

Security PACE Book 6 - Basic Access Control Concepts

Basic Access Control Concepts is Book Six in this PACE series on Security Basics. It provides an overview of Access Control systems, including the concepts behind Access Control and hardware and software components required for a functional Access Control system.

Learning Objective

After completing this PACE Book, you should be able to:

- ◆ describe the goals of an Access Control system
- ◆ list the benefits of an Access Control system for an end-user
- ◆ identify basic Access Control technologies and components
- ◆ identify and explain the common LAN topologies and protocols
- ◆ list the configurable parameters of an Access Control system

Use the Menu at left to navigate through the course.

[Course Introduction](#)

Basic Access Control Concepts

[Access Control and Its Benefits](#)

[Basic Access Control Technologies](#)

[Network Architecture](#)

[Access Control Software System Configuration](#)

Access Control and Its Benefits

Access Control

Access Control utilizes technology and procedures to manage who is able to go where and when. An Access Control system is composed of:

- ◆ input/output devices
- ◆ devices to control ingress/egress (doors and related equipment)
- ◆ system(s) to manage information regarding identified risks
- ◆ system(s) to manage information regarding personnel.

To accomplish this, an Access Control system has several components:

- ◆ entryways (doors)
- ◆ locking devices for the entryways
- ◆ sensors to monitor the door status - open or closed
- ◆ devices to identify properly authorized users
- ◆ devices to permit exiting from the secure area to the outside
- ◆ notification protocols and external system control devices
- ◆ PC (a personal computer to provide overall system control)

Using this technology in accordance with clearly defined and carefully implemented security procedures affords an organization a highly effective means of managing risk.

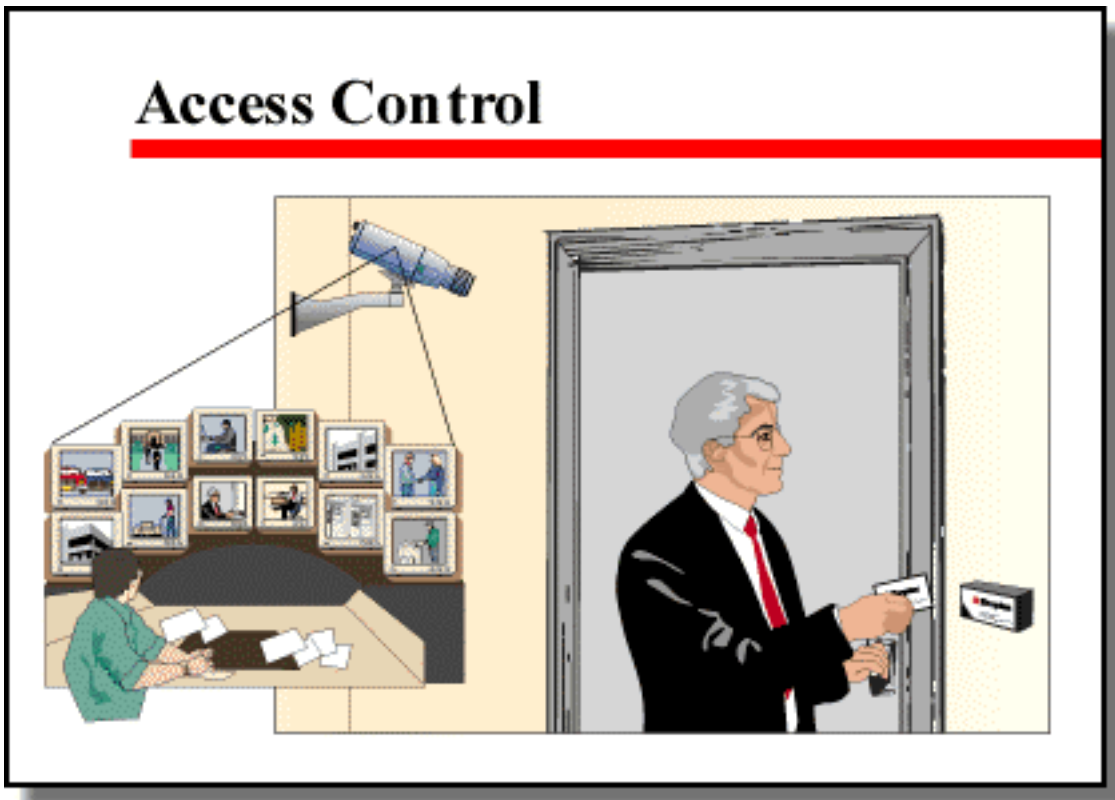
Risk management is the ability of an organization to minimize their vulnerability to potential losses. Without effective methods of risk management, costs associated with responding to losses or disruptions of business operations can have severe impact on short-term profits and long-term positioning of the organization in the marketplace.

A 1996 study by the Security Industry Association (SIA) revealed that industry specialists in risk management generally view an effective fire alarm system as their greatest asset in the effort to manage risk - specifically, loss of material and potential damage to the organization's infrastructure.

The study further reported that the next level of protection against risk was a proprietary security organization; that is, security officers hired and trained by the organization to perform tasks related specifically to the organization's own specialized security needs. (Note: this contrasts with contract security officers, provided to an organization from an outside vendor, who, in fact, rank very low on effectively managing risk.)

Following proprietary security officers, intrusion detection and Access Control systems are seen to offer the next highest level of risk management. The study also indicates that insurers often fail to recognize the benefit of

Access Control in managing risk as evidenced by the fact the insurance companies require organizations to implement intrusion detection twice as often as Access Control systems. Interestingly, an outcome of this research has led to an ongoing dialog between the SIA and representatives of the insurance industry regarding Access Control capabilities and benefits.



