MasterLibrary

The new role of Access Control systems

Improve security, capital planning, and operations with a better understanding of how Access Controls are increasingly the heart of your district's security systems.

MasterLibrary by Follett Software

As today's K12 school security systems have become more complex and interconnected via a common IP platform, Access Control systems have taken on new-found importance.

This guide is intended to give school district Facility Managers, IT Directors, and Business Officials a better understanding of the complexity of today's building-based security, life safety, and communications systems and end-point devices.

In the past, these systems used discrete devices that were hard-wired back to individual controllers.

Today, these devices are typically connected via a common Internet Protocol (IP) backbone—your district's intranet—where Access Control systems have become the heart of of security, lockdown, and access control functionality.

A better understanding of Access Control systems will help all parties make more informed decisions that directly impact the safety and security of students, staff, and community.

Access Controls of the past

Access Controls used to be comprised of simple standalone systems that included:

- Card readers
- Electronic strikes
- Request-to-exit (REX) buttons or sensors

The electromechanical end-point devices were each hard-wired back to the main Access Control control panel.

Generally, system controls were:

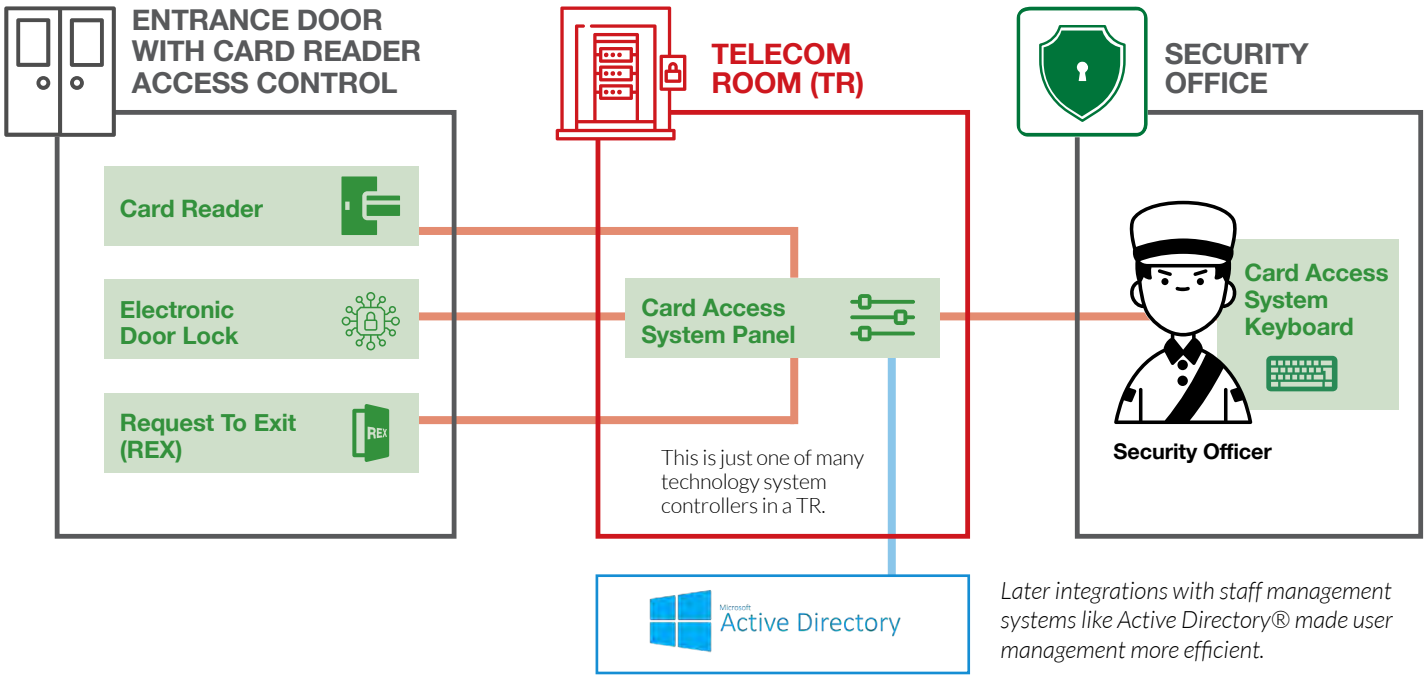
- Manually updated for hold-open times.
- Cards were added and removed on an individual basis.

These systems began integrating with staff management systems—e.g., Active Directory®— to make adding and removing users more efficient.

But while Access Control's system capabilities expanded, its operational scope did not—the only job of the system was to control doors.

Contents

Access Control devices were separately hard-wired to a Control Panel housed in a Telecom Room (TR). A hardwired keyboard in a Security Office was used by security staff to manually update door schedules and manage access cards.



