CHAPTER

38

Alarm System Fundamentals

Doug Durant, Kevin Pound, Jeffrey A. Slotnick

OUTLINE

Introduction 433

Alarm Monitoring 434
- *Local Monitoring* 434
- *Central Station Monitoring* 434
- *Direct Fire or Police Monitoring* 435
- *Proprietary Monitoring* 435

Operator Interface 435
- *Customized, Data-Driven Reports* 436

Alarm Sensors 436

Duress Alarms 438

Nuisance Alarms 438

Alarm Response 439
- *Fire Alarm Systems* 439
- *Fire Alarm Sensors* 440
- *Building Automation Sensors* 441
- *Building Automation Systems (BAS)* 441
- *Network Video Systems* 442
- *Integrated Systems* 442

Emerging Trends 442

References 443

CHAPTER OBJECTIVES

- Define an alarm system
- Explore the fundamentals of alarm systems and operations
- List four types of alarm monitoring
- Explain alarm sensors and how they work
- Describe fire alarm systems
- Provide effective alarm response guidelines
- Explain network video systems

INTRODUCTION

In many cases, alarm systems form the backbone of a facility's physical protection program. Universally used, alarms are very likely to be encountered by the protection officer or security specialist as they perform their daily duties. In fact, regardless of your industry, employer, shift schedule, or geographic location, it is likely that you will have some involvement with alarm systems.

An understanding of basic alarm systems and their operation should be considered a "core

https://doi.org/10.1016/B978-0-12-817748-8.00038-9
© 2020 Jeffrey A. Slotnick.
Published by Elsevier Inc. All rights reserved.

knowledge" requirement for anyone responsible for the protection of people, property, profits, and information. This chapter provides the fundamental information you need to know to be successful at your job. It is important to point out that this material must be supplemented with specific information as it applies to the alarm systems at your duty location. While all alarm systems perform the same basic function, each manufacturer's product may operate in a slightly different manner at the location. The site may require some specific alarm system component that makes the operation of the system different from other sites that you may attend or be involved with as a security practitioner.

Starting with the basics, a definition of an alarm system is in order. Quite simply, an alarm system is used to provide early warning of an intruder. There are three components to an effective alarm system: sensor, signal, and response. The "system" can consist of a relatively simple switch that activates a local audible device (e.g., siren and/or flashing emergency lights). If the system is monitored, a signal can be sent to alert authorities or response personnel, who can then investigate the cause of the alarm. It can also be quite complex, consisting of hardware and software elements that require considerable skill and training by assigned security staff.

The most effective physical security is "layered." An alarm system should be designed to provide one or more layers of detection around an asset. Each layer is made up of a series of detection zones designed to isolate the protected property and to control the entry and exit of authorized personnel and materials.

In more sophisticated systems, sensors are interfaced with electronic entry-control devices, network video, alarm reporting displays (both visual and audible), critical communications, and security lighting. As you can see, the alarm system can serve as a crucial "layer" in any physical security plan.

ALARM MONITORING

Your involvement with an alarm system will depend largely on how it is monitored. There are four methods of monitoring.

Local Monitoring

This is the simplest form of alarm monitoring. It consists of a bell or horn located near the protected door or window. In the event of an attempted penetration, the resulting sound is intended to alert nearby police, security personnel, neighbors, or company employees.

A major drawback of this approach is the fact that many people will not bother to investigate a blaring alarm. Furthermore, manpower shortages often make a security or police response impractical. Although relatively inexpensive to install, this form of alarm monitoring does not provide an adequate level of protection for most situations. Also, a potential criminal can disable these alarms relatively easily. In many jurisdictions, local municipal noise laws require the bells or horns to stop after a required period of time.

When activated, the audible alert tells the intruder his activities have been noticed. In many cases, this will scare the criminal off before the crime can be completed. However, in other instances, a seasoned criminal may realize a response is dependent on someone in the local area not only hearing the alarm but also taking action to investigate it. In short, the criminal may be well aware that he has a certain amount of time to "work," despite the activation of the alarm.

Central Station Monitoring

This is the best and most popular method of alarm monitoring. It consists of a company that is paid to provide monitoring services for a variety of clients. Typically, these alarm companies

charge a one-time installation fee and then bill monthly for monitoring services. Alternatively, many larger businesses may have all of their alarm signals monitored by their own control centers and have an in-house or proprietary security force respond.

When an alarm signal is received, an employee of the alarm company is responsible for notifying the police so they can respond. In most cases, a company's security officers are also notified so they can respond as well.

