

IPVM



TABLE OF CONTENTS

Life & Safety.....	4
The Codes Behind Access Control.....	5
Access Control IBC International Rules.....	8
Building Occupancy Codes and Access Control.....	12
Free Online NFPA, IBC, and ADA Codes and Standards.....	19
Disability Laws, ADA and Access Control.....	22
Standard for Access Control (UL 294).....	28
Fail Safe vs. Fail Secure.....	32
AHJ / Authority Having Jurisdiction.....	38
Banned: Classroom Barricade Locks.....	43
Doors & Locks.....	46
Door Fundamentals For Electronic Access Control.....	47
Specifying Door Locks.....	57
Maglock Selection.....	65
Selecting the Right Electric Strike.....	76
Selecting the Right Type of Electric Lock.....	83
Request to Exit.....	89
Exit Devices.....	95
Door Closers Access Control.....	102
Automatic Door Operators For Access.....	111
Door Position Switches.....	117
Lock Status Monitoring.....	124
Multipoint Lock Access Control.....	131
Glass Doors and Access Control.....	139
Credentials & Reads.....	151
HID vs NXP Credentials.....	152
Prox vs. iClass Explained.....	158
Access Credential Form Factor.....	165

Vulnerability Directory For Access Control Cards.....	169
Selecting Access Control Readers.....	177
Multi-Factor Authentication Primer.....	188
Biometrics Pros and Cons For Electronic Access Control.....	193
Fake Fingerprints - Liveness Detection Solutions.....	201
Mobile Credentials (BLE / NFC / Apps).....	205
Worst Readers Ever: Keypads.....	212
Hotel Access Control.....	217
Controllers & Management Software.....	225
Access Control Door Controllers.....	226
Access Controller Software.....	235
Axis vs HID vs Mercury Access Controllers.....	246
Wiegand vs OSDP.....	252
Access Control Management Software.....	257
Network & Cable.....	263
Access Control Cabling.....	264
Wireless Access Control Panels.....	271
WiFi & Wireless Access Lock.....	276
PoE Powered Access Control.....	282
System Design & Special Conditions.....	290
Access Control Specification.....	291
Mustering.....	309
Tailgating - Access Control.....	313
The Passback Problem.....	321
Delayed Egress Access Control.....	326
Propped Doors Access Control.....	332
Visitor Management Systems Examined.....	338
Time & Attendance.....	344
Access Control Job Walk.....	350
Hazardous & Explosion Proof Access Control.....	359
"Future-Proofing" Access Control.....	367

Life & Safety

The Codes Behind Access Control

In Electronic Access Control, there is one basic rule: Life safety above all else. While simple, this rule often appears to be at odds with the purpose of the system; keeping an area secure. When combined with the huge number of building opening possibilities, the basic rules quickly grow complex. Addressing the potential variations is the job of Codes, or 'design guidelines' adopted as law.

The Major References

While a substantial number of codes are in use worldwide, most local authorities and municipal codes draw intent from a select two or three references. For access control, those references are:

- [NFPA101](#): The official 'Life Safety Code' is the most widely used source to protect people based on building construction, protection, and occupancy ratings.
- [NFPA72](#): Created for Fire Alarms, this code is sometimes cited in electronic access control because of the special integration required between the door locks and the fire alarm system.
- [IBC](#): The International Building Code, as published by [the International Code Council](#), is the essential guidebook for designing and engineering safe buildings. If not observed directly as the authority, then whatever resulting codes that do have authority take guidance from the source.

Because they are the highest default authorities, if no other codes are cited they become the defacto regulations governing access control in the US.

Not Everyone Agrees

Because many other codes, especially locally exempted or municipal codes, are ratified for use by AHJs, the first priority of an access control designer is to establish which authority to observe for a given project. While checking [Jurisdictional](#)

Adoption is a critical first step, confirming the full scope of rules for access with the AHJ is the most important measure to take.

However, even if verbiage differs, the intent is the same: life safety must be preserved. In no circumstances, whether in normal operation, emergency condition, or even equipment malfunction, can a door prevent an occupant from escaping the premises. In most cases, free egress is preserved by the mechanical hardware configuration, but it cannot be hindered by the addition of electronic access. For every lock, there must be a mechanical or physical override. Because of this, exit devices and Request to Exit hardware are essential devices for most access systems.

Specific codes and regulations depend on 'occupancy rating' and what is permissible for one type may be illegal in another. In many cases 'one size does not fit all', and each project and system may vary depending on the facility's occupancy use classification.

Because occupancy classifications determine how codes define access, the end result to the uninformed designer or installer can appear to be akin to 'hitting a moving target'. For example, a maglock controlled exit may be permissible in one building type, but forbidden in another. Emergency Exits may be able to access controlled in one occupancy, but not in other.

Door Function Important

Aside from building classifications, the function of a controlled opening is also an important consideration. The types of doors below have special considerations when installed as part of access systems:

- Fire Doors: The openings are more than just secured openings; they provide an integral safety function to limit risk in a fire condition. Because of this function, and their special construction, fire doors must be positively latched in a fire and cannot be cut or modified for hardware.
- Stairwell Doors: Usually stairwell doors are locked, to prevent unauthorized access during normal conditions, but in a fire these locks must be dropped so

an occupant fleeing a fire cannot be trapped in a stairwell. For this reason, access controlled stairwell doors are especially configured in typical use.

- "Nanny" and [Delayed Egress Doors](#): Other systems that momentarily 'lock inhabitants in' are subject to special authority, and the full scope of operation is typically governed by code, from how long a 'delay period' can be (15 or 30 seconds?) or which doors can be kept closed to prevent unauthorized exit (ie: nursing home facilities).

Reconciling the security plan with the floorplan and facility occupancy code is vital, and clearly establishing what controls are permissible on which doors must be done up front, before any installation work commences.

Detailed Passages

Included below are specific citations that are commonly cited in access control use:

- [IBC 1010.1.9.1 - .9 \(2015\)](#): Describes the role of lock releases, egress requirements, [Request to Exit](#) hardware and other overrides on locking hardware, and defines which occupancies are mandatory.
- [NFPA 101 7.2.1.6.2\(2015\)](#): Describes how to properly install electronic access control so that emergency egress is still maintained.
- [NFPA 72 3-9.7.1 and 3-9.7.2\(2016\)](#) (Free Access with Login): Describes in detail how controlled doors are to be integrated with fire alarm systems.

Ultimately, other sources may be applicable for access control systems, including [legacy BOCA](#), [ADA](#), and Government Department Codes.

This reading has been updated in April 2016 to reflect updated code references.

Access Control IBC International Rules

Dealing with fragmented local codes is one of the most frustrating parts of electronic access control design. However, the 'International Code Council' writes the most widely adopted set of building codes, yet many EAC designers are unaware when and where those rules apply.

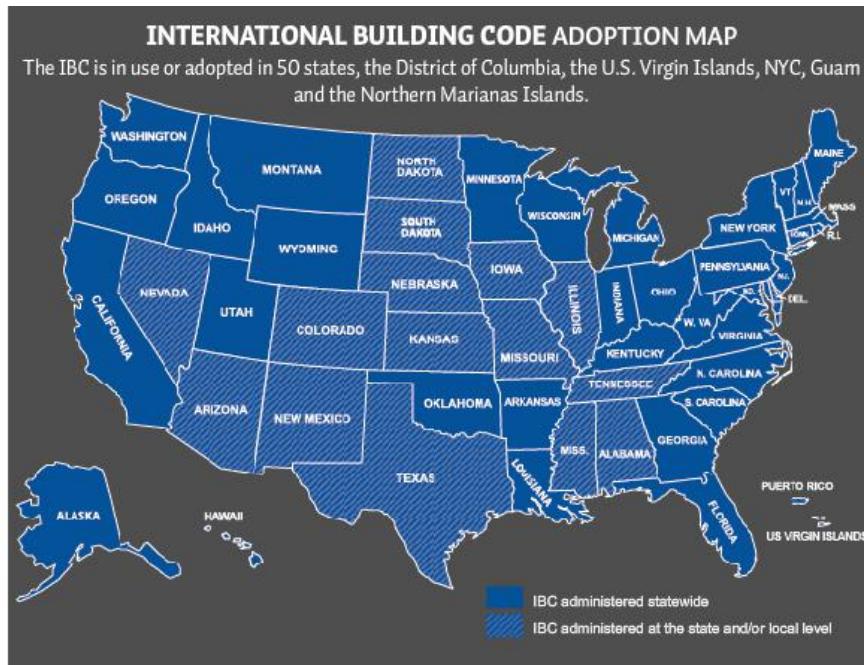
An International Code?

Simply, IBC is not recognized everywhere. Despite being named 'international', the IBC is hardly recognized as 'the authority' by every nation. The prospect of all nations agreeing on a common engineering governance might be ideal, but it is highly unlikely ever to happen. Establishing building codes is a highly bureaucratic process, and even areas willing to submit to a standard often make small changes based on their own preferences.

As noted in "The Codes behind Access Control", IBC is key in describing the safe design and installation of EAC. The broad intent of IBC is to preserve life safety in all aspects of architectural and engineering design. As a result, the majority of IBC's criteria pertaining to EAC relates to egress (or exit) through openings secured by the system.

IBC Recognition

However, regardless of the misnomer, ICC produces the most globally recognized set of building codes. According to ICC's website, "The International Building Code (IBC) is in use or adopted in all 50 [US] states, the District of Columbia, Guam, Northern Marianas Islands, NYC, the U.S. Virgin Islands and Puerto Rico."



Outside the USA, IBC is the basis of national codes several nations, including:

- USA
 - Australia
 - Canada
 - Kenya
 - Mexico
 - New Zealand
 - Brazil
 - South Africa

Even when not strictly ratified, IBC is the foundation of countless individual municipal codes throughout the world. For example, Honduras and several other Central American Countries have formal agreements with ICC to write national building codes.

US Acceptance

In the US, the [ICC Jurisdictional Code Adoption Status](#) list includes the version adopted by every state and includes local variations of major cities

within those states. The list includes adoption status of every ICC code, not only IBC. The specific version and whether it has been adopted in whole or with local exceptions is noted in the chart. Each state is shown with subsequent rows detailing adoption by local municipalities.

Global Acceptance

However, no international acceptance list is provided. We have contacted ICC and asked for a 'global' list, but acceptance of IBC in unedited form is fragmented. If no AHJ is available to field inquiries, check with national 'Codes Ministry', 'Bureau of Regulation' or similar government department for guidance.

Adopted Version Matters

Editions of the IBC are updated and published on a three year cycle, with the latest version released in 2015. However, IBC adoption often refers to one other than the latest. Version adoption for most jurisdictions routinely runs one or more releases behind the most current.

While general requirements seldom change, specific language or terms affecting interpretation may change. As such, noting the specific year a relevant code is written may help eliminate confusion or ambiguity between access designers, installers, and AHJs.

Codes vs Standards

A frequent source of confusion when dealing with IBC is to what extent the codebooks are enforceable. Determining the answer depends on the legal definition used to identify how the code is used:

- **Codes:** adopted as Legal Documents; enforceable as Laws

- **Standards:** used to meet Code Requirements, but unenforceable until referenced by code.

IBC Codebooks are used both as a 'codes' and 'standards', depending on jurisdiction preference. Noting how IBC is being locally cited will avoid uncertainty of 'which rule has the highest precedent' on a given issue. Regardless of how it is used, being familiar with IBC is fundamentally valuable as a 'benchmark' regardless of the local exceptions in use.

What about NFPA?

The IBC doesn't supercede NFPA or vice versa. IBC is usually referenced by architects and engineers, while NFPA is the defacto choice of many fire marshals and life/safety inspectors. On matters of access control and egress, IBC and NFPA compliment each other, but local adoption of either or both is not required. In many areas, especially formally organized municipalities, EAC designs may be subject to both codes. However, IBC generally has a broader scope and carries wider adoption between the two sources.

The AHJ Knows

When it comes to establishing 'which code/version applies' to a given project, the 'Authority Having Jurisdiction' is the standby resource. If doubtful about which code to use, the AHJ provides a succinct answer. Identifying this authority upfront and early in a design will ensure which IBC, or variation thereof, applies.

Building Occupancy Codes and Access Control

A building or room's classification can greatly impact which building codes must be followed. In terms of access control, these 'occupancy codes' dictate how openings can be locked and what equipment is required, often representing a range of hundreds of dollars per door.

How do you know the occupancy classification of a space and which codes apply? Sometimes, even the AHJ may not be sure, and you need to determine this on your own.

This report will guide you through the process to be sure, covering:

- Why classification is necessary
- Classification definition and key categories
- Finding classification ratings
- Comparing classification types
- Impact on lock hardware selection
- Handling mixed occupancies
- Developing manual ratings

Why Classification Is Necessary

Unfortunately, a history of tragedies and deaths are the reason classification is needed. The Winecoff Hotel Fire in 1946 is one example, where over 115 hotel occupants died because fire escape routes and enough egress had not been designed into the building based on normal occupant loads. Other disasters like NYC's 1911 Triangle Shirtwaist Fire (killing nearly 150) also drove the importance of properly operated and designated egress routes in a structure.

Modern occupancy codes are designed to make identifying critical protection areas easier, and condense egress requirements for even complex subsystems like physical access to a formula.

Classifications Definition and Key Categories

While building floorplans and construction vary widely, the purpose of the buildings are similar and can be generally defined. Regardless of the appearance of the building, the gathering spaces, sleeping areas, factories, material storage, and commercial business activities it contains usually involve the same basic activities.

In terms of categorizing this, two major metrics are used, and from them an entire range of requirements are based. The need for multiple exits, fire escapes, sprinkler systems, ventilation, lighting, and even which type of door hardware can be used on doors is based on these categories:

- Occupant Loads: This rating determines the maximum number of people who can gather in a space simultaneously, depending on factors like area, available exits, building strength, and use type.
- Building Classifications: These ratings are concise, but general descriptions given to a space based on how it is assigned for use.

Usually, both these ratings are calculated by architects or building engineers during design, but it is sometimes necessary for physical access control designers to figure these themselves.

Finding Classification Ratings

In many cases these ratings are available in drawing sets or blueprints, usually labeled as an "Occupancy Schedule" like this example:

Number	Name	Area	Non Calculate	Occupancy Schedule		Occupancy Classification	Occup	Occup	Occupancy Load Equal Test
				Net Room Area	Area Per Occ				
100	RECEPTION	479 SF	0 SF	479 SF	15 SF	Assembly without fixed	32	32	Yes
101	OPEN OFFICE	844 SF	0 SF	844 SF	100 SF	Business areas	9	9	Yes
102	CORRIDOR	343 SF	0 SF	343 SF	0 SF	Unoccupied - Corridors,	0	0	
103	TRAINING ROOM	1028 SF	0 SF	1028 SF	7 SF	Assembly without fixed	147	147	Yes
104	CONFERENCE	402 SF	0 SF	402 SF	15 SF	Assembly without fixed	27	27	Yes
105	WORKROOM	428 SF	20 SF	408 SF	15 SF	Assembly without fixed	28	28	Yes
106	STORAGE	384 SF	0 SF	384 SF	300 SF	Accessory storage area	2	3	No
107	MEN	123 SF	0 SF	123 SF	0 SF	Unoccupied - Corridors,	0	0	
108	WOMEN	134 SF	0 SF	134 SF	0 SF	Unoccupied - Corridors,	0	0	
109	OFFICE	133 SF	0 SF	133 SF	100 SF	Business areas	2	2	Yes
110	OFFICE	127 SF	0 SF	127 SF	100 SF	Business areas	2	2	Yes
111	OFFICE	127 SF	0 SF	127 SF	100 SF	Business areas	2	2	Yes
112	MECHANICAL	121 SF	0 SF	121 SF	300 SF	Accessory storage area	1	1	Yes
Grand total							252	253	

Example Occupancy Schedule Sheet in Blueprints/Floorplans

Given the data like 'Occupancy Loads' and 'Occupancy (or Building) Classification', the proper codes for the space can be determined.

In other cases, the design will need to ask the AHJ, or perform calculations to have approved by the AHJ. We address the basic calculation method in the below section "Developing Manual Ratings".

Comparing Classification Types

Here is a list of the occupancy classifications defined by the International Building Code (IBC):

1. Assembly: Groups A-1, A-2, A-3, A-4 and A-5
2. Business: Group B
3. Educational: Group E
4. Factory and Industrial: Groups F-1 and F-2
5. High Hazard: Groups H-1, H-2, H-3, H-4 and H-5
6. Institutional: Groups I-1, I-2, I-3 and I-4

7. Mercantile: Group M
8. Residential: Groups R-1, R-2, R-3 and R-4
9. Storage: Groups S-1 and S-2
10. Utility and Miscellaneous: Group U1

Rough classification is generally straightforward based on how the building or area is intended to be used. For example, houses are coded 'R', manufacturing plants coded 'F', and schools 'E'. From there, the sub-classification is based on specific use or size details further explained in Section 300 of IBC.

Take 'Factory and Industrial' codes F-1 or F-2. 'F-1' facilities carry a 'moderate hazard' rating, while 'F-2' means 'low-hazard'.

In the case of 'Institutional' or 'I' occupancies, the criteria I-1 is:

"[Area] houses more than 16 persons, on a 24 hour basis, who because of age, mental disability or other reasons, live in a supervised residential environment that provides personal care services. The occupants are capable of responding to an emergency situation without physical assistance from staff."

While I-3 is:

"[Area] inhabited by more than five persons who are under restraint or security and is occupied by persons who are generally incapable of self-preservation due to security measures not under the occupant's control."

So while the general use type is unchanged, the operational utility of the area has distinct definitions.

Impact On Lock Hardware Selection

Typically occupancy codes and physical access control intersect at which type of lock hardware can be fitted to doors. In general, occupancy codes dictate where exit device must be used to permit quick egress. With everything else equal, a residential 'R' classification would not require exit devices on doors, than an assembly 'A' classification would.

The inclusion of exit devices on doors versus lever handles can greatly impact which type of electronic lock is used (ie: mortise or surface strike) or even may exclude locks like maglocks from being legal to use. For more on exit devices (shown in the image below), see our [Exit Devices Tutorial](#).



In terms of the most common classifications, International Building Code (IBC) mandates Assembly 'A', Business 'B', or Educational 'E' occupancies with an occupant load of 50 or more require panic hardware for doors equipped with a lock or latch. For any High Hazard 'H' occupancies, panic hardware is required regardless of the occupant load.

[Another common codebook](#), NFPA 101 requires panic hardware for doors serving Assembly, Educational, Business, and Day Care occupancies with an occupant load of 100 people or more.

And finally, NFPA 70 ([National Electrical Code](#)) requires panic hardware or fire exit hardware on doors within 25 feet of the required working space

for 'High-Voltage' areas, usually handling more than 600 volts, more than 800 amps, or battery charging/storage rooms for UPSes or material handling lifts or fork trucks.

Handling Mixed Occupancies

Individual rooms or areas within buildings can be coded differently. This is an important feature in many buildings, and the exact classification of portions of a building can affect other critical variables like minimum fire protection equipment, number of elevators, emergency egress routes, or even lighting requirements for occupants.

In general, 'mixed occupancies' are a factor in access control because even if a small ancillary carries a more stringent life safety or egress requirement, it must be observed in any surrounding area.

For example, if a small 'high hazard' area is surrounded by a less stringent 'factory' rating, any egress paths must abide to the 'high hazard' classification. The same circumstance may apply on a floor of a college dormitory (perhaps an 'R' code) that contains a group study area or game room (an 'A' code). In that case, all common egress doors would need to be equipped with exit devices regardless if they were located in an 'R' area or not because of the 'A' mixed occupancy area.

Develop Manual Ratings

If precalculated Occupancy Codes and Ratings cannot be found, need may arise to do this manually. Occupancy Codes themselves are generally easy to determine, where the actual use type is compared to the criteria listed in Chapter 3 of IBC, titled "Use and Occupancy Classifications".

Exit Availability

In order to determine the maximum number of people who are able to safely be in a room or building, the IBC recommends a certain number of inches of doorway per occupant. Exits that adjoin a stairway need to have 0.3" of doorway per person, and all other exits need 0.2" of doorway per person.

Take an example meeting room hall that has a maximum occupancy of 500 people. That room needs at least 100" - 150" of doorway. With doorways at around 36 inches in width that function hall would need approximately three to five doors.

Occupant Load

To calculate the occupant load, the first step is to calculate the area of the space in question by multiplying the length times the width along the floor. For example, if a boardroom measures 40 feet (~12m) by 50 feet (~15m), the room area measures 2000 square feet (~609 sq. m).

The next step is to divide that figure by the occupant load factor found in [IBC\(2012\) Table 1004.1.2 – Maximum Floor Area Allowances per Occupant](#), which varies depending on the Occupancy Code. The resulting value provides how much floor per occupant is allowed.

Free Online NFPA, IBC, and ADA Codes and Standards

Finding applicable codes for security work can be a costly task, with printed books and pdf downloads costing hundreds or thousands. However, a number of widely referenced codes are available free online if you know the right places to search.

NFPA Online Free

The NFPA provides the standards used as code basis for multiple aspects of security integration, including the National Electrical Code, authoritative Life-Safety guidelines for access control, and multiple related standards for Fire Alarms, Firewalls, and Fire Doors.

The NFPA provides [free online reference access to all ther latest versions of all standards](#) after free registration is completed. The most relevant NFPA standards used in security include:

NFPA 70: NEC, The National Electrical Code

In most of North America, the most comprehensive guide is NFPA 70, most commonly called the 'NEC' or National Electrical Code. While the scope of the codes mainly apply to high-voltage electrical work of more than 100 Volts, security work and devices like PoE or small gauge cabled hardware using less voltage are also given prime attention. We examine NEC in detail in our [Low Voltage Codes and Video Surveillance](#) note, but the source code can be accessed here:

- [NFPA 70: National Electrical Code](#) (registration required)

NFPA 101: Life Safety

One of the most important guidelines of electronic access is NFPA 101, the foundation behind how to install access and still preserve safe egress. We examine

those elements closely in our [Codes Behind Access Control](#) post, but free access is available here:

- [NFPA 101: Life Safety Code](#) (registration required)

NFPA 80: Fire Door Modifications

Because fire doors have important functions to prevent the spread of fire and to withstand direct flames for some time, modifying them for electronic access use is limited. In most cases, NFPA 80 describes the extent and size of cutouts or holes allowed in a fire door, or the acceptable behavior of that hardware given the location of the door. The link below offers direct access to the section:

- [NFPA 80: Standard for Fire Doors and Other Opening Protectives](#) (registration required)

International Building Code

Taking central importance in legal building design, and retrofit systems like access, IBC is often cited by local jurisdictions as the authority on how to construct systems safely. As we cover in [Building Occupancy Codes and Access Control Tutorial](#) and our [Codes Behind Access Control](#) notes, the actual version that is adopted can vary by year, with verbiage and citations change between them. Below are the most common versions cited today:

- [International Building Code 2015](#)
- [International Building Code 2012](#)
- [International Building Code 2009](#)

Accessibility Codes

Finally, codes that govern how to implement access controls, intercoms, and even workstation design can be found in the Americans with Disabilities Act, that we cover in [Disability Laws, ADA and Access Control](#) note. The most recent versions of those guidelines and mandates can be accessed here:

- [ADA Standards](#)
- [ADA Accessibility Guidelines](#)

Fair Use Copyright Applies Here

In general, free online code resources are read-only and users are not able to download, notate, or print copies for offline circulation. If users want this, then standards and codes are available for purchase, often at prices ranging from ~\$100 for a single standard to upwards of \$5000 for a full set of comprehensive codes. For example, NFPA explains:

"These online documents are "read-only" - they cannot be downloaded or printed, because NFPA relies on the revenues from individuals who [purchase copies of these documents](#) to fund our mission. But these "read only" documents are available to anyone who wants to familiarize themselves with a code or check a requirement."

Under terms of 'Fair Use', citation and republishing of excerpts for public commentary or criticism is allowed, but wholesale republishing of the codes or standards can only be done under conditions given by the authoring agency.

Disability Laws, ADA and Access Control

Designing safe Access Control is paramount for everyone, especially those working with disabilities. In the USA, a specific set of codes, the 'Americans with Disabilities Act', mandates that every commercial or public building accommodates those who may have difficulty with 'traditional' building design. Access Control, in particular, is affected by this law, and many global entities pattern themselves from the same guidelines.

Summary

The Top 4 ways ADA impact access control design are:

1. Door Knobs are Illegal
2. Turnstiles Must Have Gates
3. Accessible Reader Height/Door Controls
4. Audible and Visual Alarms

Other potential impacts related to door openers, breezeway design, and double door configurations, but those elements are seldom constructed in a way needing change because of access control. Typically when corrective action is needed, it occurs because of other construction or system updates.

Mandate

The Americans with Disabilities Act was signed into US law in 1990, and since has been ratified and amended several times. In sweeping terms, [28 CFR Part 36](#) addresses building structural and subsystem design, ensuring that anyone with a 'disability' - wheelchair, blindness, hearing, or "any physical

or mental impairment that substantially limits a major life activity" has equal access to, within, and from a commercial or public building. ADA does not apply to private dwellings, 'historically significant' structures, or other specifically exempted buildings.

Nor does it apply to 'new construction' only. In fact, the most dramatic aspect of ADA is its applicability to existing buildings. The law spells out that aspect here:

4.1.6 Accessible Buildings: Alterations.

(b) If existing elements, spaces, or common areas are altered, then each such altered element, space, feature, or area shall comply with the applicable provisions of 4.1.1 to 4.1.3 Minimum Requirements

In plain terms, existing buildings are often allowed to remain in a 'noncompliant' state until audits or improvements force the update. In many situations, adding or upgrading access control systems qualify as a 'improvement', and so the move to compliance must be taken as a result.

Door Knobs are Illegal

One subtle, but potentially costly change is the prohibition of rounded knobs on door hardware sets. The code excerpt forbidding knobs below:

4.13.9* Door Hardware. Handles, pulls, latches, locks, and other operating devices on accessible doors shall have a shape that is easy to grasp with one hand and does not require tight grasping, tight pinching, or twisting of the wrist to operate. Lever-operated mechanisms, push-type mechanisms, and U-shaped handles are acceptable designs. When sliding doors are fully open, operating hardware shall be exposed and usable from both sides. Hardware required for accessible door passage shall be mounted no higher than 48 in (1220 mm) above finished floor.

Specifically, the law emphasizes that door hardware have 'lever style' handles, where rotating the lever retracts the latch. With the number of options available, it is possible to specify illegal types:



Lever Handles, Not Knobs or Thumb Latches

Especially with 'stand alone' access control locks, paying attention to the trim handle specification means making more than a cosmetic decision.

Turnstiles must have Gates

Likewise, when it comes to turnstiles or revolving doors, an adjacent gate or hinged door must be installed that permits those in wheelchairs passage through the opening:

4.13.2 Revolving Doors and Turnstiles.
Revolving doors or turnstiles shall not be the only means of passage at an accessible entrance or along an accessible route. An accessible gate or door shall be provided adjacent to the turnstile or revolving door and shall be so designed as to facilitate the same use pattern.

In many cases, the gate is a separate entry/egress path from the turnstile, and can increase required opening areas by more than double:

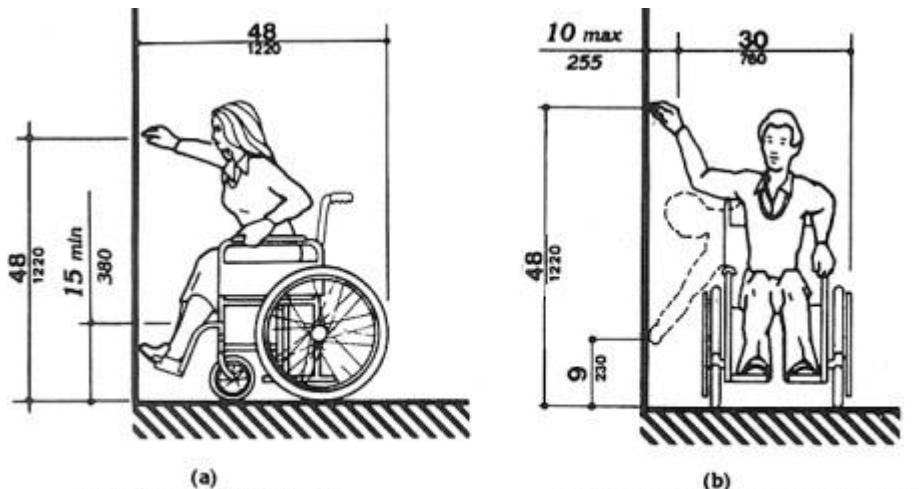


Turnstile MUST HAVE Wheelchair Access Gates

A common concern with 'ADA Gates' is that they simply become 'another opening' to be used by all occupants and become opportunities for tailgaters to 'sneak in' to a facility. For this reason, many access systems grant special access permissions to those in wheelchairs so that only they are able to open the gate. Otherwise, all other occupants can only travel through the turnstile or revolving door.

