2 page(s) will be printed.

Back

Record: 53

Title:	***Facility Security***: Access Systems--Part 1.
Source:	EC&M Electrical Construction & Maintenance, May2000, Vol. 99 Issue 5, p70, 4p, 2c
Author(s):	Rosenberg, Paul
Thesaurus Term(s):	SECURITY systems
Other Term(s):	ACCESS control
	NAICS/Industry Code(s)56162 Security Systems Services;
Abstract:	Part I. Focuses on access control systems' use of keypads, magnetic card readers or proximity readers to secure a ***facility***. Electronic access systems; Identification means; Controllers.
Full Text Word Count:	1354
AN:	3166830
ISSN:	00134260
Database:	Business Source Premier

Section: Correspondence Course

FACILITY SECURITY: ACCESS SYSTEMS--PART 1

Access control systems typically use keypads, magnetic card readers, or proximity readers to secure a facility from unauthorized access.

One of the most important objectives of modern security systems is to keep unauthorized people out of a facility. Locks and keys are among the most trusted methods for deterring unwanted visitors, due primarily to the simplicity and reliability of the technology. But lock and key systems have no intelligence built-in, and you can't program or easily reconfigure these systems.

Today, electronic access control systems are becoming more popular. These systems are extremely flexible, and you can program and quickly reconfigure them in an infinite number of ways.

We begin our coverage of "Keeping Them Out" with a discussion of a variety of access system technology currently on the market.

Electronic access systems. An access system allows only authorized people to enter certain areas of a facility. This technology goes one step further than the standard intrusion detection system: Rather than detecting an intruder who enters the facility, the access system keeps the intruder out all together.

The access system performs this function in one of several ways--virtually all of which involve automatic door locks and some sort of identification means. All modern systems have some type of microprocessor-based control to identify those people allowed in certain areas at certain times.

Access control systems are becoming increasingly popular for the following reasons:

- **Reduced risk.** By regulating access, you can protect valuable assets, reducing potential losses to a

manageable level of risk.

- **Lower overall security costs.** The use of an electronic access system may reduce the number of security guards required, which can save a lot of money in a large facility.
- **Improved morale.** When installing access systems, employees generally have a more secure and worry-free attitude, which tends to improve morale and production.

Of course, the simplest form of access is the keyed lock. However, criminals can easily duplicate or steal a set of keys. And when keys transfer from one person to another, losing them is a concern.

By using other identification means--electronic locks and microprocessor-based logic control--you can benefit from a much better system design. Not only can you gain better access control, but you can also unite this system with an intrusion-detection security system, making a more effective overall system. The three basic parts of the system are identification means, microprocessor-based, and control. Let's take a look at each in more detail.

Identification means. To operate an access system, each person who is authorized to enter the facility needs some type of identification. The system only grants access after identifying the individual.

Many different methods of identification are available for security. Let's look at some of the more common ones, along with their advantages and disadvantages.

Keypads. Keypads use push buttons, which look similar to a touch-tone phone. Personal access codes (PACs) or personal identification numbers (PINs) are the keypad code sequences assigned to a user. Each user obtains a PAC or PIN, which usually consists of four to six digits. Most systems have 48,000 different combinations or user codes.

When you enter the code into the keypad, the electronic lock opens; if you enter it incorrectly, the door remains locked. However, this type of system has its problems. Authorized users sometimes pass these codes to friends and family members, thus increasing the possibility of an illegal entry. One way to combat this breakdown in security is to give each employee his or her own identification number. Doing this not only cuts down on problems with former employees (when an employee quits, you deactivate the number), but it also gives more control. Certain people can have access only to certain doors. Some of the more advanced systems can record which employee was in certain parts of the building at certain times.

Magnetic cards. With this type of system, you pass a magnetic card (similar to a credit card) through a card reader slot, where the system reads the card and sends the code to the central controller. The controller compares the number with the programmed information, then either grants or denies access. In addition, the newer systems can print a record of the event, a valuable feature for sensitive areas.