Basic Access Control Technologies

Select the first topic below to begin this lesson:

- [Access Control Technologies](#)
- [System Architecture](#)
- [Head End PC](#)
- [Field Controllers](#)
- [Input Devices](#)
- [Access Doors and Related Peripherals](#)
- [Card Readers and Keypads](#)
- [Output Devices](#)

[TOP](#)

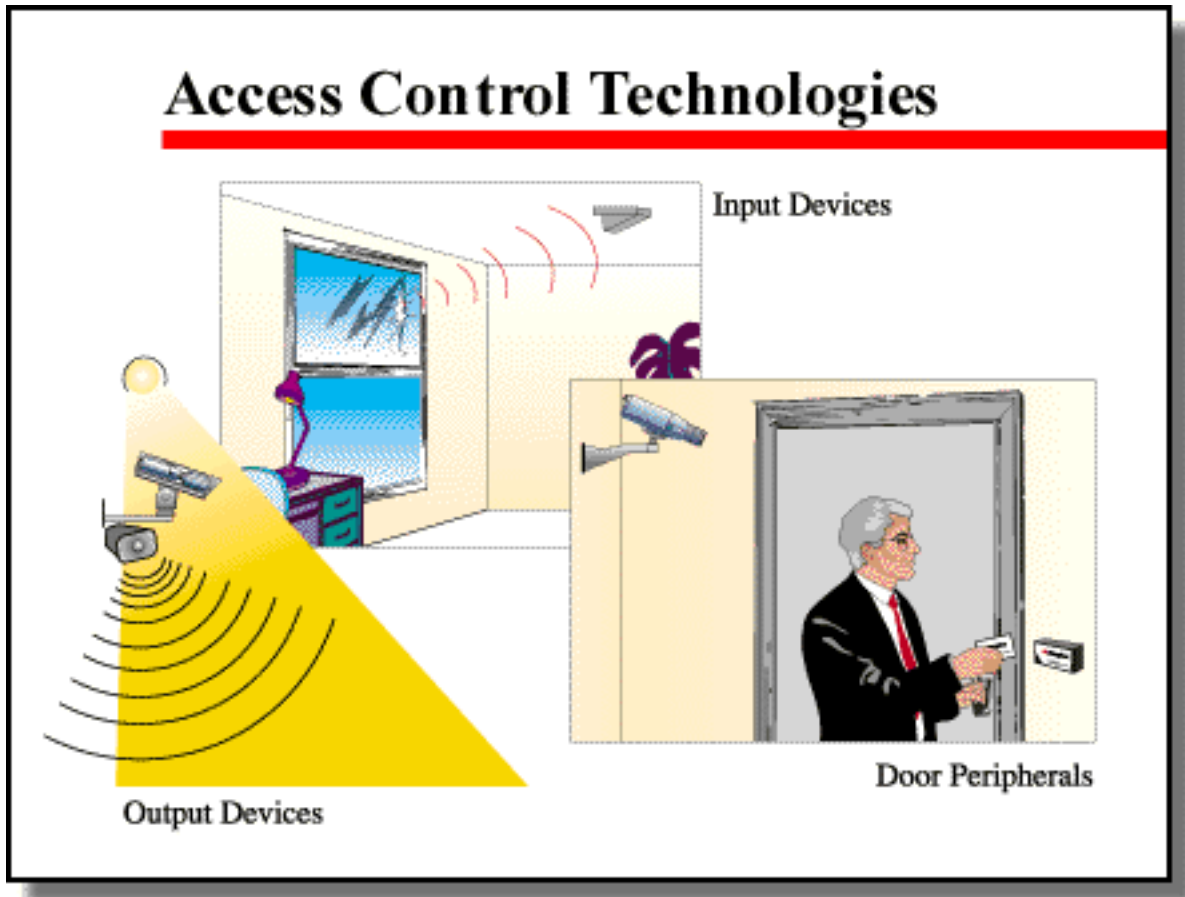
Access Control Technologies

Access Control requires four basic technologies for effective functioning. These consist of:

- ◆ a PC (personal computer) for overall system control
- ◆ input devices - devices that detect conditions or events (not specifically connected to a door)
- ◆ Access Control doors and related peripherals, including card readers and keypads, etc.
- ◆ output devices - items that respond to the input devices

How these individual devices relate to each other is

defined in the *system architecture*. We will discuss this in the following section.



System Architecture

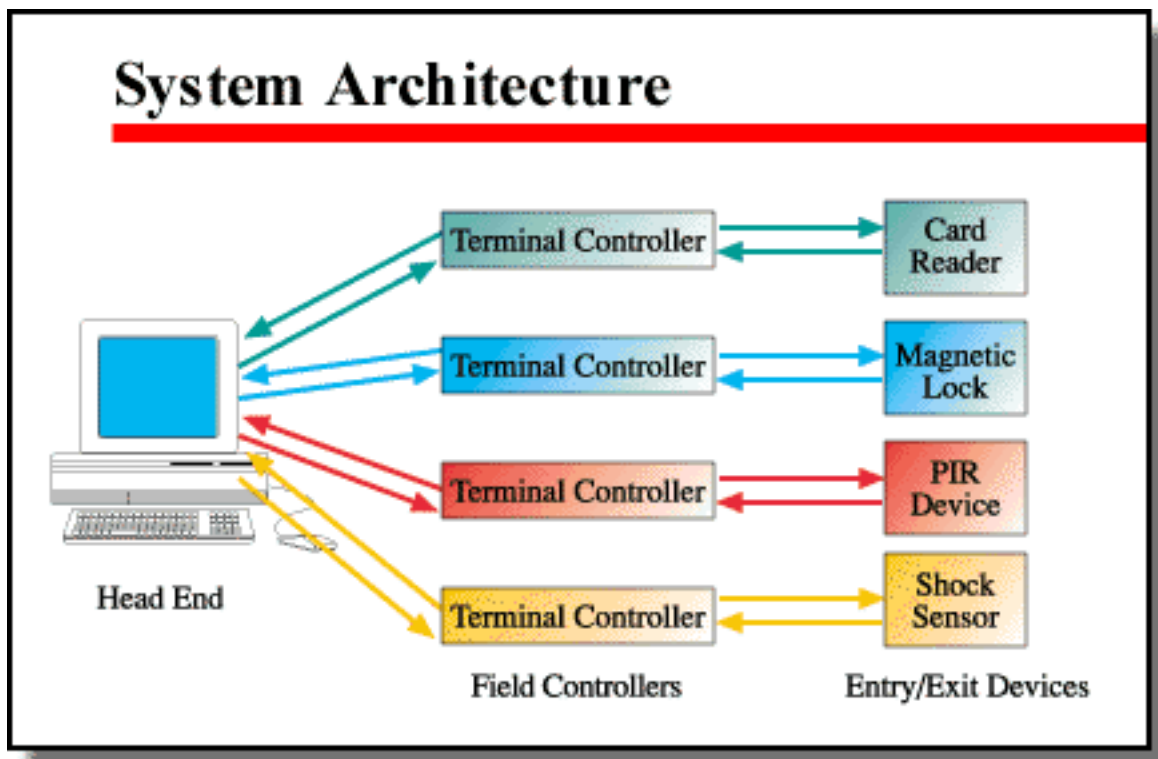
Before examining specific Access Control components, we want to discuss briefly the architecture of an Access Control system. The system architecture has three levels: head end, field controllers, and entry/exit devices.