Integration with Building Controls

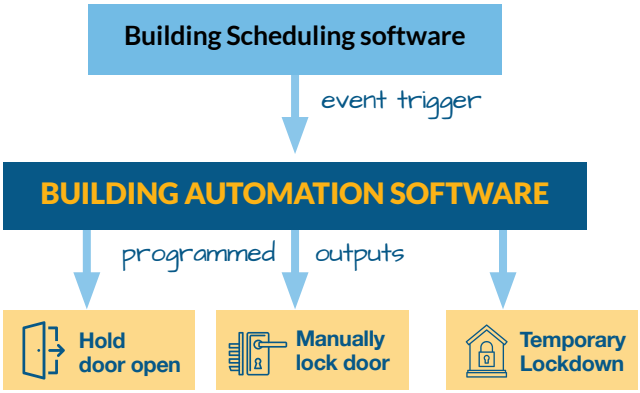
Later, as these systems became more integrated, they morphed into building control systems that expanded automation capabilities.

Building Schedules

For example, allowing access to be controlled by building schedules. While "hold opens" are typically interior door statuses controlled by the Fire Alarm system, building scheduling software can override fobs based on school or sport events to prompt special action such as:

- Hold open
- Manually lock
- Temporarily lockdown an entrance

Events programmed via building scheduling software can automatically trigger different door statuses.



Building Lockdown

The Access Control system is now typically the heart of a Building Lockdown system as well.

The system uses a lockdown button as the trigger/input, and blue lights (notification/output) to notify building occupants of a lockdown or other emergency situation.

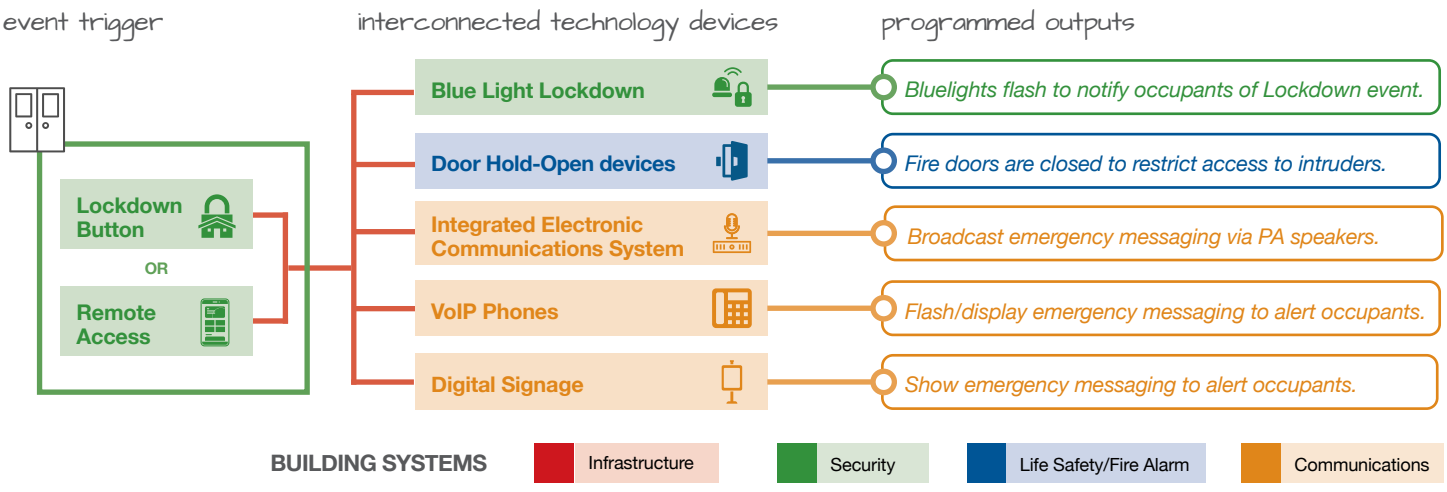
Just as the bluelights are an output relay, similar triggers/relays can be used to initiate other systems as well:

- Releasing fire doors to control/restrict access
- Trigger mass notification systems
- Trigger IP-connected Public Address (IPPA) systems to show or sound a message
- IP phones can flash or notify
- Digital signage can be pre-programmed to show emergency messaging.

These lockdown features have been evolving as their use grows and some states mandate features that increase usability such as:

- Remote access (ability to trigger from computer or cell phone)
- Network connectivity that allows multiple buildings to communicate over the network.

When a Building Lockdown is initiated from a button, remote control or software application, multiple downstream events on different building systems are triggered coordinated by the Access Control system over the shared IP backbone.



The brains of other systems' controls and devices.

Access Control systems are now increasingly the trigger for actions by a variety of other technology systems and devices for building- or district-wide emergency situations.

Generally speaking, Access Control systems are acting as central controllers that can trigger actions of many other systems and devices in the building or across the district.