Magnetic cards are relatively inexpensive and hold a lot of data. These systems may support more than a thousand employees. The main advantage of the magnetic card, or any of the card systems, is the ability to change the programming of the system quickly and easily. Aside from these benefits, criminals can easily counterfeit the cards and vandalize the card-reading slots. Also, by continual use, the magnetic stripes scrape and wear to the point where they don't work properly.

Embedded wire cards. These cards use a coded pattern of magnetic wires to generate the code number. This system has the same general characteristics as the magnetic card system, but its card readers are less susceptible to vandalism. One disadvantage is they can't hold as much data.

Proximity cards. The proximity card uses several passively tuned circuits embedded in a fiberglass-epoxy card. Rather than passing the card through a reader, you place it within a few inches of a sensing device, which checks the resonant circuits in the card (see photo, on page 70). The information then travels to the controller, where its code is checked and access is granted or denied.

These cards are durable and their sensors are less susceptible to vandalism. You can install the sensor flush with the wall, mount it behind glass, or surface-mount it. However, the cards are more expensive than the other types. Since there are no readers, these cards should not wear out.

Specialty methods. Some high security applications employ the use of combination type readers that employ dual technologies. For example, the user would swipe their issued card and then enter their issued PIN on a keypad to request a transaction.

For critical locations, special identification means are necessary. One type is a fingerprint reader. Another is a retina scanner. One other method is a hand geometry device, which can identify a person by the shape of his or her hand. Obviously these devices are far more expensive than the previously discussed systems.

Data chips are among the most recent developments in access control systems. Data chips are about the size of a U.S. nickel. You can attach a chip on a photo identification card or mount it on a key chain. You just touch the data chip to the reader plate, and the system reads its unique code.

Controllers. There are a number of different controllers available on the market. The main differences among these controllers are in the number of personal IDs and points of access they control. Some of them even work as part of a complete security system, and others work only as an access system.

Electrically operated locks. Electrically operated locks normally operate off of a 12VDC current. Upon receiving a 12V impulse, the latch opens, allowing you to open the door. When no current goes to the lock, it remains in the locked position. Facilities typically use these locks for either wood or metal jambs (see figure, on page 72).

Next month, we'll continue our discussion of access systems by outlining the most important design considerations for developing an access system.

Features Of Most Access Control Systems

- Control entry points with electronic locks.: (Check NFPA 101 or BOMA life safety and local fire codes before installing electronic door locks.)
- Control entry times (e.g., limiting someone's entry or exit during certain times of the day).
- Control timed events (e.g., limiting access during a holiday).
- Control output relays (e.g., to turn lights on/off or shunt an alarm zone).
- Time programmable limited use visitor cards. (These cards are valid for a specified amount of days or uses.)
- Attendance logging to keep track of employees for payroll purposes.
- Monitoring door positions to see how long it has been open and whether or not it has been left ajar.

PHOTO (COLOR): This type of security card system admits and controls the movement of persons within the interior of a facility.

PHOTO (COLOR): Electrically operated door locks normally operate off of a 12VDC circuit.

~~~~~~~~

By Paul Rosenberg, Datacom Consultant

Source: EC&M Electrical Construction & Maintenance, May2000, Vol. 99 Issue 5, p70, 4p
Item: 3166830
~~~~~~~~

1 page(s) will be printed.

Back

Record: 52

Title:	***Facility Security***: Access Systems--Part 2.
Source:	EC&M Electrical Construction & Maintenance, Jun2000, Vol. 99 Issue 6, p74, 2p, 1c
Author(s):	Rosenberg, Paul
Thesaurus Term(s):	SECURITY systems
Other Term(s):	ACCESS control; PRIVATE security services
	NAICS/Industry Code(s)56162 Security Systems Services;
Abstract:	Expounds on design considerations involved in customized access systems in ***facilities***. Procedures for identification and control of visitors; Assignment of at least two authorized persons in the detection of incorrect or unauthorized procedures; Automated ***security*** systems; Role of ***security*** personnel in detecting ***security*** hazards and identifying violators and intruders.
Full Text Word Count:	756
AN:	3350845
ISSN:	00134260
Database:	Business Source Premier

Section: Correspondence Course

FACILITY SECURITY: ACCESS SYSTEMS--PART 2

Before developing a customized access system, make sure you understand the important design considerations involved with this type of facility security.

