At the conclusion of this course, the participant will be able to:

- Identify the types and function of access control for non-electronic and electronic
- Understand the basics of an opening and key door terminology
- Identify industry standard fire & safety codes and fail safe verses fail secure protocols
- Specify electronic access control components required for a system, including IP
Agenda

• Introduction & Agenda

• Methods to Secure a Door
  – Non-Electronic Access Control
  – Electronic Access Control

• Door Overview
  – Door Terminology
  – Door Opening and Handing

• Non-Electronic Access Control
  – Keys & Keyways
  – Master Key Systems
  – Restricted Keyways
  – Locksets

• Electronic Access Control
  – Types of Electronic Access Control – Analog, Hybrid, IP
  – What is Electronic Access Control
  – Components – Controller, Locking Device
  – Fire & Safety Standards
  – How It Works – Relays, Fail Safe/Fail Secure
  – Components – Credential Reader, REX, PS

• Recap of Access Control
  – System Options Comparison

• Question and Answer
Methods to Secure a Door

- **Non-Electronic Access Control**
  - Keys, Master Key and Restricted Key Systems

- **Electronic Access Control**
  - Hardware systems to allow for audit, scheduling, etc

*What is Access Control?* *Wikipedia defines as,*

*The selective restriction of access to a place or other resource.*

**Access Control** should not be confused with **Door Control**

- Door Control is limited to the ability to open a door without the capability of scheduling, auditing, central management or having a key management system.
Door Overview - Terminology

- Door construction and material
- Frame construction and material
- Ratings
- Door function
- Door handing
- Infrastructure
Door Overview - Openings

- Understanding the components is only part of the system design equation.
- We must be able to look at an opening and ascertain which components to use, taking into account a few variables.
- Job walks for hardware and design specifications are critical to a project’s success.
Basic access control begins with a key

Positives
- low cost

Negatives
- no management (keys can be duplicated)
- no control of access times
- no audit
- expensive to maintain (rekey costs)
Non-Electronic Access Control – Master Key Systems

Master Key Systems allow for control of access to specified areas by key issuance.
Non-Electronic Access Control – Restricted Keyways

- Restricted Keyways are a way to reduce or eliminate the unauthorized duplication of keys.

- These types of systems can lock an end user into a contract with a service provider.
Non-Electronic Access Control – Locksets / Stand Alone
Electronic Access Control – What is Electronic Access Control

- Electronic access control has been around long enough that most of us are familiar with seeing a reader or keypad at an entrance.

- The involved components, what is behind and how it works is foreign to many.
The **Controller** is the heart and brain of a system. It interrogates the reader input and grants or denies entry. It maintains audit trails. Controls automated relays (scheduled lock/unlock).
Electronic Access Control – Types of Electronic Access Control

**Traditional Analog**
- Analog Panels from 1-8 doors
- Limited Users
- Limited Growth
- RS232/485 Communications
- Direct connection of computer/server
- Single site by design

**Hybrid**
- Analog Panels with Network interface
- Still a 1-8 door panel
- Limited doors and users
- Off site server capable, (in some cases)
Electronic Access Control – Types of Electronic Access Control

True IP Based Access Control Solution

- Multi Site
- Scalable
- Central Database
- Systems Integration
- Reduced Costs (Installation & Management)
**IP Access Control – Types of IP Systems**

- **All in One reader**
  - Controller, card reader, NIC, all included in Reader

- **At the door**
  - Single door controller is located nearby the door
  - Wires from reader and lock are run up to the controller
  - NIC is built onto controller

- **Panel solution**
  - Multi door controller is mounted in a central location, usually TELCO/IT or Electrical closet
  - All wires from door(s) are run back to this central panel
IP Access Control – Ways to Communicate

• Browser based
  – Web Browser accesses DB stored on Main controller

• Server based
  – DB located on a central server with Software
Electronic Access Control – Components

- Controller
- Locking Device
  - REX Device
  - Access Credential Reader
  - Power Supply
  - Transmission Source

- Electrified Strike
- Magnetic Lock
- Electrified Lockset

- The type of locking device used, wholly depends on the type of door and frame present.