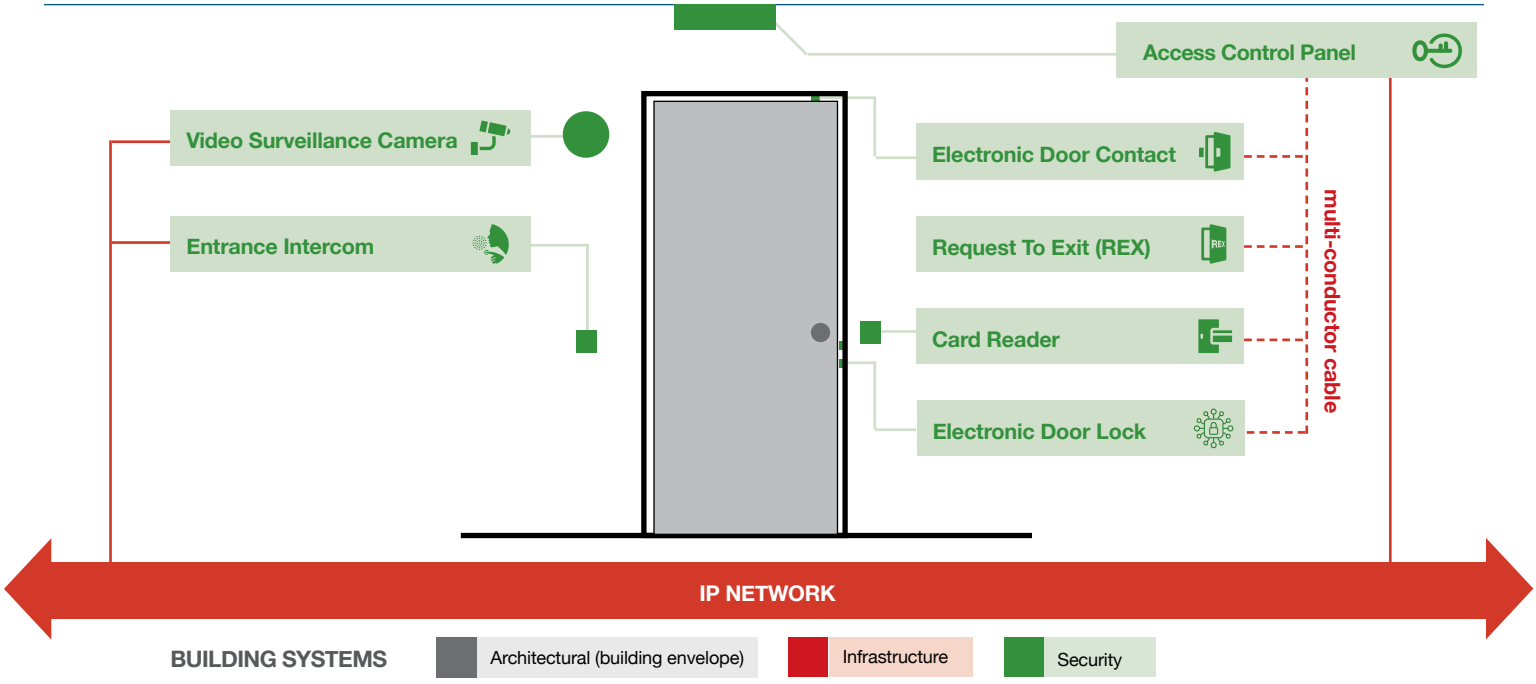
There are so many different district-specific configurations that it's difficult to define a "standard" but here are some specific examples that could be mixed and matched as needed.

- In **normal** operation, all interior doors remain locked with magnetic "hold opens."
  - Doors are held open by electro-mechanical magnetic catches to allow student and staff access during arrival and dismissal periods.
  - Exterior doors are locked before and after arrival and dismissal periods.
  - Interior doors remain locked but are held open in hallways and other areas accessed during the school day.
- When the **lockdown** button is pressed,:
  - The hold open status is canceled and all doors close into their locked positions.
  - All staff access fobs/ cards work for 3 minutes on **any** door before they shut down. This gives staff a moment to usher any students in the hallway into the nearest classroom.
  - Admin and security fobs still function as usual.
  - Normally deactivated emergency responder fobs activate and provide full access to all doors.

A typical Lockdown Button

continued

This simplified view shows some of the Door Access Control devices required for an entrance door. Main entrances, double doors, and other entrance types usually require additional devices, all of which are interconnected via the district's common IP network.



The brains of other systems' controls and devices (cont.)