Accessible Reader Height/Door Controls

All access control user interfaces must be within reach of those in wheelchairs. This limits the mounting height to no more than 48" above the floor, regardless if the reader is mounted in front or to the side of the door:



Acceptable Reader Heights

This standard also applies to other door control equipment, like RTE buttons and powered opener switches. The clearance for door swings and the time a door is unlocked may also be increased on these openings, to allow for the extra time needed to reposition the chair and roll through the opening.

Audible and Visual Alarms

While generally associated with fire or other emergency alarm systems, the requirement that all alarms be both seen and heard can apply to access control, specifically in delayed egress applications. In the advent that someone is blind or deaf, an alternate method of notifying them of a countdown period needs to be readily apparent.

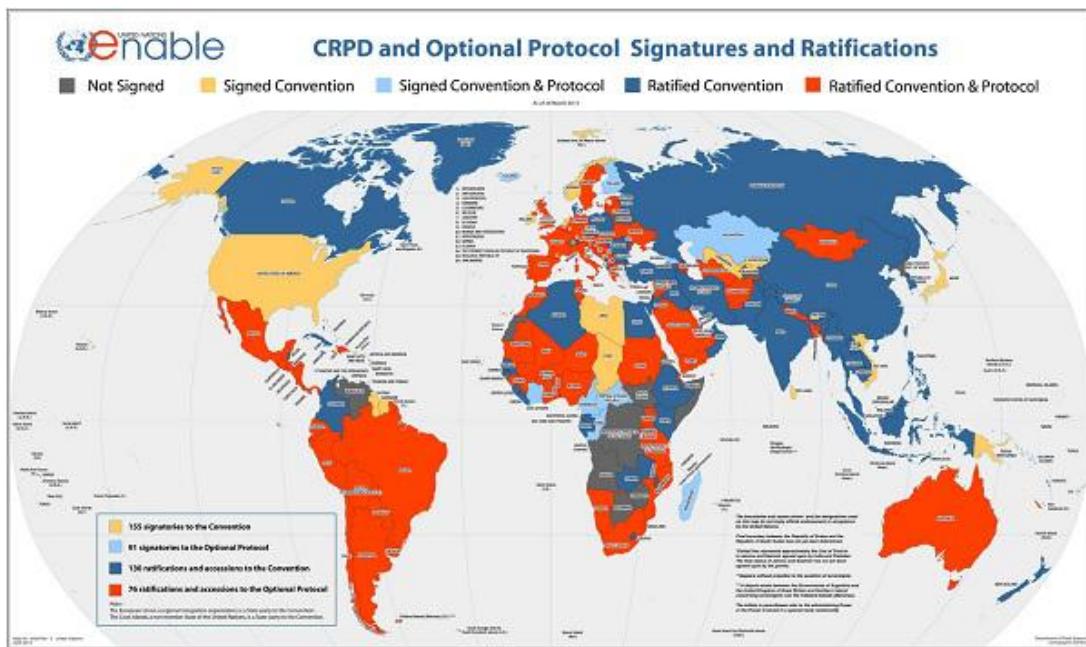
As a result, many AHJs require that digital counters accompany sirens on alarmed doors. While many equipment vendors offer 'ADA Compliant' options that are piece together in the field, several offer devices that integrate both features in one unit:



Delayed Egress: Two Factor Alarms

International Acceptance

While ADA is US legislation, it is used as a guideline internationally. While it may not be enforced as law, many countries have adopted the codes as 'best practices'. In recent years, the United Nations has accepted ADA into international accessibility guidelines that have been ratified or principally accepted by several countries (click image for larger version):



Standard for Access Control (UL 294)

Few specifications are seen more commonly in access control than UL 294. However, aside from seeing it in print, very few understand what it means. In this note, we break apart and define this spec, describing why it is a vital part of many Access RFPs.

A Standard Defined

The scope of UL 294 covers three aspects of Access Control systems:

- Construction (Installation)
- Performance
- Operation

Essentially, the heart of UL 294 is a safety standard, where testing proves that system components can be assembled and operate reliably without hazard. In the case of access control, this is a step beyond just validating devices will not catch fire or spark - it attests that the system will not harm the safety or impede egress of those using the system.

In practical terms, this means doors will not accidentally stay locked and keep people in harm's way even during a malfunction. The UL standard subjects each labeled device to a range of testing designed to show the equipment meet relevant code expectations from:

- NEC (NFPA 99): Requirements that each component will not create a hazard either during (recommended) install or use (Sparking, Grounding)

- NFPA 72: Fire Code compliance, assures that controllers include interfaces with fire alarm/suppression systems
- NFPA 101: System devices

A UL 294 mark is a 'extra step' the vendor has taken to 'prove' their equipment is safe, and it stands as a 'mark of assurance' when included in buying specifications that dubious equipment will not be purchased.

The Mark

While Underwriter's Laboratories offer a range of 'UL Symbols' that can be interpreted to signify different standards. In the case of UL 294, the mark looks like this:



The UL 'Security Mark' applies only to products such as intrusion detectors, burglar alarms, access control, safes, and vaults.

Performance Tests

UL 294 includes several tests that evaluate how well devices withstand damaging environments. Devices are subjected to atypical electrical, environmental, and brute force situations, including:

- Variable Voltage
- Variable Ambients (Environment)
- Humidity
- Endurance (Ruggedness)
- Transients
- Corrosion
- Standby Power (Battery backup)

- Physical Attack Toughness

Tests are performed individually and are not 'layered' or 'stacked' simultaneously as might occur in the field. The exact methodology for each test depends on the device being tested, but the resulting grade is given in four levels of security performance with Level I (lowest level security equipment) to Level IV (highest level security equipment).

Exclusions

However, not all parts and features of an Access platform fall under the scope of UL 294. Two areas excluded from the scope include:

- Headend Server/Database: The scope reads "The accuracy of logged data is not evaluated by this standard", and also "This standard does not apply to supplementary computer equipment that is not necessary for operation of the access control system..."
- Intrusion Detection: Again, the scope details "Where an access control equipment and/or system incorporates the features and functions of a burglar alarm control unit, the requirements of the Standard for Proprietary Burglar Alarm Units and Systems, UL 1076, shall also apply"

This is important to note when careless specs are written that "All Access Equipment shall be UL 294 Certified", because this is inherently not possible. There will be major functional aspects outside the scope of the standard.

Large System Adoption

Especially for larger systems, UL 294 is common, including devices from: Mercury Security, C*Cure, S2, Maxxess, Sargent, etc.

However, certification is done on a component basis, and there may be gaps in a brand's portfolio. If UL 294 compliance is required in a system, every hardware component must be checked for conformity, as there is no 'system' certification.

Systems and platform intended for smaller deployments (<100 doors) typically forego the certification, because it simply is not a purchasing driver for many non-enterprise customers.

Prime Use

Regardless of the 'safety' overtures, like UL certification for surveillance equipment, 294 is primarily used to exclude non-compliant systems from specifications. UL 294 evaluation is not mandatory for Access Equipment, and many vendors forego the cost of certification especially when their offerings are not well suited for larger government, institutional, and hospital verticals where 294 is commonly cited.

Likewise, while the mark's testing 'proves' that devices are safe, the onus remains on the field technician to install them in the correct fashion to indeed live up to the certification.

Fail Safe vs. Fail Secure

Few terms carry greater importance in access control than 'fail safe' and 'fail secure'.

Access control professionals must know how these concepts apply, and how to pick locks that are appropriate. Properly doing so determines whether door hardware risks harming people or assists their safety. Moreover, there is legal risk in failing to do so.

We review:

- The difference between 'Fail Safe' and 'Fail Secure' locks
- Why Free Egress Is So Important
- Controlling Entry is the Goal
- Mechanical Key Overrides Fail Secure
- When To Use Fail Secure Hardware
- Typical Access Control Locks for Fail Safe and Fail Secure
- Proper application of maglocks and strikes for 'fail safe' and 'fail secure'

Finally, after reading, take our 5 question quiz.

The difference between 'Fail Safe' and 'Fail Secure' locks

These terms have a specific meaning for door hardware. Whenever these functions are cited in specifications or code passages, they mean:

- Fail Safe: When power is interrupted (fails), the electronic locking device is released (unlocked).

- Fail Secure: When power is interrupted (fails), the electronic locking device is secured (locked).

These behaviors can impact hardware design and access control configuration, so noting the situations where each is used is very important.

Why Free Egress Is So Important

One misconception of these terms surround which side of the door they apply. 'Fail Secure' and 'Fail Safe' terminology generally applies to ENTRY control only, meaning manual egress in most Building Occupancy Codes is allowed at all times. In an emergency situation, nothing should impede egress (or exit) from a building.



Free Egress Always (NFPA 101)

Locking or chaining exit doors has a horrible and tragic historical precedent, so a significant majority of life-safety authorities simply will not allow locks to complicate exiting. This means that exit doors must always be equipped with mechanical means to override electrified locks (eg: panic bars or exit devices) and if electrified hardware cannot be made to 'fail safe', it cannot be used.

Controlling Entry is the Goal

However, 'fail safe' vs. 'fail secure' is a vital element to control entry into a building during an emergency. Fire fighters or medical responders could be locked out of an area if it is not properly configured to 'fail safe'. On the other hand, occupants could inadvertently open a firedoor, exposing

otherwise protected parts of a building if 'fail secure' is not properly implemented.

The behavior of hardware when power drops is a key part of building design, and both functions play a key role in safely entering a potentially enveloped facility.

Mechanical Key Overrides Fail Secure

Where 'fail secure' hardware is used, local AHJs often require a mechanical override. In the case of strikes, the existing lever lock or exit device provides this function, but other types of electrified hardware may require additional 'mechanical key override' components.

However, the mechanical override is also a source of trouble in many access controlled doors. If someone gains entry using a key, access is granted without the 'system' able to log who entered. Unless key control is tightly implemented, mechanical overrides result in 'door forced' errors in access control logs, and bypass system recording individual access.

As a result, use of Mechanical Override Keys are often used only on an emergency basis with relatively few keyholders - by nature, these operational restrictions are often too complex for many endusers to adopt.

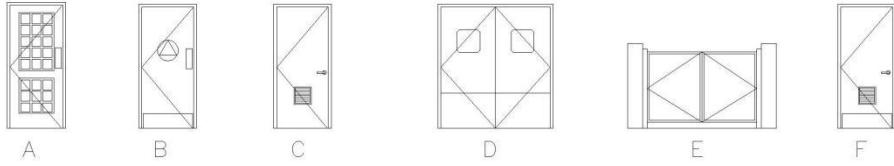
Designing Default Fail Safe Eliminates Risks

For most openings, the default function is to 'fail safe', unless otherwise noted on design documents, hardware schedules (see image below), or other engineering plans as 'fail secure required'.

The exact verbiage of this instruction will vary according to the source, but since adoption of 'fail secure' locks is limited, they are nearly always called out in a excepting or special manner:

HARDWARE SCHEDULE					
HARDWARE #1			HARDWARE #2		
THRESHOLD	PEMKO #2548D	THRESHOLD	PEMKO #2548D		
HINGES	PEMCO NO. FM95HD (1 1/2 PAIR)	HINGES	STANLEY #FBB199 (1 1/2 PAIR)		
CLOSER	CORBIN-RUSWIN	CLOSER	LEN #140		
PUSH PLATE	BUILDERS BRASS WORKS #99	PUSH PLATE	SCHALGE D-SERIES		
LOCKSET	BUILDERS BRASS WORKS	LOCKSET	LOCKSET		
LOCK	#5055v-620/5035	LOCK	LEVER TYPE		
	PEPSI-CARLSON		PANIC HARDWARE		
BEST #1E-7-E-CARP3-826			REINFORCED #1E-7-E-CARP3-826		
DOUBLE KEY HOLE			DOUBLE KEY HOLE		
KICKPLATE	NONE	KICKPLATE	BUILDERS BRASS WORKS		
MISC	WEATHERSTRIPPING DOOR SWEEP	MISC	ALUMINUM KICK PLATE		
 HARDWARE #3					
THRESHOLD	NONE	THRESHOLD	PEMKO #2548D		
HINGES	STANLEY #FBB199 (1 1/2 PAIR)	HINGES	STANLEY #FBB199 (1 1/2 PAIR)		
CLOSER	LEN #140	CLOSER	LEN #140		
LOCKSET	NONE	LOCKSET	SCHALGE D-SERIES		
PUSH PLATE	BUILDERS BRASS WORKS #99	LOCK	LEVER TYPE		
KICKPLATE	BUILDERS BRASS WORKS		PANIC HARDWARE		
MISC	ALUMINUM KICK PLATE		REINFORCED #1E-7-E-CARP3-826		
 SYMBOL OF ACCESSIBILITY					
		KICKPLATE	BUILDERS BRASS WORKS		
		MISC	ALUMINUM KICK PLATE		
			DOOR STOP		

DOOR SCHEDULE						
DOOR NO.	DOOR TYPE	SIZE	MAT.	FINISH	HRDW	REMARKS
1	A	3'-0"x7'-0"	WOOD	P-1	1	PANIC HARDWARE ON THE INSIDE
2	A	3'-0"x7'-0"	WOOD	P-1	1	PANIC HARDWARE ON THE INSIDE
3	C	3'-0"x7'-0"	STEEL	*	2	NO LOCK FROM THE OUTSIDE * FINISH SHALL MATCH EXTERIOR FINISH
4	C	3'-0"x7'-0"	STEEL	*	2	NO LOCK FROM THE OUTSIDE * FINISH SHALL MATCH EXTERIOR FINISH
5	F	3'-0"x7'-0"	WOOD	P-1		
6	E	6'-9"5"x7'-0" PAIR	STEEL	*	MANUFAC.	NO LOCK FROM THE OUTSIDE * FINISH SHALL MATCH EXTERIOR FINISH
7	E	6'-8"5"x7'-0"	STEEL	*	MANUFAC.	* FINISH SHALL MATCH EXTERIOR FINISH
8	B	3'-0"x7'-0"	WOOD	P-1	3	PANIC HARDWARE
9	D	3'-0"x7'-0"	POLYMER	MANUFAC.	MANUFAC.	ELUSON DOOR #SCP-11 OR APPROVED EQUAL
10	F	3'-0"x7'-0"	WOOD	P-1	4	
11	F	3'-0"x7'-0"	WOOD	P-1	4	LOCKABLE FROM INSIDE
12	A	3'-0"x7'-0"	WOOD	P-1	1	
13	F	3'-0"x7'-0"	WOOD	P-1	1	LOCKABLE FROM INSIDE



When To Use Fail Secure Hardware

In common commercial occupancies, fail secure is most commonly used in:

- Fire Doors: These doors provide structural barriers to the spread of flame during a building fire, and are common features of fire control design, where a closed door is used to seal off a portion of an engulfed structure. As such, it remains critically important for a fire door to remain closed in a fire, and 'fail secure' hardware is often specified to ensure a positive lock is always achieved.
- Stairwell Doors: One of the most modified and scrutinized pieces of code surround stairwell doors, and whether or not they are allowed to be locked from the outside (entry) during an emergency. The net effect of so many code revisions is widespread confusion and fragmented understanding among AHJs. It is best to establish the

prerogative of the approving body when planning work to avoid future problems when controlling these doors.

Less common occupancies, like jails, prisons, mental health care facilities, or nursing homes may use Fail Secure almost exclusively, but are typically heavily regulated and other methods of safe emergency egress are often required.

Typical Access Control Locks for Fail Safe and Fail Secure

Maglocks: By design, maglocks require electricity to operate, so when power is removed they 'fail safe' by default. The drop in power is often a condition of the fire-alarm system, so that if any fire pull is activated, all maglocks drop power at the same time. This can cause issues with building security, as then certain exterior doors are unlocked and able to be accessed from the outside, so mechanical locks are an important feature in many of these doors.

Supplying backup power to maglocks is not widely adopted for most openings. When backup power is used with maglocks, it must happen with the concurrent blessing of the AHJ and still be installed so power fails during an emergency event. See our: [How To Use Maglocks With Battery Power Legally](#) note for guidelines.

Strikes: These devices are commonly configured for either 'fail safe' or 'fail secure' function as afforded by their design. Our [Selecting the Right Electric Strike](#) guide covers low level operation, but since most 'keeper' elements of strikes are driven by solenoids, changing the default polarity of the solenoid can cause the keeper to be rigid on loss of power, or completely moveable.

Since the configuration of either function is typically a simple switch setting in the device, strikes are often the favored devices to provide 'fail secure' functionality. Since the mechanical hardware on the door already permits mechanical egress, strikes are simple additions to the controlled opening to provide this feature.

Other Hardware: There are a number of other 'fail secure' hardware devices available, including electronic deadbolts, keypad locks, and electrified locks. However, the adoption and use of this hardware may not comply with codes relating to emergency egress paths, and are not commonly used in fail secure configuration.

Quiz

Finally, after reading, [take our 5 question quiz.](#)

AHJ / Authority Having Jurisdiction

One of the most powerful yet shadowy characters in all of physical security is the AHJ, the Authority Having Jurisdiction. Often, these authorities get involved only when problems arise, and AHJs frequently leave a flood of delays, redesign, and cost increases in their wake. How can you spot an AHJ? How difficult is it to work with, not against, their authority? What can you do to improve your interactions?

AHJs Defined

'Authority Having Jurisdiction' is an official designation used in many organizations, including governments, military, construction, and a variety of trades. The term identifies the specific people or organization responsible for ensuring all work complies.



The realm of 'compliance' varies according to who the authority represented. For access control, the AHJ is most often interested in confirming the system will not endanger life safety during an emergency. However, AHJs often represent other interest security installers do not typically consider - the cosmetic appearance of equipment, modification of

landscape (ie: trimming trees), and if the security system somehow interferes with another building system.

Because individual 'jurisdictions' vary, the actual job title of AHJs are diverse. However, without exception, AHJs represent the interests of overarching regulations, codes, or local influence. For physical security companies, the following section lists the AHJs frequently encountered:

Who Are They?

The AHJs often change depending on the type of work you are performing, but for most intrusion alarm and access control work, they are found in two prime authorities:

Fire Marshals: Also called the 'Fire Inspector', this office is tasked with enforcing fire codes. The scope of enforcement includes field surveys of installation work, and may even mandate project plan signature approval.

Building Inspectors: This authority ensures that all work is performed within the constraints of written building codes. Not only are they versed with interpreting national codes, but they know the local exceptions and addenda.

Other less common, but potentially influential, organizations that have AHJs are found in:

- Health Departments
- Engineers/Architects
- Senior Executives
- Utility Companies
- Military Installation Commanders

- Insurance Companies

In general, the best method of identifying the AHJs for a project is to start by asking the owner's representative and the local Fire Chief for contact names in the area of your work. The type of answer you receive will often lead expectations of how strict or complex the tiers of authorities are for an area. In some areas, there might be a single AHJ to get approval from, while there may be a disjointed litany of AHJs in other areas.

Regardless knowing who these individuals are, and the prerogative they are checking your work from, becomes an invaluable part of getting your job done right, on time, and within budget.

Why AHJs Matter

Right or wrong, AHJs play a huge role in the outcome of security projects. Few individuals are given authority to stop work based on their decisions, but AHJs wield this authority daily. Where does this authority come from, and why do they have it?

- They are Educated: While they may not be technical experts on alarm system or door access control design, AHJs have extensive knowledge on specific codes or regulations that constrain security work. They seldom will express a pure opinion, but instead cite specific code passages or laws when objecting to a work element.
- They are Experienced: AHJs are often elevated to their positions after years of ground-floor, in-the-trenches experience. When they do share a strong opinion, it is frequently tempered by 'having seen it before'. Most AHJs take the lessons learned from other similar projects and apply them forward.

- All the Risk, None of the Reward: Often, it is not a matter of agreeing or disagreeing with their views, because their determination is final. They are bound to their decisions by oaths, laws, and general liabilities. When a system is safe or compliant, an AHJ 'wins', and only when a disaster occurs will many AHJs even be recognized.

AHJs vs. Video Surveillance

While important to security operations, many video surveillance systems fall outside the oversight of AHJs. Because video does not determine or impact Life Safety for facilities, its use is not subject to the same regulations as fire alarms and access control systems.

Practical Examples

Our experience as integrators has turned up a variety of AHJs specific to particular jobs, including:

- Fire Chief: Most cities yield life/safety determinations to the local fire marshal, who in some cases might also be the top ranking local fireman, or the 'Fire Chief'. The issue of 'Fail Safe vs. Fail Secure' is foremost to many of these firefighters.
- Flightline Officer in Charge: For many airports, the flightline is the hub of activity, and any equipment that impacts flight operations is significant. For example, USAF bases often have a hard restriction on an equipment installed higher than 8', because it could interfere with aircraft movement on the flightline.
- Director of Maintenance: These entrusted individuals know relevant codes in a facility. Getting 'buy-off' from the head of maintenance often puts others at ease, knowing the 'local AHJ' approves.

- Arsenal Commander: For a munitions storage facility, any activity involving the running of electricity (regardless of voltage) required explicit approval from the commander, who required a defined work plan of equipment review, laborer background checks, and safety briefings before permitting work.
- Municipal Codes Inspector: Like the Fire Chief, the code inspector often acquires responsibility of signing off on installed systems as part of their job. Knowing the local inspector, and sharing codes interpretation in the course of normal communication can yield trust and understanding during the course of many installations.

Take the First Step

The best approach in working with AHJs is to be the first to reach out for approval. AHJs are frequent challenged by the volume of work they should be monitoring, and they are not always patient or understanding when they are indirectly informed of your project.

In the attitude of 'asking for permission, rather than forgiveness', security designers and installers can win cooperation of an AHJ before commencing work, rather than skirting the matter and being 'caught' later. Not only will the basis of the relationship be 'proactive' rather than 'reactive', the AHJ can offer information or contacts that benefit the installer in future efforts.

Banned: Classroom Barricade Locks

In this age of classroom shootings, many are looking for barricade locks - a cheap and easy stopgap to bolster door security.

Critics condemn barricade locks as dangerous and even deadly because they do not satisfy basic building codes, while proponents claim their simple operation and cheap price outweigh the risks.

Access dealers, worried parents, and school administrators alike have waited to see if building code exemptions would be made.

The world's biggest building code group have weighed all these arguments, and made clear their position in the upcoming 2018 edition of international building codes. Inside, we examine the changes, the proposed code, and where current barricade locks run foul.

Summary of Changes

For the new 2018 version of IBC, the industry group responsible for proposing lock and egress codes BHMA has published their recommended language for 2018 IBC 1010.1.4, called "Classroom Lock Requirements":

- Any locked rooms must be able to be unlocked from the outside of the room
- Egress requirements apply in that 'no special knowledge or tools are required to unlock them, and unlatching can be done in a single movement (per IBC Section 1010.1.9).
- Modifications shall not be made to listed panic hardware, fire door hardware or door closers.

Current Barricade Locks Illegal

Even with the clarification, most (if not all) existing barricade device products will remain forbidden. For example, these ~\$125 devices which have gone viral on Facebook:

Note: [Click here to watch the video on IPVM](#)

As an example, these simply will not meet the clarified requirements, specifically:

"The door **shall be capable of being unlocked from outside the room** with a key or other approved means" and "**Modifications shall not be made to** listed panic hardware, fire door hardware or **door closers.**" (emphasis ours)

We examined this barricade lock series, and a range of other similar products in our [Barricade Locks - Pros vs Cons](#) note. Because the majority of these devices are little more than improvised hardware, prevailing concerns and objections to their use still apply in the scope of the new language.

For Many Countries, IBC Codes Are Laws

IBC language changes are important, because they directly compose architectural laws in many areas of the world. Especially for systems like access control, where many products might unintentionally contribute to injury or death of building occupants when used incorrectly, codes like IBC are important to observe to maintain life safety. If products do not meet these codes, punitive fines, building closure, and urgent corrective actions can be enforced by courts and police.

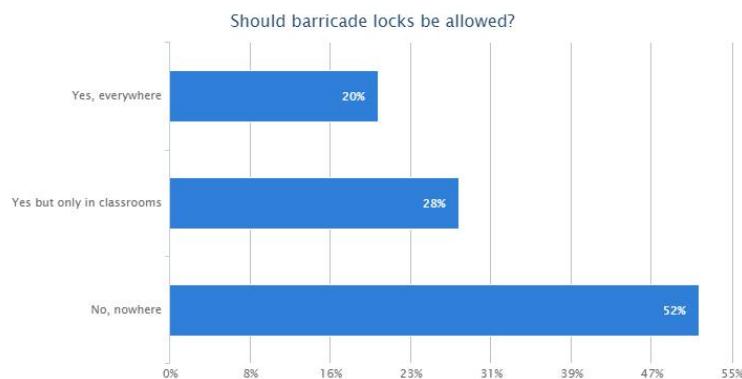
For the 'classroom lock' market, IBC requires all products or devices for securing doors must satisfy code requirements designated by version or year. While the 2018 IBC version will not be ratified as the authoritative code in all areas immediately, in three to five years it will be the most widely used and referred to version in North America and many part of the world.

For more on the jurisdiction of IBC and other important building codes commonly applied to locks and access control, see:

- [The Codes Behind Access Control](#)
- [International Rules / IBC for Access Control](#)

IPVM Opinion Mixed

In our previous reports on barricade locks and after laying out the potential upsides and risks of the units, IPVM member opinions remain mixed on whether or not IBC barricade lock prohibition is too strong and should be exempted for classrooms:



Indeed, opinions are mixed nearly 50/50 between continuation of the ban and outright or conditional acceptance in classrooms.

In any case, IBC has upheld its former prohibition and shows no signs of changing in the future.

Doors & Locks

Door Fundamentals For Electronic Access Control

Assuming every door can be secured with either a maglock or an electric strike can be a painful assumption in the field. While those items can be applied flexibly with various openings, there are occasions where certain hardware cannot be used.

A common pitfall is inadequately or inaccurately describing the door resulting in avoidable specification mistakes. In this note, we examine how to properly identify a type of opening using industry terms:

- Leaf
- Mullions
- Frames
- Lites and Transoms
- Door Swing

And we examine common door types often used in access control:

- Steel, Wood, and Glass Doors
- Automatic Sliding Doors
- Rollup Overhead Doors
- Reading Door/Hardware Schedules

Leaf

The 'leaf' is the main swinging part of a door. A single door is often called a 'leaf', while a double-doored opening has two 'leaves'. On double doors, sometimes one of the 'leaves' is held stationary and is locked in place, while the other swings freely. This is typically called the 'active leaf'.

Mullions

Sometimes 'leaves' are separated by a bar stop running vertically between them called a 'mullion'. Here's an example of leaves separated by a mullion:



Mullions can be permanently affixed as part of the frame assembly or may be a removable type, which are typically locked into place to prevent unauthorized removal (and threaten the security of the opening).