- Is the door subject to FLS (fire, life, safety)?
- What current locking prep is present?
- What level of security is needed?
- What is architecturally pleasing?
NFPA 101 – Life Safety Code®, 2003 Edition, access control sections of importance include:

7.2.1.6.2 Access-Controlled Egress Doors. Where permitted in Chapter 11 through Chapter 42, doors in the means of egress shall be permitted to be equipped with an approved entrance and egress access control system, provided that the following criteria are met:

(1) One of the following shall be provided:

   (a) A sensor on the egress side, arranged to detect an occupant approaching doors that are arranged to unlock in the direction of egress upon detection of an approaching occupant or loss of power to the sensor
   (b) Listed panic hardware or fire exit hardware that, when operated, unlocks the door

(2) Loss of power to the part of the access control system that locks the doors shall automatically unlock the doors in the direction of egress.

(3) The doors shall be arranged to unlock in the direction of egress from a manual release device located 1015 mm to 1220 mm (40 in. to 48 in.) vertically above the floor and within 1525 mm (60 in.) of the secured doors.
Continued... **7.2.1.6.2 Access-Controlled Egress Doors**

(4) The manual release device specified in 7.2.1.6.2(3) shall be readily accessible and clearly identified by a sign that reads as follows: PUSH TO EXIT.

(5) When operated, the manual release device shall result in direct interruption of power to the lock - independent of the access control system electronics - and the doors shall remain unlocked for not less than 30 seconds.

(6) Activation of the building fire-protective signaling system, if provided, shall automatically unlock the doors in the direction of egress, and the doors shall remain unlocked until the fire-protective signaling system has been manually reset.

(7) Activation of the building automatic sprinkler or fire detection system, if provided, shall automatically unlock the doors in the direction of egress, and the doors shall remain unlocked until the fire-protective signaling system has been manually reset.
7.2.1.6.1 Delayed-Egress Locks

Approved, listed, delayed-egress locks shall be permitted to be installed on doors serving low and ordinary hazard contents in buildings protected throughout by an approved, supervised automatic fire detection system in accordance with Section 9.6 or an approved, supervised automatic sprinkler system in accordance with Section 9.7, and where permitted in Chapter 12 through Chapter 42, provided that the following criteria are met:

(1) The doors shall unlock upon actuation of one of the following:
   (a) An approved, supervised automatic sprinkler system in accordance with Section 9.7
   (b) Any heat detector
   (c) Not more than two smoke detectors of an approved, supervised automatic fire detection system in accordance with Section 9.6

(2) The doors shall unlock upon loss of power controlling the lock or locking mechanism.
Continued... 7.2.1.6.1 Delayed-Egress Locks

(3)* An irreversible process shall release the lock within 15 seconds, or 30 seconds where approved by the authority having jurisdiction, upon application of a force to the release device required in 7.2.1.5.9 under the following conditions:

(a) The force shall not be required to exceed 67 N (15 lbf).
(b) The force shall not be required to be continuously applied for more than 3 seconds.
(c) The initiation of the release process shall activate an audible signal in the vicinity of the door.
(d) Once the door lock has been released by the application of force to the releasing device, relocking shall be by manual means only.

(4)* A readily visible, durable sign in letters not less than 25 mm (1 in.) high and not less than 3.2 mm (1/8 in.) in stroke width on a contrasting background that reads as follows shall be located on the door adjacent to the release device:

PUSH UNTIL ALARM SOUNDS
DOOR CAN BE OPENED IN 15 SECONDS

6.15.7 Door Unlocking Devices

6.15.7.1 Any device or system intended to actuate the locking or unlocking of exits shall be connected to the fire alarm system serving the protected premises.

6.15.7.2 All exits connected in accordance with 6.15.7.1 shall unlock upon receipt of any fire alarm signal by means of the fire alarm system serving the protected premises.