- Pressing the **lockdown** button triggers several relays within the access control panel that initiate actions from other systems:
  - **IP Phones** that have messaging applications such as Informacast® can broadcast messages on phone displays while flashing lights to attract attention to the message.
  - IP-based **Public Address** systems with similar messaging applications can trigger pre-recorded messages/recordings to be played.
  - **District messaging** systems can send messages to admins/staff and/or parents.
  - **Bluelights** can be illuminated to notify occupants of the lockdown situation.
  - Power to **corridor door hold-open devices** can be dropped to restrict access or slow travel of unwanted occupant(s).
  - IP-connected **smartboards** can program override messaging that takes over the lesson and displays the emergency messages.
  - **Lighting systems** can be triggered to illuminate all lights in the event of a lockdown.
  - **Multi-Building systems** when multiple buildings are on the same campus or in close proximity. Choose to lockdown one or both buildings.

- All of these connections can also be used for emergency situations other than Lockdown.
  - Fire (triggered by Fire Alarm, not Access Control system)
  - Tornado
  - Earthquake
  - Hurricane

continued

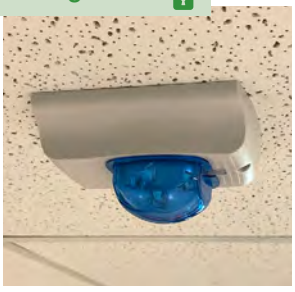
PA Head End

Public Address (PA) headends (controllers) installed in an IT equipment rack in a Telecom Room. These headends can be programmed to trigger actions based on specific events.

IP Phone

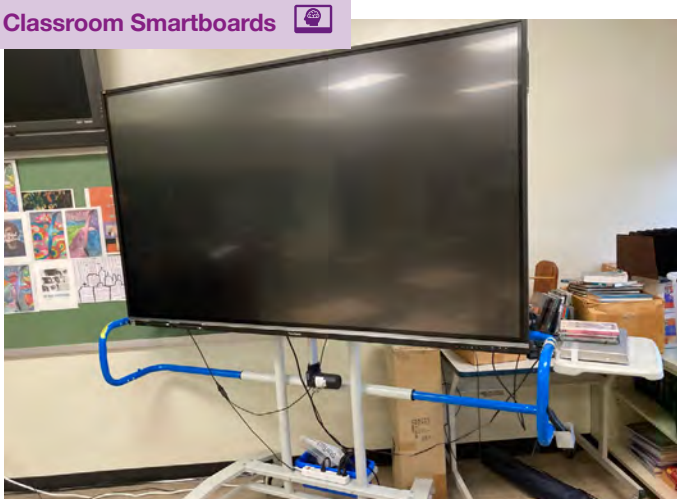
IP Phone handsets can display emergency messages.

Blue Lights



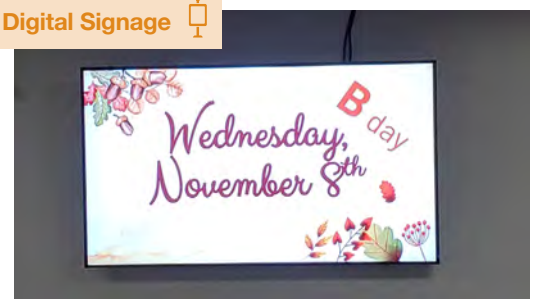
An interior ceiling-mounted blue light.

Classroom Smartboards



Classroom Interactive Flat Panel (IFP) displays can also be programmed to display emergency messages.