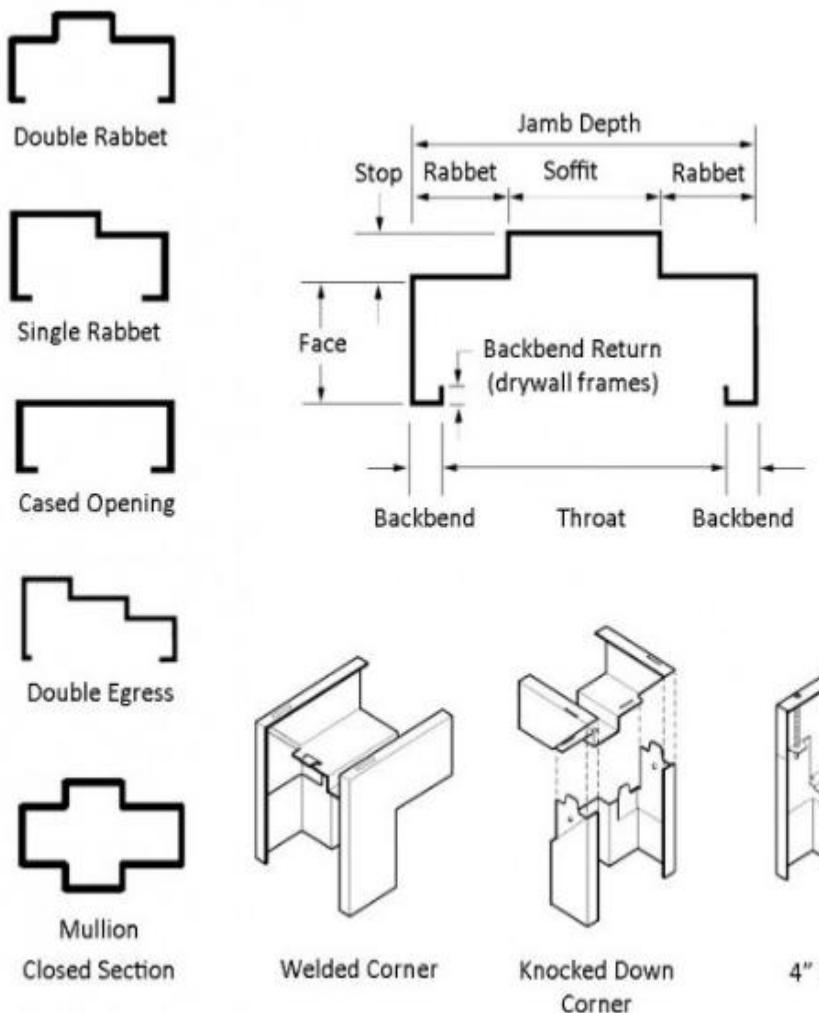
The mullion often plays a key role in securing the door, because it contains the cutouts that the companion door locks physically extend latches into. When mullions are not part of a double leaf opening, vertical rods that secure door latches into the top or bottom edges of a door are used.

Frames

Key elements of "Frames" include material used and its 'profile':

- Steel and Aluminum are common materials used to construct frames, although wooden frames can sometimes be found on older buildings.
- The 'profile' of the frame - or the shape in which it constructed is often dependent on aspects like the adjacent wall to which it is attached, the type of door it is intended to frame, the swing of that door, and the type of hinges it is designed to work with.

The image below is an example of the most basic frame profiles (and frame feature names) used in commercial openings:



The shape and dimensions of a frame, especially the 'face' depth, can impact how much space for access control devices like strikes and door position switches are available, or how cabling is run to devices like readers. When specifying electronic strikes or hanging readers from frames, make sure that enough room for the device and the device wiring exists inside the frame.

Lites and Transoms

'Lites' and 'transoms' refer to the pieces of glass within or adjacent to the door leaf itself. It is a common feature to have a full-height glass sidelight adjoining an entry door. These features are important to note due to the

impacts they may provide access control features like wire runs or the mounting options of items like maglocks.

Here's an example:



Door Swing

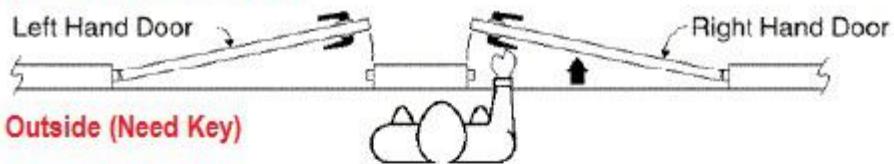
The direction a door swings can greatly impact door hardware selection. There are four basic ways a door can swing, and knowing how to properly describe it is critical when designing access control systems and ordering door hardware.

Openings are configured to have doors swing in four separate ways:

- Right Hand
- Left Hand
- Right Hand Reverse
- Left Hand Reverse

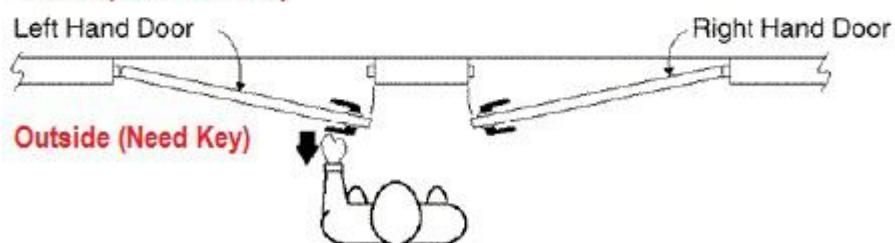
The differences in these types are best described with diagrams. The images below show all four types:

Inside (Secured Side)



Inswingng Doors

Inside (Secured Side)



Outswingng (Reverse) Doors

Especially when using maglocks, not noting door swing can be a costly mistake either due to improper installation or a security risk due to exposed power cables. For more, see our [Door Swing Primer](#) post.

Type of Doors

In general, care must be taken to understand the construction of the door and any special ratings it may possess (ie UL rated Fire doors, etc.).

For example, consider the distance between a card reader and the swing of a door upon a card read. Will the swing of the door make it awkward for the card holder to gain entry after scanning a card? Would a card reader located on the door frame itself or with a longer read range make the opening easier to use?

A low-level perspective is important during the design and installation phases of implementing an access control system, especially in how the access control system impacts the usability of the door.

Steel Doors

In the commercial architectural market, 'hollow-core steel doors' and 'steel frames' are a mainstay product. Many access controlled doors fall into this category; the products are typically constructed of 16 - 22 gauge steel sheeting and then cut, formed, and welded into assemblies. 'Hollow core' indicates a steel shell with a fiber composition or polystyrene honeycomb core.

Here's an example of a steel door:



Steel doors provide a good rigid medium to hang a variety of security hardware upon. However, over time the perpetual hanging and rehanging of different types of hardware can damage the door and result in a structurally unsecurable opening. For example, make sure that maglocks are mounted with 'thru-bolts' and not only surface mounted.

While a steel door allows for mounting various accessories, this can result in awkward interaction of mechanical devices and access control systems. If the intent of an opening is to open upon a card read, make sure that no existing mechanical device (ie - dead latching exit device) prevents this action.

Wood doors

'Wood veneer', or 'solid core wood' doors are also very common, especially in institutional and education buildings. The term is self-explanatory; instead of a hollow-core steel door, one composed of wood or wood veneer is used in its place. These types of doors are still commonly installed in steel frames.



Surface mounting hardware like maglocks to wood doors can sometimes be troublesome. Not only are those finishes especially sensitive to damage like tool marking and hole break-outs but the actual door itself will 'move' depending on environmental variables like heat and humidity. Because of that, special care should be taken to mount hardware so that it will always remain aligned, i.e. - a good electromagnetic bond is achieved.

Glass Doors

Glass Doors, sometimes referred to generically by specific brand 'Vermiculite', are very common in architecturally significant openings like storefronts or main entries into highrise structures. These types of doors usually present cosmetic constraints to hardware specification, and due to the thin frame, or frameless, opening types great care must be taken to ensure the constraints of movement and interaction of hardware is well understood.

These types of doors are especially costly to modify in the field if improperly configured. Often



times, the glass must be cut during manufacturing to accommodate for items like hardware and hinges. Making sure the build and action of these doors is understood will ensure cost controls when working with them. See [Glass Doors and Access Control](#) for more on this often difficult combo.

Electromagnetic locks are most commonly used in glass doors rather than strikes. A variety of factors account for this: these doors see high traffic counts and strikes are more burdensome to maintain than electromagnetic locks, and it is difficult to 'hide' the strike in such a way that is aesthetically pleasing.

Automatic Sliding Doors



Another type of commercial opening designed for high volume throughput are sliding doors, where an operator moves door leaves laterally rather than swing them in or out. In many markets, these types of doors are serviced, maintained, and installed by specialty vendors like [Stanley Security](#) who have exclusive service contracts for them, and integrating them with access often requires a joint effort with those providers.

Because of the complexity in configuring these doors, critical values like close time or sensor activation points must also often be included into access door controller configurations.

Rollup Overhead Doors

Finally, traditional overhead doors are commonly connected to electronic access for vehicle or loading dock applications. In many cases the door

segments roll upward into a coil a fraction of the height of the extended door.

The image below is one example:



Because the action of the door is not a swinging type, the arrangement of standard components (ie: door position switches) require alternative mounting locations like floor mounting. Not all rollup types use automatic operators to raise, and some use conventional bolt locks to secure, while other automatic types may require logic programming delays to ensure doors are unlocked before raising actions are activated.

Reading Door/Hardware Schedules

The standard method of expressing door, frame, and lock details is done via Schedules that are part of drawing sets. Usually in a near complete or '100%' set of floorplans, a sheet showing a chart of door details and elevation views is included.

In many cases, while a building may contain hundreds of individual openings, only a few basic types are used and repeated throughout. The door schedule is key in determining how the door and frame types are best integrated into an electronic access system.

The example schedule below shows standard details for just two basic types of opening used in several places in a building:

Specifying Door Locks

Mechanical door locks regularly remain even after electronic access control is added. Indeed, most are designed to work with what is already hung on the door. However, what happens when a lock needs to be replaced or changed? Understanding the basics of selecting and installing door locks is valuable for every designer, installer, or end user to know.

Major Types

The range of lock hardware is broad, with each type having its own 'best use' and relative strengths. The major types used in commercial buildings are shown below:



In the sections below, we discuss where each type is used and how to make the best choice depending on the application.

Door Preps Largely Decide Lock Choice

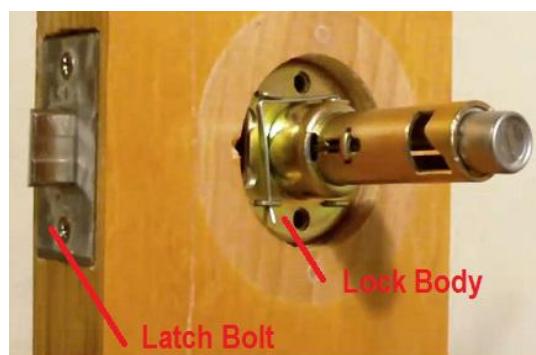
The most important aspect driving door lock selection is how the 'door is prepped', or how it has been fabricated to work with locks. Different forms of locks require different configurations of holes and pockets cut into the door, and in most cases these preps are done at the manufacturer well before they are hung.

Therefore, in many cases, lock selection is decided by the door type, and the task is condensed to finding which product can be installed without modifying or replacing the door. In the sections below, we address the major types of 'door preps' and which models of hardware they accept.

Cylindrical Lock

This type of lock is also called a "Bored" lock, which essentially is designed to slip inside a 2 1/8" hole drilled thru the door. The locks designed to use this prep are round in shape, and typically use the hole to support the lock in the door. While the majority of doors include this prep, it is not the most common seen in Electronic Access Control, because most of the time these locks are used for interior, or low-security doors.

While these types of locks are well suited for light-duty use, they contain only one latch - the piece that slides into the frame. High security doors often include several points of latching and even when a cylindrical lock is built to withstand many cycles, it still need other separate components (like a deadbolt) for high security applications.



Cylindrical Door Prep / Leverset

- Pros: Inexpensive (\$50 - \$300), easy to install
- Cons: Single latch not as secure as other types, not as durable as mortise locks

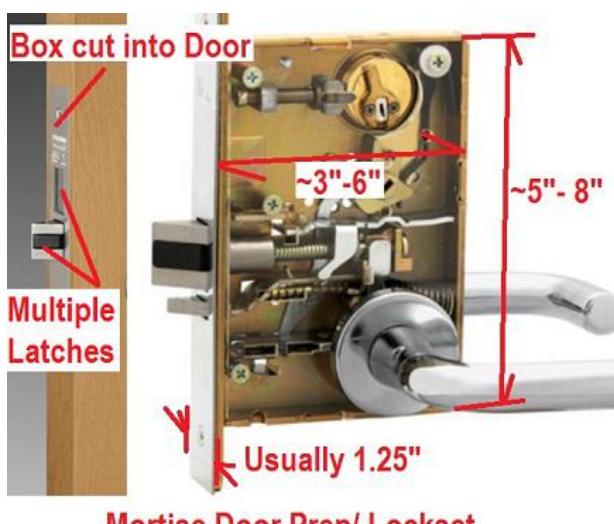
- Where Used: Interior Doors, Offices, Passageways, Low-Medium Volume Doors

Mortise Lock

One of the oldest types of locks is also the most secure. Compared to a cylindrical lock, a mortise lock is big, heavy, and full of complex parts. However those properties make it very durable, strong, and able to withstand constant use. Mortise locks require a pocket cut into the edge of the door, which requires more craft skill than a single bored hole. However, because that pocket is larger than a cylindrical lock, multiple latches are typical features of mortise hardware.

Not only do multiple bolts slide into the frame, but mortise locks support full-size 'high security' mortise lock cylinders featuring 'bump/pick resistance', special security pinning, and other tampering protections.

Mortise locks are commonly used in doors requiring high security and high volumes, but are generally too expensive to use on interior doors or light-duty office/ passageway openings. Doors using mortise hardware must be specified to handle both the size and weight of a mortise lock:



- Pros: Very durable, support multiple security latches
- Cons: Expensive (\$400 - \$2000), field cutting a door to support a mortise lock is difficult
- Where Used: Exterior Doors, High Volume Doors, High Security Doors

Surface (Exit) Device

Also called 'Rim style, or Edge-prepped Locks', these locks typically require minimal door prep, and some types do not even occupy the core of a door at all. The most common type of hardware in this category are exit devices, a mainstay of high-volume, emergency egress openings. In the picture below, notice the latch of the lock is attached to the 'surface' of the door, hence the name:



Surface door hardware is typically secured with surface strikes (not mortise strikes) or maglocks where permitted. Exit devices are costly but are very durable and typically withstand high amounts of abuse and tampering.

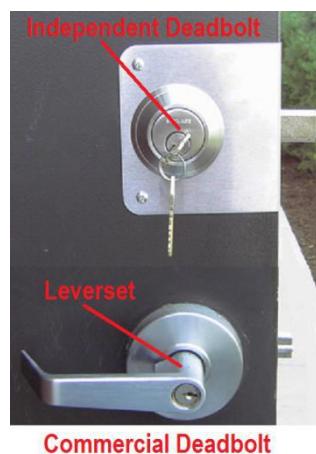
- Pros: Meets Life/Safety Emergency Egress Codes, Most doors, regardless of factory prep, support Surface Hardware installation

- Cons: Expensive (\$1000 - \$3000), and potentially disruptive to aesthetics. Difficult to hang on glass doors.
- Where Used: Egress Doors, High Security Doors

Deadbolt

This type of lock is seldom used alone without additional separate handles, and NEVER on emergency egress doors because the bolt typically requires rotation of a key or thumb turn to retract. Like cylindrical locks, deadbolts are easy to install, requiring only a hole to be drilled through the door. However, because of their limited convenience, deadbolts are primarily used to enhance the security of other locks hung on the door.

For example, when used with a cylindrical lock, a deadbolt means another independent lock must be defeated to gain illicit access. Deadbolts are typically used to increase security during 'dark hours' - used when a facility is locked up for the night or when it is unoccupied. The image below shows a typical example of how deadbolts are used, in conjunction with a leverset on a perimeter door:

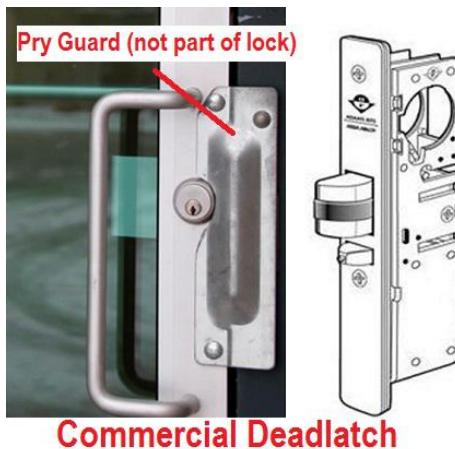


- Pros: Inexpensive (\$50 - \$200), easy to install

- Cons: Cannot be installed on egress doors, Separate lock must be pinned to match other locks in use
- Where Used: Generally used to increase security by provide another latching point.

Deadlatch

This type of hardware is a hybrid between a deadbolt and a mortise lockset. Deadlatches are commonly used on glass storefront doors with thin frames. Most properties using latchbolt equipped doors are unlocked during occupied hours, and free egress and entrance is permitted. Therefore, a latchbolt is only used to keep a door locked when occupants are gone. Like a deadbolt, most models lack handles to retract the latch, although some types feature 'exit device'-like paddles when required by code. Unlike a deadbolt, a door frame cannot simply have a bored hole for install, and the frame must be prepped similarly to a mortise style lock. Most latchbolts are very strong, and may include multiple latches or even hook bolts that anchor firmly into the adjoining frame.



- Pros: Stronger than traditional deadbolts, the ideal architectural/security compromise for glass doors

- Cons: Handles must be installed separately, retraction functions from key only. Doors difficult to field prep to fit latchbolts.
- Where Used: Thin Frame (Glass) Storefronts

Lock Selection

Doors clearly drive the types of locks that can be used to secure them.

When it comes to selecting the specific type of lock to install, these factors:

- How is the Door Prepped? The section above clearly defines how door prep influences lock hardware selection. Taking note of the prep will narrow selection criteria to a few basic types.
- How thick is the door? Doors have varying thicknesses. In the Americas, doors usually are 1.75" or 1.375". However, European models range between 30mm and 55mm thick. This measurement is critical in determining the latch position in the door, and can limit the overall thickness of the lock.
- Is this an Egress door? If the door falls in an egress or emergency egress path, certain lock types (like deadbolts) should not be used. Hardware like exit devices maybe be required, excluding selection of other types.
- How do codes affect lock selection? Many municipalities outlaw maglocks, meaning that 'electrified hardware or strikes must be used. Local code interpretations often exclude types of locks, or otherwise conditionally approve their use depending on building classification.
- How frequently will this door be used? How often the door and lock is cycled influences hardware grading. For heavy duty commercial use, ANSI/BHMI Grade 1 hardware is ideal, while an infrequently

used closet or storage door is better suited to use economy-grade Grade 3 hardware.

Choosing the right lock is typically driven by the 'context' attributes of the opening, rather than selecting the lock first and sizing the opening to fit.

Maglock Selection

One of the most misunderstood yet valuable pieces of electrified hardware is the maglock. Few locks are stronger, but myths and confusion surround their proper use. Many access control designers avoid using them altogether, but should they? We examine maglocks, their proper application, and how to avoid problems when using them, including:

- Fail Safe vs Fail Secure Concerns
- The Core Components of a Maglock
- Legality of Maglocks
- Shear vs Conventional Pull Action options
- Bond Ratings
- Power Considerations
- Matching Maglock to Door Operation
- RTE / Fire Alarm Considerations

Fail Safe vs Fail Secure Concerns

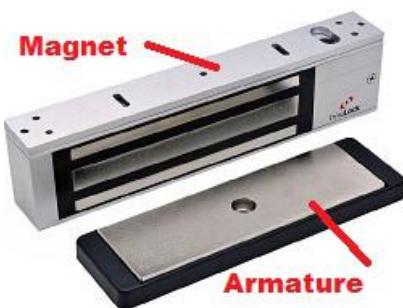
Despite misconceptions about their safety, all maglocks fail safe. Unlike other pieces of electrified hardware that can be configured to fail secure - potentially complicating egress in an emergency - maglocks lose all holding force when power drops.

Because a maglock is essentially an electromagnet, if energy is not present - it simply does not operate. Unlike electronic cylinders or electric strikes that have moving mechanical components that can break or bind, a maglock has no moving pieces and does not wear over time.

While concerns perpetually surround the 'life safety' of these devices, when they are properly installed they are safest locks available. The 'solid state' construction means that a maglock either operates according to design, or it does not operate at all.

The Core Components of a Maglock

Despite their 'high-tech' latching method, a maglock is a very simple device composed of just two pieces:



- **Armature:** This is a flat section of steel that matches the magnet 'box' installed on the frame. The armature must be securely fastened to the door in order to achieve a strong bond and keep the door shut.
- **Magnet:** The larger of the two components contains an electromagnet core. Unlike the armature, this piece never physically moves in relation to door swing, and is the only component that receives power during operation.

While not essential to keep doors secured, maglocks are often equipped with or require additional components that aid their function in access control deployments. Among these other elements are:

- **Bond Sensor:** A simple contact closure than confirms the maglock is energized and matched with the armature, signaling a valid 'bond'. This indicates the door is both closed and locked/secure.
- **Integrated RTE PIR or REX:** Some maglocks include a motion sensor or switch that drops power to the lock. This feature is required by

life/safety codes (addressed below) so that in an emergency egress situation the lock drops power and permits exit.

- Door Closer: The closer returns the door to a 'closed' position. Because the door's armature must be in contact with the magnet to bond properly, a door closer device is necessary to always ensure the door is shut after opening.
- "MOV" , or "Metal Oxide Varistor": If not factory equipped, the maglock may require an MOV to be field installed, typically across the power leads of the lock. Because a maglock causes a magnetic field to collapse every time it is de-energized, it can backfeed a small but damaging surge into the power supply. A MOV dissipates this field and prevents this type of damage from happening.

Which Type Should I Choose?

Selecting the proper type of maglock for an application is not difficult, if a few basic parameters are addressed during specification. The basic questions that must be answered, and the order they must be asked are listed below:

- Legality/ AHJ requirements
- Action Type (Shear vs. "Conventional"/Pull)
- Bond Ratings
- Voltage Type
- Operation Type
- Required RTE Hardware/Fire Alarm Tie-In

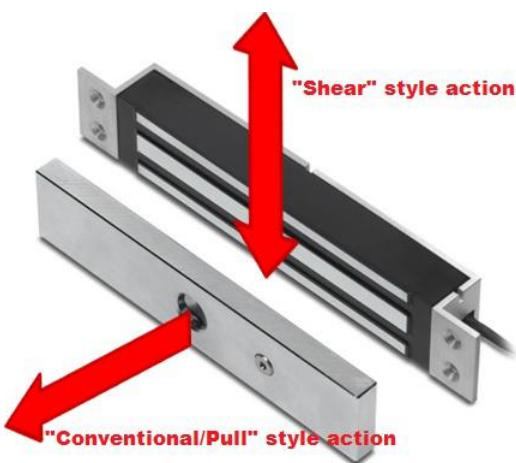
Legality of Maglocks

The first, and most critical aspect that must be addressed is whether or not use of maglocks are permitted by the local code authorities, or what special restrictions apply to their use. Permission or prohibition is granted on a municipal level, and can vary from one town to the next. In general, a call to the local Fire Marshal or City Codes department will yield proper guidelines. In the examples below, note that accepted use may vary depending on door locations, door types, and maglock type:

- [New York State \(Education Dept.\)](#)
- [City of Chicago](#)
- [Harris County \(Houston\), Texas](#)
- [Rogers, Arkansas](#)

Shear vs. Conventional Pull Action Options

Maglocks are available in two functional types; either Conventional/Pull style or Shear style actions. The difference between these types is noted in the drawing below:



The action determines the intended mounting location of the maglock. As depicted in the drawing, the movement direction the lock is designed to 'hold' distinguishes the type. Because of the differences in coil windings, a 'conventional' maglock is not suited for use in a 'shear' application, and vice versa.

While the operating principle is the same, the installation locations and door preparations are different according to maglock types. In the sections below, we address the two types and how they differ:

Shear Locks

This style of maglocks is ideally used where maglocks must be low-profile, as they can be completely recessed (hidden) into frames. Because these units are installed flush with exposed surfaces, they are tamper-resistant. However, shear style locks are less common than the 'conventional' type because both frames and doors must be previously fabricated with lock clearances in mind.



Since many, if not most, of electronic access control systems are 'after-market' or 'retrofitted' to existing doors (without the proper cut-outs), shear locks are not frequently used. However, because of their low-profile and strong bond in the intended direction of travel, special applications like gates or rolling grilles often employ shear locks.

Cost for shear locks is roughly equal compared to other maglock types, however due to the additional fabrication required to doors and frames to fit them, the deployment cost is higher.

Conventional / Pull Locks

The most common type of maglock installed today is the "Conventional/Pull" type. In contrast to the shear action, this type is installed with the magnet exposed, meaning the magnet must be installed on the 'secure' (or unexposed) side of the door. The direction of door swing can complicate this, since some doors will swing in - resulting in a modification to the installation position and armature bracket - a point we examine later.

Power cabling is typically installed inside the frame, and the armature plate is installed flush onto the door itself. Because this plate must be installed so it is integral with the



door leaf itself, it is drilled and attached with through-bolts. While not an issue for hollow metal or wood doors, this can present a problem for frameless glass or thin bezel doors. In those applications, a 'low profile' maglock may need to be used instead.

Bond Ratings

Maglock holding force is measured in hundreds of pounds, frequently more than 1500 pounds per lock. This rating describes the amount of pulling force required to match the magnetic bond of the lock - any amount greater will overcome the electromagnetic bond.

Typically, the lowest bond rating available is 600 pounds, while the strongest models are rated to 2700 pounds. In general, the stronger the holding force the higher the cost anywhere from a few hundred dollars to more than \$1800 for the strongest units. However, considering the structural elements of the door, (eg: leaf, frames, pull hardware) will fail before the maglock itself, it is exceedingly difficult and uncommon for the bond of a maglock to be defeated.

In general, exterior doors should not be secured with less than 1500 pound rated maglocks. Less expensive and weaker locks have a variety of uses (eg: securing cabinet doors, sliding gates, or closets), but they should not be used where a brute force attack using tow chains or mechanical come-alongs is possible.

Power Considerations

Maglocks require power for operation. Most modern models are field selectable to either 12 or 24VDC, but other voltages and AC versions are available. Power for these locks is often recommended to be supplied by an independent, individually fused power supply. Because the effectiveness of these locks is entirely dependent on the strength and dependability of the power source, maglocks do not typically share power sources with surveillance equipment.

Additionally, while 'low-draw' maglocks are available, supplying power via door controller in the way that electric strikes are powered is not recommended. Unlike a strike that only intermittently draws power when activated, a maglock continually draws power during operation. The heavier duty-cycle of the maglock calls for a supply source that is more robustly built and able to handle the constant supply of current to the lock.

Matching Maglock to Door Operation

The next step in deciding which lock to use comes from examining the door itself. Because openings are constructed in several ways, maglocks must be specified to match the opening. We examine a few of the most common installation locations in the list below:

- Outswinging Door: This is the simplest, and default location that maglocks are installed. In this position, because the door swings away from the magnet, the maglock is installed beneath the top edge frame of the door, and the armature is mounted to match the location. While the lock will encroach into the 'headspace' of the opening, typically this is only a few inches. Given the standard 8 foot height of the door, the unit does not present a hazard.
- Inswinging Door: In this orientation, the swing of the door would interfere with the lock if hung in the 'outswinging' position, so the lock is moved up and mounted flush with the side of the top frame. In addition, the armature is moved outward and upward with a 'z-bracket', which may be an additional cost. Note in the picture below how the door swing affects installation location:



- Double-Door Units: Maglocks can be installed on 'dual-leaf' or 'double-doors'. Typically codes require adjacent door leafs to release

simultaneously. While this can sometimes be achieved with two single-door maglocks, many electronic access door controllers are only able to be connected to a single locking device. In this case, a double-door unit must be used so a single release command will allow adjacent doors to open at the same time. In general, these units are able to be installed on the frame like single units, and the presence of a door mullion does not impede installation.