Despite its popularity, central station monitoring is not without problems. There have been several documented cases where the alarm company failed to make the proper notifications. Some alarm companies will provide their own security officers to respond to and investigate alarm conditions. In these instances, the alarm company's employees must be given keys to the protected premises in order to investigate alarms. From a security and business viewpoint, this should be considered an additional risk.

Mobile technology. Alarm communication is now available via mobile devices and mobile technology. More and more we are seeing this technology develop.

Direct Fire or Police Monitoring

This is no longer a common method of alarm monitoring. However, in some rural or remote jurisdictions, the local police or fire station will monitor alarms from their headquarters. When used, this method tends to be a relatively reliable way to monitor alarms.

Proprietary Monitoring

In this approach, alarms are monitored by the company's security staff. In most cases, a security control center is on the premises and serves as a focal point for all security operations. During an alarm event, the situation can be assessed by dispatching security staff to the alarm location or by using an integrated network video to "check things out."

In a proprietary monitoring approach, the alarm system is operated and controlled by the property owner. In most cases, this means assigned security specialists are adequately trained and are very familiar with their property and its various security systems. They have a vested interest because they are protecting "their" company.

A drawback, however, is that proprietary monitoring can be very expensive. This is because the company must not only buy the required monitoring equipment but it must also pay people to operate it. Likewise, a proprietary system may provide inferior results if it is not designed for the specific needs of a building and its occupants.

OPERATOR INTERFACE

Regardless of the type of alarm monitoring used at your current location, eventually the system's operation will come down to a human being. This person might be a monitor in central station hundreds of miles away, or they could be one of your coworkers, assigned to the security control system on the first floor of corporate headquarters. In all cases, the operator interfaces with the alarm. He or she interacts with the alarm system through devices that can be seen, heard, or touched, as well as manipulated. In most modern systems, visual displays and printers can be used to inform the operator of an alarm or the equipment's status. Likewise, audible devices are frequently used to alert an operator to an alarm or the equipment's failure. Such computer workstations permit an operator to acknowledge and reset alarms.

Visual displays. The type of display used to visually inform the operator of the system's status is determined mostly by the system's

complexity. Today, status information is usually displayed on computer workstations or large high-definition video screens.

Computer workstations provide great flexibility in the type and format of alarm information that may be displayed. Both text and graphic information can be presented in a variety of colors. Multiple alarms may also be displayed. If alarms are prioritized, higher-priority alarms may be highlighted by blinking, changing colors, or by using bold print, and so on. To assist the operator in determining the correct response, alarm-specific instructions may be displayed adjacent to the alarm information.

Audible alarm devices. In conjunction with the visual display of an alarm, the system must also generate an audible alarm. The audible alarm may be produced by the ringing of a bell or by the generation of a steady or pulsating tone from an electronic device. In any case, the audible alarm serves to attract the operator's attention to the visual alarm display. Most systems have a switch to silence the audible signal before the operator resets the alarm.

Logging devices. All alarm system activity (such as arming the system, disarming the system, maintenance, and system faults) should be logged and recorded. Logged information is important not only for security personnel investigating an event but also for maintenance of personnel checking equipment. This is especially important when trying to troubleshoot nuisance or "false" alarms.

Customized, Data-Driven Reports

Integrated systems can produce data-driven reports which can perform analysis on the various types of alarms. These reports are user configured depending on the type of reports needed.

Alarm printers. Alarm printers are typically of the high-speed, continuous-feed variety. The printer provides a hard copy record of all alarm events and system activity.

Report printers. Many modern systems include a separate printer for printed reports, which use information stored by the central computer.

Operator control. A means is required to transmit information from the operator to the system. The types of controls provided usually depend on the type of display the system uses. For example, keypads consist of a numeric or LCD display system that is generally provided with a 12-digit keypad and several function keys. These allow the operator to perform such actions as to secure, access, acknowledge, and reset alarms.

ALARM SENSORS

A basic alarm system is divided into three layers: perimeter protection, area protection, and spot protection. Perimeter protection is the first line of defense to detect a potential intruder. Alarm sensors on the perimeter are typically mounted on doors, windows, vents, and skylights. Since a vast majority of burglaries are committed to using such openings, it is important that they be a priority for protection. Commonly used perimeter sensors include the following:

Glass-break sensors. These detect the breaking of glass. The noise from breaking glass consists of frequencies in both the audible and ultrasonic range. Glass-breakage sensors use microphone transducers to detect the glass breakage. The sensors are designed to respond to specific frequencies only, thus minimizing such false alarms as may be caused by banging on the glass.

