified as a linear network. As such, the tree configuration is a hybrid combination of a star and multiple linear networks. Unless the root node fails, communication failures are isolated to the affected “branch” or “leaf.”

A tree network with redundancy uses redundant root notes with all linear nodes connected to both root nodes. This is a very reliable and robust network topology but can also be expensive to implement over long distances and as a redundant and diverse network. This topology is recommended for high security applications.
14.3 Alarm Display

14.3.1 Data Processing

<table>
<thead>
<tr>
<th>Introduction</th>
<th>There are three basic types of AC&amp;D systems and associated methods for data processing.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Annunciator panels – with or without data processing</td>
</tr>
<tr>
<td></td>
<td>- Independent systems</td>
</tr>
<tr>
<td></td>
<td>- Integrated Systems</td>
</tr>
</tbody>
</table>

**Annunciator Panels**

Annunciator Panels, as shown in Figure 14-1, are the simplest type of alarm reporting system and may or may not have data processing. In many small systems, the sensor information is directly wired to the annunciator panel to display the status of individual sensors or sensor zones. The status of each sensor is indicated by a set of colored lights and pushbuttons.

An annunciator panel is a simple system in which the electrical components and correlation with the sensors is easily understood. Therefore, the system is easy for the operator to understand and for maintenance personnel to troubleshoot and repair. However, complexity increases with the size of the system because separate circuitry is required for each sensor, or zone. Also, the larger the system, the larger the panel and the more difficult for the operator to learn to use. This type of system usually does not have the ability to automatically log assessments or provide for data archival.

Newer annunciator panels may incorporate small processors, or computers, to reduce amount of wiring and to provide additional information to the operator.

This type of panel may be optimal for small systems in which sensors are within a building, such as a home security system, or small geographical area.

**Evolution of Alarm Reporting Systems**

As processing technology became faster and more affordable, systems to monitor alarms, control access and manage video became available. Implementation of such systems became more complicated and has the potential to overload the operator.

**Independent Systems**

When alarm reporting systems implement independent alarm, entry control and video systems, there are “many systems and multiple displays” for the...
operator, or operators, to monitor and control (Figure 14-2). The pertinent information from each system is presented to the operator; however, the operator must monitor and be trained on multiple systems. Implementation and maintenance of each system is simpler when not integrated with other systems.

When the AC&D system integrates the alarm, entry control and assessment system there are “many systems and one display.” Integrated systems are more efficient for the operator, or operators. Only needed or prioritized information is presented to the operator. As such, the operator monitors and is trained on only one system.

Data is managed differently for the different types of displays. As seen in Figures 14-2 and 14-3, data can be managed by either the system or by the alarm station operator.
For annunciators without processing, the information is provided directly to the operator, who determines all subsequent actions. For annunciators with processing, the system provides pertinent information and may be capable of providing supplemental information upon request.

For independent systems, each system collects and stores the data collected and displays information per the designated configuration.

For integrated systems, each system not only collects and stores the data collected, but is also configured to discriminate what is displayed and provide automated control functions. For example:

- Alarms can be integrated with entry control such that the door alarm is not displayed when the entry control system provides authorized access through the door.
- The video for an alarm zone can be automatically displayed upon alarm.
- When operator function confirmations identity, the entry control system can display of the individual’s picture upon badge swipe.

### 14.3.2 Data Presentation

#### Introduction

There are several types of AC&D displays. Examples include:

- Annunciator panels
- Geographic maps or mimic displays and
- Computer monitor displays

#### Annunciator Panels

As described in earlier sections, for annunciator panels sensor information is directly wired to the panel to display the status of individual sensors or sensor zones. The status of each sensor is indicated by a set of colored lights. A disadvantage of this display is that the exact location is not presented. Also, for legal purposes, many agencies require records be kept of the alarms, alarm assessments and actions taken. When using most annunciator panels, these records must be generated manually.