Dual-Door/Leaf Maglock

- Hold-Open Function: Maglocks are also used to hold doors open. Especially in applications like hospital corridors or busy hallways, fire doors may be critical opening that are only closed when absolutely necessary. Because maglocks can easily be integrated into fire alarm systems, they are sometimes used to lock doors in the 'open' position, and in a fire-alarm situation, the maglocks drop and associated door closer then shuts the doors. The image below shows a maglock used in this application:



RTE / Fire Alarm Considerations

Briefly stated, 'RTE', or 'Request to Exit' Hardware are accessories required by code where maglocks are installed. These devices, typically PIR motion sensors and/or 'Exit' pushbuttons, must be installed so a maglock loses power when people want to egress through the door.

While the topic is substantial, and will be addressed separately in a future post, the requirement to install RTE Hardware is often cited by the following passage in the IBC Code:

From the 2012 Edition:

1008.1.9.9: Electromagnetically locked egress doors. Doors in the means of egress in buildings with an occupancy in Group A, B, E, M, R-1 or R-2 and doors to tenant spaces in Group A, B, E, M, R-1 or R-2 shall be permitted to be electromagnetically locked if equipped with listed hardware that incorporates a built-in switch and meet the requirements below:

1. The listed hardware that is affixed to the door leaf has an obvious method of operation that is readily operated under all lighting conditions.
2. The listed hardware is capable of being operated with one hand.
3. Operation of the listed hardware directly interrupts the power to the electromagnetic lock and unlocks the door immediately.
4. Loss of power to the listed hardware automatically unlocks the door.
5. Where panic or fire exit hardware is required by 1008.1.10, operation of the listed panic or fire exit hardware also releases the electromagnetic lock.

Many jurisdictions require maglocks to automatically release when the fire alarm is activated, so that emergency egress in a fire is completely unabated by maglocks. Incidentally, the requirement to release maglocks upon activation of the fire alarm in addition to RTE hardware has been removed in the 2012 edition of the IBC code, but many jurisdictions will still require this integration despite the recent revision.

Vendors

Because they are technically door hardware, maglocks are available from most 'traditional' door hardware conglomerates within the ASSA ABLOY, Ingersoll Rand, and Stanley brands. However, there are a few brands that specialize in offering maglocks or units with special designs. While not a comprehensive list, the following list details a few of these recognized names:

- DynaLock: A large manufacturer with a broad portfolio of action types, voltages, and integrated features.
- SDC: Electrified Hardware manufacturer that specializes in access control hardware, including low-profile, low current draw, and high bond rating maglocks.
- Rutherford Controls: This manufacturer was recently purchased by Dogma (a transaction we covered in this report) known for its line of 'multifunction maglocks' that incorporate delayed egress, visual/audio annunciation, and even CCTV cameras.
- Securitron: This ASSA company offers several lines of maglocks, including the low-profile M680 series, configurable to include an intergrated RTE PIR and CCTV camera in an architecturally styled finish. (See our report on this product for more details.)

Selecting the Right Electric Strike

Despite being one of the most common components of access control, specifying the right electric strike can be deceptively complex.

Understanding the particulars of each device can be overwhelming.

Function Explained

Strikes are basically moveable portions of the door frame, consisting of 3 main components, shown to the left:



- The Strike Box contains the internal components to the strike that sits inside the frame. Electric strikes are typically driven by one or more solenoids, either directly or via a simple geared carriage inside the box.
- The Strike Plate affixes the device mechanism to the frame and is responsible for the proper alignment the device in relation to the door locking hardware.
- The Keeper is the component of the strike that moves. When 'locked', the keeper is rigid and forms a positive stop - interfering with the latch to prevent opening of the door. When 'unlocked', the keeper swings out of the way of the latch and allows the door to open.

Unlike other types of hardware, strikes do not replace or improve the existing hardware mounted on a door. In fact, a strike totally relies on mechanical door locks for securing the door. The strike simply allows for

the locking hardware to remain locked and still gain entry through the opening.

Fail Safe/Fail Secure: Unlike maglocks that 'fail safe' on power loss, strikes can be configured to 'fail secure' - meaning the keeper remains rigid regardless if they are powered or not. In order to preserve the life/safety compliance of the opening, the door hardware must accommodate free egress in an emergency. Whether through panic bars/exit devices, lever sets, or even latch sets, egress doors cannot be locked to prevent escape, and hardware must take no more than one, intuitive action to open the door.

AC or DC powered: Most modern strikes either allow selecting between AC and DC or available in AC or DC versions. All strikes are low-voltage, with either 12 or 24 volts standard. Final polarity and voltage selection depend on several design criteria:

- **Noisy vs. Quiet:** Due to differences in the way solenoids handle power types, AC electric strikes make a characteristic 'buzzing' noise when operating, while a DC model is quieter (or even 'silent'). In the past, solenoid reliability was tied to polarity types, but modern strikes can be purchased to exceed 'Grade 1' reliability, leaving polarity choices subject to matching existing power supplies or tolerated noise.
- **Battery Backup vs. Low Current Draw:** Since 12 VDC 'backup' batteries are common to many electronic systems, they are an inexpensive option for backup power compared to 24 volt cells. However, the current draw of 24 volt strikes is typically lower than 12 volt versions, so if multiple devices are to be powered from a

single source or if overall energy consumption is a concern, 24 VDC devices are a popular choice.

Integrated Readers: A newer trend in strike design is integrating a proximity-style reader into the device and running both power and communication bus down a single cable. This integration allows a more streamlined installation and offers a less intrusive install by combining the reader and strike into a single unit. Variants exist that include 'read-in' and 'read-out' capability, with the unsecured side reader being connected through the frame or wall assembly via bluetooth.

Door/Latch Monitoring: A common option for many strikes is a latch monitor, or a simple contact switch that detects when a latch bolt is being contained inside the strike. This sensor also functions as a defacto 'door position' contact, since the door must be shut for the latch to be present. While not all strikes feature this switch, it usually does not add significant cost to the device but greatly enhances the reporting function of the device.



Strike Types

Selecting the right type of strike includes considering the 'form factor' of the device. Strike are available in two common types:



Mortise Strike | **Surface Strike**

Mortise: The most common type of strike is the mortise variety, which typically requires a cutout in the frame for install. Mortise Strikes are used when the door locking hardware is a mortise or cylindrical lock - or any other lock whose latch is retracted into the door leaf during operation. Since the bolt protrudes into the frame, a mortise strike's keeper replaces a portion of the reveal. As we will cover in the installation section, installing a mortise strike requires the strike to be installed deep into the frame, often requiring frame material to be precisely cut away for a clean fit.

Surface: These types of strikes are used when the companion locking hardware is a 'rim style' device, meaning it is mounted to the inside surface of the door rather than inside the door. Common 'rim' devices are 'exit devices' or surface deadbolts. Even though a portion of the device protrudes on the 'door rabbet', the strike box may still require an additional cutout in the frame for proper mounting.

Strikes Vs. Other Hardware

The relative value of strikes compared against other electrified hardware types

Pros

- Inexpensive: Strikes are among the least costly electrified devices, with Grade 1 quality devices selling between \$100 - \$300. Compared to locks like maglocks that range between \$400 - \$1000 per unit. Even when considering the installation labor, the cost of a strike is between \$175 and \$375 per door.
- Reuses Existing Hardware: Another benefit of strikes are they are specified to work with door hardware already in use. Not only does this reduce the 'hard cost' of buying more locks, it saves on the 'soft costs' attributed to re-keying, installation labor, and redistribution of mechanical keys.
- Energy Efficient: Unlike maglocks that require a steady impulse of electricity to operate, a strike uses only intermittent impulses to operate. While the operational amperage is relatively small for either device, when multiplied over tens or even hundreds of doors, using strikes can cut hundreds of amps from a facility's electricity consumption.

Cons

- Wear: Unlike maglocks, strikes cannot be installed once and operate for years without attention. Since electric strikes have moving parts, they can wear or break over time. Components like load springs and solenoids require periodic maintenance attention.
- Adjustment is Vital: Since the strike is totally dependent on the door's locking hardware for security, the relationship between strike and latch is vital and the tolerances for movement are limited. Even during the course of normal operation, door hinges sag, door frames

shift, and door latches fall out of throw range of the strike.

Anywhere strikes are used, a companion door maintenance problem is vital to guarantee security.

- Extra Hardware: In some cases, additional hardware is required to protect the strike. Take the example below, where an exposed exterior strike is vulnerable to outside tampering unless additional 'latch protectors' are installed on the door:



Installer Skill Required

Properly mounting a strike takes considerable skill in precision measurement and often requires cutting metal. While the overall installation process is typically straightforward, the installer's craftsmanship and trade skills determine more than cosmetic quality - the operation of the device is affected as well.

For example, while frame cuts are simplified by the use of mounting templates included with the device, the position of the template is subject to accurate measurements and assumptions that the frames, doors, and existing hardware are square and properly mounted.



Successfully mounting a strike free of problems like "preloading" (often caused by misalignment and warping of the door) requires the installer to apply a skillful eye to the door condition before beginning work, and be prepared to correct structural problems by shimming hinges or even replace a warped door leaf. Will will examine the problems, and their corrective actions in an upcoming report on "Maintaining Electrified Hardware".

Selecting the Right Type of Electric Lock

Picking between electric strikes, magnetic locks, electronic bolts and locksets can be a complex decision. A number of factors determine what the best choice is, but picking the wrong type can land you in jail. The most appropriate method of securing a door depends on a large number of factors, including the type of opening itself, applicable life/safety codes, and door usage type.

Observing the Law

Local laws should be checked before installing any piece of electrified hardware. They are written to ensure emergency egress is always possible. Unfortunate historical examples exist of electrified hardware contributing to death and injury of occupants unable to exit a building during an emergency. Many codes, laws, and regulations have been written that apply to the correct use of this hardware. Some commonly cited code references establishing use of electrified hardware are:

- IBC 1008.1.4.4. 'ACCESS CONTROLLED EGRESS DOORS'
- IBC 1008.1.9.8. 'ELECTROMAGNETICALLY LOCKED EGRESS DOORS'
- NFPA 7.2.1.6.2. 'ACCESS CONTROLLED EGRESS DOOR ASSEMBLIES'
- NFPA 7.2.1.5.5 'ELECTRONICALLY CONTROLLED EGRESS DOOR ASSEMBLIES'

These sources are for reference only and legal interpretation of electrified hardware codes should be approved by a local AHJ, commonly a building inspector or fire marshal. The acceptance of these devices are highly disparate, even from county to county in some areas of the United States.

Check with your local authorities to see what regulations apply in your area.

Many counties or cities will publish a guideline document similar to these examples:

- [Harris County \(Houston\), Texas](#)
- [Orange County, California](#)
- [Winnipeg, Manitoba](#)

'Fail Safe' versus 'Fail Secure'

These terms describe the default behavior of the lock when power drops from the device. If a device is configured for 'fail safe' operation, this means that if power is lost, then the lock will fail in an unsecured position. This may mean the door can freely swing open or close, but in an emergency will allow unimpeded egress through the opening. By contrast, if a device is configured to 'fail secure', this means the device will default to keeping the door locked when power is lost. Usually this behavior is permitted in special conditions or if other aspects of the door hardware allows unimpeded egress through the opening in an emergency.

Common electrified locking device types

- Electric Strikes
- Magnetic Locks
- Electronic Bolts
- Electronic Locksets

Electric Strikes

Electric Strikes are a common and favored method of securing electronic access controlled doors. Strikes are typically built with a mechanical latch

that swings out of the way when a door opens. This is a very important characteristic of strikes; they are only as secure as the accompanying door hardware. The strike itself is designed to permit access even when the mechanical hardware is locked and the bolt is thrown.

Here is an image of a strike:



Strikes can be surface mounted on the frame (typically required when used with rim mounted hardware like panic bars) or mortised into door frames. A variety of other access control components can be furnished in this type of hardware, including latch position sensors and card readers.

This type of hardware can be bought in a variety of finishes, power options, mounting dimensions, and accessory options. The most commonly applied versions of the hardware cost about \$125, and require periodic maintenance (cleaning and lubrication) to remain operational.

Magnetic Locks

Also commonly called 'maglocks', these devices are some of the strongest and most durable pieces of locking hardware available. They consist of two magnetically bonded components, typically measured by a shear force strength from hundreds to several thousands of pounds.

Here is an image of a maglock:

A weakness of these type of devices is that they always must be mounted on the 'secured side' (inside) of the door. This is due to the vulnerability of cutting power connections to the device, or simply knocking the device off the frame from



the unsecured side. This requirement may disagree with the swing of the door as it relates to the frame, but a variety of adapter plates are made to facilitate uncommon mountings.

These devices also require constant and uninterrupted power to remain secure. 'Fail Safe' conditions are not always desired, so battery backup is a common feature of the power supplies for these locks.

A common code restriction for these devices is that power is made to drop entirely when a fire alarm occurs. It is also very common for 'Request-to-Exit' (RTE) PIR sensors and Emergency Exit Buttons to be required for every opening that has a maglock installed.

These devices are more costly, often selling for \$400 or more per lock. However, other auxiliary pieces of equipment like power supplies and RTE devices also add significant cost to this type of secured opening. It is not uncommon to spend \$2000 on all pieces of hardware for this type of opening. Once installed, due to lack of moving or wearing parts, these devices are relatively maintenance free and suitable of heavy use.

Electronic Bolts

This type of lock features solenoid driven, hardened steel bolts that retract into the frame allowing the door to swing open. These bolts are most commonly mortised into the frame, but alternatively might be located on the leading edge of a door (the strike side), the hinge side of the door, or even the top edge of the door. However, these bolts are seldom located on the bottom (sweep side) of the door, due to the how comparatively dirty that edge is and how it may affect mechanical function of the bolt.

Here is an image of an electronic bolt lock:



This type of hardware can be bought for \$200 USD, but requires periodic maintenance (cleaning and lubrication) and door adjustment to remain operational.

Electronic Locksets

This type of locking device is more of a hardware assembly than a specific device. These units often contain all components required to be a fully functional, self contained device for securing a door. Everything from a card reader to a power pack are included with these devices, and they are intended to replace existing unpowered hardware. These units often have some provision for wireless networking built into the device, and they are sold as a true 'bolt-on' access control solution with no additional cabling or wiring required.

Here is an image of an electronic lockset:



The features and pricing of these units are widely varied, and we intend to cover the more popular types in future updates. For the sake of contrasting to the other device types, however, the cost of these devices can be anywhere from \$1,000 to \$3,000 USD per device.

Applications

The following are rules of thumbs for where these devices are most commonly used:

- Moderate traffic, single leaf interior openings: Electric Strikes are most commonly used. These devices are a good selection for

security office doors, computer rooms, and storage closets. Weather proof and heavy duty versions of this hardware exists for applications like securing gates.

- High traffic, single or double leaf exterior openings: Magnetic Locks are a good fit. Many 'main entry' openings are secured with maglocks. These devices are very strong, have a low operation cost, and require minimal maintenance. Higher cost and less discrete mounting options limit these locks for general application.
- High security lock is desired but where maglocks cannot be placed: Electronic Bolts can be used. This type of locking hardware is very strong, but require more attention to keep maintained and aligned properly than strikes or maglocks.
- 'Package solution' desired for retrofitting a door: Electronic Locksets are best used. Units are available that for both single and double leaf openings. These 'all-in-one' solutions are more costly than building a solution from component parts. However, these solutions are the best answer when a quick integration is required.

Request to Exit

Locks are not always the most important pieces of door hardware. For access controlled doors, especially those with maglocks, 'Request to Exit', or 'RTE' devices are required to override electrified locks to guarantee free egress.

Life Safety is King

The need for RTE hardware is defined by several life/safety codes, with the predominant and most common reference found in the [International Building Codes](#). While other RTE references exist, like those found in [NFPA 101](#) and BOCA, most entities refer or copy verbatim the language in two parts of the IBC. In the final section, on 'Code References', we include the relevant passages from the 2009 version.

Exit Devices

In many cases, RTE hardware is not required. Doors using electric strikes and electrified deadbolts are often mechanically overridden by door mounted exit devices. Free egress is maintained regardless of powered security state of hardware, and so traditional panic hardware often satisfies code requirements.

However, when maglocks are used to secure doors, exit devices alone are not enough. Even if the exit device mechanically retracts the bolt the maglock remains energized keeping the



door locked. While RTE codes can apply to many types of locks, they are most relevant for doors secured by maglocks.

Types of RTE Hardware

When RTE is required, there are several types of devices that can be used to meet code. Often, local AHJs will require more than one type of RTE per opening based on interpretation. In the section below, we detail each major type of device or sensor:

- RTE PIR
- Push Buttons
- Pressure Pads

RTE PIR

Commonly used as 'motion sensors' in intrusion alarm systems, 'passive infrared' RTE detectors are mounted above doors to detect those exiting. When triggered, power to maglocks is killed with no human intervention. While any PIR can be used for RTE purposes, specialty RTE PIRs are built with a detection range limited to the area immediately in front of a door rather than the large area used in intrusion detection. PIRs are often considered the 'most convenient' form of RTE due to no human intervention being required for operation.



When PIRs are used, additional RTE devices should also be installed, due to the fear of rising smoke potentially obscuring the sensor in a fire. Installing a pushbutton in addition to a PIR allows for a 'manual' override should the PIR malfunction.

Using RTE PIRs is not without security risks, either. If a PIR is mounted incorrectly, it may actually sense movement on the wrong side of an opening, or they can potentially be 'tricked' to unlock maglocks through a simple piece of cardboard slid under a door. For more details on that risk, see our "[Risky PIRs?](#)" report. Installers and maintainers should periodically check PIRs for proper function and alignment during the course of use.

PIR RTEs typically range in price between \$20 and \$125 USD, with the most being priced towards the less expensive end of that range.

Push Buttons

This form of RTE is the most common and typically the least expensive to install. According to code, these buttons are solely marked for RTE use and are designed to mechanically interrupt power to maglocks or other hardware. These buttons typically feature a mechanical or pneumatic timer so that power remains interrupted for a period of at least 30 seconds.



Code requirements do not always define the shape, size, color, or design of the button. The code often simply defines the marking on the button, and establishes a time range it must be effective once pressed. The timing function of RTE pushbuttons is generally accomplished by either of two methods:

- **Electric:** This type of button features a low-voltage or battery powered electronic logic timer that ensures a configured period expires before restoring power to locks.
- **Pneumatic:** These button feature a plunger and an air-powered piston that retracts at a slow interval. The RTE buttons require no outside power source or air supply for function, and generally are configurable for the same periods as the electric versions.

Regardless of type, push buttons range in price between \$15 and \$55 each.

Pressure Pads

A less common RTE device is a pressure pad, typically a mat placed in front of an opening that is designed to break power to locks when a human stands directly over it. These pads are generally composed of a stiff rubberized, foam filled mat connects when a weight presses the top surface in contact with the lower surface. The images below are an example of these pads:



A drawback of the pads is that they can actually become a nuisance or hazard if simply laid in front of a door, a problem typically resolved by installing them under carpets or flooring. However, while installing them below the floor keeps them from being kicked or inadvertently becoming door props, it also greatly inhibits maintenance and troubleshooting.

In addition, while pressure pads are reliable and can last many years of heavy use, they are expensive, with standard sized pads costing more than \$500 for a single door. Unless RTE must be used in an area where hand contact or PIRs are not permitted (Eg: clean rooms or explosive areas), pressure pads are not a common choice.

Fire Pulls: While not technically an RTE device, and used only to signal a fire or emergency situation, if a facility has a fire alarm it must be configured to drop lock power when the fire alarm is pulled. Most maglocks and access control systems feature contacts to tie in the fire alarm, and AHJs require proof of successful maglock override by the fire pulls.



In no situation do fire pulls substitute for RTE hardware, however they should be installed to function in the same way.

Code References

While codes can vary by jurisdiction and country, the following are commonly cited in the United States:

1008.1.4.4 Access-Controlled Egress Doors

- A sensor must be mounted on the egress side to detect an occupant approaching the doors. Doors must unlock upon a signal from the sensor or loss of power to the sensor.
- A manual unlocking device (push button) shall result in direct interruption of power to the lock – independent of the access control system electronics. When the push button is actuated, the doors must remain unlocked for 30 seconds minimum. The push

button must include signage stating “Push to Exit” and must be located 40” to 48” vertically above the floor and within 5’ of the doors. Ready access must be provided to the push button.

- If the building has a fire alarm/sprinkler system/fire detection system, activation of the system must automatically unlock the doors. Doors must remain unlocked until the system has been reset.

1008.1.9.8 Electromagnetically Locked Egress Doors

- The door must be equipped with listed hardware mounted on the door leaf, which incorporates a built-in switch to directly release the electromagnetic lock and unlock the door immediately.
- The release device must have an obvious method of operation, and must be readily operated with one hand under all lighting conditions.
- Loss of power to the listed hardware must automatically unlock the door.

Exit Devices

One of the most common locking devices is poorly understood. Exit Devices, also called 'Panic Bars' or 'Crash Bars' are required by safety codes the world over, and become integral parts of electronic access control systems.



Mandatory Use

The application of exit devices is determined during building design by codes. Depending on occupancy classification, openings are required to meet specific criteria related to their opening during a 'panic' or emergency situation. Many code passages through IBC and NFPA relate to this subject, but the sections below provide the basic performance requirements of this hardware:

NFPA 101 : 7.2.1.5.9 - 7.2.1.5.11, 2006 edition:

Latches or other fastening device on a door shall be provided with a releasing device having an obvious method of operation under all lighting conditions. The releasing mechanism (except existing installations) shall be located between 34" and 48" above the finished floor. Doors shall be openable with not more than 1 releasing operation:

- each leaf of a pair in a means of egress shall have its own releasing device, and each device has to operate

- independently (can not require 1 device to be released before the other), except
- no additional locking device (padlock, hasp, chain, deadbolt, etc.) shall be installed on a door which requires panic hardware

Exit devices are not specifically identified in codes as the only solution for these openings, however the design of modern panic hardware typically represents the least expensive and most reliable products marketed to be code compliant. 'Paddle devices' are an alternative but may not be compatible with the door leaf or be code compliant according to local interpretations (ie: 'under all lighting conditions')

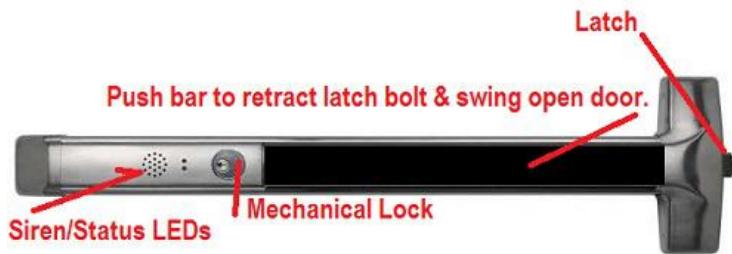
In general, exist devices are required in any facility where:

- medium/large groups congregate: (halls, public buildings, daycares, hospitals)
- where commerce to public is performed (commercial/retail properties)
- where risk requires evacuation plans (most commercial/industrial classifications)
- where large quantities of materials are stored (warehouses, storage facilities)

This criteria cover the majority of non-residential properties.

Major Components

While large, bulky, and potentially mechanically complex, the operation of an exit device is simple: Push the bar, retract the latch, and swing open a door. The basic anatomy of exit devices are shown below:



In addition to the above features, the ability to 'dog down' a device, or lock the bar/latch into an unsecured position, is a common feature. Usually this function uses a common hex key to lock a device open.



Exit Devices are complex devices because of the 'not more than 1 releasing operation' code requirement that often means the locked latches must be

retracted in multiple locations in multiple directions with one motion. Exit devices often include mechanical linkages and are sensitive to adjustments and orientation with the door frame.

While the 'secured side' configuration of an exit device is similar regardless of unit, the 'outside' or 'unsecured' side of a device is subject to wide configuration. In many cases, a simple door handle is used, but 'outside key access' that allows an outside lock to unlock the door from the unsecured side is used.

Latch Location

The location of the latch is a critical feature, especially when exit devices must work with EAC systems.

The latch is important because it is the physical



Exit Device Latch

component that secures the door. With exit devices, there are typically three different latch locations, with a single device controlling up to three latches simultaneously.

In large occupancies, double doors are common because they permit more people to enter or leave than a single door. As such, exit devices are often found on double doors. In many cases, the omission of a center post, called a mullion, changes the latch position. When the mullion is present, latches are generally contained in the 'device head'. However, when the mullion is missing, the door must be secured into the top or bottom of the door opening. The images below display these differences:

First, no mullion:



Next, with mullion:



Because the latch location changes, this affects the way the door interfaces with an access system. For example, it may affect the selection of an electric strike to be a top-frame mounted double vertical rod strike. Or the location of the vertical rods may complicate the mounting

location of a maglock. In either case, selection of electrified locking hardware is affected by the type of exit device hung on the door.

Electronic Latch Retraction

Another option is to apply 'electronic latch retraction' to the device. This powered feature acts on the latch as if the bar was being pushed when a credential is read. This allows an exit device to remain 'undogged', but opened from the outside regardless of what is happening on the inside of the door:



Even when the device is not initially specified with this feature, retrofit kits are available from many manufacturers to convert units.

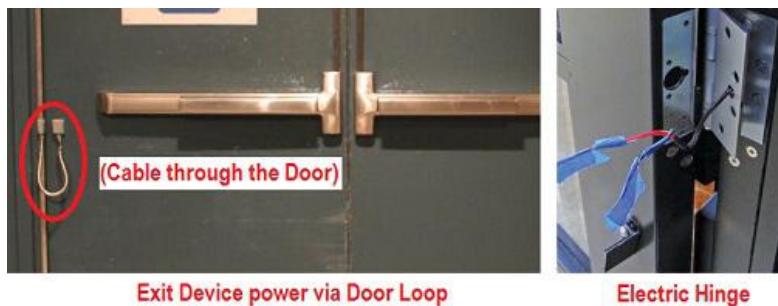
When used with EAC, the exit device interfaces with the controller like a strike - generally the unit is unpowered until a credential read causes the system to apply power to the retraction mechanism. Regardless of the type of latches used - concealed/surface rods, or strike latches, variations on electric latch mechanisms are available.

Power Problem

When exit devices need electricity, powering them can be a challenge.

Unlike other electric locks that are powered by cabling run through the frame, exit devices hang on, and must swing with, the door leaf.

Usually cabling for latch retraction and other electrified features is run to the device in one of two ways: Door Loops or Electric Hinges:



Electric (or Powered) Hinges are not motorized or mechanically different than standard hinges, they simply are constructed to pass through power from one hinge to the other with internal pivoting contacts. Because the door (often) swings on hinges, the reliability and safety of these conductors is critical. Unfortunately, power hinges often wear and break over many years, and the equipment may need to be periodically replaced.

Another big constraint of electric hinges are they must be run inside 'hollow core' doors. While running power internally to the door is safer and more secure from tampering risk, it excludes 'solid core' doors, like wood doors often are.

In this situation, a 'door loop' is used, which is essentially an externally run cable, usually in some form of flexible armored conduit. The loop is run on the secured (inside) of the door, and externally vandalism is not generally an issue, but internal tampering and damage can be.

Other common features requiring power in exit devices are:

- Sirens: Devices are available that emit an alarm when the bar is pushed and the door opens. This is a useful feature for 'emergency exits' that are not 'normal' passages. When someone opens the door, the alarm attracts attention.
- Delayed Egress: In some cases, the door can be kept locked for a short period of time before opening. Local codes heavily legislate acceptable use of delayed egress, but in all cases a siren must sound during a delayed period. As we covered in our '[Delayed Egress Examined](#)' report, this is a useful feature to keep people secured for a short period of time while still allowing emergency exiting.

Relative Cost

The price range for an exit device ranges wildly, from under \$500 economy grade devices to \$4,000 heavy duty, architecturally styled units. In general the retrofit retraction kits cost around \$400, and other locking hardware like strikes or maglocks fall inline with typical pricing, from \$100 to \$700 depending on style and holding power.

Other Details

Most of the time when installing EAC on exit device doors, the actual devices have already been specified, installed, and in use. However, other constraints factor when specifying new exit devices on doors, namely UL rating and door type (glass, wood, or metal). We will address those topics individually in upcoming notes.