Balanced magnetic switch. Balanced magnetic switches (BMSs) are typically used to detect the opening of a door, window, gate, vent, skylight, and so on. Usually, the BMS is mounted on the doorframe, and the actuating magnet is installed on the door. The BMS has a three-position reed switch and an additional magnet (called the bias magnet) located adjacent to the

switch. When the door is closed, the reed switch is held in the balanced or center position by interacting magnetic fields. If the door is opened or an external magnet is brought near the sensor in an attempt to defeat it, the switch becomes unbalanced and generates an alarm.

Area protection is also sometimes called volumetric protection. The sensors used for this purpose protect the interior spaces of a business or residence. These devices provide coverage whether or not the perimeter is penetrated and are especially useful in detecting the "stay-behind" criminal. As a general rule, area sensors may be active or passive. Active sensors (such as microwave) fill the protected area with an energy pattern and recognize a disturbance in the pattern when anything moves within the detection zone.

By contrast, active sensors generate their own energy pattern to detect an intruder. Some sensors, known as dual-technology sensors, use a combination of two different technologies, usually one active and one passive, within the same unit.

Sensors used for area protection include the following:

Microwave motion sensors. With microwave motion sensors, high-frequency electromagnetic energy is used to detect an intruder's motion within the protected area.

Passive infrared (PIR). These motion sensors detect a change in the thermal energy pattern caused by a moving intruder and initiate an alarm when the change in energy satisfies the detector's alarm criteria. These sensors are passive devices because they do not transmit energy; they monitor the energy radiated by the surrounding environment.

Dual-technology sensors. To minimize the generation of alarms caused by sources other than intruders, dual-technology sensors combine two different technologies in one unit. Ideally, this is achieved by combining two sensors that, individually, have high reliability and do not respond to common sources of false alarms. Available dual-technology sensors combine an active ultrasonic or microwave sensor with a PIR sensor.

Proximity sensors. Spot protection is used to detect unauthorized activity at a specific location. It serves as the final protective layer of a typical alarm system. Assets most commonly secured with spot protection include safes, vaults, filing cabinets, art objects, jewelry, firearms, and other high-value property. These sensors (sometimes referred to as proximity sensors) detect an intruder coming in close proximity to, touching, or lifting an object. Several different types are available, including capacitance sensors, pressure mats, and pressure switches.

Capacitance sensors. These detect an intruder approaching or touching a metal object by sensing a change in capacitance (storage of an electrical charge) between the object and the ground. A capacitor consists of two metallic plates separated by a dielectric medium (an insulating substance through which electric charges can travel via induction). A change in the dielectric medium or electrical charge results in a change in capacitance, and thus an alarm.

Pressure mats. Pressure mats generate an alarm when pressure is applied to any part of the mat's surface. For example, an alarm is triggered when someone steps on a mat. Pressure mats can be used to detect an intruder approaching a protected object, or they can be placed by doors or windows to detect entry. Because pressure mats are easy to bridge, they should be well concealed, such as hidden beneath carpeting.

Pressure switches. Mechanically activated contact switches can be used as pressure switches. Objects that require protection can be placed on top of the switch. When the object is moved, the switch actuates and generates an alarm. Naturally, in such applications, the switch must be well concealed. The interface between the switch and the protected object should be designed so that an intruder cannot slide a thin piece of material under the object to override the switch while the object is removed.

DURESS ALARMS

In addition to perimeter, area, and spot protection, alarms can also be used for specialized applications. For example, duress alarms (sometimes called "panic buttons") are frequently encountered in many business settings. They are often concealed under a desk or countertop. Duress alarms are often used by receptionists, cashiers, bank tellers, security officers, and customer service employees engaged in transactions with the general public. In short, anyone who may encounter a threatening, hostile individual in the course of his or her work may find a duress device of value.

Duress alarm devices may be fixed or portable. Operations and security personnel use them to signal a life-threatening emergency. Activation of a duress device will generate an alarm at the alarm monitoring station. Police or security personnel are then dispatched to render assistance.

Fixed duress devices are mechanical switches permanently mounted in an inconspicuous location. They can be simple pushbutton switches activated by the touch of a finger or hand or foot-operated switches attached to the floor.