Digital Signage



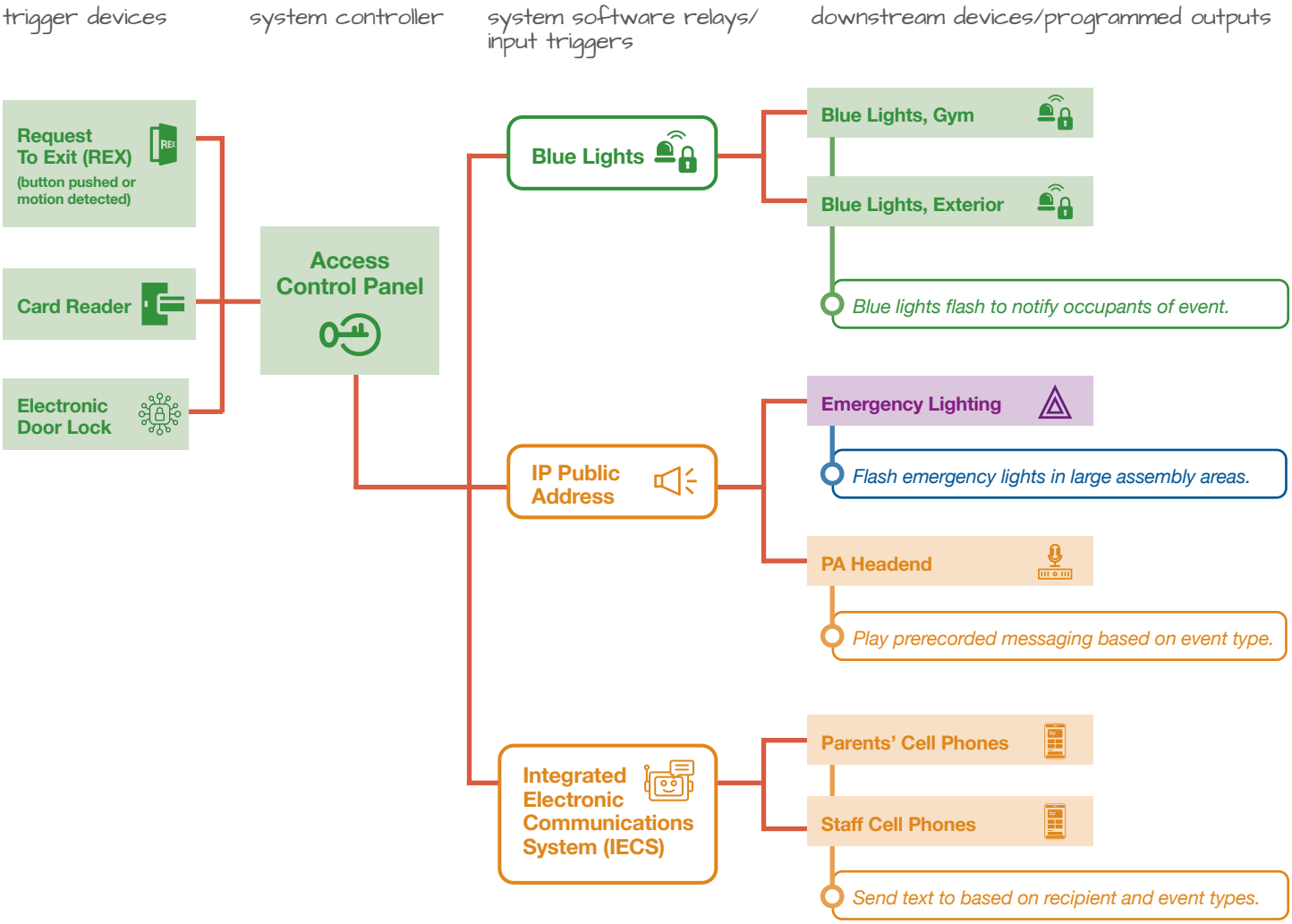
Digital signage can also display various emergency messages based on the triggering event.

The brains of other systems' controls and devices (cont.)

Relays play an important part of the Access Control system. These parcels of software code electronically activate downstream events on specific systems using the building's technology infrastructure as a digital highway to transmit the data signals.

Here is an example of how three digital relays are used to transmit signals from trigger devices to the required systems for downstream actions.

The building's technology infrastructure is used to transmit signals from trigger devices to the Access Control Panel where software-based relays send pre-programmed commands to various systems and devices based on the specific event.



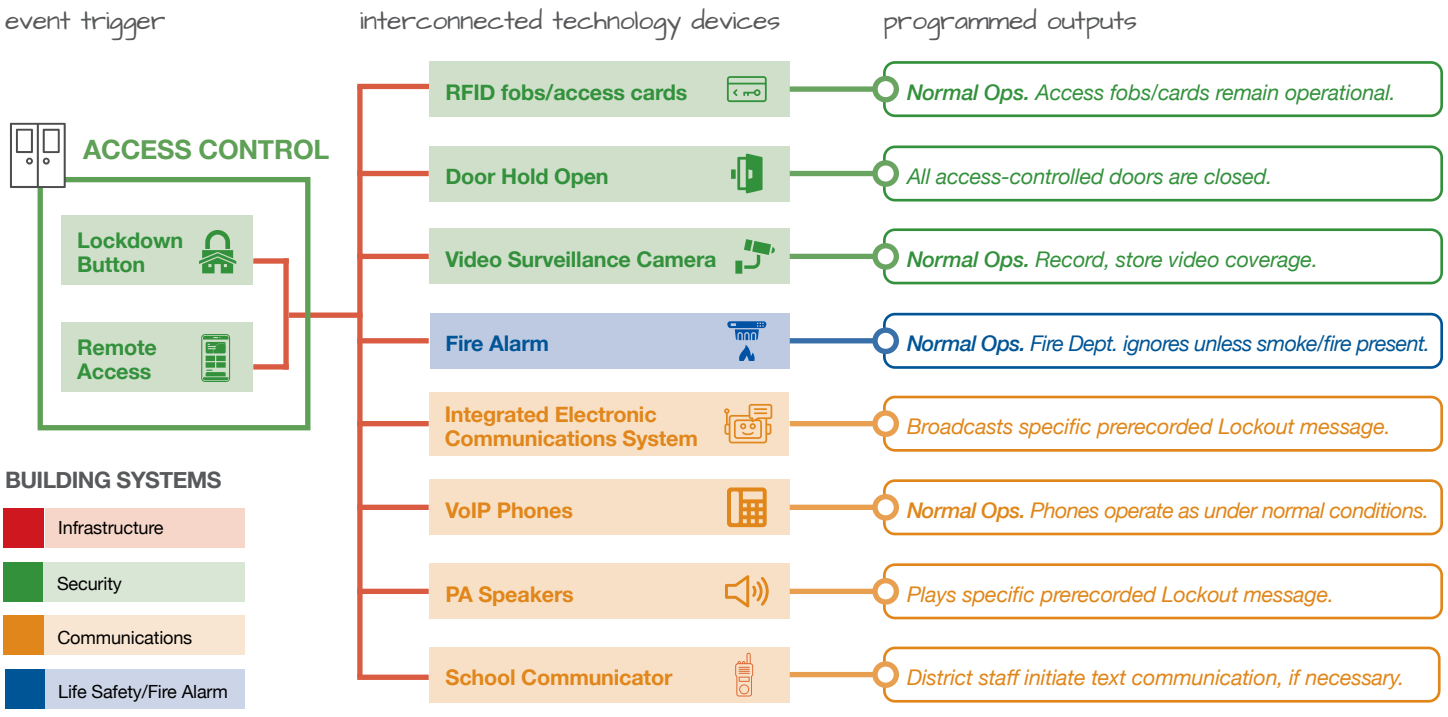
BUILDING SYSTEMS Infrastructure | Security | Communications | Life Safety/Fire Alarm | Electrical

