Business & Company Resource Center

a tad dated

Security Management, July 1998 v42 n7 p112(4)

Understanding central station design.

(security operation)(includes related article on backup systems)
Warner Speakman, Richard Brandon, Mel C. Urban

Abstract: Developing an effective central monitoring station for security requires planning. A central station usually consists of touchscreens that monitor alarms and intercoms, fire alarms, database computers and CCTV cameras. Adjacent to the main station is an equipment room which contains all other support devices. Before purchasing and installing equipment, factors such as building codes, electrical codes, room size, corporate security requirements must be considered.

Security managers should understand how a central station should be configured before beginning any integration project.

Central monitoring station is the nerve center of any security operation. Whether the station is proprietary or operated by a third-party service provider, the security manager must know enough about its design and function to make intelligent choices about its construction, initial setup, long-term operation, and maintenance.

A typical monitoring center consists of three touchscreen computer systems used to monitor alarms and intercoms; two additional PCs to manage the company's security database and to be used as a backup system; several fire alarm panels (the exact number depending on the size of the facility and the number of alarm points); and several CCTV monitors, usually one for every four to eight cameras.

The equipment room, which is usually located adjacent to the monitoring center, will contain multiplexers, VCRs, and the wiring and control racks for various systems, such as surveillance cameras and access control devices.

In addition to the actual equipment, however, the security manager who installs the company's proprietary monitoring station has several other important considerations. The security manager must pay attention to the size and functional layout of the equipment room; the company's control station must meet all local and national building and electrical codes; audio lines must be installed with extra care; all equipment must be backed up in the event of failure; and monitors and equipment must be positioned properly so as to be used most effectively by officers.

Equipment room. While the visible part of the operations will be the control station where the officers watch monitors and handle calls, the behind-the-scenes brain of any monitoring station is the equipment room. Video, audio, communications, and computer hardware should be centralized in this area, which should be located as close to the control station as possible for easy access and to minimize cabling costs. Also in this room will be industrial processors, intercom controls, programmable controllers, multiplexers, and switching devices. If the monitoring station and equipment room are located in a high-security facility, such as a prison, they should both be constructed with reinforced concrete - essentially making them security vaults.

Build for future growth. The security manager should ensure that the equipment room is planned with the future in mind. The room should be large enough to accommodate not only the equipment being installed at the time but also additional devices that might be needed to meet growing demand. If the company plans to double the size of its facility within the near future, for example, the security manager putting in a new station should set up an equipment room capable of meeting that future capacity requirement.

Neatness counts. It is vital that the equipment room remain neat and clean. Dust and dirt will cause operational problems for electronic equipment. Furthermore, an untidy equipment room with wires coiled together like a bowl of spaghetti can be more difficult to maintain and fix when problems arise. Panels, such as circuit breaker boxes and input/output devices, should have doors that are easily accessible and can be closed to protect instruments against dust.

Cables should be labeled using a technique like the Brady labeling system, which uses nonremovable, easy-to-read tags on all wires. Tied-on or taped-on labels eventually fall off. The longer it takes for maintenance personnel to identify wires, the longer a security system may be down when a problem arises.

The security manager should also set up the equipment on racks in such a way that "status indicators" are properly displayed and easy to read. The indicator will show the status of the particular piece of equipment on an LED or meter, telling security whether the machinery is experiencing any problems.

Equipment status should be checked at least weekly by either security or facility management personnel. For example, the LED of a microprocessor will say either "communication OK" or "processor fault," meaning that it has lost communication with, say, a PC or access control panel. Although all systems are different, quality systems have features that allow the security manager to determine quickly where the fault has occurred.

Electrical codes. All equipment wires must meet the national electrical

accessible to electricians when problems arise. However, because the wires are exposed, they can be susceptible to damage from rodents, vandalism, and other sources.

The security manager should determine which method to use based on the company's requirements as well as local building codes. For example, some local jurisdictions require conduit to be used in certain areas where large machinery is operated, such as a warehouse.

When using open racks, troughs, or large conduit, the security manager should ensure that electricians do not mix voltages and classes of cable, such as 120 A.C, and low voltage cable, in the same ducts. Doing so can cause wires to interfere with each other, creating noise for equipment, which may then malfunction.

Audio wiring. Audio systems can be the trickiest aspect of the entire security system installation, The slightest interference in the signal can make it difficult for security to hear audio messages.

Induced voltages caused by improper shielding or audio wires that are too close to an A.C. system will cause a hum on the audio signal that will make it difficult to hear messages transmitted over these lines. In rare instances, equipment can be damaged by these induced voltages.

Audio wires should be grounded, shielded, and installed using a twisted pair method in which two wires are wrapped together. These measures protect the wires from other electrical devices and eliminate "noise."

Operator friendly. Monitoring stations must be easy for operators to use. Officers will spend many hours working in the station. If equipment is difficult to see or use, it may cause operator fatigue and make officers less effective.

The positioning of the equipment will affect how quickly officers can interpret signals and react to an incident. For instance, video monitors placed either too high or too low may be out of the officer's direct line of vision. Monitors should, therefore, be installed at approximately eye level.

The size of the room is also important. As in the case of the equipment room, the security manager should ensure that the station is large enough to handle future growth. If the company plans an addition to its corporate headquarters, the central station should be large enough for the number of officers and equipment that will be needed to monitor the added space. The security manager wants to avoid having to split the station between two rooms.

At the same time, the station should not be too large. In general, an average control room that will hold two to three officers should be about

225 square feet. If a control center must be larger in anticipation of future growth, it should be laid out so that equipment is concentrated in a small area so that it can be quickly accessed by security staff,

Software. When purchasing software for access control, alarm monitoring, surveillance, and other systems, the security manager will have to choose between proprietary software and off-the-shelf software. Proprietary systems used to be required because of the special needs of security equipment, but this is no longer the case. Off-the-shelf applications save time and money in training and setup. These products typically use a Microsoft Windows 95 or NT operating system with open architecture to allow the system to run in a multitasking environment.