Portable duress devices are wireless units consisting of a transmitter and a receiver. The transmitter is portable and small enough to be conveniently carried by a person. The receiver is mounted in a fixed location within the facility. Either ultrasonic or radio frequency (RF) energy can be used as the communication medium. When activated, the transmitter generates an alarm that is detected (within range) by the receiver. The receiver then activates a relay that is hardwired to the alarm-monitoring system.

NUISANCE ALARMS

A vast majority of alarms are nuisance or "false" alarms. In many jurisdictions, this places a great deal of stress on local law enforcement agencies. Each time a police officer is dispatched to investigate an alarm, valuable resources are being consumed. To make matters worse, most faulty alarms are generated by the following:

1. User error
2. Poor installation
3. Alarm monitoring
4. Substandard materials
5. Employee indifference
6. Inadequate training and system information

Security officers and business owners must learn as much as possible about their alarm systems. Where are the sensors located? What type are they? Who monitors the system? Awareness is the first step in effective alarm management. There is simply no excuse for arming a security system only to have alarms activated because people are still in the building.

Similarly, at some larger facilities, people sometimes simply forget to turn the alarm system on. Checklists should be used to arm and disarm various parts of the alarm system as required during the business day. This will also provide documentation of who did what and will minimize the chances for oversights between shift changes.

When it comes to installation, many alarms are the result of inappropriate sensor selection or placement. Alarm installations and equipment selection are not jobs for amateurs.

Alarms are electrical/mechanical devices. As such, they require periodic maintenance. Routine operational checks should be included to ensure sensors and related components are working properly. For example, security staff should walk-test every motion detector each day. This involves physically ensuring that each detector is functioning properly.

Likewise, there is considerable truth in the saying, "you get what you pay for." Substandard materials can include sensors, mounting hardware, wiring, and even software. There is nothing wrong with going for the lowest bid on an alarm installation. However, make sure you are not chasing a false economy by using

inadequate materials which will break and require continual replacement and repair.

Many nonsecurity employees have little understanding of security issues. This includes even the most basic awareness of the company's alarm system. Often, employees will think nothing of coming into work early, staying late, or visiting the office on a holiday. There is usually nothing wrong with such an activity. However, if it results in continuous alarm activations, an employee awareness program is probably in order.

Nuisance alarms consume security and law enforcement resources which could be more usefully employed in other activities. Those which come to the attention of the police can also be expensive. The nuisance alarm rate has become so bad in many areas that local governments are now assessing fines on businesses and residences. These can run into thousands of dollars.

Your organization's ability to operate its alarm system may not only protect property but also help protect hard-earned profits as well.

ALARM RESPONSE

Earlier, the various types of alarm monitoring were discussed. In some cases, the protection officer or security specialist will be dispatched to investigate an alarm event. The alarm might be the result of an employee entering his office before the alarm is deactivated. It could have been caused by a stray cat wandering the interior of a warehouse. The simple movement of balloons, plants, or a sign from the building's air conditioning or heating system can activate a motion detector. Then again, it could be something much more dangerous.

One of the major problems with nuisance alarms is that they invariably reinforce a mindset that every alarm is a nuisance alarm. For both public law enforcement and private security, this leads to complacent attitudes and poor officer safety procedures. For the private sector protection officer, the following alarm response tactics are recommended:

1. Never assume an alarm event is "nothing." Assume you are responding to an intrusion until proven otherwise.
2. Maintain radio contact with fellow officers and your security control center.
3. Maintain sound discipline. Keep radio volume low. Secure noisy keys and other equipment.
4. If upon arrival to the scene, you detect broken glass or other indications of an intrusion, do NOT proceed into the building. Call the police and assume a position from where you can be a "good witness."
5. Evaluate all alarm information. Has there been just one alarm? Is there a series of alarms which might indicate someone is actually moving around the interior of the building? The professional evaluation of all alarms can assist you in determining where the intruder is. Relay this information to responding police units.
6. Know your company's policy for alarm response. Use common sense and avoid complacency that can lead to tragic consequences.
7. Know of or how to locate appropriate phone numbers and passwords for your monitoring station.
8. Keep emergency call lists, updated with appropriate call-out lists, as well as local authorities.
9. Any alarm system is only as good as the people who operate, monitor, and respond to it. Protection officers must be properly trained to respond to alarms. They must understand how their system works and the need to treat every alarm seriously.

Fire Alarm Systems

Of all the alarm systems, it is most critical for security officers to understand the basic operation and interaction of fire alarm systems. Fire

alarm systems are regulated by building and fire alarm codes adopted by the municipality in which the facility resides. Because different municipalities may adopt different codes, how a system operates or is installed at one location might be quite different at another location. As fire alarm systems are so essential for the safety of the employees and the well-being of the facility, it is critical to have a thorough working knowledge of the operation of the system and the security officer's role in its successful use. It is also very important to understand the proper operation of the system and the expectations of the fire department.