At the high level of operation, the "head end" provides a system management capability for all devices in the system; and related information. This is typically a PC (personal computer) that receives inputs and initiates responses at the appropriate locations with the

appropriate devices. All operator interfacing takes place at the head end.

In most systems today, field controllers, which reside between the head end and the entry/exit devices, provide much of the moment-to-moment control for the system. In older systems - without intelligent field controllers - the head end almost exclusively provided this control, and if a fault occurred which took the head end off-line, then the entire system became inoperative. Today that is not the case. In today's systems, if the head end is off-line, the field controllers are able to ensure the system continues to operate effectively.

Entry/exit devices are "end-of-the-line" components. As with field controllers, these low level components must be able to provide at least minimal decision-making capability independent of the higher level devices, again, in order to ensure a basic level of Access Control functionality in the event of a fault.



Head End PC

The PC functions as a system control unit. It receives, processes and sends data to other devices on the Access Control network. It provides a display for the operator to monitor system operation. In addition, it provides a means for the operator to "interrogate" the system; that is, the operator can request specific information regarding the status of any of the devices within the system and can initiate specific actions at any specified location within the system.

The PC also provides a means of storing and retrieving information, creating reports, and backing-up data.

In larger applications requiring advanced capabilities there may be multiple control units located throughout the system. It should also be noted that security designers prefer to have an Access Control system built on a dedicated Local Area Network (LAN). This offers significant advantages over systems which exist on an organization's standard LAN.

Head End PC



Field Controllers

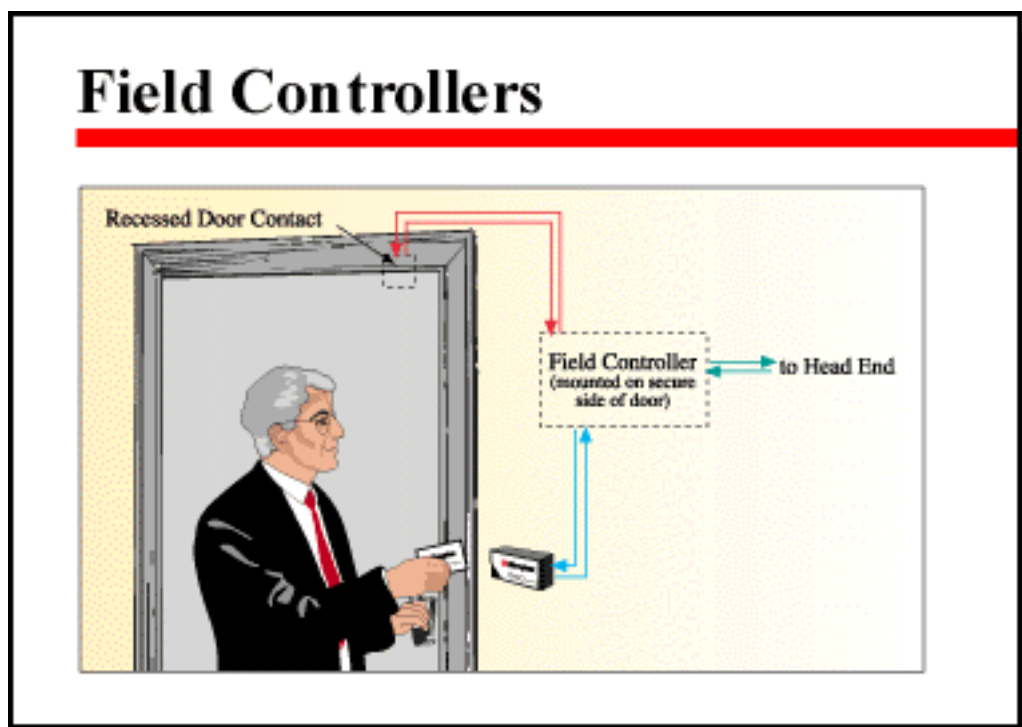
Today, security systems are networked. More important, they feature a "distributed architecture." This simply means that rather than having all processing capability residing at the head end, processing is "distributed" at points throughout the network. Field controllers provide this processing.

A field controller consists of:

- ◆ a CPU (central processing unit)
- ◆ Network communications capability
- ◆ I/O (input/output) modules (printed circuit boards)
- ◆ card reader modules (printed circuit boards)

Using field controllers allows the majority of the system to continue to function, even if the head end is temporarily unavailable or if another region in the system is down. In this instance, the field controllers store all event activity for later uploading to the head end once it is back on line. If a field controller requires additional information in order to process a command, it is able to request information from the head end. In addition, scheduled exchanges of data between the head end and the field controllers allow for events to be tracked in history logs and the current information will be available to the field controllers.