Inter-system operability example: LOCKOUT

Here is an example scenario of the multi-system coordination required specifically for a **Lockout** condition/event.

CONDITION/EVENT: LOCKOUT	
Description	In the event of a concern outside of the school with no immediate risk to students or staff (e.g., suspicious person on/near school property): 1. No one enters or exits the building. 2. Classroom instruction continues as normal. 3. All exterior windows and doors are locked. 4. Outdoor activities are canceled. Move into the closest classroom or secure area, and lock all doors.
SYSTEM/SUBSYSTEM	**THEORY OF OPERATION**
Access Control	Access Control systems receives initial input from application, web interface, or remote control unit. 1. Sends signals to PA and other inter-operable systems. 2. All access controlled doors are locked. 3. All RFID badges will remain operational during this event.
Video Surveillance	1. Records video 24/7. 2. Retains video for 30 days. 3. Can be viewed live from mobile device for authorized users.
Public Address (PA) System	The PA system receives a signal from the Access Control system for a Lockout event which plays specific prerecorded messages based on a the event type.
Phone System	No special operation based on event.
Fire Alarm	Continues to operate as normal. The district has communicated with staff that the Fire Alarm should be ignored during a lockdown event unless smoke and/or fire are seen, heard, felt, and/or smelled.
School Communicator	District staff initiate necessary communication if applicable.
Area Of Refuge (AOR)	No special operation based on event.
Intercom (Main Entrances)	Functions as normal. No change. Based on the district's current protocol, if the Intercom is activated the call will be ignored.

*Example of just one possible multi-system coordination programming for a **Lockout** condition. Almost countless programming permeations could be used for any specific event/condition type based on District's needs/preferences.*



Security
Communications
Life Safety/Fire Alarm

Inter-system operability other examples

Here are three more examples of the multi-system coordination required for specific conditions/events.

CONDITION/EVENT	LOCKDOWN	SHELTER-IN-PLACE	SCHOOL CANCELED, FULL DAY
Description	In the event of security threat in or near the school all students shall: 1. Move into the closest classroom or secure area, and doors are locked. 2. Be moved to a safe area in the classroom away from the door. 3. There should be no communication through the door or room phone. 4. Stay hidden until physically released by law enforcement.	In the event of a threatening event (e.g., tornado): 1. Students move to their classrooms, or may receive instructions to move to a designated safe area. 2. Move away from windows.	Usually weather related.
SYSTEM/SUBSYSTEM	**THEORY OF OPERATION**		
Access Control	Access Control system receives initial input from push button, mobile device app or GUI, and performs these actions: 1. Sends signals to PA system. 2. All access controlled doors are locked. 3. All staff RFID badges are disabled. Select Admin, Safety Resource Officer, and First Responder badges remain operational. 4. Blue lights are turned on.	No special operation based on event.	All doors remain locked as if it were a weekend or holiday.
Video Surveillance	1. Records video 24/7. 2. Retains video for 30 days. 3. Can be viewed live from mobile device for authorized users.		
Public Address (PA) System	IECS receives signal from ISMS for a Lockdown event and performs the following functions: 1. Plays specific prerecorded messages. 2. Initiates blue light devices.	1. District Staff utilize the PA as necessary with specific instructions. 2. There are no pre-recorded messages.	No special operation based on event.
Phone System	No special operation based on event.		
Fire Alarm	1. ISMS triggers fire alarm system to release all fire doors with hold-open devices (i.e., doors close). 2. The district has communicated with staff that the Fire Alarm should be ignored during a lockdown event unless smoke and/or fire are seen, heard, felt, and/or smelled.	No special operation based on event.	
School Communicator	District Superintendent calls District Communication Director who uses School Communicator to send text, email and phone call messages notifying that the district is in a lockdown event and that more information will follow. This is typically a prerecorded message that is automatically sent when an event is triggered.	District staff Initiate necessary communication if applicable.	Not applicable.
Area Of Refuge (AOR)	Operation of System is unaffected by a lock down event. Based on the district's current protocol, if the AOR is activated the call to the office will be ignored which will send the call to the monitoring service.	No special operation based on event.	
Intercom (Main Entrances)	Functions as normal. No change. Based on the district's current protocol, if the Intercom is activated the call will be ignored.	No special operation based on event.	