Door Closers Access Control

Door Closers have an important job: automatically shut doors when they are opened, because an open door cannot control access.



We review Door Closers, examine how they are selected, and how to avoid misusing them:

- Why closers are important for access control
- Why using closers as barricade locks are illegal
- Applications other than security where closers help
- What normal closer operation should look like
- The 3 standard movement phases and configuring locks for them
- How to properly size closers
- Typical closer pricing

Crucial Security Role

Closers address a fundamental access problem: doors must be closed before they can be locked.

Unless people are in the habit of pulling every door behind them, there is no guarantee it is closed unless these devices are used. Since basic access

control requires keeping unauthorized people out of areas they do not belong, an open door simply offers no security to the people or assets inside.



One of the oldest pieces of door hardware, closers are designed to shut doors behind every user so relocking can automatically take place, mitigating the risk of an open door allowing anyone free access into an area.

Illegal Use As Barricade Locks

A recent trend in classroom barricade locks involves for using a metal sleeve that fits over the closer's arms when closed, preventing further opening of the door with the unit in place. These devices must be installed with the door closed, and tout they protect teachers or students from dangers in hallways when fitted:



However, these devices are often illegal because they risk trapping occupants behind barricaded doors when exit might be crucial. Most local authorities have adopted codes that dictate emergency egress is a simple, instinctual action.

The model code for most of these local regulations is International Building Code (2009) 1008.1.9 that states:

"Except as specifically permitted by this section egress doors shall be readily openable from the egress side without the use of a key or special knowledge or effort."

Bottom line: any piece of security door hardware must also guarantee safety, and closer barricade locks are risky for protecting lives as much as keeping them safe. We examine closer barricade locks further in [Classroom Closer Lock Illegal](#) note.

Other Benefit For Installing Door Closers

However, security is not the only benefit closers provide. They are often designed into a facility for other reasons, including:

- HVAC Efficiency: Keeping air handlers balanced and minimizing conditioning cost requires keeping zones sealed. To avoid circumstances like an conditioned office from being heated/cooled by an adjacent warehouse space, door closers are used to keep the zones separate.
- Noise Isolation: Likewise, a closed door offers some noise isolation. Closers help keep quiet areas quiet by keeping doors shut.
- Fire Protection: With so much emphasis on 'positive latching' of locks to keep firedoors closed, closing the firedoor first is a huge factor in

enabling the firewall to do its job. AHJ approved Fire Door closers automatically shut open firedoors during an emergency, typically triggered by the fire alarm.

Hydraulic Closers Are Most Popular

Most modern closers are a 'hydraulic' (oil filled) box that are surface mounted on the secured side of the door. In order to prevent occupant injury, closers have 'stages' using different timing and closing force as the door is shut.

In the short animation below, a hydraulic closer displays the three different stages of closing in one fluid movement:

Note: [**Click here to watch animation on IPVM**](#)

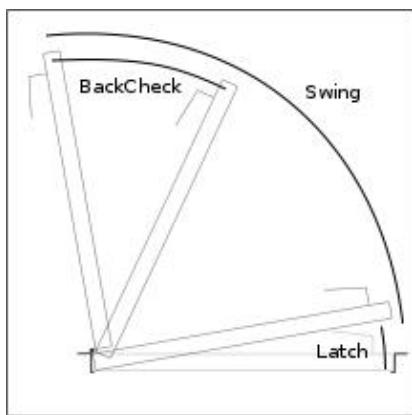
The importance of these positions are noted and explained in the following section.

Standard Movement Positions

The three typical phases are shown in the top-view door image below:

1. Back Check: This phase is similar to an 'over-travel' that allows the door to open fully, even beyond 90 degrees, so that wide loads can pass through. The back check phase typically places the closer at a mechanical disadvantage and requires more directional force at a leverage disadvantage, without damaging the door or the closer.
2. Swing: This is the 'primary' phase of the closer, that swings the door closed. A variety of closers match the door, taking variables like Door Handing / Swing Direction and duty cycle into account.

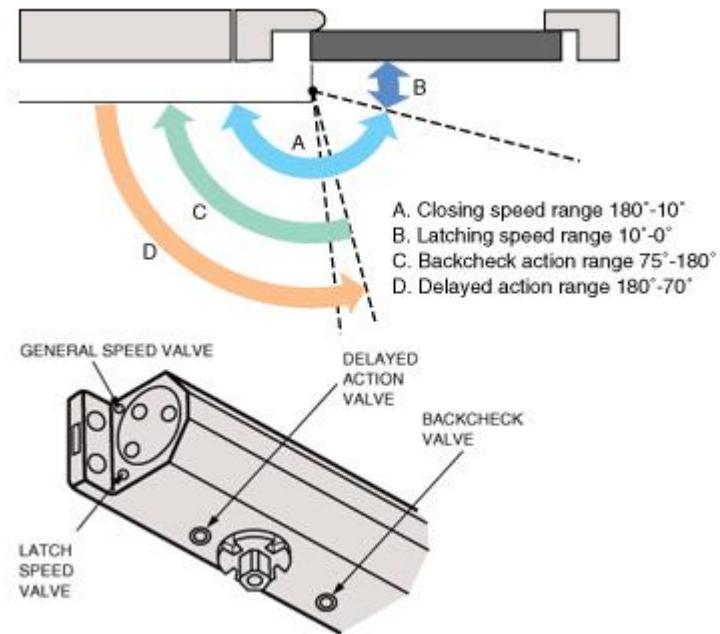
3. Latch: The last, most subtle stage may be the most important:
'latching' slows the swing action down and makes the movement much more stable and rigid so the accompanying door locks can reliable relatch. Instead of a door slamming shut and bouncing off the frame, the latch phase is a controlled close.



When in the 'latch' phase, locks should be adjusted to accommodate for delayed unlock or relock times if needed, and while the overall operation of a close can take 45 seconds, the 'latch' phase alone may account for 5 - 7 seconds despite only moving a few inches.

Timing Adjustment Critical For Access Control

Fortunately for access systems, modern adjustable closers typically have multiple screws that tweak timing or free travel when they are tightened or loosened. The exact location and number of adjustment points vary, but they generally are found on the underside of the unit and can be adjusted with small standard hex keys or allen wrenches:



A closer is properly adjusted when there is no slamming and reliable positive latching of all companion locks. Usually spending ten or fifteen minutes adjusting a closer after three to five years of use is needed, but it may be critical for getting the door to work with electronic access control properly.

Other Uncommon Closer Types

While hydraulic closers are the most common, there are many different types used in a number of applications:

- Electromechanical: When combined with Door Holders (devices that keep doors open), electromechanical devices are often used that pair maglock holders with door closers in an electrified unit.
- Full Concealed/Specialty: Where architectural design and aesthetics matter, closers that can be hidden inside doors, frames, or hinges/pivots are often used. Unlike other types, these are often

matched and installed at the factory and may not be field serviceable using conventional components.

- Pneumatics: In hazardous or contaminate-sensitive environments, hydraulic closers may not be permitted. While uncommon in commercial openings, air-powered closers (often with accompanying compressor units) are used to eliminate the risk of oil-based units.

Sizes Based On Closer Form Factor and Door Width

Most access jobs will not require installing new door closers, however replacing worn or broken ones may be fairly common. Additionally, installing new closers on doors previously prone to be left open can tighten up access in vulnerable areas.

For access installers ordering replacement retrofit units, noting the current type of closer and how wide the door dimension it is attached provide the right information for ordering new closers. The three basic closer form factors are:



The right type to use is typically limited by Door Swing and by the aesthetic appearance of the devices. In general, Regular or Top Jamb units are used unless the way their arms project are considered obtrusive. In that case, Parallel Arm types are used as long as the door width is not over 42".

The strength of the closer is determined by standard 'size', also called 'spring size' despite also applying to oil-filled, springless hydraulic units. In general, the greater the 'size' number, the stronger and physically larger the unit is when mounted onto the opening:

Door Closer Selection Chart	
Door Width	Min Closer Size Needed
Less Than/To 30"	#3
30" – 36"	#4
36" – 42"	#5
Widths More Than 42", Use #6 Regular/Top Jamb Closers Only (Too Wide For Parallel)	

While often preferred for their flush arm action, Parallel Arm closers are often too mechanically weak to close doors wider than 42", and other action types with more mechanical strength must be used.

Closer Cost

In most cases, Regular/Tom Jamb adjustable hydraulic closers should be installed for access control, the other types are too uncommon, too application specific, or too inflexible to be retrofitted to existing doors.

Not only can they be specified to fit most openings, but installing them can be done with basic tools, the units can be tweaked for the specific opening, and for most common door widths using #3 or #4 size units, pricing less than \$300 - \$350 from security distributors.

For wide doors, closers sized #5 - #6, the cost is ~\$450. For very wide or nontypically sized openings, units can be priced ~\$1000 or more and specialty training to install and adjust may be required.

Door dimensions, door weight, hinge type, and expected uses per hour all play a key role in selecting the right unit. Most closer manufacturers provide a [specification guide](#) to help zero in on the recommended unit.

Quiz Yourself

Take the six question [Door Closers For Access Control quiz](#) now.

Automatic Door Operators For Access

Opening and closing doors might sound simple, but it takes a high-tech piece of door hardware to pull it off. Integrating automatic door operators with access control can be tricky if the basic fundamentals of these devices are not understood.



We explain:

- Door closers vs door operators
- Sliders vs Swing Arm operators
- Demo of operation
- Low energy specification
- Access control integration
- Direct vs Indirect control
- Controlling the button
- Common vendors

Door closers vs door operators

Unlike Door Closers whose job is solely closing doors, Door Operators also open them as well. Whether to assist users in wheelchairs to gain entry, or simply to make it easier for shoppers to enter a retail store, operators are included where opening the door safely is as critical as shutting it.

To do both functions, operators not only move bulky door leaves, but typically also include safety sensors and interlocks to prevent people from accidental harm.

Sliders vs Swing Arm operators

Operators generally fit into one of two major types:

Sliders: These operators control doors designed to be opened by shifting to the left or right, and are common in many 'big box' retail stores or high occupancy gathering areas. The door types these operators control are frequently pane glass that can weigh hundreds of pounds and must rapidly open by four feet or more in mere seconds.



Swing Arm: Designed to control more traditional hinged doors, these operators generally use a steel arm to push or pull a door on the strike side so it pivots normally on its hinges. Since these operators can be retrofit to normal openings, they are the most common and the most likely to integrate with access control.



Demo of operation

The promo clip below shows a 'swing arm' example in use, and shows one method of integrating it with a card reader. We describe other options in later sections:

Note: [**Click here to view the video on IPVM**](#)

Notice that each operation phase is a timed event. The entire cycle to fully open and close a door can last a minute or longer, and travel is determined by safe cycle speeds and by the force needed to successfully relatch door hardware.

Low energy specification

A common attribute of operators is how much force is used to open the door. Most modern specifications call for the use of 'low energy' operators, but what this actually defines is commonly misunderstood.

"Low Energy" does not describe the electrical draw of door operators or actuators, but rather the ADA (see our: [Disability Laws, ADA and Access Control report for more](#)) mandates that all doors open with a reduced speed/kinetic energy force than earlier 'full energy' types. The design of the

operator and the door therefore is safer because it is less likely to jam, hit, trap, or wedge potential users with harmful force.

Access control integration

Combining access control with operators is a common task, but can prove to be fairly complicated. Note in the picture below a double swing arm operator is combined with a maglock locked set of doors:



In this application alone, both the operator and the access system need to be configured to release the maglocks first, then begin the process of opening doors or else permanent damage to the operator, door, or even maglock can take place.

In this way, access integration must take place in both the operator and the access system together, and may be a custom configuration based on the particular door locks, access system, and operator used.

Direct vs Indirect control

However, outside of operator configuration, controlling door operators with access control systems is possible through one of two methods:

- Direct - controlling the operator via contacts
- Indirect - controlling the button that activates the operator

Controlling the button

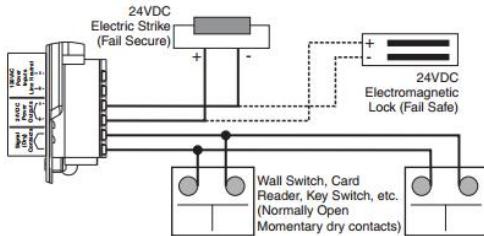
In many cases, but not all, the operator itself will be furnished with auxiliary input contacts that if triggered automatically start the opener

after unlocking the other hardware on the door. The operator's technical manual typically includes specific schematics on how this integration safely takes place:

Fail Safe Electric Strike 24VDC

Wiring

- Doors are normally closed and latched.
- Activating switch will unlock electric strike or mag lock and door will automatically open. Door will close after hold open time delay has expired.
- The door will remain **unlocked** during power failure.
- Current draw at Power Outputs not to exceed 1.3 amps.



Controlling the Button

This method puts a single reader outside adjacent to the push button trigger. A user presents his or her credential to turn on the button, connected to a relay contact in the main controller. In this situation, the controller may not interface with the door or locks at all, and only powers the button for use on valid card read. This is a simpler method of integrating access, but also is the most crude and relies entirely on the existing mechanical door locks for security:



While simpler to integrate, indirect methods may not satisfy AHJ requirements that the button works at all times regardless of operator state. Getting AHJ approval beforehand is key if this method is used.

Tailgating Risk

Because opening and closing a door is potentially dangerous to users, and the speed is often further slowed by ADA requirements, doors can remain open for long periods.

This leaves operator controlled openings vulnerable to the Tailgating risk, where unauthorized users can sneak in through open doors. This makes operator equipped access control openings idea for companion entry detectors or surveillance cameras.

Common Vendors

Operators are usually available from specialty vendors and range in cost from \$500 to \$3500 or more. Some vendors, or even certain models may require specialty installation training before resell or field modifications to work with access systems are supported. Some of the main commercial brands are:

- Besam
- Stanley
- Norton
- Detex
- Dorma

Quiz

Finally, after reading, take our 5 question quiz.

Door Position Switches

Door position switches get no respect. They make Access Control possible, yet they are frequently ignored or forgotten. Every EAC relies on these switches, labeled "DPS", to make the right logical decisions about sending alarms and locking doors. Choosing the right switch for a door is not complicated, but it's more than a 'One size fits all' answer.

Function Overview

Door Position Switches detect whether a door is opened or closed. Typically the access control system controller or door interface module is where this sensor is connected. The method of sensing is simple: when a door is shut, the circuit is complete. However, when the door opens, the circuit breaks open, signaling to the access system the door is not closed. Since doors cannot be locked or 'secured' when opened, this sensor describes where a facility is most vulnerable.

Broad Selection

Because door position switches are used in a variety of systems, there are thousands of options available. Among those thousands, there are five or six basic types used in electronic access:



Basic Types of Door Position Switches

Many installers use the 'magnetic' bullet types in every situation, and struggle with seemingly sporadic false alarms and system trouble ever after. Like other access components, choosing the right door position switch depends significantly on the door - which type of door it is, how often it is used, and even which direction it faces. We address these factors in detail below.

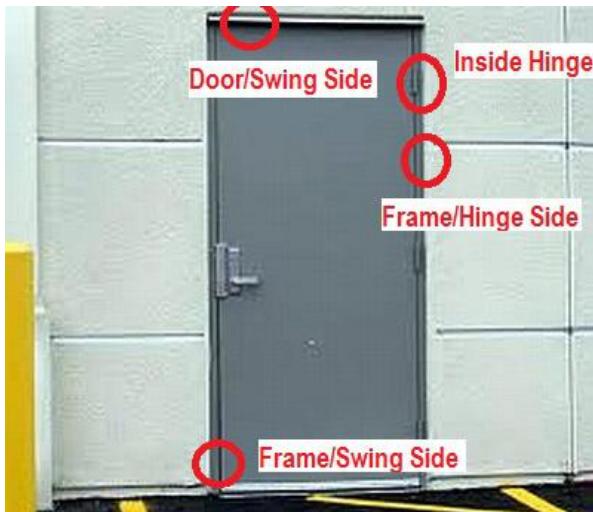
The Opening Matters

Switch selection is typically based on familiarity, when they are installed at all. This constraint is not trivial - some types of DPS switches are more difficult to install than others depending on the door itself. For example, if a door frame is installed into a solid concrete or masonry wall, drilling enough clearance and running wire to a "Plunger" frame style will be difficult. However, a "Magnetic" door mounted type cannot be field installed into plane glass or Herculite doors.

Likewise, the alignment of the door to the frame is critical as well. Most DPS rely on parts of the sensor being a fixed distance immediately adjacent to each other. If the door or frame is out of square or not aligned properly to start with, the sensor may not reliably function. For detail on how to evaluate and correct these issues, see our Door Alignment Primer post.

Mounting Location

The next factor to consider is where the sensor should be installed. There are a number of standard locations to choose from, shown in the image below:



Typical Switch Mounting Locations

The type of opening once again influences this location. Aside from the physical type of door, how its used and where its located play a key role, including:

- Exterior/Interior: What kind of environmental conditions is the sensor exposed to? An air-conditioned office, or an opening exposed to extreme weather?
- Wind/Ice/Snow: If the gaskets or thresholds around the door fail, will the sensor be exposed to moisture, mud, or grime?
- Traffic Volumes: How often is the door opened? Once per shift, or a hundred times per hour?

Taking a survey of the door and recording how it is used help define the best sensor type, attributes that we cover in the section below:

Type Selection

Magnetic 'Bullet' Style: This type of sensor is the most common, usually requiring the wired piece to be installed into the frame, and the solid 'magnet' piece being installed into a drilled hole in the door. In most cases

this type of sensor is hung on the 'swing' side, and is recessed during installation so tampering/detection is difficult.

- Pros: Magnet 'bullet' sensors are concealed and aesthetically accepted in most facilities. Installation is easy requiring a minimum of drilling and wire run difficulty.
- Cons: Very prone to alignment issues. The detection range can be very precise, with sensors needing to be installed immediately adjacent to each other. Vulnerable to false alarms, especially if doors are buffeted by wind or vibrations.



Plunger Style: A mechanical, not magnetic, style of sensor. When the door is shut, the leaf presses a button, completing the circuit. When the leaf opens, the button is released, signaling an open. Because plungers are mechanical, they are not subject to false alarms caused by wind or vibration. Typically plunger DPS are installed on the hinge side.



- Pros: Very durable, usually lasting millions of cycles. A 'one sided' sensor that avoids alignment issues.

- Cons: Prone to sticking because of dirt/grime. Easy to tamper or defeat with a card or screwdriver unless protected by frame and jamb threshold.

Surface Mount Style: Easy to install on most types of doors: wood, aluminum frames, and hollow core steel. Alignment problems are somewhat mitigated with larger sensor area.



- Pros: Rugged and general resistant to negative environmental effects (heat/cold/rain/snow). Minimal installation skill required.
- Cons: Exposed and subject to vandalism. Potentially unattractive in architecturally sensitive doors.

Recessed Style: A hinge side-mounted sensor, very useful on thin frame storefront glass openings. Generally only one side is wired, which is run inside the frame side.



- Pros: Not prone to the tampering vulnerabilities of plunger types, and fully concealed.
- Cons: Generally more expensive and more difficult to install than Surface styles. Risk of damaging door or not having frame clearance could be undetected until trying to install them.

Overhead Door: A specialty sensor designed for doors that separate 'up' rather than swing. Overhead/roll-up doors are difficult to monitor with traditional sensors, due to size and location of structural features.



- Pros: Easy to install, and generally equipped with a substantial armature and armored housing for heavy-duty use.
- Cons: Still susceptible to false alarms due to wind buffeting. Vulnerable to dirt, grime, and forklift damage.

Sensor Price

The cost of DPS sensors is generally negligible, with installation labor running higher than the price of the sensor itself. Most types are available for under \$10, with only 'high security' or ruggedized models being more expensive.

Common Drawbacks

DPS are not without trouble, however. Many choose to sidestep potential performance issues by simply omitting them from designs, however most manufacturers support and best practices recommend their use. In general, when a sensor becomes a source of false alarms, one of the following situations is the culprit:

Dirty/Sticky Contacts: Magnetic or mechanical sensors are coated in grease, dirt, or floor wax so they cannot reliably break contact. A simple rag and light solvent wipe can fix the problem, but continual exposure may require frequent replacement.

Misalignment: Doors and frames move over time, through simple use. Sometime the door shifts enough that realigning the door or tightening up the hinges may be required.

Weather Damage: Thermal exposure can cause magnets to become less sensitive over time, and greater issues of contact corrosion in some environments can prematurely end sensor life. Replacement may be required more frequently on exposed doors than others.

Magnetic Tampering Risk

Non-mechanical sensors typically use magnets to sense open/close state. Because of this magnetic sensitivity, some sensors make it possible to 'fool' the sensor into staying in a 'closed state' if a more powerful, stronger magnet is placed adjacent to the sensor, even for sensors recessed into frames.

While magnetic tampering is a well publicised risk, it mostly applies to an intrusion alarm system, not electronic access. With EAC, several other security layers are in place, namely credentialing and physical door lock security. Simply fooling the DPS into remaining 'closed' and then actually opening the door is likely to trigger an alarm, not prevent it!

Selection Guide

Based on door type and installation location, guidelines for sensor type selection are:

- Perimeter Doors: Use Bullets or Recessed Magnetic styles, depending on 'drillability' of door.
- Glass Doors/Thin Frames: Use Surface Mount or Recessed styles depending on frame clearance and door frame mounting area.
- Office/Corridor: Use Bullets or Surface Mount styles, because weather is not usually an issue and quick installation keeps down cost.

Lock Status Monitoring

Just because your doors look secure does not mean they are. Unless access systems are using lock status monitoring, the doors and areas they protect may not be left insecure. Can you tell whether the door below is locked? How?



Lock status monitoring addresses a key vulnerability of many access control systems, but its value is commonly ignored or misunderstood. We explain:

- How Lock Status Monitoring Prevents Security Risks
- Why Shut Doors Do Not Mean Secure Doors
- Tradeoffs Of Door Position vs. Lock Monitoring
- Typical Solution Cost
- Examining Latchbolt Monitoring vs Latchbolt Strike Monitoring
- Explaining Maglock Bond Sensors

How Lock Status Monitoring Prevents Security Risks

Simply put, lock monitoring checks to see whether an opening's lock is reporting itself as 'locked'. Because most electrified locks can only lock properly when the door is shut, Lock Monitoring tells access systems the door is both closed and secured.

Even with sophisticated electronic access locks, door hardware is vulnerable to tampering. Unless the lock hardware itself is monitored as being locked, tampering can defeat their strength and be undetected by the system.

For example, electric strikes can be neutralized by placing foreign objects in the strike so the latchbolt never fully engages, or held in with tape so they never extend at all. The image below shows how common trash can be used to prevent the latch from extending into the strike to keep a door locked:



And while maglocks generate large amounts of holding force, it works only when the magnet and the armature have full contact. The rated holding force drops drastically if their pieces are not allowed to contact each other, even just through covering the surface with tape or paper, dropping the bond from thousands of pounds to just a few hundred, allowing for doors to be easily kicked open. The image below shows a strap of tape used to

interfere with a maglock's bond so the door can be opened even if it should be locked:



Why Shut Doors Do Not Mean Secure Doors

The scary part is that these doors may otherwise appear fully closed to an access system, but be significantly insecure and unlocked or weakly locked in reality. Even a door equipped with Door Position Switches can only tell access operators if a door is open or shut, leaving the assumption that 'closed' also means 'locked'.

Unfortunately, many attempts to defeat access controls come from insiders, often for convenience and not malice, as noted in our Propped Doors Access Control Tutorial. However, even if done without criminal motivation, tampering with the access lock can leave free, uncontrolled entry through the door to employees or outsiders alike.

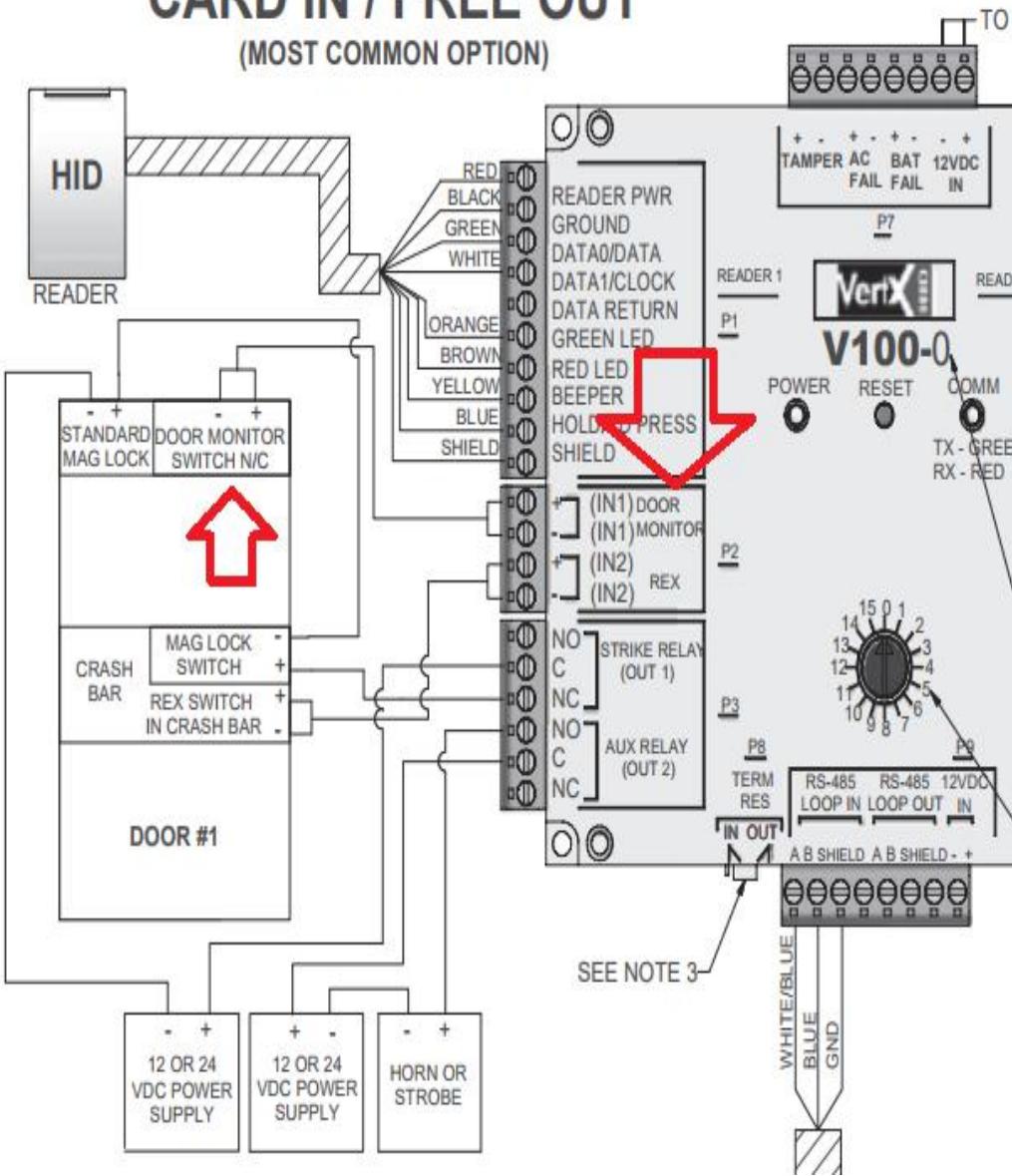
Tradeoffs Of Door Position vs. Lock Monitoring

In many cases, using lock monitoring costs moderately more than door position switches. For many access Door Controllers, either Door Position Switches or Lock Monitors are connected at the 'Door Monitor' input,

usually a simple Normal-Closed circuit on the controller board. Here is an example for an HID VertX controller:

V100 - DOOR/READER INTERFACE CARD IN / FREE OUT

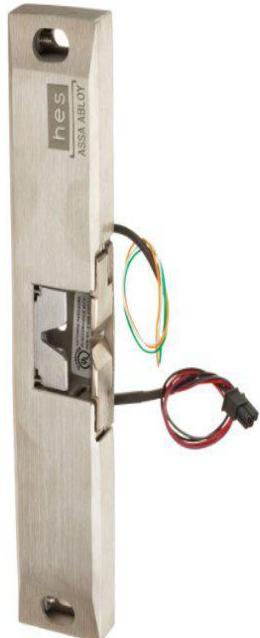
(MOST COMMON OPTION)



The cost of adding a surface-mount door contact can cost as little as \$5 per set, and with a few minutes of install work be connected to an access system. However, specifying integrated lock monitoring in the lock itself can add 5% - 10%, often \$20 or \$30 to the item's cost. The cost difference

may explain why lock monitoring is not as commonly used as Door Position Switches.