   Exception: Where otherwise required or permitted by the authority having jurisdiction or other codes.

6.15.7.3* All exits connected in accordance with 6.15.7.1 shall unlock upon loss of the primary power to the fire alarm system serving the protected premises. The secondary power supply shall not be utilized to maintain these doors in the locked condition.

6.15.7.4 If exit doors are unlocked by the fire alarm system, the unlocking function shall occur prior to or concurrent with activation of any public-mode notification appliances in the area(s) served by the normally locked exits.
Electronic Access Control – How It Works, Relays

- Access Control components work off a basic relay principle.
- Relays are either Normally Open or Normally Closed.

**Normally Closed (NC)** relay has the power passing to the locking device keeping it energized. When the access controller grants access, the relay changes state *removing power* and releasing the locking device.

**Normally Open (NO)** relay has no power passing to the locking device keeping it secured. When the access controller grants access, the relay changes state *giving power* and releasing the locking device.
Electronic Access Control – How It Works, Fail Safe & Fail Secure

• Fail Secure
  – locked **without** power

• Fail Safe
  – locked **with** power

**Important to Remember**

✓ Use a locksmith if unsure
✓ Codes must be followed
Electronic Access Control – Components

Controller
Locking Device
**REX Device**
Access Credential Reader
Power Supply
Transmission Source

- Request to **Exit** device. This device releases the locking device when activated, allowing egress.
  - PIR sensor
  - Push button
  - Physical hardware
Electronic Access Control – Components

Controller
Locking Device
REX Device

Access Credential Reader
Power Supply
Transmission Source

- The Reader receives and transmits an input signal to the controller.
  - Keypad
  - Proximity Reader
  - Card Swipe
  - Biometric Reader
  - Key switch

- The Credential presented to the reader will be one, or a blend of the following:
  - Something you HAVE - like a prox card or key fob
  - Something you KNOW – like a passcode
  - Something you ARE – your finger tip (biometric), eye retina scan
Electronic Access Control – Components

- Each device will usually have a low voltage current draw. After the system has been designed, it is necessary to look at the voltage and amp requirements for each device.

- After volt and amp requirements are determined, an appropriate power supply can be specified.
Electronic Access Control – Components

Controller
Locking Device
REX Device
Access Credential Reader
Power Supply

Transmission Source

• Access control systems use a variety of wire types to transmit everything to include; power, communications and signaling.

• The most common wires used are:
  – 18/2 stranded (power, relays)
  – Cat5e
  – 22/8 OAS (readers, keypads)
Recap of Access Control - System Options Comparison

- Access Control systems can vary in cost and provide different levels of manageability and flexibility.
- Proprietary systems can raise costs and sometimes limit flexibility.

<table>
<thead>
<tr>
<th>Customer Cost</th>
<th>Panel-based</th>
</tr>
</thead>
<tbody>
<tr>
<td>High $$$</td>
<td>RF-based</td>
</tr>
<tr>
<td></td>
<td>PC-managed</td>
</tr>
<tr>
<td></td>
<td>stand-alone locks</td>
</tr>
<tr>
<td></td>
<td>Stand-alone keypad locks</td>
</tr>
<tr>
<td></td>
<td>Standard locks &amp; keys</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network-based</th>
</tr>
</thead>
<tbody>
<tr>
<td>RF-based</td>
</tr>
<tr>
<td>stand-alone locks</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Ethernet-based</td>
</tr>
<tr>
<td>Wi-Fi based</td>
</tr>
<tr>
<td>stand-alone locks</td>
</tr>
</tbody>
</table>

Manageability & Flexibility

Low

High
Questions & Answers

This concludes the Presentation

Basic Principles of Access Control

BlueWave Security
www.BlueWaveSecurity.com
Corporate: Carlsbad, California
Tel: 760.929.9596

BlueWave Security Presenter
James Botek
James.Botek@bluewavesecurity.com