As stated earlier, there are almost unlimited combinations of trigger events and downstream actions that can be programmed into IP-based integrated security, life safety, and communications systems. Your district's needs may be different from these examples; explore all options with your District's Safety Coordinator.

Access Control at every door

This newer style system that covers (nearly) every door in the building using wireless battery-powered lock sets that remove the need for keys all together.

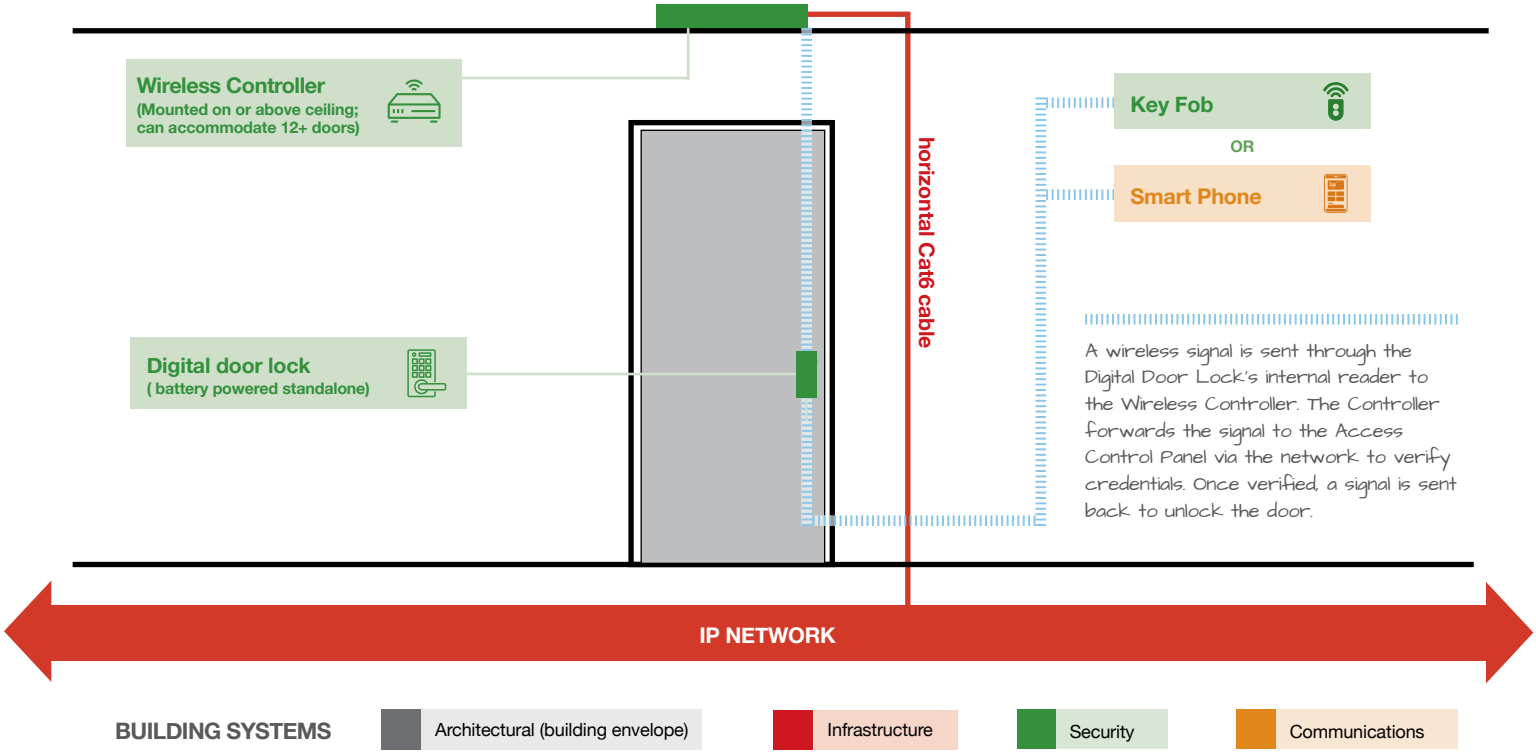
These new types of Access Control systems:

- Require additional network cabling and hardware.
- Are typically proprietary wireless receivers that live in or on ceilings and provide 12 or more doors with wireless connections.
- Monitor all wireless lock hardware with low battery warnings.