In addition, increasingly, security networks are designed to use industry-standard communications protocols - TCP/IP, for example. This ensures high levels of reliability and minimum downtime in the event of a component failure.



Input Devices

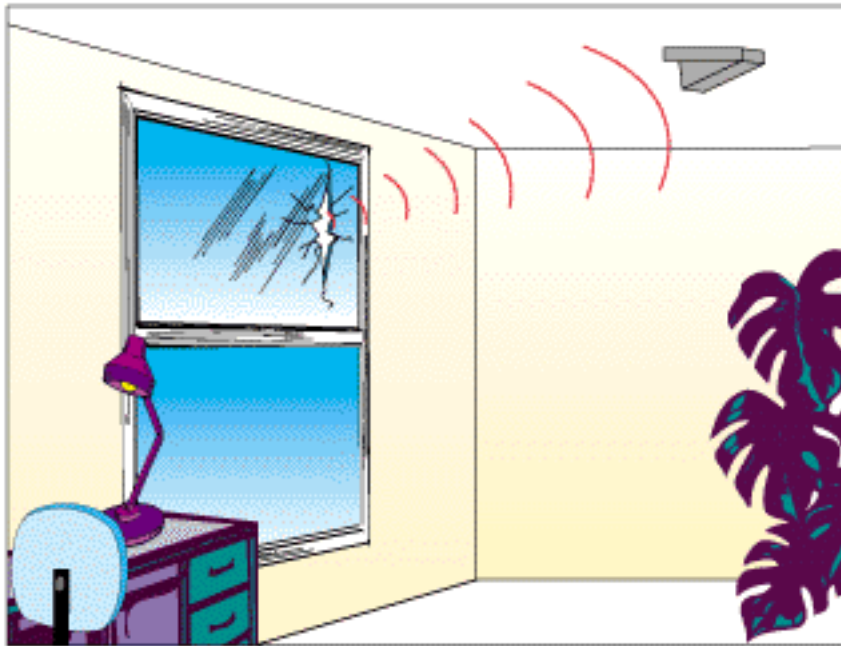
Input devices in Access Control systems are any detectors that report their status to a PC electronically. Their purpose is to provide data to the processor regarding the current condition at a given location. They may include a variety of detector types, including:

- ◆ temperature monitors
- ◆ motion detectors
- ◆ glass break detectors
- ◆ panic buttons

Some of these devices, or similar ones, will be familiar to you if you have completed Book Five in this PACE Series, Intrusion Detection Systems and Concepts. In addition to the devices listed above, there are similarly functioning items that physically reside on or near a door and which provide data specifically related to the door's open or closed status. These devices are discussed in the following section, Access Doors and Related Peripherals.

Each of these devices provides data to the head end PC. The PC can perform a variety of analysis capabilities, graphical user interface and a wide range of output options.

Input Devices



Access Doors and Related Peripherals

There are many devices designed to control the status of an Access Control door. These devices include:

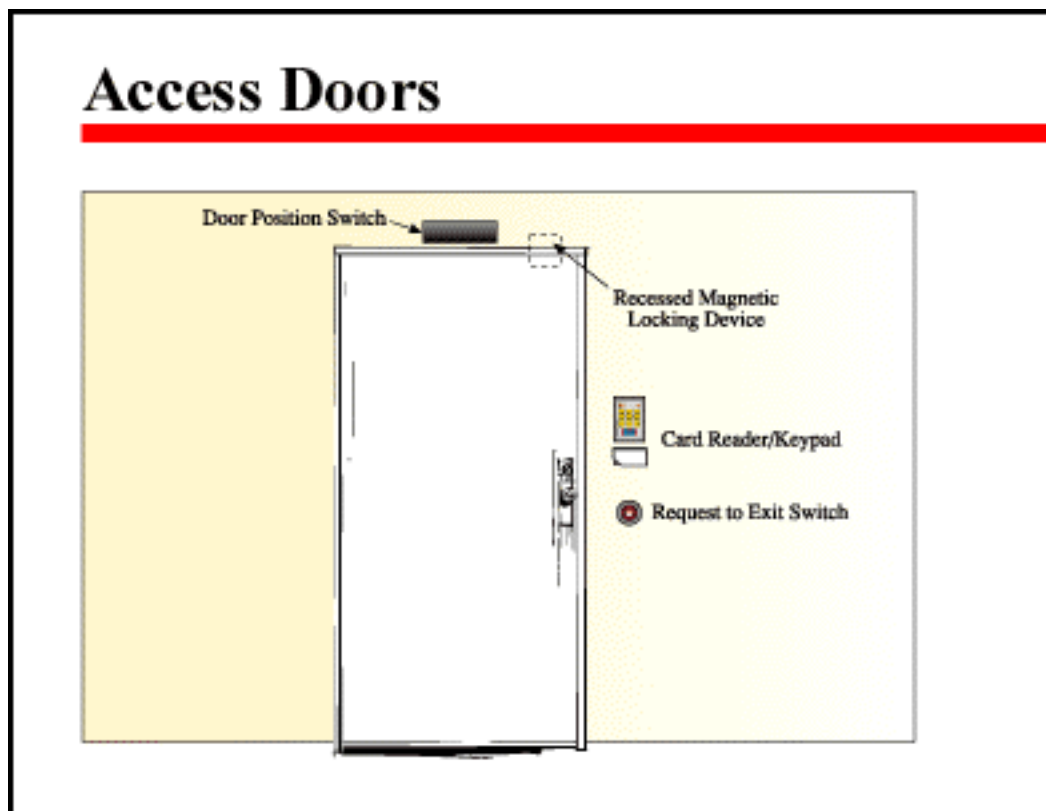
- ◆ door position switches (door contact switches)
- ◆ request to exit devices
- ◆ card reader or keypad devices
- ◆ locking devices

Door position switches indicate the current status of a door — whether it's open or closed. They are simple electrical devices, which complete a circuit when the door is closed and open the circuit when the door is open.