The panel in Figure 14-1 is over 30 years old but such panels are still being made and sold for use in building fire panels, for small process control systems and where ruggedized interface is required.

#### Geographic Map Displays

An annunciator-type geographic map display, as shown in Figure 14-4 provides the alarm status information in a graphical arrangement that corresponds to the geographical location of the alarm. This provides the operator additional alarm information; however, modifications to an annunciator-type graphic display require significant modification to the display hardware.
Define Physical Protection System Requirements

Figure 14-4 – Annunciator-type Geographic Map Display

As computer systems became more commonly used at work, computer graphics displays became available for security systems, as shown in Figure 14-5. These systems originally used an older touchscreen technology such that the operator could interface with the system in a similar fashion as the annunciator panel – lights and pushbuttons. These systems provided not only the geographical location to the operator but were capable of logging assessment information and being interfaced with video systems. Modification of the display was also easier.

Figure 14-5 – Computer Graphics Geographic Map Display

Computer Monitor Displays

As computer systems became more powerful and more commonly used at home, operators became more comfortable with the mouse and keyboard interface with the computer. Computer displays, such as those shown in Figure 14-6, are able to provide more information, systems became integrated and operator responsibilities became more interactive.

In addition to displaying information on a map computer systems are now able to provide additional information in text form. A modern AC&D console may
include two displays: one with graphical information and one with text.

Figure 14-6 – Computer Text and Map Displays

14.4 Operator

14.4.1 Data Interpretation

Introduction

The human decision remains the most important factor in the alarm assessment process. The ability for the operator to quickly and accurately initiate appropriate action depends on the ability to interpret the data provided to the operator. Care must be taken to not overload the operator when designing and implementing the AC&D console. For large or independent systems, two operators may be necessary to monitor and maintain control of the security system.

A major task when designing a system is to identify the required operator functions and then the interface required to support the identified functions.

Human-machine interface considerations include answering the following questions:

- How should the information be presented?
- How should the equipment be arranged at the operator's workstation?
- How does the operator interface with the system?
- What information should be presented to the operator?
- How much information should be presented?
- When should the information be presented?

The human factors – ergonomics – of the various hardware components and software techniques should be considered. Because the operator spends much time at the console, the system should be designed to make the work area comfortable and easy to use (Figure 14-7).

Before designing the work area, consider the following factors:

- What the operator must be able to see (people, equipment, displays, controls).
Define Physical Protection System Requirements

- What the operator must be able to hear (other operators, warning indicators).
- What the operator must be able to reach and manipulate (computer controls, communication equipment).

The space around the operator consists of zones of varying accessibility and visibility (Figure 14-8). All displays and controls must be given spaced needed for their intended function. Displays should be visible from the operator’s normal working position and controls should be easily accessible. The operator should be able to identify controls rapidly and correctly.

Primary displays and controls – those displaying critical information – should be located within the operator’s immediate line of site, requiring very little eye or head movement. These displays and controls should be in or very near the center of the console.
The location of any support equipment should be related to its importance and frequency of use. Secondary displays and controls – frequently used displays – should be located such that very little head movement is required to view the display. Communication equipment, such as microphones and telephones, should also be within easy reach.

Auxiliary displays and controls – non-critical and infrequently used displays – should be outside of the secondary control area.

Another major task when designing a system is identifying what information to display to the operator. The basic information to display includes:

- Overall System Status
- Site Layout, including alarm zone status
- Alarm System Monitor Displays:
  - Alarm Annunciation: “lights,” horns, map, text
  - Location of the alarm
  - What sensor is in alarm
  - Time of the alarm
- Video Monitor Displays:
  - Live video
  - Assessment video
  - Surveillance video
- Entry Control Displays:
  - Entry control alarm events
  - Entry control logs
- Network Communication Status

The design should consider when to display information to the operator: always, upon alarm, upon request and never. For example, information to display:

- Always
  - Zone status - secure or access
  - Alarm status – no alarm, alarm, alarm reset, alarm acknowledged
  - Site layout – with or without zone status
  - Systems status, including status of backup systems and power
  - Operators logged in, including system administrator
- Upon Alarm
  - Alarm location and time (map and/or text)
  - Video of alarm zone
- When Requested
  - Alarm history
  - Procedural instructions
  - Entry control information

Techniques to organize and manage the information displayed can make the operator interpretation and action more effective.
Because of limited screen space, some techniques for managing the space include:

- Use of auditory alarms to alert the operator that an alarm has occurred. Different sounds can be used to separate classes of alarms.
- Using colors to emphasis and categorize information (for example: red for alarms.)
- Using separate computer monitors for graphic and text displays
- Using multi-layer graphics with links between layers. For example, a map of a floor plan may indicate there is an alarm in a particular room. Selecting the link to that room would bring up a display of the room and the specific sensor in alarm.

In many systems the processor can be configured to prioritize what is displayed. For example, alarms from sensors protecting nuclear material can be given a higher priority than other zones. Therefore, any high priority alarm would displace any lower priority message on the display if there is no room on the display for the priority alarm.

14.4.2 Action

<table>
<thead>
<tr>
<th>Introduction</th>
<th>The overriding design philosophy for any security system must allow for the operator to always be in command of the AC&amp;D system and be able to take appropriate action.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm Monitoring and Control</td>
<td>The operator must be able to monitor overall system status, respond to alarms, log assessment of alarms, place alarms in access or secure and request procedural instructions.</td>
</tr>
<tr>
<td>Alarm Assessment and Surveillance</td>
<td>The operator must be able to either perform video assessment of an alarm or be able to request guard or response force assessment of an alarm. When applicable, the operator should be able to provide video surveillance of an intruder or of a specific operation.</td>
</tr>
<tr>
<td>Entry Control</td>
<td>The operator may be required to control entry at some locations. The operator may be required to verify identity and authorization of an individual to some locations, such as into the Central Alarm Station. The operator may be required to verify entry for alarmed doors without entry control, such as delivery doors.</td>
</tr>
<tr>
<td>Communication with Others</td>
<td>The operator must be able to communicate with others, including guard forces, response forces, emergency responders, staff and employees, and maintenance personnel.</td>
</tr>
<tr>
<td>Operator Training</td>
<td>The operators must be trained to use the system and take appropriate action. The roles and responsibilities for the operator should be well established and documented in formal, written procedures. The operator should understand how to control the system during normal operations, abnormal conditions and during emergency and security incidents. The operator should not be overloaded and should be trained to not ignore alarms.</td>
</tr>
</tbody>
</table>
14.5 Implementation Considerations

14.5.1 Availability

<table>
<thead>
<tr>
<th>Desired System Characteristics</th>
<th>As stated earlier, the operator must always be in command of the system and be able to take appropriate action at all times. Therefore, there are implementation considerations for the system itself.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability</td>
<td>The primary design consideration is for maximum system availability. Availability is the ability of the security system to perform required functions, over the life of the system. Availability is commonly expressed as:</td>
</tr>
</tbody>
</table>
|                              | \[
| Uptime \quad \frac{\text{Uptime}}{\text{Uptime + Downtime}}
|                              | The availability requirement for a physical protection system is to perform required functions 24 hours per day, 7 days per week. |
|                              | Availability is related to the reliability of the equipment and the ability to effectively maintain the system. |