Utilizing a full wireless Access Control system like this can provide many security and safety benefits.

- Allows doors to be locked or unlocked in emergency situations.
- Allows teacher key fobs to allow access into other classrooms only in emergency situations.
- First responder key fobs can be loaded into Knox Boxes to give 100% access to emergency personal.
- Cleaning crews and building maintenance can automatically lock or unlock entire wings to more efficiently perform tasks.
- Districts never need to worry about the incredibly costly task of re-keying due to lost keys.
- Greatly increase building security. Any fob can be deactivated and replaced at anytime rather than having the liability of lost keys.
- Rules can be setup to restrict access during particular times or days.
- Doors can be remotely operated to let in sports teams or after school activities while a manager is off site.

Newer wireless Access Control systems eliminate the need for physical keys, fobs, and cards by using battery-operated electronic door locks paired with wireless receivers. This drawing shows one door—of 12 or more—connected to the wireless controller.



Ensure inter-system operability at every stage of each project

Capital improvement projects often include security, life safety, and communications systems upgrades. Meeting system interoperability needs requires close coordination.

Here are some practical considerations for district Facilities and IT staff, safety officers, business officials, and vendors during each phase of a project that includes security, life safety, and communications systems upgrades.

Planning

Your systems vendors should be able to help your district address these issues during project planning.

- What, if any, inter-system functionality current exists?
- Will the system upgrades/replacements be IP based?
- What new inter-system functionality is desired to meet district needs?
- How will system vendors coordinate their efforts to ensure system inter-operability?
- Can existing technology infrastructure (the physical network's cables, pathways, and spaces) handle increased system demands or are upgrades needed? Cabling contractors need to tightly coordinate efforts with systems contractors and district architects.
- Is the district maximizing its available funding sources for safety and security systems (e.g., SAFE Act)?
- Are projects prioritized so that foundational infrastructure upgrades are made before system upgrades are deployed?

Design

This project stage requires a close cross-team review of all design and construction documentation to ensure systems are designed for both interoperability and constructability.

- Do the design specifications of each system provide the required functionality?
- Do systems include any/many feature sets that the district does not want or need? While you want to plan for future upgrades, be wary of system that are too complex (and expensive) for your needs.
- How involved will the district's Architect of Record be with design reviews of these systems? Oftentimes the architects is focused on other aspects of capital projects building-base technology system do not always get the attention they deserve.
- Is there a professional vendor-agnostic (i.e., objective) party that will review all systems vendor design and construction drawings—including those for infrastructure—to ensure interoperability and constructability?

continued

Ensure inter-system operability at every stage of each project (cont.)

Construction Management

During the Build phase, it's critical to perform regular construction site inspections to be sure what's being built matches what was designed…including infrastructure.

- What district staff is responsible for overseeing Construction Management (CM) for the project(s)?
- Is an outside CM firm being used? If so, do they have the experience to oversee building technology system construction? (Many do not.)
- If not, is there a professional objective party that will periodically inspect the site to ensure all design and construction requirements are being met?
- What district staff and/or contractor is responsible for responding to Requests For Information (RFIs) and other inquiries from systems contractors that involve other inter-connected systems (e.g., Door Access [security] and Public Address [communications])?

Hand-off and Maintenance

A solid project hand-off—including training and all electronic facility records—is critical to optimal system performance.

- What district staff will be trained to use each system? Is there a system primary contact in the district as well as building-level coordinators?
- In addition to testing all specific system requirements with the vendor, be sure to also test all inter-system functionality with all vendors present. Be sure to document any gaps that remain to be corrected prior to project hand-off.
- Has each vendor provided all systems design and construction documentation including specs, drawings, and Operations & Maintenance (O&M) manuals in PDF format?
- Is all system documentation available via secure online platform with restricted permissions based on role?
- If the district has an automated Work Order system, are there Electronic Facility Records for all new systems' controllers and devices?
  - Have all system drawings and specs been linked to the facility records?
  - Have Preventive Maintenance procedures been developed, scheduled, and assigned for all new system devices?

Acronym Definitions

ACRONYM	TERM
GUI	Graphical User Interface
IECS	Integrated Electronic Communications System
IFP	Interactive Flat Panel
IP	Internet Protocol
IPPA	Internet Protocol-based Public Address
ISMS	Integrated Security Management System
IT	Information Technology
PA	Public Address
REX	Request To Exit.
RFID	Radio Frequency Identity
TR	Telecommunications Room