Request to exit devices are also simple electrical switches. They are used to indicate someone on the secure side of an Access Control Door wishes to have the door unlocked. This action is usually reported to the PC.

Card readers and keypads are perhaps the most sophisticated door peripherals used in the operation of an Access Control system. These devices, which may exist as a single or integrated unit, will be addressed in the following section.

Finally, an Access Control door must be equipped with a locking mechanism — either an electric door strike or magnetic lock — which can be controlled by a field controller.



Card Readers and Keypads

Card readers are devices which read data from a user supplied card. There are a variety of distinct media used for such cards:

- ◆ proximity (active or passive)
- ◆ magnetic stripe
- ◆ Wiegand
- ◆ bar code

Passive proximity cards contain electronic circuitry (including an antenna) which stores ID data. When these cards are passed near a reader, electrical energy radiating from the reader actually charges or "excites" the circuitry in the card. The circuitry then transmits the data (ID information) contained in the circuitry to the reader. Active proximity cards share this circuitry, but in addition contain their own power source. This "on-board" power supply increases their range (effective working distance from card to reader.) Proximity card technology is easy-to-use and provides high levels of security. It is, however, higher in cost.

Wiegand card technology stores information in a unique pattern of small wires embedded inside the card. When inserted into or swiped through a card reader, the wires are excited by a magnetic field. This, in turn, produce a unique bit pattern, which can then be translated to usable data by the reader. Wiegand technology, although higher is cost, is a high security option that makes duplication

extremely difficult.

Magnetic stripe cards use a technology identical to standard credit cards. While they are less secure than Wiegand or proximity cards, they have benefits in their ease of programming and flexibility. In addition to Access Control, magnetic stripe cards may serve other applications as well, including credit, debit, library, and time and attendance. Because of their ease of programming, replacement of lost cards is a relatively simple matter.

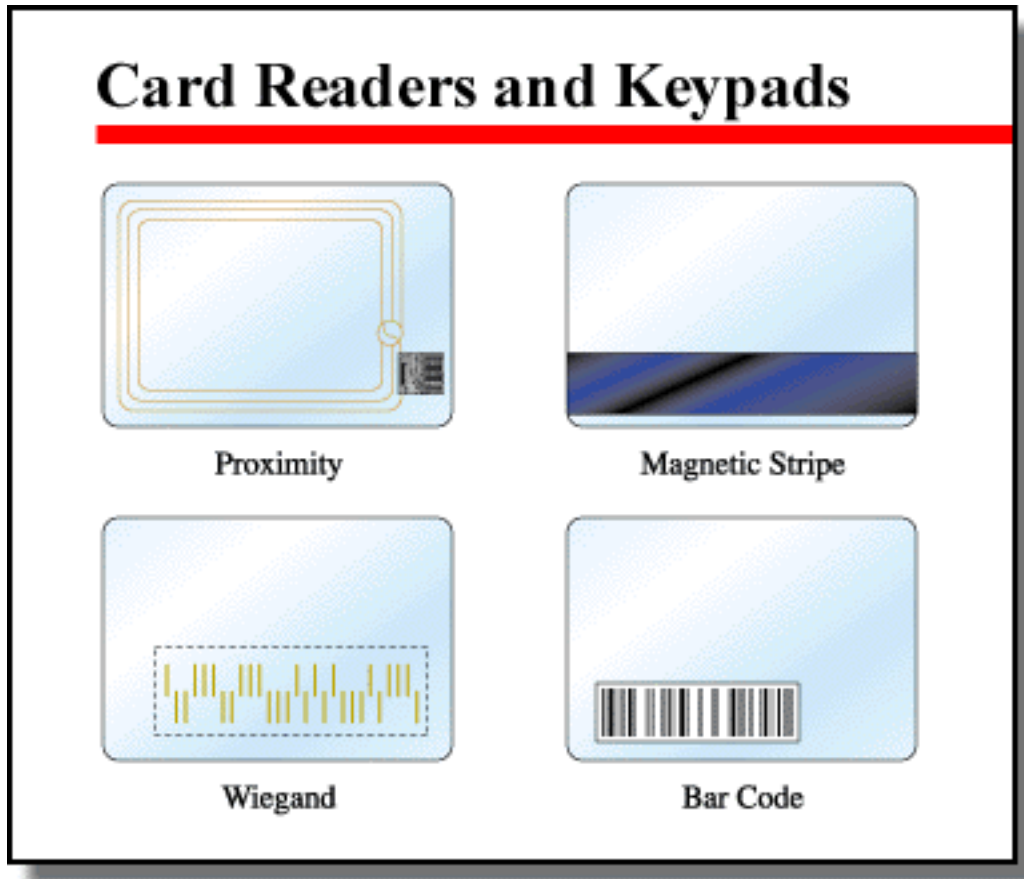
Cards employing bar code technology use industry-standard bar coding. The data is placed on the card's surface. The reader then accesses the data much as store price reading applications read UPC labels on various products. While inexpensive and easily produced, bar coded cards have a low level of security, deteriorate quickly and are subject to higher instances of mis-reads by the reader.

With each of these reader/card technologies, the reader is placed near the door. Swiping the card through the reader or, in the case of proximity cards, passing nearby the reader will transmit the data to the field controller. The field controller then compares this data to a verified database of information downloaded from the head end PC. If the cardholder is confirmed to have valid access to the door at the reader location, the door locking mechanism is released, and the user may enter.

Another method of determining authorized entry is through a keypad. Here a user is required to enter a

specific PIN - Personal Identification Number - which, in theory, is known only to him or her. The effectiveness of this system is dependent on the integrity of the user.