In the strike below, the integrated latch monitor is connected to controllers by way of the yellow and green wires:



The wiring harness for these components in all types of locks (ie: strikes, maglocks, or electric latches) is often totally separate from power wires, and leaving latch monitoring unconnected generally still leaves the lock normally operational.

Three Common Forms

Lock monitoring is usually deployed in three ways:

- Latchbolt Monitoring (LBM)
- Latchbolt Strike Monitoring (LBsM)
- Maglock Bond Sensors

While the first two seem to be labeled almost the same, the monitoring methods are drastically different. And even a lock with no moving parts, like a maglock, can be monitored by checking its bond strength. We examine the three methods below:

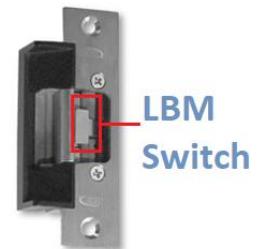
Examining Latchbolt Monitoring vs Latchbolt Strike Monitoring

One way to check if doors are closed and their latches engaged is by 'latchbolt monitoring'. In this method, a mechanical or inductive switch built inside the strike checks whether or not the door's latchbolt or deadbolt is extended. If the latch is thrown, the LBM pressed in. If the latch

is not thrown, the door is unlocked, and the switch remains unpressed or uncontacted by the latch.

Here's an image showing the position of the monitoring switch inside a lock:

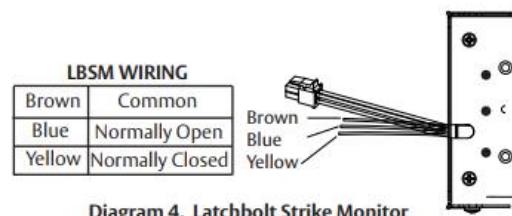
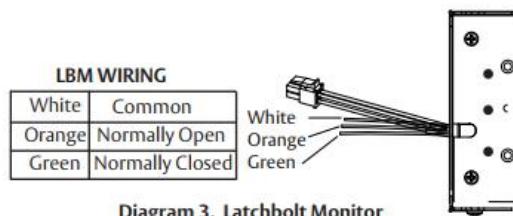
Users should expect approximately this feature adds 5% - 10% per lock, often \$20 or \$30, and adding it usually requires replacing existing locks.



Latchbolt Strike Monitoring

Another method of monitoring strikes involves checking the internal solenoid position, as that in turn indicates whether or no the strike itself is rigid or flexible in retaining lock latches. The advantage of LBsM is that they are less exposed, and less prone to malfunction and breakage, but they are not as common as LBM options on strikes.

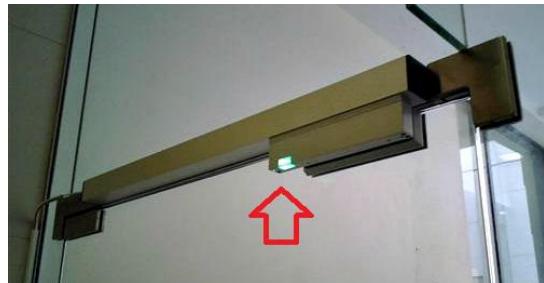
Some strikes offer both as an option, like this HES 1006 Series strike:



Explaining Maglock Bond Sensors

The most common method of monitoring maglocks involves a sensor that checks the field strength of the electromagnetic coil inside the unit. When the field is strongest or within spec, an integrated LED or wire output loop

signals the lock is firmly bonded. The image below shows the 'green is good' LED indicator on one example:



In many cases, bond sensors are a default option, and using them adds no cost since they are already included. However, these sensors can go 'bad' over time, and the sensitive circuits fail with regular use. Periodic replacement involving a technician onsite and a replacement sensor costing a few dollars may be needed once or twice in the span of five years for these maglocks.

Using Both DPS and Lock Monitoring Together

For highest security, some installers use both door position and lock monitoring at the same time by wiring the contacts in series with the door position switch. Instead of simply knowing a door is open or closed, the system would see it as open and not secure or closed and secure.

Optionally, lock monitoring outputs may be run to separate general controller inputs. If users want to display door status separately, this method may also be needed to get accurate status. For example, if doors unlocked during the day should be kept closed, separate monitoring from both DPS and lock monitoring is required.

Multipoint Lock Access Control

Doors are notoriously weak at stopping entry, and money can be misspent on wrong locks that leave doors quite vulnerable.

While closed and locked doors might deter entry for typical people, breaking in with basic tools often takes mere seconds. In the video below, busting a normal locked door secured by a single lock takes less than a half-minute:

Note: [Click here to watch the video on IPVM](#)

However, most doors can be better hardened against these attacks, by installing multipoint locks or latching points. For every latch that is added, burglar and thieves need more time to overcome it, slowing crime so that authorities have more time to react. When multipoint latches are used, simple exploits are made difficult.

We examine multipoint latching, and how it typically is deployed to still be code compliant, yet increase the toughness of doors:

- Door Latches Explained
- Why More Latches Are Better
- What Illegal Latching Looks Like
- The Code Citations Behind Multipoint Latches
- Commercial Multipoint Latch Locks including Detex, Schlage and Securitech
- Passive Hinge Pins Add Multipoint Also
- Configuring Electronic Access To Work With Multipoint Latching

Door Latches Explained

Locking a door usually is a very simple action. "Latching" involves a portion of the door lock or bolt extending or pivoting into the adjacent door frame. Mechanically the operation is simple, and although locks can be quite complex devices, unlatching a door from the adjacent frame is all that is needed to unsecure it for opening. The split image below shows the basic process; twisting the door lever or key turns the latch into or out of the strike plate:



Typical residential and commercial locks work the same way. Often instead of swinging a hook latch, a spring loaded latch pops into a hole in the frame (strikes).

Why More Latches Are Better

In general, a single latch is easily defeated. Subjected to brute force, the single latching point can absorb little integral damage before it is broken or the frame itself is compromised. Often a kick or hammerblow in the single latch spot is all that is needed.

To overcome this weakness, many doors employ multiple latches. Instead of a single point securing a door into a frame, doors have three, four, or

even more latches that protrude on all sides into the frame surrounding an opening.

While defeating these latches may still be possible, it takes more time for brute force to break them all. Given the relative low cost and easy installation of multiple locking latches, it is a common method of improving door security.

What Illegal Latching Looks Like

However, easy and inexpensive it might be, doing it correctly takes careful consideration. Common building codes require that no more than one action unlock/unlatch a door, regardless of how many are securing it.

The most common code citation describing this is NFPA 101:

7.2.1.5.10 (2009): Where door leaves are required in a means of egress, one of the following criteria shall be met:

(b) Unlatching of any leaf shall not require more than one operation.

As a result, many 'homebrew' and illegal examples of multiple latching can be found, including the door below that includes four additional (extra unlatching operation) pin latches in addition to the door lever lock itself:

For those looking for formal code citations online, see [Free Online NFPA, IBC, and ADA Codes and Standards](#) for area relevant versions and actual code language.



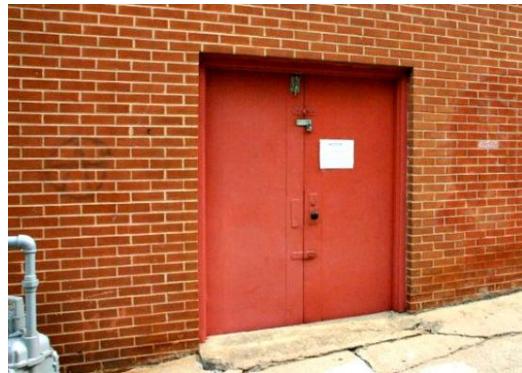
The Code Citations Behind Multipoint Latches

Multi-point latching done legally is possible and common. While not an egress door, extreme examples include bank vault doors that may include 30 or more latching points.

Even in traditional commercial and industrial facilities, these doors are found:

- Backdoor Retail: A huge security risk for many retailers is the rear or freight door. The risk of thieves breaking opening this single door and emptying a location of inventory takes mere minutes. Beefing up this door is very common, to mitigate the risk of 'prybar attacks'.
- Warehouse Doors: In the same way open backdoors are gateways to valuable inventory, all the doors on the perimeter of a warehouse are a risk.
- Hazardous/Valuable Item Storage: Anywhere materials of great value or great risk are stored, multipoint latching is a common sight, even if the area is well within a protected facility surrounded by other access controlled zones.

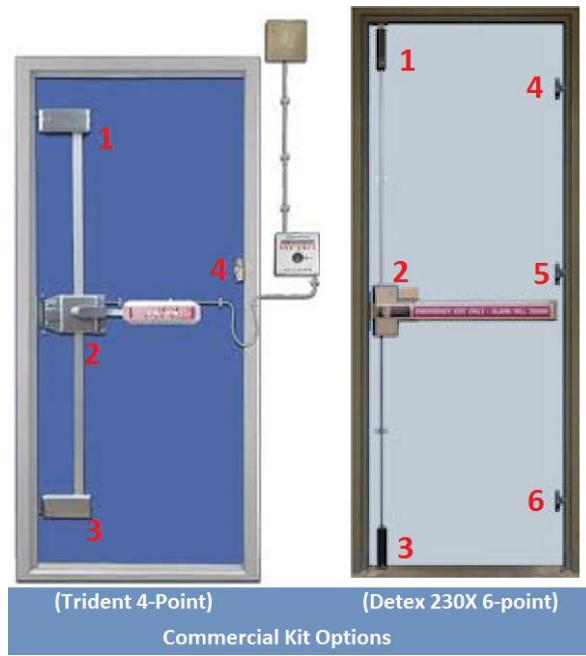
Especially for non-public, but often still emergency egress openings on the backside of retail and restaurants, finding illegal and potentially harmful secondary latches are common. This restaurant rear door has illegal bolts and latches installed on the outside, greatly hindering emergency egress and violating basic free egress rules of life safety access control codes.



Commercial Multipoint Latch Locks including Detex, Schlage and Securitech

There are a number of 'off the shelf' mechanical multi-point latching kits available. Usually these kits can be installed in less than four hours, with common hand tools, and by inexperienced installers; although technical assembly and detailed installation skills are needed. While a singlepoint lockset regularly costs \$300 - \$900, a multipoint lock often costs 2x to 3x more. Some of the more popular units include:

- Securitech: This electromechanical hardware company essentially specializes in multipoint latching but code-compliant door hardware/exit devices. Most kits cost less than \$2,000 but dealer status may be required to buy Trident devices.
- Schlage: Multipoint can be fitted to more than exit devices. Take this Schlage unit for example, that is a mortise lock with surface mounted vertical rods. This device can be retrofitted to steel or wood doors, and costs about \$1,000.
- Detex: A 'budget' exit device, Detex's 230x costs \$600 - \$1,200 and retrofits most steel doors. Step by step installation videos are available online, including basic adjustment and troubleshooting.



Usually, commercial kits offer at least three points of latching, and hinge-side pins can be added as needed. For example, the two kits above offer 4 and 6 point latching systems, but the major difference are the addition of more non-mechanical hinge-side door pin bolts in the 6 point kit. There is no limit or restriction to the number of points used, as long as underlying life safety codes are still satisfied.

As a general rule, the mounting door and frame must be suitable and sturdy enough to support multiple latches. Generally, steel doors and frames with a gauge thickness of 18 or less (thicker) are ideal, but specific kits may require specific door types.

Passive Hinge Pins Add Multipoint Also

Not all 'points' in a multipoint system need to be retractable by lever or pushbar. Rather, using the hinge action of a door to separate the leaf from the frame often proves an ideal spot to place security hinge bolts:



The location of the pins means that doors cannot be easily pulled away from the frame. Especially for outward swinging doors, the exposed hinges cannot simply be cut away or hammered open, because the safety pins hold the hinges together unless swung open normally, through the strength of the door locks.

In contrast to 'active' latch locks that may cost thousands, hinge security pins often can be purchased and installed for \$50, and are not impacted by life safety/egress codes because they do not change operation of the door.

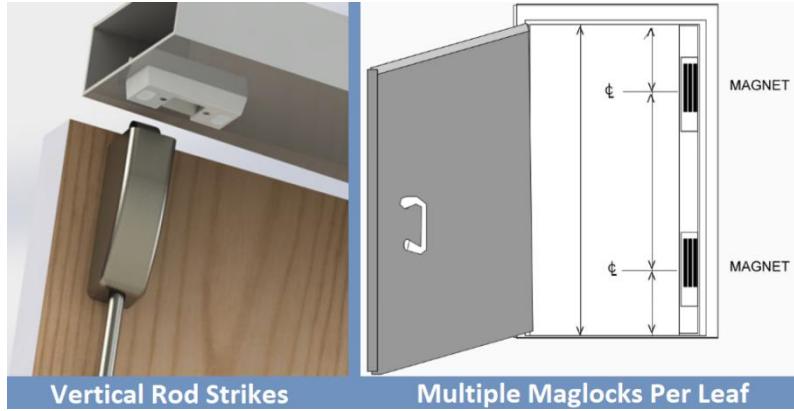
Configuring Electronic Access To Work With Multipoint Latching

Generally integrating electronic access control with multipoint latching takes two basic forms:

Electronic Latch Retraction: Retrofit multipoint device sets often include a solenoid kit that simultaneously retracts all latching points. However, these kits are generally expensive, costing \$2,000 or more and requiring 5-10 man hours to install and adjust properly. These kits also typically require aggressive adjustment and maintenance or they may not secure the door at all points for proper use.

Multiple Maglocks or Strikes: A more difficult to configure method is pairing mechanical latches with multiple electric strikes, or using more than one maglock to secure a door. However, this solution is more difficult to install, because controlling panels need to have multiple outputs for

controlling locks, and even then, timing them for synchronized release can be time consuming.



Not all controllers are equipped with multiple lock output relays, and even the ones that do may not permit multiple locks to be synchronized unlocked to support multipoint latching. While most enterprise systems like Lenel, Software House, and S2 support the feature, entry level systems or 'lightweight' commercial controllers and systems like [Dahua Access](#) and [Axis Entry Manager](#) do not.

Quiz Yourself

Take the [Door Multipoint Latching For Access Control Quiz](#).

[**UPDATE:** This tutorial was originally published in 2014 and substantially revised in 2017]

Glass Doors and Access Control

The biggest challenge for many access control systems are glass doors.

Here's what happens when a maglock is improperly installed to an existing glass door:

Note: [**Click here to watch the video on IPVM**](#)

Unlike wood or steel doors that can be modified to work with electrified locking hardware, glass doors present great challenges. Is all hope lost when requirements call for controlling glass doors? We explain the options and tradeoffs inside.

Problem Defined

Retrofitting electrified locks to 'regular' doors requires drilling or cutting door, frames, and sometimes both. Take maglocks for example: the two major pieces of a maglock must be mounted to both door frame and door in order to secure the opening. In most cases, mounting instructions call for drilling a few holes, slipping in a few sex bolts, and not looking back.

However, doors made of glass are a completely different situation. Glass, even thick tempered glass used in doors, cannot be drilled or cut once manufactured. Despite being very durable to blunt forces, a sharp hard drill bit, or even a slight warping of the pane can cause a dramatic, expensive shatter.

The solution is not any easier using strikes, because in many cases glass doors are 'architecturally significant' features that are not cluttered up with standard locking hardware. In many situations, standard hardware like

hinges, exit devices, and leversets are replaced with low-profile, custom pieces designed to maximize beauty. The latch bolt a strike depends on to keep a door locked might not even be included!

So, how do you control a door that cannot be modified, may not have rails/frames for mounting locks, and likely uses non-standard hardware anyway?

Best Answer: Plan Ahead

The least expensive and 'best looking' electrified solutions for glass doors require the door to be constructed with cutouts, holes, or clearances in mind.

Since these changes do not normally add cost and facilitate the best design of the door with locking hardware in mind, planning for electronic access hardware with door manufacturers is the preferred option.

However, electronic access control specifications and specialists are not often included early enough in the design process to impact door design.

As a result, the 'problem' of retrofitting hardware is a common issue. In the sections that follow, we address how do determine which retrofit option is best.

Two Types of Glass Openings

Modern buildings typically use two different types of glass openings. The access control options can vary widely based on which type is used:

Thin Framed

In many retail storefronts and commercial buildings, 'glass doors' are at least partially framed and trimmed by metal sections.



These openings can often use typical access hardware like strikes, maglocks, or latch retraction as long as 'low profile' or 'glass bead kit' versions are used.

Frameless Glass

The other type, more difficult to work with, are 'frameless' or 'butt jointed' glass openings, also informally called 'Herculite' due to a common brand. These types have no framing metal, and often no locks or traditional hardware like hinges or closers:



This style is often used in architecturally significant or minimalist openings, and can prove very difficult to find locks that can be installed without factory specification.

Moreover, even if factory prepared to mount locks, networking or cabling the components together can be equally difficult, since there is no raceway or channels to 'hide' conductors inside.

Retrofit Lock Options

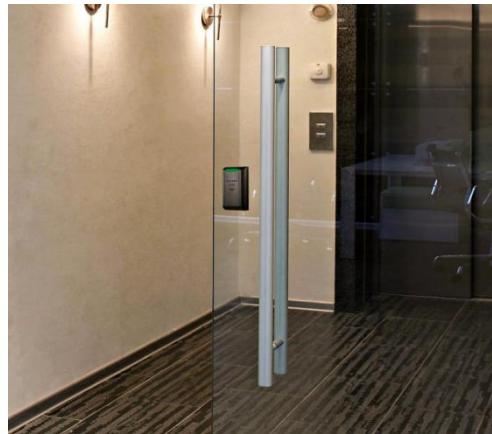
Regular varieties of access control devices are difficult or not an option to mount on glass doors. For these device types we examine options for thin or frameless glass options:

- Readers
- Strikes
- Maglocks
- Specialty Locks
- Standalone Units

Readers

In many cases, a thin mullion or wall mounted reader can be used to control a glass door. However, if no thin frame exists, or if a frameless opening is used, readers can be a problem not only due to mounting area, but also because of unit wiring that carries power/data back to a door controller.

For these applications, a wireless (battery powered) reader is an option. Mounting uses adhesive pads and small batteries to hold the unit in place without any cables:



The Securitron R-100, examined in [Wireless Access Control Card Reader](#), is one option. However, battery replacement, limited credential format support, and adhesive becoming unstuck/loose over time can be a big operational problem.

However, in terms of true wireless readers, market options are uncommon, and the Securitron unit uses a Mercury-based interface module that is compatible with many access systems on the market.

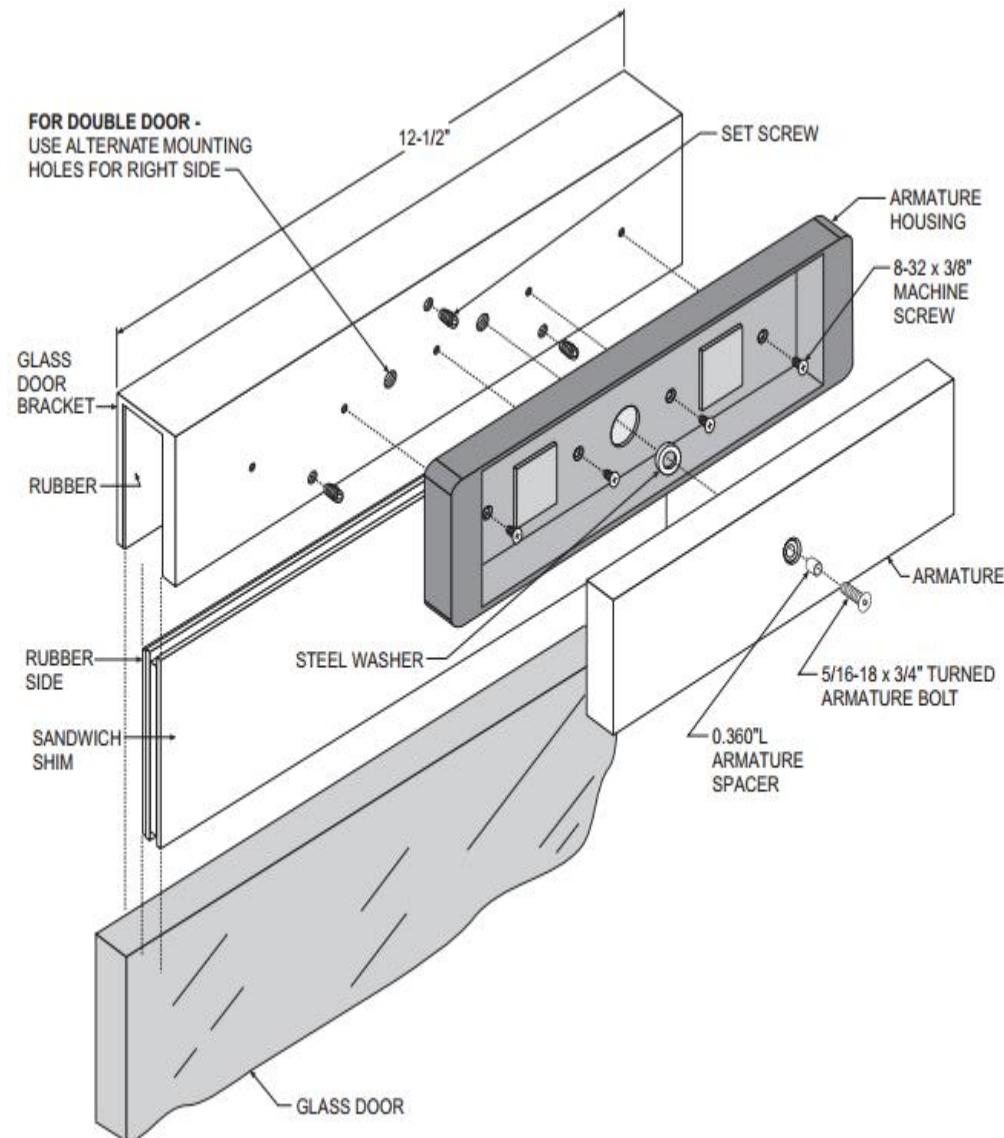
Strikes

In traditional forms, electric strikes are not generally adaptable to most full glass frameless doors. By design, the strike itself is an integral part of a frame and so one must be present for an electronically releasing version to be fitted.

For this reason, when strikes are used to control glass doors, they are either mounted per specification into a thin adjacent door frame and door lock latch, or not at all.

Maglocks

Retrofitting maglocks to frameless glass doors may be an option, but only when the door uses a top jamb. Several manufacturers offer a sleeve bracket that slides down over the top edge of the door for an armature to mount:

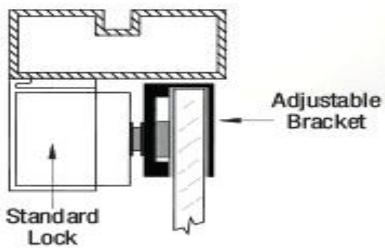


The benefit of this approach is that no drilling or epoxy gluing to the door is required, and the entire assembly is rather strong and secure when the door is shut and maglock is energized. In most cases, the bracket is held in

place with a compression shim adjusted by set screws, and is not able to be moved or pried loose.

Door Header Required

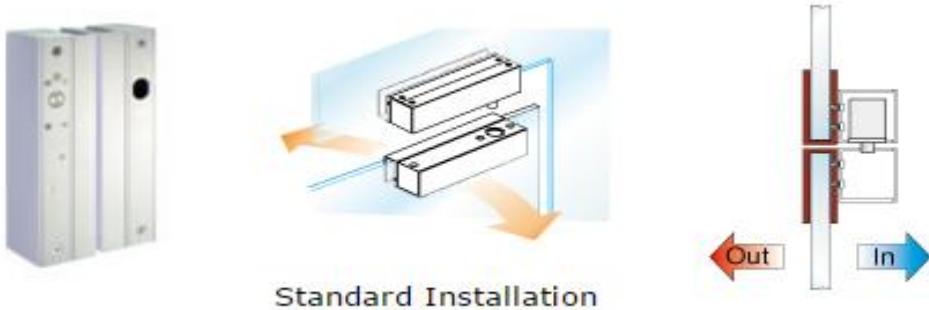
However, while the door/armature installation can be fitted on most glass doors, the assembly often requires the door be mounted in an opening featuring a top frame to anchor the magnet:



While this arrangement may be available on some glass openings, it typically is not on high volume openings or ones with a significant architectural appearance value, often in main building entries or lobbies.

Dangerous Floating Top Brackets

Some products may use double compression brackets for doors without headers. However, these products are typically not approved for use because of the dangers they present:

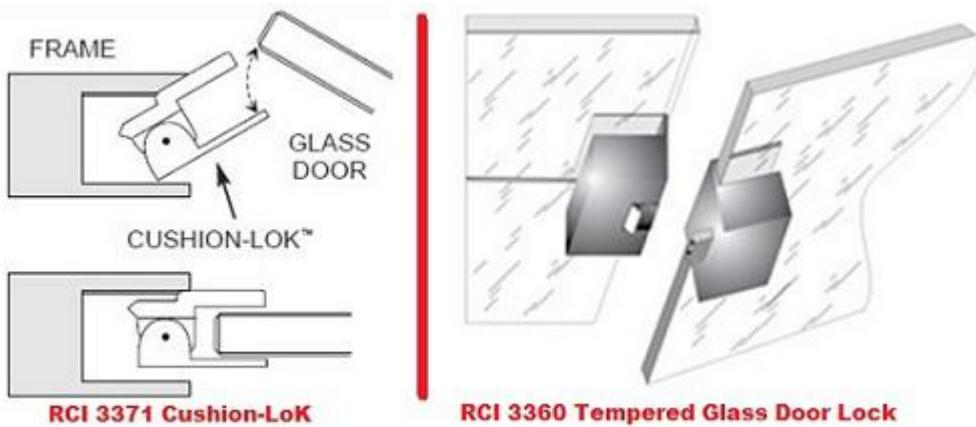


If the top bracket is knocked loose these units may be a code violation or injure building occupants if they fall from place. Dropping from the

installed location may cause the bracket to jamb a door closed, or otherwise prevent egress and AHJs should be consulted before use.

Specialty Locks

When neither strikes nor maglocks can be used, a specialty lock is often the only option. Rutherford Controls International offers the [3360](#) and [3371](#) glass-door retrofit devices. They are neither a maglock nor strike, but are still able to be locked/unlocked by standard door controllers:



Both products feature a 'swinging strikebox' that when locked is stationary and not permit door swing. When unlocked, the motion of the door moves the strike box, and when door is closed the 'bolt' returns back into the box which returns to 'locked' position.

While the actions of the hardware are the same, the mounting surfaces differ. The 3360 is glued directly onto glass slabs, while the 3371 must be mounted into a door rail or accompanying frame.

This video demo shows the RCI 3371 in action:

Note: [Click here to watch the video on IPVM](#)

Both products are 'Fail Safe' devices, include Latch Monitoring switches, and are available in 12V or 24V DC types.

Pricing

Internet pricing for the 3371 is less expensive than the 3360, but requires additional labor and supplies to install:

- RCI 3360: ~\$625 online, and includes materials and adhesive to prep doors for install.
- RCI 3371: ~\$400 online, but may require additional rail prep or mounting hardware.

Both devices are 'non-handed' and can be reversed in the field according to door swing. A potentially important constraint is the matter of exposed power wiring that must be run inside of conduit or otherwise concealed to prevent tamper. This conduit could disrupt the 'clean' installed appearance of the 3360 or require additional clearance inside the mounting rail of the 3371.