14.5.2 Reliability

| Introduction                  | Reliability is the ability of an item to perform a required function under given environmental and operational conditions, for a stated period of time. |
| Reliability Considerations    | System reliability design considerations include: |
|                              | - Selection of reliable equipment |
|                              |   - Quality components |
|                              |   - Rated for environment |
|                              | - Eliminating failure modes |
|                              | - Including appropriate redundancy |
|                              | - Design for system integrity |
|                              |   - Security |
|                              |   - Physical protection |
|                              | The system design should consider the quality and environmental rating of the components. Ensuring components are installed and operating well within specifications provides conditions for maximum availability for the component. |
|                              | Failure modes should be evaluated to understand the extent of the outage due to the failure. For example, in the tree network all components attached to a “branch” that becomes isolated from the network are affected, but the other branches remain unaffected. Installing redundant equipment on the same network branch would result in both being affected by the same outage. |
Define Physical Protection System Requirements

| Redundancy | Redundancy allows components to fail without catastrophic consequence.

Use of auxiliary or Emergency power sources – emergency generators, uninterruptible power supplies (UPSs) and batteries – provide for continued use of the security system during loss of normal power.

Although often difficult to implement correctly, implementation of redundant and redundant and diverse system servers (main system computers) provides continuity of service during scheduled and unscheduled outages.

Less difficult to implementation is duplicate and duplicate and diverse AC&D consoles (the workstations attached to the servers). High-security system requirements frequently specify that the system is to include a central alarm station and a diverse secondary alarm station.

Note:
Redundancy requires two, or more, operational and available systems. Some systems are designed such that the second system to automatically assumes control upon loss of the primary system. Other designs allow for the second system to be manually assigned control very rapidly upon loss of the primary system.

Redundant and diverse requires two, or more, operational and available systems in geographically separate locations.

| System Integrity | Maintaining system integrity ensures that the system continues to provide its security function and is not modified without proper review and authority. Methods to maintain system integrity includes design features for: denying access to the equipment and denying and detecting access to the information.

| Deny Access to Equipment | An alarm reporting system is of little value if the communications link for the system to the control center fails to report alarms because of accidental or intentional damage. The system computers, operator consoles, field panels and all network equipment should be physically protected by locating them within a secure area in which access limited to authorized personnel.

Communication wire or fiber cables should be physically protected by installation in metal conduit with all joints security welded.

Where possible, all cable runs should be inside the protected area of a facility to limit physical access to the data cables. The data cables can be physically protected by burying the communication lines when routed between buildings. Burial of the communication line can be costly for long distance: however the burial delays access to even the most determined attacker. During the planning stage, extra lines should be included to allow for future expansion or individual line failure. The cable can also be encased in concrete, or the soil directly above the cable/conduit, can be covered with concrete or asphalt. If the entire area surrounding the cable path is paved, any digging will be easy to detect.

To administratively protect the equipment, procedures, such as two-person rule and configuration management should be implemented. Configuration
management ensures that modifications to the facility or to the systems themselves are designed and installed to security standards and do not introduce vulnerabilities into the system.

Denying or detecting access to the system information includes restricting access to the system and system components.

Controlling access to the system includes providing intrusion detection and surveillance for the system and system components, including spare parts. Since the system administrator is considered one of the ultimate insiders, strict control of physical access to the system computer is critical.

Tamper alarms should be installed for all sensors and equipment, including field panels. Data links are vulnerable at the sensor and at various enclosures along the data communication route. At these points, additional security can be achieved by equipping the enclosures with tamper switches and equipment rooms with BMSs to indicate an intrusion.

Controlling access to the system itself also includes implementing password control. The operator and maintainer privileges should be restricted, such that the ability to modify the system is restricted.

The system network should implement inherent and available security features. One common temptation is to place the security hardware on an existing office network, which usually has a connection to the Internet. However, even with the availability of robust firewalls, keeping the system completely isolated from the Internet is the only highly reliable means for protecting the security system from an “outsider.”

Fiber optic transmissions are inherently self-protecting because the transmitter and receivers usually include line supervision, and network switches may include a port control feature that can be monitored. The drawback is that integration of network alarms into the alarm system itself is not fully developed. Therefore, separate network monitoring must be added to the operator duties.