Note that all these technologies have advantages and disadvantages. Which technology is chosen by system designers is determined by the Access Control requirements for a specific location.



Output Devices

Output devices include a wide range of devices, auto-dialers, Heating, Ventilating and Air Conditioning (HVAC) controls, and CCTV camera control devices. Audio/visual output devices may include:

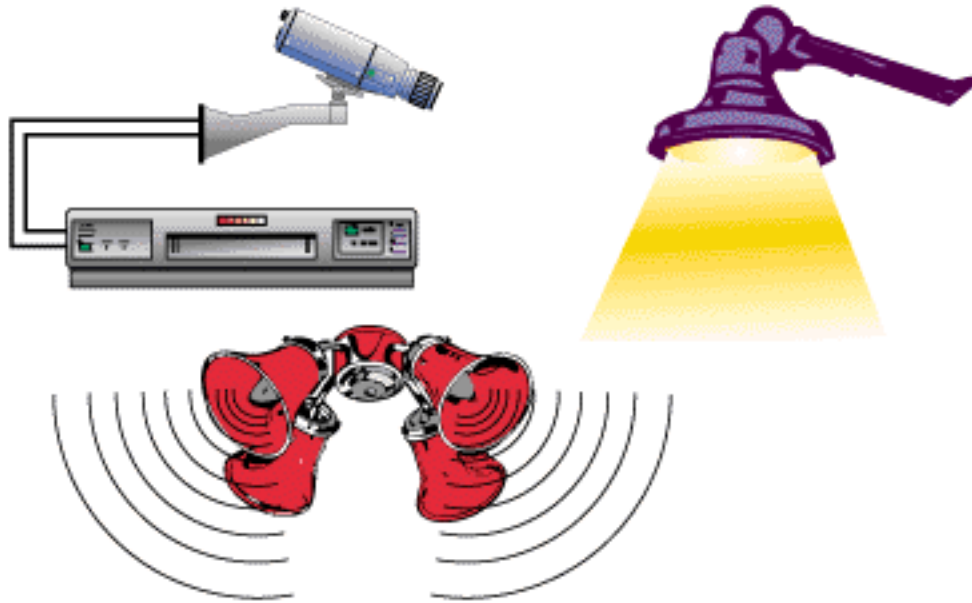
- ◆ Lights
- ◆ Horns
- ◆ Buzzers
- ◆ Bells

All these devices respond to specific events as detected by sensors to Access Door peripherals at a given location. For example, a glass breakage detector may cause an audio device to sound, or input from a card reader may cause the field controller to direct a CCTV camera to a present position to provide a visual record of the person entering the Access Control door.

Other output devices include:

- ◆ parking lot gates
- ◆ lighting
- ◆ elevator control

Output Devices



Network Architecture

Select the first topic below to begin this lesson:

- [Network Architecture](#)
- [Network Topologies](#)
- [Network Hardware/Software Protocols](#)

[TOP](#)

Network Architecture

As mentioned earlier, many Access Control systems have multiple workstations. In these instances, the entire system resides on a Local Area Network (LAN).

Fundamentally, a network is simply a system that manages the exchange of information from one point (node) on the network to another. A "node" is any point on the network where data is generated, received, processed, or stored.

There are several ways to describe a LAN. First, a LAN may be identified by "topology." Topology is the physical layout of cabling connecting the nodes of the network.

There are three basic types:

- ◆ Star
- ◆ Ring

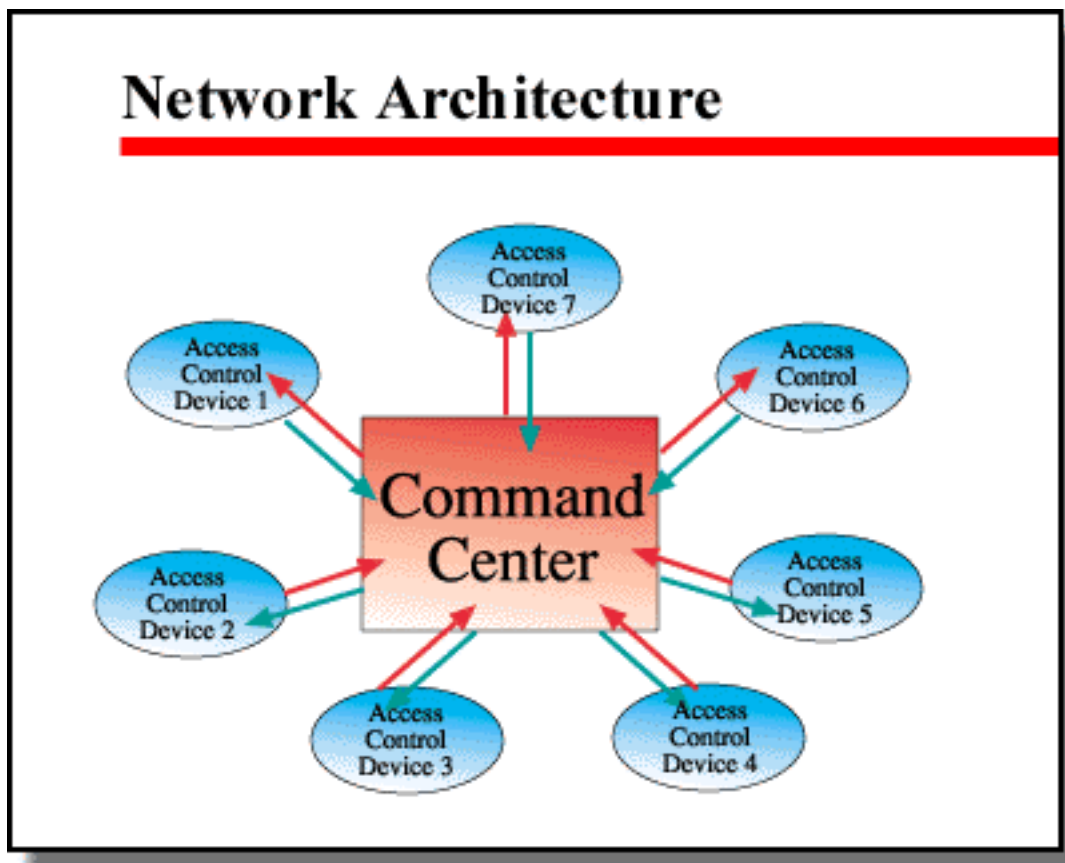
◆ Bus

In addition, a LAN may be identified by hardware/software protocol. Here a protocol is a "set of rules" which describe how the network passes data from node to node, which processes (internal operation of network) have priority, etc. Common network protocols include:

- ◆ Ethernet
- ◆ Token Ring
- ◆ Arcnet

In addition to these general network protocols, more and more networks, including security system networks are incorporating TCP/IP protocol. This is the industry standard network communications protocol and benefits networks in reliability, interoperability and system maintenance.

In the following sections, we will examine topologies and hardware protocols in more depth.



Network Topologies

There are three common network topologies:

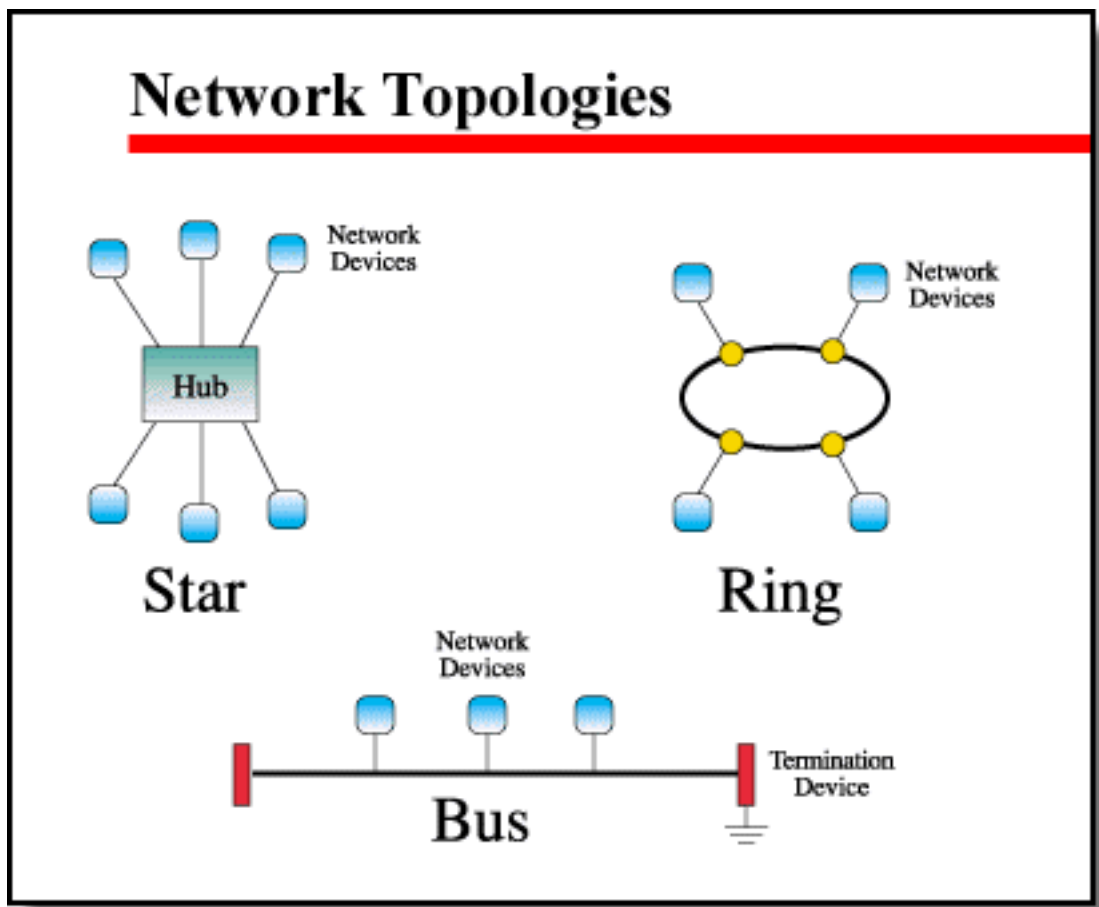
- ◆ star
- ◆ ring
- ◆ bus

These define the routing through which data is passed throughout the network.

The star topology arranges the nodes of the network at the end of "spokes" with a central "hub" through which all data is passed.

Ring topology arranges the nodes on a loop. At a scheduled time, a node places an addressed packet of data on the loop where it travels around the loop until the node with the correct address recognizes the packet and accepts the packet.

A network using bus topology simply is a ring topology with a break in the loop, becoming a length of cable with two ends onto which is connected the network's nodes. Bus topology requires a termination device at both ends of the bus cable. Nodes can send packets of data whenever they sense a clear space on the bus. All nodes must contend for the opportunity to send a packet of data.