In today's security-conscious society, it's not enough to simply have the right access control equipment. You must install it in the right configurations and oversee the system properly. Following are the most important design considerations for access systems. Since no single installation needs them all, apply the ones that best fit your application.

Visitor identification and control. Physical security requires screening, identification, and control of visitors. We generally place visitors in the following categories: persons with whom every installation or facility must have dealings with in order to conduct business; and individuals or groups who want to visit an installation or facility for nonessential purposes.

When dealing with visitors, you should follow a few basic rules. First, verify their identity. Next, security personnel should contact the person the visitor is there to see to validate the visit. Finally, record visitor information, issue visitor badges, and use registration forms.

Procedures for identification and control of visitors may include:

- Positive methods of establishing the authority for admission of visitors.
- Positive ID of visitors.
- Availability and use of visitor registration forms.
- Availability and use of visitor ID cards/badges.

- Procedures for escorting visitors who have limited access.
- Establish controls to recover visitor ID cards or badges upon expiration or when no longer required.

Entry roster. Security personnel should grant admission of persons to restricted areas only after positively identifying and checking names on an authenticated roster. How can you accomplish this task? Make sure you adhere to the following guidelines:

- Each time you need to make a permanent addition or deletion, document it.
- Publish changes in the same manner as the original roster.
- Maintain rosters at access control points to facilitate positive control.

Two-man rule. This security approach requires at least two authorized persons, each capable of detecting incorrect or unauthorized procedures with respect to the task being performed and who are familiar with applicable safety and security requirements, to be present during certain operations. This rule works well in the following situations:

- When uncontrolled access to vital machinery, equipment, or material might provide opportunity for intentional or unintentional damage that could affect the operation of the installation or facility.
- Where uncontrolled access to funds could provide opportunity for diversion by falsification of accounts.
- When uncontrolled delivery or receipt for materials could provide opportunity for pilferage through "short" deliveries and false receipts.
- When uncontrolled delivery or receipt for materials could provide opportunity for planting bombs, listening devices, etc.

Mechanized/automated systems. Identification and access control systems base their identification judgment factor on a remote capability through a routine discriminating device for positive ID, as opposed to the manual system's using a guard force member to conduct identification based on access rosters and personal recognition. In a mechanized system, the following occurs within the machine: 1. Receives physical ID data from an individual; 2. Encodes this data for use; 3. Compares this data to stored data; 4. Makes a go or no-go decision; and 5. Translates the results into readable form.

Several mechanical devices, which use magnetic coding, embossing, optical characters, and dielectric coding, add to the security of a facility. An all--inclusive automated ID and access control system reinforces the security of an installation because it can be changed quickly and easily. The computer can do this through its memory, stored on magnetic tape or disc. You can make changes by remote use of specific code numbers.

Execution of security activities. First, security personnel must understand the methods and techniques that will detect security hazards and assist in identifying violators and intruders. They should also require written reports for all security activities. Each person should prepare and turn these documents into the supervisor for necessary action. Personnel assigned to fixed posts should have some designated method of securing relief when necessary. The security advisor should also establish a simple but effective plan of operation for the security force to meet every foreseeable emergency. This means conducting practice alarms frequently to test the effectiveness of this plan as well as the security force's understanding of their roles. Finally, vary routes for security patrols at frequent intervals to preclude establishing a routine that potential intruders may observe and use to gain entrance.

Next month, we'll explore sensing and monitor intrusions and how to get help when you need it most.

PHOTO (COLOR): Security personnel must understand the methods and techniques that will detect security hazards and assist in identifying violators and intruders.

~~~~~~~~

By Paul Rosenberg, Datacom Consultant
~~~~~~~~

Source: EC&M Electrical Construction & Maintenance, Jun2000, Vol. 99 Issue 6, p74, 2p
Item: 3350845