Fire alarm systems typically have a main control panel with a display. If necessary, additional displays can be installed in other areas. Larger systems may incorporate a graphical display of the facility and locations of the various sensors therein. Where the alarm must be monitored off- site, a communicator is installed to allow the fire alarm to send alerts to an alarm company's central station or, in some rare cases, to the fire department.

Like intrusion alarm systems, fire alarms can be connected with a number of devices on a zone. Newer, larger fire alarm systems (and intrusion alarm systems as well) utilize a multiplex loop, where all of the devices are connected on the same loop, with each device having its own unique identifier or address. This type of system is known as a multiplex or addressable system. The largest fire alarm systems integrate dozens or hundreds of control panels across several facilities, with a dedicated main computer in the company command center for monitoring.

Fire Alarm Sensors

The ability of fire to devastate lives and property should never be underestimated. Fire alarm sensors seek to prevent significant damage by detecting fires in their earliest stages, allowing protection officers and fire officials ample time to respond. Fire alarm sensors include[1]:

Heat detectors. These measure changes in a room's ambient temperature. They are programmed to a certain baseline temperature and when the room's temperature exceeds the baseline, a fire alarm is triggered.

Photoelectric smoke detectors. This type of detector contains an electric eye, generating a beam of infrared light within its housing. When smoke enters the detector, it refracts that infrared light and an alarm is triggered in response.

Ionization detectors. These devices contain a tiny amount of radioactive material, which creates radiation in an ionization chamber. Any smoke that enters will absorb some of the radiation and change the electrical charge within the chamber, prompting the device to send an alarm signal to the monitoring station.

Air sampling detectors. These are often used to protect rooms filled with sensitive equipment, such as computer servers. They continuously take in air from the room and analyze the air samples for smoke or combustion particles. If a positive result is received, the detector generates an alarm and in many cases, immediately causes a fire suppressant to be discharged within the room.

Beam detectors. These utilize an electric eye, which extends a beam of infrared light across an entire room, rather than within the housing of a photoelectric detector. They are most often used in rooms with very high ceilings, where it would be impractical to install and maintain a smaller detector. Again, the beam of light will be refracted by smoke in the room and an alarm will be triggered.

Flame detectors. These are able to spot actual flames, rather than sense smoke or combustion particles. They typically incorporate ultraviolet

1. J. Russell, personal communication, July 8, 2009.

light sensors, infrared light sensors, or visible light sensors.

Pull stations. These switches are strategically placed throughout a protected facility, and when a person observes fire or smoke, he or she is encouraged to manually pull the nearest switch, triggering a fire alarm and speeding evacuation of the area. Unfortunately, pull stations are easily abused. To activate a pull station in order to cause a false public alarm is a criminal offense in most jurisdictions; therefore, protection officers responding to such alarms should be prepared to enforce their organization's relevant policy or involve local law enforcement as appropriate.

Building Automation Sensors

Building automation sensors are typically used to measure and adjust the heating, ventilation, air conditioning, lighting, and other environmental conditions in a protected facility. They include:

Gas detectors. There are several different types of gas detectors, each of which will measure the levels of a particular type of gas in the air (such as natural gas, carbon monoxide, carbon dioxide, and radon). If the gas levels exceed a preset tolerance, an alarm is generated.

Level indicators. These are often applied to tanks that hold liquids or gases that are critical to a facility's operation. When the amount of liquid or gas in the tanks drops below a preprogrammed level, a notification can be sent to the central monitoring station or to personnel who will refill the tanks.[2]

Temperature sensors. As the name suggests, these measure the ambient temperature in a room. They are often utilized in rooms where scientific experiments are being conducted and the temperature must be kept extremely hot, extremely cold, or within a specific range. If the temperature falls out of the preset range, an alarm is triggered.

Power failure sensors. These are integrated with the electrical system of a facility. When a power failure occurs, a notification alarm can be sent to the central monitoring station. At the same time, devices such as backup generators and emergency lights can be automatically activated.

Integrated sensors. Some of the same devices used to detect intruders—magnetic door switches and motion sensors, for example—can be integrated with lighting systems. In this way, lights can be programmed to turn on automatically when a staff member enters a darkened room.