Network Hardware/Software Protocols

There are three common protocols describing a LAN's operation, i.e., specifically defining electronic "rules," or standards, for exchanging information throughout a network. These protocols are:

- ◆ Ethernet (with TCP/IP)
- ◆ Arcnet
- ◆ token ring

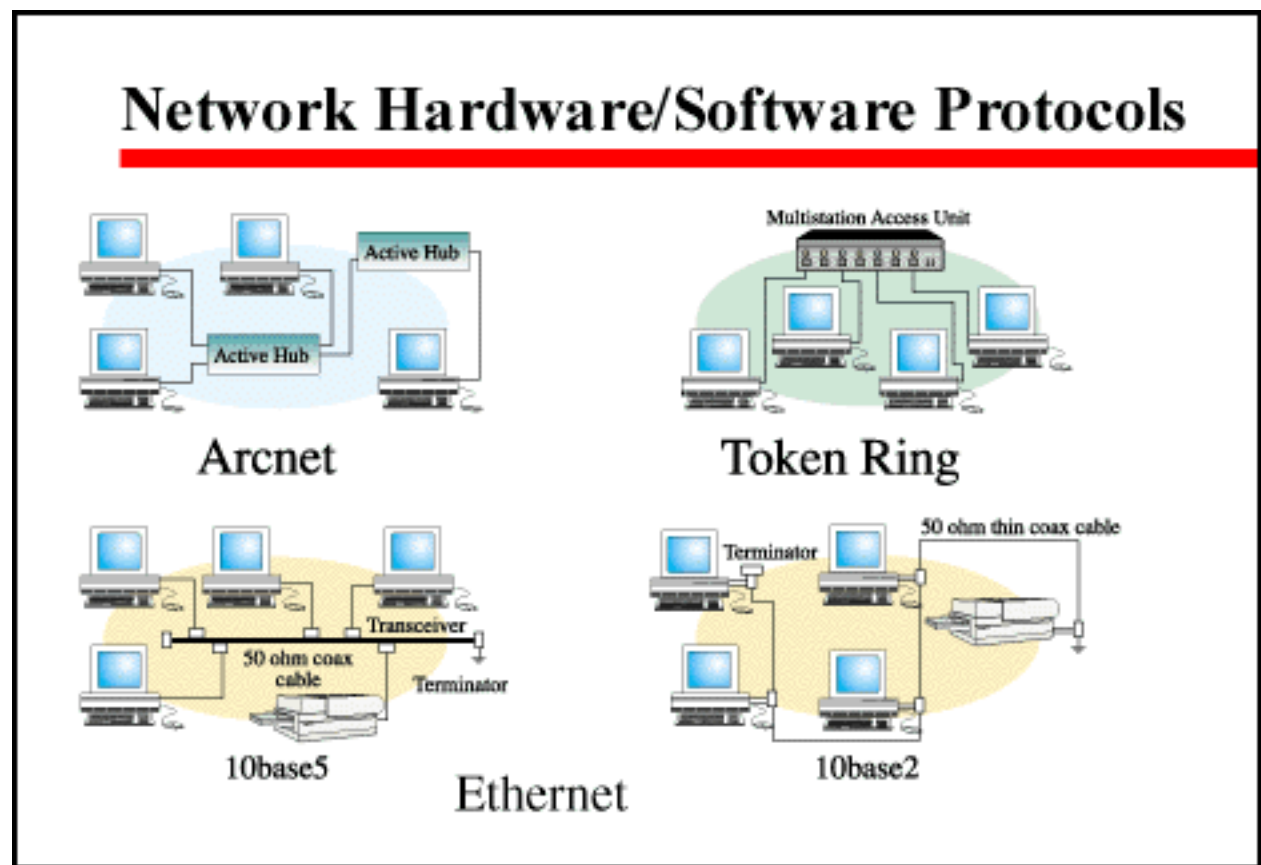
The first version of Ethernet was developed by Xerox in 1972. In 1980, the Ethernet standard was revised by Xerox in partnership with Digital Equipment Corporation and Intel. Ethernet uses a bus topology. In the 1980 revised Ethernet standard, a data transfer rate of 10 megabytes per second (Mbps) was established, i.e., ten megabytes of data can be passed along the network each second. There are variations in Ethernet wiring schemes, including:

- ◆ 10 base 5
- ◆ 10 base 2
- ◆ 10 base T

Arcnet was originally developed for the Department of Defense by Datapoint Corporation in 1977. It employs a modified star topology with all devices linked to the network via hubs. There may be several hubs on one network and hubs may be active or passive. Arcnet has a transmission rate of 2.5 Mbps.

Token Ring was developed by IBM in 1980 in consultation with the Institute of Electrical and Electronic Engineers (IEEE). Token ring is a variation of the ring topology, which

also uses a hub. It allows transmission rates of 4 and 16 Mbps. The token ring hub is called a "multistation access unit." Lobe cables are used to connect the network devices to the multistation access unit.



Access Control Software System Configuration

System Configuration

Access Control offers system administrators tremendous flexibility in customizing the system. To take full advantage of such a system, administrators must perform a software system configuration. The configuration procedure permits administrators to uniquely tailor the system for the specific needs of the organization.

There are four broad areas available for customization. These include:

- ◆ time periods
- ◆ access levels
- ◆ alarms
- ◆ policies

Setting organization-defined parameters in each of these areas, allows the Access Control system to anticipate and respond to any unique needs of the organization.

By defining time periods, for example, administrators can accommodate unique usage requirements at any number of different locations throughout the system. For example, one organization may define time periods for regular day

shift operations, night shifts, weekend schedules, plant shut down for vacation and holidays. With these time periods defined, the system administrator can then define monitoring and responses to events which are dependent on the time period in which they occur.

The system administrator can also define access levels for groups of personnel. By assigning the same access level to specific doors, the administrator is able to determine who is able to enter into a specific door.

Access Control systems also allow the administrator to associate classes of events or even individual events with specific alarms, including which alarms are triggered, whether reports are generated and even which displays or printers present the alarm message.

Finally, the system administrator can define a range of policies regarding how the Access Control system will operate. The most typical policies define how a cardholder gains access to a region and how they must exit.

An anti-passback policy is designed to prevent a card from being used repeatedly for entry to a region without first existing. This prevents a cardholder from entering a region, then handing the card back to a person who does not have an authorized card for entry into the region.

Occupancy restriction policies set minimum and maximum numbers of personnel permitted in a given region at a time. This allows the system to notify operators should too few or too many people be in an

area during any given time period.

This concludes Book Six, Access Control Basics: Concepts and Application, in this PACE series on Security Basics.