The manufacturer recommends either options be powered with independently fused power supplies, and does not recommend powering them from door controllers. This potentially adds an additional \$25 - \$50 in cost per device.

Standalone Units

Options like Adams Rite RT1050D is a retrofit keypad, card reader, and mechanical deadbolt that mounts to a door without drilling. Instead, the

unit uses an adhesive-backed mounting clip that secures both the lock and strike plate to the glass door.



The battery powered standalone lock uses either PINs or MIFARE credentials cards, but is not networkable to existing access control and is strictly offline and standalone.

Another benefit of the RT1050D is that it can be mounted on either single or double frameless glass openings with a maximum thickness of 1/2" or 12.7 mm.

Pricing

The Adams Rite standalone lock is available from online sources for ~\$350, but is typically discounted when purchased from dealers or in volume.

Other Solutions

Lacking other options, it is possible to mount 'traditional' maglocks to glass doors using high-strength adhesives and special armature plates. While using standard form factor maglocks for glass may seem the best of both worlds, using mounting adhesives comes with risks:

- High Skill: Simply sticking a maglock up on a door may seem easy, but installing it properly with glue takes 'know-how'. Maglock armatures need to be installed so they can move and shift when bonding, and unlike metal or wood, glass doors have no flexibility at all. Unless the installer understands where the armature needs to move, the maglock can break the door. (See video clip above as example)
- Special Adhesives: The type of glues or adhesives that can both bond to glass, support the weight of the hardware, and withstand pulling forces equal to the rating of the maglock are very exotic and expensive. Installers may be able to initially mount hardware using common automotive-type glass adhesive, but this bond will fail over time because it is not rated for maglock use. Hardware adhesive kits, like Securitron's Glass Door Adhesive Kit (~\$100 online) must be used instead.
- Failed Bond: Once a bond fails, it results in an immediate security flaw and is very difficult to repair even with new hardware. The adhesives used cannot simply be scraped or sanded off. When a glued bond fails, it often results in replacement of the door and locking hardware.
- Breakable: Whether or not glass itself can withstand hammered blows, the brittle bond of glued hardware can sometimes be defeated with knocking it loose. While new adhesives are generally more resistant to jolting blows than old, cold, potentially flaking urethane adhesives, glued hardware is vulnerable to tampering not comparable to physically fastened devices.



Credentials & Reads

HID vs NXP Credentials

Two companies dominate the global market for access control credentials: HID Global and NXP Semiconductor. Both companies own or influence huge chunks of the credentials game, so which one should you choose?

Credentials Dominated by Giants

Upwards of three quarters of the credentials market uses formats developed or licensed by HID Global and NXP Semiconductor.

HID Overview

Since the market began migrating away from 'magstripe' credentials in the mid 2000's, HID Global rose to prominence with its 125 kHz "Prox" offerings. After being purchased by ASSA ABLOY, the company became 'the credentials house' for a huge swath of the security market, and OEMs products for access brands like Lenel, Honeywell, and Siemens. The company's best-known formats include:

- "Proximity": an older 125 kHz format, but still regularly used and specified even in new systems
- iClass: an HID Global specific 13.56 MHz 'smartcard'

HID is the 'defacto' choice for credentials in the US. Because of commanding market share, HID is able to license the use of its credential formats to a variety of credential and reader manufacturers. Even when marketing general 'ISO 14443 compliant' offerings, HID strictly follows "Part B" standards (vs Part "A" - described in more detail later).

NXP Overview

Formerly Phillips Semiconductor, Europe-based NXP offers a number of 'contactless' credential components used in a number of markets - security, finance, and industrial. With widespread adoption of ISO standards in credential specification, NXP offers a catalog of types built to spec, including:

- MIFARE PROX: NXP's 125 kHz format built on early drafts of ISO standards, but not as widely adopted as HID's "Proximity" lines
- MIFARE/DESFire: an ISO Standards based NXP 'smartcard' format, also operating on 13.56 MHz. The 'DESFire' moniker was introduced in the early 2000s to distinguish the format from 'MIFARE Classic' credentials. DESFire credentials feature stronger encryption than required higher performing chips. The 'Classic' format fell under scrutiny for being vulnerable to snoop attacks, and DESFire countered this threat. Because these improvements were made only to credentials, and existing MIFARE readers could still be used, the new format became known as 'MIFARE/DESFire'.

Unlike HID, NXP's credential formats are 'license-free' and the according standards are available for production use for no cost. NXP manufacturers all ISO 14443 product to "Part A" standards.

Other Credentials

To a much smaller degree, other RFID-based data formats sporadically pop up in physical access control, including:

- Gemalto IDprime.NET: IT-centric smart card format, originally used for logical access credentialing built on .NET framework

- Sony FeliCa: Widespread use in Japan, especially for cashless proximity systems (mass transit, banking)

While not widely used in access control, those formats accomplish the same primary task and use the same basic methods of doing so as the 'market giants'.

US vs the World

Because of NXP Semiconductors's strength in EMEA and the lack of licensing, MIFARE, DESFire, and the associated derivatives are popular pretty much everywhere outside the US.

However, HID Global's strongest markets are in the Americas, especially in the US. Despite the additional cost of licensing compliant credentials and readers, the company also produces product that uses the unlicensed NXP formats and has equal or greater operability as a result.

The ISO/IEC 14443 Division

Very little separates HID's iClass from NXP's MIFARE offerings, and if not for ambiguous interpretation of an ISO standard, they would 'look' the same to most readers. However, because early versions of the standard left room for differentiation, HID and NXP designed their 'compliant' standards with a different encryption structure.

The end result of this is both versions of credential claim 'ISO 14443 Compliance', but are not entirely interchangeable. To reconcile this difference, ISO revised 14443 to include parts 'A and/or B' to segregate the two offerings. Some aspects of these cards are readable across 'Parts', but any encoded data is unreadable between the two.

In general, because there is no licensing cost in using 'Part A' standards, many low-cost and new products start here.

The specification sheet includes the following details:

Parameter	Description
Fingerprint Algorithm	GSA FIPS 201 PIV approved matcher/3M Cogent proprietary
Fingerprint Sensor	500 ppi capacitive sensor, FIPS 201 PIV approved
Image Capture Size	360 x 256 pixels
Enrollment Method	Single-finger, multiple enrollments
Allowable Finger Rotation	+/- 45 °
I/O Interface	RS485, USB 2.0, Secure OTG port
Ethernet	10/100, TLS encryption
Memory	256 MB, 4 GB secure SD flash
Contact Smart Card Reader	PC/SC ISO 7816 Contact Smart Card Reader (optional)
Contactless Smart Card Reader	PC/SC ISO 14443 MIFARE/DESFire contactless card reader (optional)

Readers often with partial ISO 14443 adoption

Meanwhile, readers marketed specifically in the US or from vendors with a broader global market license use of 'Part B' compliance from HID:

Parameter	Description
Memory	8Mb Flash + 8MB RAM
Fingerprint sensor	500 dpi optical sensor
Identification speed	2,000 match in 1 second
Fingerprint capacity	10,000 templates (5,000 users)
Log capacity	50,000 events
RF card	EM, HID Prox, Mifare/DesFire, iClass, Felica

Both ISO 14443A & B Adoption

However, determining which 'parts' a reader or credential is compliant with is not always listed, and confirming a specific brand/type of credential can be used is required.

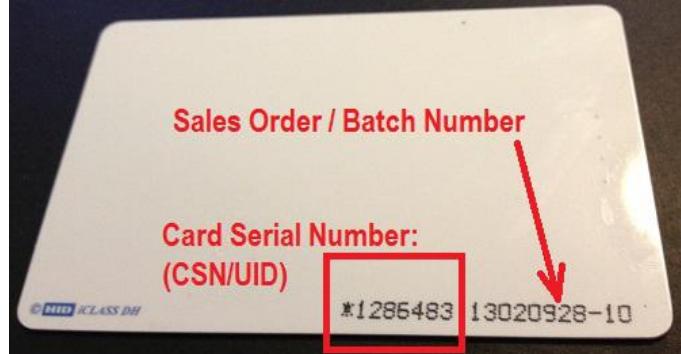
Interoperability

While the 'Part A & B' division in ISO 14443 separates formats from being the same, it does not always mean they are unusable with each other.

Portions of ISO 14443 are the same in both parts, including the 'Card Serial

'Number'. For some access systems, this is the unique number that identifies unique users, and because this number is not encoded, it will register in 'non standard' readers:

- CSN/UID String: Essentially the card's unique identifier is readable because it is not stored in the deep 'encrypted' media. Many simple EAC platforms use only this number to define a user, and instead use the internal database to assign rights, schedules, and privileges.
- Encoded Read/Write: However, the vast majority of storage within the card is encrypted and unreadable unless compliant readers are used. Especially for access systems using the credential itself for storage (eg: Salto, Hotel Systems) and for multi-factor authentication (eg: biometrics) high security deployments, the simple CSN is not sufficient.



System Impact

In terms of access systems, credential providers/formats matter most during design. Reader selection must consider the credential format, and all subsequent badges or fobs must agree with that choice. In terms of 'Access Management Platform' selection, this format does not generally matter, because the reader itself negotiates credential communication. As long as the platform is compatible with the reader, credential choice is a

marginal impact, and most specify credential types based on logistics and ease of purchase rather than technology difference.

However, once this decision is made, changes are costly because they typically require replacement of credentials or reader devices. Changing from one format to the other can cost thousands and affects all users, so changes are uncommon.

Prox vs. iClass Explained

The differences between 'contactless' proximity credential formats are significant, yet the details are not well understood. Most access designers and users are familiar with 'Prox', but replacing them with 'iClass' has no real benefit... or does it?

Key Pros and Cons

The key advantages of Prox cards are:

- Low Cost: The huge number of (persistent) Prox users contribute to lower prices compared to iClass.
- "Good Enough" Security: While vulnerable to "snooping", that risk is uncommonly exploited and most users are comfortable with Prox's "security through obscurity".

By contrast, the key advantages of iClass are:

- Encrypted Security: Unlike Prox, iClass uses a two or three factor encryption of card data, and only a iClass reader can decode the string, meaning it is nearly a 'snoop-proof' credential.
- More Capacity: iClass features more bits, and subsequently more storage, than Prox. There is enough room in an iClass card to store user information for a number of different systems aside from only EAC

Prox is (still) King

Despite heavy marketing of iClass as 'next generation proximity', the majority of all access control platforms worldwide still use 'Prox II' format

credentials. In a recent IPVMU Access Fundamentals discussion, ~75% of attendees explained they use, design, or install EAC systems that use 125 kHz Prox credentials. While many designers and end users are aware of other 'contactless' credential options, many are unclear of the functional differences between the two and simply continue to use the Prox format they are familiar with.

Similarities

A good part of iClass's slow uptake is a result of how closely it resembles Prox technology to the end user and casual eye. Both formats are 'contactless' credentials typically used by waving a card, fob, or token in close proximity to an reader. In this section, we look at the two aspects that are common between either formats:

- Data Format
- Read Range

Data Format: A Prox card and an iCLASS card 'look' identical to an access control system. While the data written to the credential is formatted differently on the card, the reader pushes the same Wiegand or clock and data format to the access control head end.

Read Range: From a technical perspective, iClass carries further distances than Prox, however in reality the ranges are very close to same. Because so many 'contactless' credentials are passively powered by the reader, the cards must be close to the reader in order to work. This requirement limits data read ranges are typically between 0.25" - 6.0", however distances between 18.0" - 24.0" are possible with active (battery powered) credentials.

Differences

However, despite the similar use pattern to end-users, there are many technical differences between the formats including:

- Frequency
- Encryption
- Readers
- Cost

Frequency: The single biggest difference between the two credentials is transmissive radio frequency, where Prox is a low frequency 125 kHz and iClass is high frequency at 13.56 MHz. The higher frequency offers faster transmission speeds and greater bandwidth, more 'bits' of information are able to be exchanged between card and reader in a nominally quicker period of time.

With contactless credentials, a lower RF band constrains performance. 125 kHz is roughly 100X lower in frequency than 13.56 MHz, and the tolerance to wait for a credential to scan at a lock door is seconds. Anything longer results in a high level of impatience by users, so Prox credentials are limited in the data volume of information they exchange. As a result, the maximum number of bits for Prox is typically 64 and commonly 26 bits, well beneath the 128 bit, 256 bit or greater encryptions afforded by the iClass category.

The higher frequency also occupies a less 'noisy' radio band. In some environments, especially industrial, sources like VFDs can generate sufficient interference to prevent 125 kHz readers from being reliable. Higher frequency iClass typically resolve these problems.

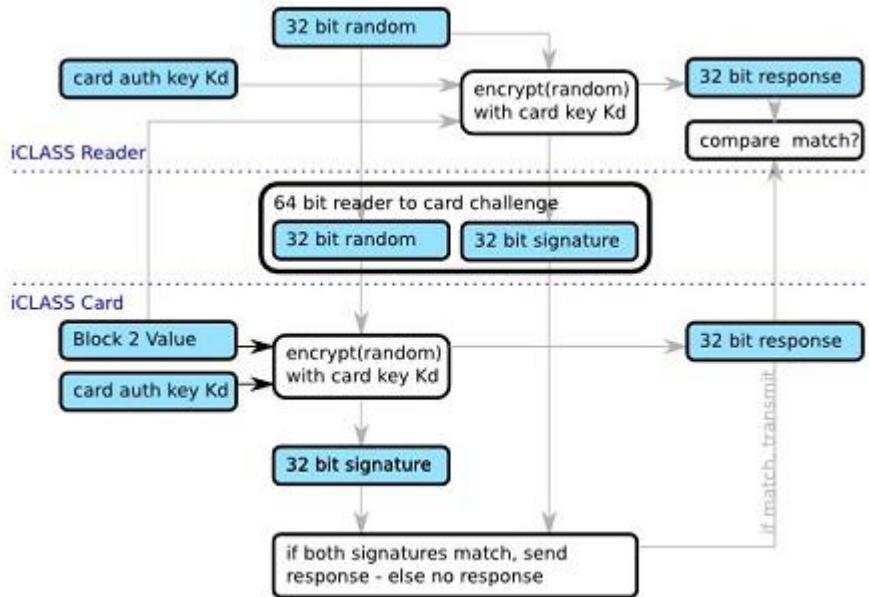
Encryption: With the improvements in bandwidth and speed, iClass offers encryption against 'man-in-the-middle' attacks brought about by snooping unencrypted 125 kHz credentials. HID offers this explanation in their iClass product catalog:

"The communication between an iClass reader and card is encrypted using an algorithm. The transaction between the card and reader cannot be "sniffed" and replayed to a reader. The encryption protocol uses unique 64-bit card serial numbers and mutual card and reader authentication. (or, keys only known to the card/reader)"

A simplified overview between the two formats is shown below. With Prox, all transmission is unencrypted. However, with iClass, all transmission is encrypted and only can be decrypted in the reader once a specific 'key' is shared by the credential:



Also, this image from a hacker's conference shows the 'handshaking' between iClass credential and reader:



The comparison between "keys" (part of the "signature" in the chart above) is a process not possible with Prox. iClass therefore attempts to mitigate the 'snooping risk' although several sources [claim to have exploited iClass](#) using modified snooping methods.

Readers: The readers must match the frequency of the credential; in other words, iClass cards cannot be read on Prox readers and vice versa. A user cannot simply migrate from Prox to iClass credentials without also replacing every reader. The cost of an iClass reader is generally more expensive than an Prox reader, the average price being about 15% higher.

However, the power and data utilities are the same for both formats, and switchovers typically are a quick process of installing the iClass reader in the same place as the removed Prox. All the reader form factors for Prox are available in iClass versions, and therefore changes can even be 'bolthole-to-bolthole' matches.

Certain readers are designed to handle both frequencies simultaneously. Not only does this potentially simplify designs and inventory, but allows

credential migrations to happen over time - rather than forcing everyone to be issued a new card at once, the normal attrition process of card reissue when expired can be followed.

Cost: Despite a lower credential manufacturing cost than Prox, iClass typically costs more. Because of the frequency difference, 125 kHz credentials need more wire coil loops than 13.56 MHz to achieve the right resonance level. iClass credentials use less expensive components than Prox, and despite higher prices, the cost of manufacture is lower. In previous years, HID offered pricing for either formats at near the same prices, although in recent years iClass is typically priced higher. The chart below lists typical internet pricing of standard parts:

Average Component Cost Comparison

	Prox	iClass
Cards	\$2.75	\$4.75
Readers	\$110.00	\$135.00

Should I Upgrade?

Many answer the question of "Prox or iClass?" simply, and stick with the less expensive and familiar Prox format. Undoubtedly, millions of electronic access control systems use the format every day with satisfactory result, despite claims of being a security risk. The persistence of Prox, aside from its widespread market share, is due to the relative satisfaction with its use.

However, if Prox is the stubborn 'status quo', then iClass has true operational advantages not possible otherwise. For high-security deployments, or where there might be a high volume of other identity

details carried in the credential (for logical or multi-system use) the higher bit capacity and encryption level of iClass is ideal.

Access Credential Form Factor

Deciding which type, or form factor, of access control credential to use and distribute can be a difficult task. Knowing the limitations and strengths of common form factors will help the integrator recommend the right choice.

The common 'form factors' of credential are:

- Card/Badges
- Clamshells
- Key Fobs
- Stickers or Tokens
- Embedded Chips

Card/Badges

This format is the popular thin, flexible plastic card that many people associate with electronic access control. Because the user can directly print images on these cards, they commonly double as Picture ID badges. The physical size of this credential varies. The most common size of this credential is described by ISO 7810 as 'CR80', but other sizes exist. This variation in sizing is considered to be a security attribute by some, because unique sizing makes the credential difficult to counterfeit.



These are inexpensive credentials, designed to be cheaply replaced. Sometimes these credentials are even considered 'disposable', like the

example of hotel keycards or public transit passes. Blank card credentials can be purchased from distribution for about \$0.70 per piece in bricks of 50 pieces.

Clamshells

In contrast to the 'card/badge' format, clamshells are thick, rigid pieces of plastic. This bulky form factor withstands abuse better than cards, and may be cheaper than other more durable options. Clamshell formats are older than 'card/badge' credentials, and they were designed to accommodate larger (older technology) components. These credentials can be made into picture IDs by applying a preprinted label.

The cost of this form factor depends heavily on the other design characteristics of the card. Clamshell credentials can be purchased from distribution for about \$1.50 per piece in bricks of 50 pieces.



Key Fobs

Fobs are small devices intended to be located on keyrings. While these formats are not printable, they are very durable and can withstand harsh punishment. These credentials are designed to be crammed into pockets, dangle roughly from keyrings, and endure exposure to all weather environments.

This form factor is expensive compared to other options, however they are designed to be replaced much less often. These credentials can be purchased from distribution for about \$4 per piece in sleeves of 50.



Stickers or Tokens

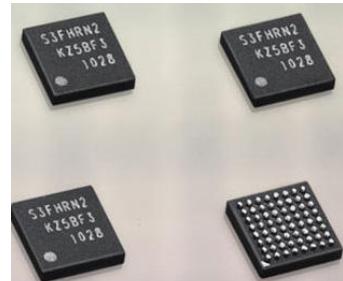
This form factor is often applied to other items (like the heads of keys). This format is useful for making other devices 'hybrid' credentials. This format is always passively energized. This format's primary advantage is that they can quickly be externally applied to other devices. For example, applying this type of sticker to a car windshield is common method of credentialing through vehicle gates.



Pricing varies broadly for this form factor, depending on the expected service life for these credentials. This format can be customized according to a specific size or shape, or can be furnished in adhesive backed 'buttons'. This form factor can be purchased from distribution for about \$2.50 per piece in quantities of 50 pieces.

Embedded chips

Embedded chips or tags are buried in multi-function devices. The chip may be actively powered, and often this type of credential has more than one function. NFC, or 'near field communication' chips are an example of this format.



Pricing for this format is usually done in OEM component part lots and is not relevant for discussions of public purchase.

Applications

We find that certain form factors of credentials perform better than others in certain situations. We provide the following application guidelines based on our field experience:

- Picture IDs: Cards are great for facilities that also require picture IDs. Easily worn and unobtrusive. Low cost of issue and maintenance. Printed images are sensitive to scratching or scarring, but will still function behind a clear protective sleeve.
- Field Use: Clamshells are ideal for workers in the field or shops. Durable construction will not bend or break easily. Can withstand moderate abuse well.
- Demanding Environments: Key fobs are the best option for highly demanding or abusing environments. Resilient to shock or thermal abuse. Small size makes pocket storage easy.
- Tools / Machines: Not typically used as stand alone credentials, stickers or tokens can be discretely mounted to many surfaces. Useful for applying credentials to tools, machines, or other types of credentials like metal keys.
- Phones and Devices: Embedded chips are most used as component parts in other devices. Never used as a stand alone credential, but useful for integrating access control credentials in devices like cell phones.

Vulnerability Directory For Access Control Cards

Knowing which access credentials are insecure can be unclear, especially because most look and feel the same. Even the most insecure 125 kHz types are still widely supported, and using 13.56 MHz smartcards is no sure guarantee the format has not been hacked.

We take a deeper look at:

- Why To Stop Using 125 kHz Formats
- Which 13.56 MHz Formats are Uncracked (So Far)
- The Cracked 13.56 Types Still Widely Used
- Why No Formats Are Uncrackable
- Thousands Are Working On Hacks
- High Technology Skills Needed
- Steps To Defend Against Hacks

Why To Stop Using 125 kHz Formats

While the vulnerability of specific 13.56 MHz formats is mixed, older 125 kHz are highly vulnerable to pragmatic copying with cheap and widely available components. We covered the risk in our [Hack Your Access Control With This \\$30 HID 125kHz Card Copier](#) test, and then how to address the vulnerability with the [Hackable 125kHz Access Control Migration Guide](#).

Which 13.56 MHz Formats are Uncracked (So Far)

The list of vulnerable, unencrypted 125 kHz formats used in access is substantial, easily reaching into millions of credentials still in use daily. The common formats include:

- [HID Prox](#) (discontinued, but still widely available as a generic)
- [HID ProxII](#)
- [ISO ProxII](#)
- [Indala](#)
- [EM 4100/4200/4300](#)

The Cracked 13.56 Types Still Widely Used

The list of popular access formats currently not claimed as hacked is small and contains three main types:

HID iClass SE

HID's latest 13.56 MHz format has yet to be proven and confirmed as cracked using commercial tools. However, [some have claimed success without 'peer corroboration'](#), and multiple sources [1,2,3] claim 'to be close' to publishing an official crack.

MIFARE DESFire EV1 (announced 2006)

This specific NXP 13.56 MHz format has been widely adopted outside North America, by non-enterprise access control vendors, and with less-expensive Asia-manufactured access credentials and readers, and uses 128-bit AES encryption for onboard card details.

MIFARE DESFire EV2 (announced 2016)

This 'next gen' NXP format claims to offer multiple advantages related to how information is structured on the credential, but does not incorporate security improvements. In general, readers designed to use EV1 can also read EV2, although the way information is read and the formatted is different by access systems.

The Cracked 13.56 Types Still Widely Used

The current status of exploits is not always realized by integrators and end users. Two formats still used in many of systems have been hacked, but unknowingly sold as 'secure' by access professionals:

MIFARE DESFire Classic

Though NXP confirmed MIFARE DESFire Classic was exploited in 2011, this has not been widely recognized in the PACS market, with many users assuming the 13.56 MHz encrypted format is safe. However, the method of extracting unhashed security keys prompted the company to discontinue production. The format is still available from aftermarket vendors.

HID iClass Elite (non SE/SEOs Formats)

The effort of extracting 'keys' from HID's original 13.56 MHz format takes multiple readers and cards and was publicized heavily in the 'Heart of Darkness' crack. Once achieved individual credential information can be decoded on all cards. HID still sells these vulnerable credentials, although the most recent SE/SEOs format use a different format and multiple layers of encryption to prevent similar exploits.

Why No Formats Are Uncrackable

Similar to claims of 'unpickable' or 'unbumpable' locks that are often exploited given time and exposure to the public, no credential formats should be viewed as 'uncrackable'. Given broad interest from hackers and hobbyists looking for notoriety in breaking formats essentially 'keeping the doors locked' in countless sites, efforts to hack them are ongoing and relentless.

No access user, installer, or consultant should regard formats permanently secure, and planning for Multi-Factor Authentication and possible migration is prudent.

Cracking Encrypted Formats Is Highly Technical

The equipment and skills needed to crack encrypted formats typically use analytic bench instruments that require software development, electrical engineering, and debugging lines of code.

One of the most popular commercial RFID hacking tools, the open-sourced Proxmark3, has this disclaimer on the intro wiki:

It should be pointed out quite early that the Proxmark3 is not really for beginners. If you are not already fairly familiar with electronics, embedded programming, some RF design and ISO standards, this device will probably bring you more frustration than anything else ! Users that do not understand the basic principles behind RFID may have difficulty using the device.

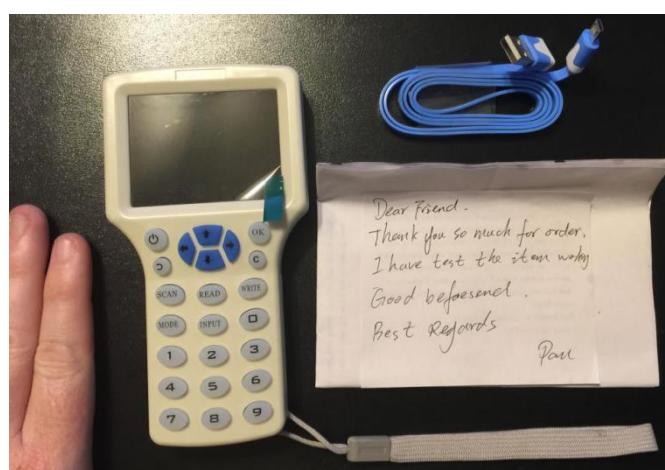
For users looking for the most powerful tools, they should not expect a 'point and click' card copier, but rather a kit of components that include processors, antennas, and firmware that must be integrated together for access credential copying:



Only for older unencrypted 125 kHz formats, are cheap, ready-made, and easy to use copiers available, like the \$30 unit 125 kHz copier we tested with confirmed success:



However, not all 'point and click' copiers are risks to access systems. For example, we tested a Smartcard (13.56MHz) Copier that did not work with common access formats, despite its claims of copying advanced, encrypted formats:



Thousands Are Working On Hacks

Similar to the 'locksport' community of hobbyists interested in picking mechanical locks, there are thousands online who actively participate and contribute to hacking access credentials.

One of the bigger forums where these users gather is the [Proxmark Developers Community](#), with thousands of users and hundreds of posts every month, where collaborative sharing of exploit progress and methods for multiple formats (including iClass, MIFARE, Legic, and UHF credentials) take place.

Other freely available, open source resources are easy to locate. Multiple exploit projects can be found on Github, a large and often freely collaborative source of niche applications. While there are many relating to credential exploits, an example few are:

- [ColdHeat's iClass Cloner Project](#)
- [DESFire / NFC Relay Attack](#)
- [iClass \(Legacy\) Card Copier](#)
- [Mifare Classic Offline Cracker](#)

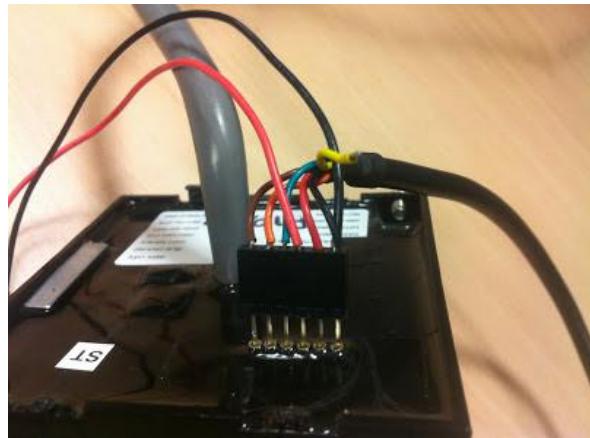
Private Efforts

- [Milosch Meriac's 'Heart of Darkness' iClass Crack](#)
- [K. Chung's RFID/iClass Exploit Blog](#)
- [Brad Antoniewicz Open Security Research Blog](#)

High Technology Skills Needed

Further impacting the pragmatic risk of cracks, is that physical access and modification of equipment is often needed. For example, one of the most

commonly used methods of extracting encoded keys from iClass readers involves physically wiring a harness or splicing the output connection.