When looking at various security system software packages, the security manager will have to choose between touchscreen technology and a mouse-based, point-and-click system. Both are icon-driven and allow officers to call up camera images, check access control points, or activate intercom systems by either touching the screen with their finger or using a mouse to point-and-click on an icon.

Touchscreen technology is an add-on feature to most security systems and will require additional software and hardware, including a computer monitor that responds to touch. Touchscreen technology will add about $1,000 per computer to the cost of a security system. Both touchscreen and point-and-click technologies are effective, but touchscreen is slightly easier and quicker to use.

In well-integrated systems, touchscreen or point-and-click systems allow for event-driven capabilities so that when an alarm goes off in one part of a facility, the computer automatically calls up images from the cameras in that part of the building.

Graphic panels. In small operations where computer-based systems are not economical, security can use a graphics panel, which is an electronic panel that is hardwired to field equipment, such as surveillance cameras, CCTV switchers, intercom hardware, and access control equipment. The panel usually has a representation of the company's building on it (usually a map that is engraved, etched, or painted on the panel) with alarm and monitoring points indicated with LEDs. When an alarm goes off in the building, a light on the panel illuminates, showing officers where an event has occurred. Officers must then turn to a CCTV monitor and call up an image from the camera in the area where the alarm occurred.

Access control. Access to the critical security systems in the central station must be restricted not only through computer security, such as the use of passwords, but also through physical security. An access control system should prevent unauthorized personnel from entering the monitoring center and equipment room.

The use of an interlocked sally port entrance system provides added security. Under this system, a person must walk through two doors to enter the control room. The doors cannot be opened at the same time, which prevents a criminal from attempting to rush into the control room when an officer is exiting.

The best access control system is one that keeps an audit trail of all those who use it. Cards or some combination of cards with biometric readers or keypads that require authorized users to provide a fingerprint or personal identification number before they can enter are advisable.

Cameras should be positioned to watch the room's immediate perimeter. Windows should be narrow or barred. In addition, the station should be equipped with panic buttons that send an alarm to local police in the event that there is a break-in and officers are held hostage.

Central stations offer many benefits to security departments and their corporations, but as the electronic brains that run every security system, these systems also can create headaches. To avoid trouble, security managers need to direct the planning of these facilities with careful forethought and attention to detail.

Backup Systems

Any downtime in a computer system can create the opportunity for a security **breach**. Therefore, another key component to consider when building a monitoring station is the necessity for adequate backup systems. There are two types of backup typically used at a central station: redundancy and hot backup.

Redundancy. With a redundant system, two or more computers act independently or concurrently, running everything from access control to CCTV. The PCs are operating at the same time, with each capable of running the entire security operation by itself. If one computer goes down, the other continues operating with no interruption to security systems.

In large facilities, the security manager can split security functions between multiple PCs. For example, one PC may monitor access control, alarms, and CCTV in the west wing of a building, while the other runs the same systems on the east side. Either system can be used to monitor the entire building if one PC goes down. Redundancy is the most effective backup, but it tends to be slightly more expensive than hot backup since the company must pay to operate multiple computers at all times.

Hot backup. In a hot backup system, the company has two computers equipped with all of its security software. However, only one PC is used to run the system. The second one may be used for other functions, such

as word processing for writing reports. The backup computer kicks in only if the primary PC goes down.

While a hot backup is less expensive, it creates a slight delay. It can take a few seconds before a hot backup PC begins operating the security systems after the primary computer has malfunctioned. This is because the operator must reboot the backup system or switch software operations and call up the security system on the backup PC.

Other options. The security manager should also consider hiring a third party to act as a backup central station if the proprietary center goes down completely. This option can be expensive, however. When using a contract service, the security manager should establish two modes of communicating signals to the remote center, such as telephone lines with a cellular or radio backup.

When purchasing equipment for the center, the security manager should negotiate for spare parts. One or two spare CCTV monitors as well as extra panels for intercom and access control systems, for example, should be on hand.

Power supply. As part of the backup system, the security manager should use uninterrupted power supplies (UPS), generators, or both. A UPS is basically a battery backup system with an inverter that kicks in immediately after the primary electrical power is lost. There can be virtually no interruption in power, and computers can operate on a UPS for about two hours.

Generators provide longer-term backup. They can run indefinitely as long as they are fueled; however, they take ten to twenty seconds to resume power, which can cause a serious security **breach** if they are used to back up security systems. In most cases, therefore, a UPS is used as the principal backup for a computer and security system, while generators are used for lighting and other general building power operations. Generators can also be used as secondary backup for security operations if power is expected to be out for long periods.

The security manager should also ensure that all computer systems are equipped with high-quality surge protectors, which guard the machines against sudden changes in voltage, such as lightning strikes. Many security professionals believe that the UPS is a surge protector. It is not.

Some UPS systems have a form of surge protection, but it is not as reliable as a quality silicon avalanche device, or SAD. A SAD uses a semiconductor to short out the surge. This differs from a varistor-only surge protector, which is usually good against only one major surge. A varistor device can cost less than $10, while a SAD can be priced at more than $100 - but it is worth the extra cost.

Warner Speakman is the founder and president of ESI Companies, Inc., of Memphis, Tennessee, which installs central stations and security equipment in prisons. Richard Brandon, PE (professional engineer), is the company's vice president of engineering, and Mel C. Urban is vice president of local services and an expert in communication systems.
Bus. Coll.: 110P2929

Article A20976818