Building Automation Systems (BAS)

Building automation systems operate much the same, and in a similar configuration, as access control systems. Building automation systems control heating, ventilating and air conditioning (known collectively as HVAC), as well as lights. More expansive systems can assist in controlling elevators, escalators, and irrigation systems. Building automation systems may integrate with, or share the same software and hardware as, an access control system. Building automation systems share several industry standard protocols such as BACnet, which allows systems or components from different manufacturers to communicate with each other. Some BAS functions such as lighting, heating, and cooling can be controlled or initiated by security functions such as a swipe of an access card after hours. Still, other BAS functions can be controlled by the security system to act as a deterrent such as stopping the elevators from running or activating the irrigation system outside.

2. Ibid.

Network Video Systems

Network video systems allow dispatchers to watch over a large number of areas at once. They provide an excellent (and cost effective) way to monitor high-sensitivity and high-risk locations at all times, without needing to post a protection officer at those locations. The cameras used may be easily visible to the public or they may be hidden to the point of near-invisibility, depending on the needs of the organization and the locations at which they are stationed.

From the central monitoring station, a dispatcher may be able to view up to 16 separate images in real time on a single monitor (Nelson, 1999). Alternatively, he or she may view a single image at a time, and switch to other images on demand or at preset intervals. The video images may be in color or black-and-white format. According to Nelson (1999), color images are better for identification purposes, while black-and-white images have better performance in low light. Cameras may be stationary, but those with pan, tilt, and zoom capabilities can easily be installed wherever they are necessary. From the central monitoring station, dispatchers can control these cameras at will, in order to focus on locations or individuals that require close observation at a given time. These cameras can also be set up to focus on a series of locations, one after another, each for a preset length of time.

Network video cameras generally incorporate a method of recording the images they monitor. This allows protection officers to revisit images to verify descriptions of individuals and events and also to retain those images for use as evidence. At particularly sensitive locations, video may be recorded on a continuous basis, but this very quickly consumes a great deal of data storage space. Cameras that are integrated with other sensors—intrusion sensors, for example—can be set up to focus on a specific area and begin recording when an alarm is received from the associated sensor. A dispatcher typically has the ability to begin and end a video recording at any time and to take a single snapshot image. Images have typically been stored on video cassettes, in either real-time or time-lapse format (Ruiz, 1999). However, the current trend is for image files to be digitally stored onto computer hard disk drives either using digital video recorders (DVRs), or with several drives together, or onto large capacity storage devices known as network attached storage (NAS) or storage area networks (SANs). It is possible to connect the hard disk drives into a configuration known as a redundant array of independent disks, or RAID. Such a configuration has the capability of either manually or automatically backing up drives so that the failure of any one drive does not result in the loss of all recorded data. Other options for exporting images include CD-ROM compact disks, digital video disks, or even USB flash drives.

Integrated Systems

As security and fire alarm systems become more expansive in scope and operation, it is sometimes necessary to link the systems together under one controlling piece of software or application. Other times it is necessary to link various systems together, such as human resources systems, parking applications, and payroll systems, so that there is greater functionality and more accurate information flowing automatically between those systems. Such systems are generically referred to as "integrated systems."

Integrated systems and the fundamental use of integrated systems create system redundancy and improved reporting.

EMERGING TRENDS

Alarm systems have and will continue to form a part of a protection plan in the foreseeable future. However, the technology and reporting mechanisms that form part of an alarm system continue to broaden. As with any technology, end users will continue to look

for smarter, faster, and more economical solutions. The use of video analytics, in combination with network video, along with voice verification, will help to provide verified alarms. Alarm signals that generate attached video or captured images of the location of the alarm will provide the end user with a clearer picture and understanding of the situation and allow them to respond effectively. This will continue to help lower the false alarm rates and will help organizations comply with local and regional false alarm legislation.

Sensor technology continues to change, allowing for larger and more complex facilities or structures to be protected, along with new ways to send those signals. Methods of alarm notification continue to be explored with improved ways to provide mass notification alerts to the large employee or student populations. Instant messaging, text alerts, and cellular messaging are some of the options being used and improved.

References

Nelson, L. A. (1999). Designing operations centers. S. J. Davies, & R. R. Minion (Eds.), (2nd ed.). *Security supervision: Theory and practice of asset protection* (pp. 277–279). Burlington: Elsevier Science.

Ruiz, H. C. (1999). Security technologies. S. J. Davies, & R. R. Minion (Eds.), (2nd ed.). *Security supervision: Theory and practice of asset protection* (pp. 263–271). Burlington: Elsevier Science.