Use of encryption, especially when communication lines are routed through lower security areas, can also increase security of the system. Some commercial systems have implemented proprietary or standard encryption techniques on portions of their systems. Independent encryption algorithms may often be implemented throughout or in sections of the network. Encryption can create significant communication delays and should be evaluated for impact to overall alarm communication and assessment time.

When the system communication protocol uses polling, the time to report and alarm depends on the time required for the local field panel to be queried. One advantage, however, is that the polling requires a response from the field equipment on a regular and frequent (less than a second) basis. Therefore, loss of communication with any field panel is an indication of line loss or tampering and can be indicated to the operator as an intrusion.
**14.5.3 Maintainability**

**Introduction**

Maintainability is the ability of a system to be retained in or restored to a state in which the system can perform required functions when scheduled or unscheduled maintenance is performed.

Impacts to not maintaining the system manifests results in implementing costly compensatory measures for the duration of the outage. Stationing personnel to protect radioactive assets is also a concern.

**Monitor Performance**

Periodic inspections and tests – scheduled maintenance activities – are necessary to ensure continued ability for and reliability of the system to collect and communicate the data from the systems. The tests should confirm continued operability and effectiveness of the systems.

Examples of items to inspect include:

- Data collection and communication of each alarm
- Wire terminations, which tend to loosen with temperature variations
- Sensor coverage which may be degraded due to age of the equipment
- Impacts from environmental conditions such as rain, dust, rodents and insect activity

Each facility should determine the inspection procedures and schedule for the systems based on the equipment installed and conditions under which the equipment operates.

**System Documentation**

Maintenance is easily accomplished when system documentation is readily available and maintained to represent the system as installed. Such documentation should include: vendor manuals, as-built drawings and site and system configurations. Establishing configuration management procedures for implementing changes provides an excellent mechanism for maintaining documentation in as-built condition.

**Efficient Replacement and Repair**

The ability to replace and repair the system – scheduled and unscheduled maintenance – is also necessary to ensure continued availability of the systems.

Consideration of the life-cycle of components and systems ensures that components are replaced before end-of-life failure.

Anticipating component failures ensures effective mechanisms are in place for maintenance of the system, and include:

- Modular design of the system to allow for rapid replacement and return to service.
- Frequently backing up the system software and alarm configurations ensures the most current system configuration, and thus operability and functionality, can be restored.
- Disaster recovery processes and procedures should be documented and practiced to ensure the system is correctly restored to full operability.
and functionality as quickly as possible.

The availability of security system maintenance resources is a major consideration for site operators. Trained maintainers and, for high security systems, the ability to respond to system outages 24 hours 7 days a week is critical to continued operation of the system.

Availability of exact or compatible spare parts and tools is also a concern for proper maintenance. Vendors frequently update algorithms and modify the physical configuration of equipment which can result in incompatibility of new components with the older system. In the case of one fire alarm system, the incompatibility resulted in a complete system outage.

Most importantly, is the absolute necessity for funding to ensure immediate availability of trained maintainers and adequate spare parts.

### 14.6 Summary

| Role | The role of the AC&D system is to collect and display data from the PPS, to provide the human-machine interface with the PPS and to support communication to others. The ability for the operator to quickly and accurately identify and assess an alarm and take appropriate action is the goal of the AC&D system. |
| Key Aspects and Functions | The three key aspects the AC&D systems are alarm communication, alarm display, and the operator. |
| Alarm Communication functions | Alarm Communication functions are data collection and data communication. |
| Alarm Display functions | Alarm Display functions are data processing and data presentation. |
| Operator functions | Operator functions are data interpretation and action. |
| Implementation Considerations | AC&D implementation considerations include: |
| | • Availability: 24 hours a day, 7 days per week |
| | • Reliability: reliable equipment, eliminating failure modes, implementing redundancy, and ensuring system integrity |
| | • Maintainability: monitor system performance, efficient replacement and repair, ensuring availability of resources and system documentation |