For many access systems, the visibility and time needed to use this method on a door significantly mitigates the risk, as the effort would be easily detected by authorities.

The time required for many methods often takes hours of processing. Some methods may take as few as 5 minutes (with the [Proxmark III](#)), while others take multiple hours or even days (with the [PN532 based RFID cracker unit](#)).

Steps To Defend Against Hacks

One key observation is that with the high skill and devoted energy need to crack credential formats, the biggest risk to electronic access control of spoofing and copying cards still takes time.

Granted, the \$30 125 kHz copier can be used in seconds and semi-covertly, so those formats should be avoided. But for 13.56 MHz formats, even those already hacked, hours of time, multiple keys, and physical modification of readers is often required.

The most pragmatic defense against hackers: maintain tight administrative control of user keys, 'turn off' lost keys promptly, do not reissue credentials, and keep sharp eyes open for tampering to installed readers and controllers.

Selecting Access Control Readers

Given the variety of types available, specifying access control readers can be a daunting process. However, focusing on a few key elements will help you arrive at the right product no matter which system you are using.

These factors are:

- The Basic Reader Types: Contactless, Barcodes, Keypads, and Biometrics
- Quick Overview Of Contactless Frequencies and Formats
- How Mounting Surfaces Impact Selection
- Why Establishing Contactless Read Range Is Crucial
- Awareness Of Infrastructure Requirements Like Power and Connectivity
- Protocol Support (Wiegand vs. OSDP)

The Basic Reader Types: Contactless, Barcodes, Keypads, and Biometrics

The first attribute that defines card readers are which credentials they are designed to read.

For existing access control applications, the credential type has already been established and in use. Systems in long-term service may use non-standard credential types and may require specific readers from the original manufacturer, limiting replacement options as a result.

However, modern systems are equipped to read several credential types, so taking an accurate inventory of the various formats in use is a critical step.

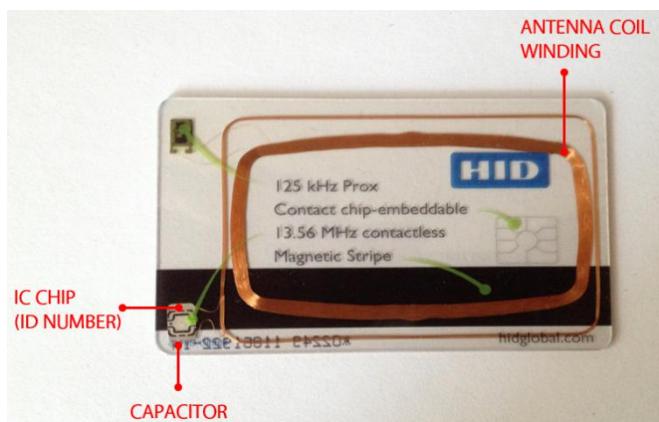
Credentials often double as picture IDs, and frequently take the form of cards and can take several forms - see our [Access Credential Form Factor Tutorial](#) for more details. The following list details the major types of credentials used in modern access control systems:

- Low Frequency, 125 kHz Standard Proximity: The most common credential types in use require the holder to wave the credential near the reader, but not make contact with it. These credentials can be read through wallets, pockets, and glass - and they are commonly used in ID cards, keyfobs, and windshield stickers.
- High Frequency, 13.56 MHz Smartcard: The newest type of card includes an onboard circuit chip (ICC) that offers higher encryption, more storage, and data rewriting capabilities. Facilities using this advanced credential often use one card for multiple systems, including logical access and payment cards.
- Barcode/Magstripe: While quickly becoming obsolete in the face of standards like FIPS-201, older access systems may still use these credentials. While convenient to program and inexpensive to issue, magstripe/barcode based credentials lack the security of other options and can be copied or spoofed easily. In addition, the durability of these credentials is not well suited for commercial use, as even mild degaussing or cosmetic scratches can impact reliability.
- Biometrics: Using physiological features belonging only to specific users is also popular. Fingerprints, palmviens, iris/retinas, and face recognition readers are commonly used by systems.
- Multiple Technology: These types of credential blend two or more of the listed types in a single credential. While more expensive, these types are the most flexible since they can be used with several different systems and can be provisioned from one database.

Quick Overview Of Contactless Frequencies and Formats

For contactless credentials, a type of RF technology called 'resonant energy transfer' is used to transmit card information.

In basic terms, the principal operation of either 125 kHz and 13.56 MHz contactless card readers is for the reader to excites the coil embedded in the card/ delivers power wirelessly to the card, which then momentarily stores energy and then uses it to broadcast card details back to the reader. The image below shows a transparent example of a card, revealing all these components:



A huge risk for 125 kHz credentials is how easy and cheap it is to copy card details without knowledge of the holder. These formats are not encoded or encrypted and can be lifted by copiers with little effort.

One device used to copy the cards works much the same way as normal card readers. Our demo video below from [Hack Your Access Control With This \\$30 HID 125kHz Card Copier](#) shows how the \$30 copier can be used in seconds to spoof HID 125kHz formatted access cards:

Note: [Click here to watch the video on IPVM](#)

13.56 MHz Format Differences

The two most 13.56 MHz common options today come from two different vendors:

- MIFARE/DESIRE (NXP)
- HID Global iClass/ iClass SE

In general, HID format iClass is more expensive on a per-reader and per-credential basis compared to MIFARE/DESFIRE. The source of the cost difference is largely one of licensing, as all HID product is licensed, if not manufactured directly, by HID or their parent Assa Abloy. In contrast, the non-HID formats are 'open use' and essentially open for any manufacturer to build product meeting spec with no licensing cost.

The actual pricing difference between either vendor greatly varies based on individual part numbers, but the cost difference typically ranges 10% - 40% less for non HID products. However, especially in North America, support, project/account pricing, and product availability can be better for HID who retains significant market share in that market. Elsewhere in the world, NXP-based formats may be more popular, and pricing/support may be more favorable.

For detailed contrast between the two vendors, see our: [HID vs NXP Credentials post.](#)

Multifactor Credential Readers

If readers accept more than one credential type to validate users, they are known as 'multifactor readers'.

These types are often required for high security applications or to offer users credential flexibility. For example, a common multifactor unit combines a proximity card reader with a keypad, so if a user forgets or misplaces a card they are still able to key a code for entry. Combination 'multifactor' units often combine card credentials with biometrics like fingerprints, retinas, or palm prints.

If a given door entry reader supports proximity cards, fingerprint scans, or a keypad code in order to be 'multifactor', two or more credentials would be required for entry, not just whichever credential option was convenient for the user to present at the time. The image below gives an example of a typical 'three factor' reader device:



With additional 'factors' come additional credential overhead, including biometric databases that often are independently maintained from the access control system. The speed that multifactor readers process additional credential factors often largely is affected by the total number of records that must be searched, and the degree of

confidence a credential must have to be validated.

While most EAC systems integrate readily with basic keypad code readers, compatibility with biometric readers or high security components (eg: [Hirsch Identive Scramblepad](#)) is subject to individual access control systems.

How Mounting Surfaces Impact Selection

Identifying the specific mounting location for the reader is the next step - while many readers are 'multipurpose', more advanced types (especially biometric combo units) are not suited for every location. In the following section, we address the most common mounting locations, and identify the variables for specifying the correct readers:

Outdoors/Indoors: Like most electronic devices, the units intended for mounting outdoors must be sealed against moisture and protected against freezing. Readers are commonly available in 'potted' varieties, where the internal electrical components are sealed in resin to prevent contact with moisture. Confirming a reader is suitable for outdoor use is frequently noted as 'potted' on datasheets, which departs from industry standard IP ratings. Furthermore, the actual appearance of the reader may not change between potted/nonpotted varieties.

Wall Mount: The most basic orientation for mounting readers is on the wall nearby the controlled opening. While smaller readers may be designed to mount directly to drywall or masonry with simple screws, heavier readers may require additional brackets. Wiring harnesses can be directly pulled through bored holes in walls, or otherwise may be terminated in single-gang junction boxes - in this case, the reader is frequently mounted directly onto a junction box cover plate.



Mullion Mount: Where glass is adjacent to openings, or where control cabling cannot be fished through wall construction, a common solution is mounting readers onto hollow door frames. Because the mounting surface is typically metallic, insulating gaskets and shielded cabling may be required. These readers are identifiable by their thin profile, often only a few inches wide. Even though these readers are narrower than typical wall-mount types, they are available in the same read-ranges and offer the same multi-factor (eg: biometrics, keypad) options.



Bollard Mount: Readers used for gate/parking lot applications are frequently mounted on metal or concrete posts outdoors. These devices typically need longer read ranges than door mounted types, since the credential can be feet away within an automobile or windshield mounted. While these readers are typically connected to access controllers the same as other readers, they may require extra power supplies and cable shielding/grounding. These type of readers may also require the use of media converters or other expander modules to increase their communicating distance to controllers.



Turnstile Mount: One of the most challenging mounting locations for a reader is on a turnstile - not only are these units typically outdoors, they are frequently exposed to thermal shock, UV exposure, and impact force. Standard outdoor readers may require frequent replacement. As a

result, ruggedized / vandal resistant readers are recommended for turnstile applications.

Why Establishing Contactless Read Range Is Crucial

Determining the distance a card reader is needed to detect a credential is the next step. Understanding the space between the reader and the controlled opening is critical - not only does it take time to physically travel from a reader to open a door (especially with wheelchair accessible openings), the standoff distance between a gate reader and an automobile may require special consideration.

Credential readers are typically available in three roughly defined distances. Each manufacturer defines the exact distance differently, and the range is typically influenced by mounting environment, interference sources, and line of sight. The standard breakdowns are:

- Short: these units read anywhere between close contact and 6" - 8", and are found located immediately adjacent to doors on mullions or walls. Power for these readers can be typically drawn directly from the controller without extra power supplies.
- Medium: readers in the class generally reach between close contact and 32" - 48", and are suited for use in parking lots and on bollards or posts adjacent to doors. These units feature different antenna coil configurations, consume more power than short range readers, and typically cost more.
- Long: units falling in this range typically work between 2 feet and up to 30 feet. Because of the extreme distance, readers in this category must be mounted with the same considerations as wireless networking equipment: physical line of sight must be maintained,

adjacent wireless systems can be sources of interference, and reader orientation is critical for credential detection.

Maximum read range length also is significantly different, with the lower frequency 125kHz format covering longer distances. While the maximum range is not a typical factor for wall mount or mullion mount applications where cards pass less than 4 inches away from the reader, using high frequency 13.56MHz formats cannot read at ranges needed for parking garage or vehicle gate applications.

For example, many 125 kHz long range readers reach up to 24" with standard non boosted credentials, but their 13.56 MHz counterparts only reach 18" and have warranted HID to sell a different UHF format credential and reader system instead for that application.

It is important to note that not all credential types have all range selections available. Less common credential types may not have the selection of 'long range' readers available, and credential formats commonly used in Europe may not be licensed for free use in the US, and vice versa.

Awareness Of Infrastructure Requirements Like Power and Connectivity

The other factor to consider is what utility or secondary resources are required at the opening. Reader infrastructure aspects to consider include:

- **Power:** Most readers are designed to operate on 12VDC/24VDC and even PoE, but ruggedized and long range types may require different utilities. In general, readers are low current draw devices, typically pulling only milliamps. Some types of 'stand alone' readers operate from battery packs and require no outside power connection.

- Data: Most readers are connected to controllers with UTP or 18/6 cable, but individual reader types may require non typical wire gauges or special features like drain cables or shielding. Wireless variants, typically using a point to many point transceiver system, are especially popular in low-cost and non-high security applications. Frequently, data cabling is grounded or shielded to prevent interference from corrupting data exchange between reader and controller units.
- Secondary Means of Security: While not a traditional infrastructure component, an often overlooked feature is a backup method of securing the opening. Because most backup power systems have a finite battery life, and some hardware lock components cannot have backup power (eg: maglocks), a mechanical lock and key must be installed. Managing and maintaining this hardware is not expensive, but the only occasional use of these locks require a well organized and managed key control system.
- Intercoms/Cameras: Finally, while not essential, secondary systems like intercoms and video surveillance cameras can help identify those requesting assistance or entry without system credentials. Invariably, a credential holder forgets or loses a credential and does not realize this fact until standing at the controlled opening. Having an intercom available allows security staff to communicate with a someone lacking credentials, without compromising area security by permitting access to secure areas.

Protocol Support (Wiegand vs. OSDP)

A reader's output option must be compatible with the controller. Both devices must support Wiegand or OSDP, or direct reader interface

compatibility for proper operations. Readers are only useful when compatible with the larger access system, specifically the door controller.

For many years the standard interoperable communication protocol between readers and controller has been Wiegand, an interface that predates modern serial or TCP/IP communication. Since the early 1970's Wiegand was used to standardize reader outputs in a way that controllers could interpret, regardless of manufacturer.

However, Wiegand has some weaknesses that are only amplified in the modern era. Lack of encryption, unidirectional transmission, and the physical limitations on transmitted data size have been far outpaced by modern credential and access system design. As a result, a new standard protocol called OSDP is being promoted by leading access companies.

Our Wiegand vs OSDP note has deeper technical details, but the primary advantage of OSDP is better device manageability, status monitoring, and data handling than the old Wiegand protocol. At the current time, adoption of Wiegand is widespread and common, with OSDP less so. However, this is changing, with most manufacturers offering new products supporting the protocol and plans to expand it in years ahead.

Multi-Factor Authentication Primer

Can a stranger use your credentials? One of the oldest problems facing access control is making credentials as easy to use as keys, but restricting them to certain individuals. The technique of 'multi-factor authentication' is applied when the end-user is concerned about who actually can use access control credentials.

Multi-Factor Authentication Defined

In simple terms, the concept means that more than one credential must be presented in order to gain access. However, the credentials must be 'layered' in a way that they validate each other. This means that for 'multi-factor' systems, more than one credential type is simultaneously required, not simple an option of more than one type to chose from.

If a given door entry reader supports proximity cards, fingerprint scans, or a keypad code in order to be 'multifactor', two or more credentials would be require for entry, not just whichever credential option was convenient for the user to present at the time. The image below gives an example of a typical 'three factor' reader device:



The individual authentication 'factors' cannot be all of the same type, and must be diverse, discrete, and separately managed types of credentials.

These 'factor groups' are commonly cited as:

- Something the User Has: A

credential/permission granted administratively to the user. Typically

an access control badge, token, or fob. Also includes a mechanical key, membership ID, or passport.

- Something the User Knows: Typically a code or password kept private by the user. Typically a PIN number, but also include 'Security Questions' or 'Last 4 Social Security digit' confirmations.
- Something the User Is: Biometric features only the user is able to possess. Typically fingerprints or palm prints, but other readings possible including face recognition, heartbeats, retina/iris scans, and even gait.
- Someone Trusted Verifies the User: Under certain conditions, another human positively IDs and vouches for the user. This could be a manned guard, or even a receptionist that grants access based on familiarity.

Different Types

The actual number of applied factors vary according to an end-user's security concerns. Users simply concerned about the improper use of lost credentials may require two factors, while high-security installations may require three or more. We define and explain these tiers below:

Two Factor: Most often a combination of 'something the user has' and 'something he knows', seen as Access Control access card and accompanying PIN number. Even if the user loses the card, an unauthorized finder cannot use it to gain access unless they also know a code, which is known only to the user.



Because duplicating biometrics traits are very difficult, it is also common to see fingerprint or other physiological factors used as 'something the user is' in two factor authentication.

Three Factor: When identity requires an even higher level of validation, three factors are required. Most often this is a combination of biometrics, PIN codes, and access control credentials, and become significantly more costly to implement and manage than simple 'single factor' authentication.



As a result of both cost and time to use this level of authentication, it is used in critical infrastructure, military, and research facilities but not typically for commercial end-users.

Four Factor: The highest level of authentication is often seen at military and other sensitive locations, where manned checkpoints are used in conjunction with the other factors. Because this process takes the most time and is the most labor intensive, it typically is not employed unless the security risk is very high and existing manpower is available.



Multi-Factor Applications

Most would assume 'single factor' authentication is most common, but multiple factors are required everyday in routine circumstances outside of access control. Take these everyday examples:

- **ATM Machines:** Not only are debit cards required to be swiped, but PIN numbers are required every time a cash transaction takes place at one of these machines.
- **Online:** Everything from social media, email, to web based banking takes advantage of usernames 'something you have' and passwords 'something you know' to protect online identities.

When it comes to securing access, credentials play a vital role. When it comes to securing credentials, multiple factors are required.

Single Factor Still Most Common

A majority of electronic access control systems use 'single factor' authentication, and this is sufficient for the operational security of most end-users. The single credential card or code is tied to the identity of the bearer, and all system activity (ie: entries, exits) is booked against that person.

The traditional key remains the most common 'single factor' credential. No other verification of the bearer is required once the key has been issued. While primitive compared to high-tech electronic access credentials, mechanical keys still provide an adequate 'first layer' of security for many millions of facilities.

For these systems, using multiple factors to verify identity would be needlessly costly. Because readers supporting extra inputs are more expensive, and hiring manned verification staff is overhead not easily justified without pressing circumstances, single factor remains the frequent method used.

Biometrics Pros and Cons For Electronic Access Control

Biometrics has been long sought as an alternative to the security risks of cards, pins and passwords. While biometrics has improved somewhat over the past decade and has some clear advantages, other problems or limitations remain.

The Pros

Advantages of biometrics have key value in some access applications. While manufacturer marketing often blurs the claims and overstate the advantages, biometrics can offer:

- Credentials Always Available
- User Identity Verification
- High Credential Validity
- Tough Against Passback

The Cons

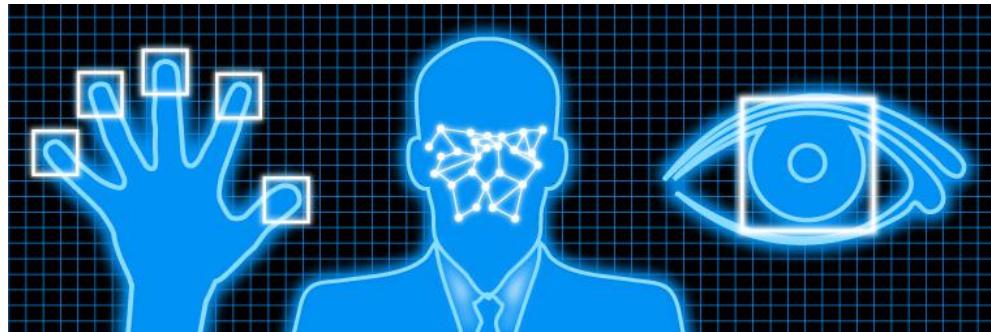
On the other hand, there are operational weaknesses or risks that are not commonly realized before deployment. Some of those are:

- User Unwillingness & Distrust
- User Biometric Incompatibility
- User Removal of Clothing
- User Positioning
- Injuries & Biometric Stability
- Lengthy Authentication Cycletimes

- No More Picture IDs
- Myth: Biometrics Are Distinctive

Biometrics Is More Than Fingerprints

One of the contributing misconceptions with biometrics is the sheer number of technologies that are mistakenly assumed as having the same general strengths and weaknesses.



We cover the most common biometric form in our [Fingerprint for Access Control](#) post, but other common but distinct technologies include:

- Palm Prints: The outer layers of palm skin are uniquely contoured in a similar manner as fingers.
- Finger/ Palm Veins: Rather than scan the outer layers of skin, these sensors image the inner layer of capillaries just under layers of skin. These small veins are patterned in a unique way, and the deeper tissue is less prone to surface damage or contaminants.
- Iris/Retina: This type of reader takes an image of the inside of user eyes. Both irises and retinas can be used to distinguish individuals.
- Face Recognition: Taking an image of a face and measuring the size and distances between eyes, nose, mouth, and other identifying

features with high accuracy and precision is becoming more common.

But there are a myriad of lesser used, but still 'user unique' biometric forms. For more, catch our [Favorite Biometrics](#) post.

Biometric Benefits

In the sections below, we take a look at four advantages of biometrics. While individual methods and readers may offer distinct pros compared to others, biometrics as a general segment offer keys or minimize the risk of other credential types:

Credentials Always Available

With biometrics, the user themselves are the credential, and forgetting a PIN or losing a badge is simply not a risk. Because physiological elements are indeed used to verify users, biometric credentials are available when needed and users simplify credential management by eliminating key, cards, and codes than can be misplaced or forgotten.

User Identity Verification

Because users cannot lose or lend credentials for others to misuse, biometrics are useful to declare users are specifically themselves. Just as users can share cards or PINs, they cannot lend of fingerprints or irises, increasing the confidence that only authorized users are entering an area.

High Credential Validity

Unlike common credential types vulnerable to copying or spoofing without notice ([Hack Your Access Control With This \\$30 HID 125kHz Card Copier](#)),

biometrics generally mitigate the problem. Cheap gadgets like the ones below can't be used to copy biometrics:



While 'cheaper' and low-quality biometrics reader can be vulnerable to low-level spoofs, the units used in access typically employ one or several layers of Liveness Detection regardless of which biometric technology they use.

Tough Against Passback

Biometrics essentially eliminate the risk of credential sharing as users cannot simply hand off their biometric identifiers to friends or coworkers. As covered in our The Passback Problem post, the problem is not easily solved with other credential methods and often requires advanced system configuration to stop. Biometrics often are less expensive to implement and are less complex to configure.

Biometric Weaknesses

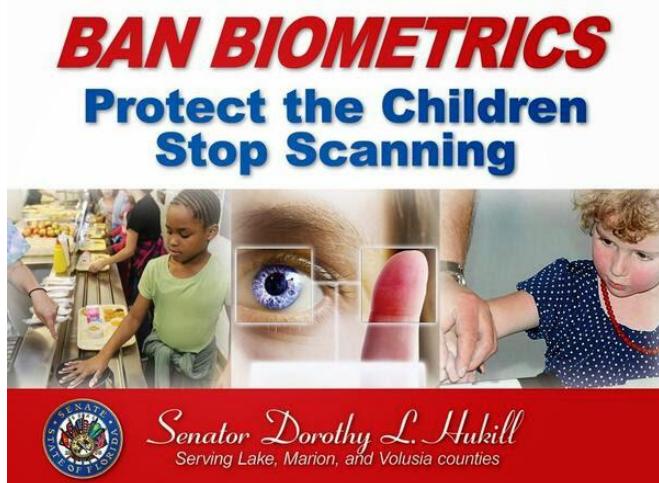
However, while biometrics may solve some problems, they amplify or create others. In the sections below, we detail seven common issues that can be showstopping problems if not recognized beforehand:

User Unwillingness & Distrust

Not all users are comfortable and willing to have biometric traits used as identification. A myriad of cultural, political, religious, or general lack of trust in the collecting agency or enterprise to use and protect biometric information can be a factor.

Campaigns to 'ban biometrics' in government use to identify citizens is one common hotbed of debate that often carries into private systems as well.

The image below is from a recent campaign in Florida:



User Biometric Incompatibility

Quite simply, not all users may either possess or have satisfactory function of the physical biometric trait used to verify identity. Some users may lack

the physical feature outright, while others may experience a 'temporary' lack of ability due to injury or infirmity. Even a biometric as common as fingerprints assume that all users have working, healthy fingers to authenticate on, and other methods of credentials must be provided for when they do not. This typically results in using multiple credential systems regardless.

User Removal of Clothing

Another key hindrance for biometrics is the assumption the environment or location they are used will experience no user variation in the biometric trait being measured. This is often not the case, as something as simple as users wearing gloves in cold weather can be a major hassle to remove for fingerprints, or sunglasses for iris/retina scanners, or hats in rain, and so on.

User Positioning

Not all biometrics are suitable for use in every situation, and are often less flexible than 'traditional' keys, cards, or PINs. For example, reading fingerprints while users are seated in vehicles is highly problematic due to the physical reaching and hand positioning needed, while simply scanning a contactless card is much easier.



Complying with [Disability Laws, ADA and Access Control](#) can be difficult to adapt for all users, especially those who have mobility or ambulatory issues.

Injuries & Biometric Stability

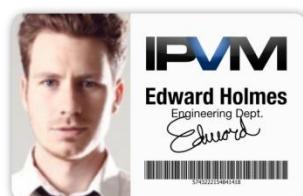
Relying totally on a biometric trait can be shortsighted for multiple reasons, when physiological changes due to aging or injury are common. For example, collagen elasticity and volumes degrade over time, so even 'unique' features like fingerprints change over the course of years, and sometimes even disappear or become negligible to read. Other factors like eye mobility, gait patterns, or even facial structures can change over time. User enrollment of biometric features is often a perennial, if not annual, task.

Lengthy Authentication Cycles

While waving a badge or punching in a PIN can take seconds, properly registering a biometric can take much longer, even a minute or longer if retries are needed. For high-volume entrances, multiple card reader openings can handle hundreds of users per hour, but a biometric reader like fingerprints may handle a fraction of the needed total as every user must present a specific digit in a specific way every time.

No More Picture IDs

Finally, one factor not typically realized is which other ID factors are given up by adopting biometrics. While full color picture ID pictures are

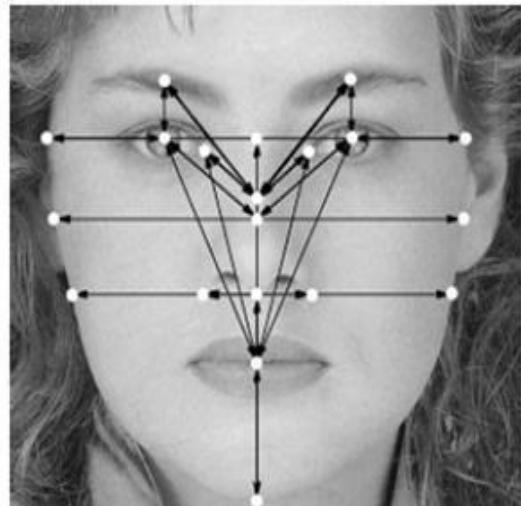


often printed on the same card as a contactless card and then subsequently carried around user necks on lanyards for quick visual identification, that media is forfeited when adopting biometrics and must be redundantly reissued.

Myth: Biometrics Are Distinctive

One of the biggest errors users make when adopting biometrics is assuming all users will be enrolled uniquely and no one will be mistaken for someone else. This often results in unwelcome surprises, because any biometric is only as 'unique' as the number of sampling points collected and used.

For example, while a fingerprint or iris may indeed be unique, it may take twenty or more data sampling points before it is classified as 'distinct' in a database. Other users may have similar biometric signatures, with the same distance between features or similar (but not exact) physical traits, especially in large user databases.



In many cases, the 'confidence interval' of reading biometric features or traits requires configuring the reader or system to spend more time collecting data. The increased read time can greatly impact read efficiency and slow down user volumes passing through an opening, but will gather more information about the user, increasing the 'distinctiveness' of the biometric credential.

Fake Fingerprints - Liveness Detection Solutions

One of the biggest concerns with fingerprint readers is how easy they can be fooled. While biometrics are typically more difficult to steal or fake headlines still break news of fake fingers or stolen prints being used to fool sensors.



For this reason, many access control fingerprint readers include live finger or liveness detection that checks the finger being scanned is authentic.

Stealing Fingerprints To Spoof Identities

The root cause of the problem is that while fingerprints are unique, they can be copied or used without permission. Throughout the years, various methods of stealing prints, by completely casting replicas of finger tips, using gummy bear candy transfers, super-glue capture of latent prints, or even using cadaver fingers have been reported.

While the effort of producing someone else's print takes more effort than stealing a card, fob, or key, the risk is the same - unauthorized people will gain access to sensitive areas they do not belong.

Four Common Methods

While fingerprint reader manufacturers frequently add liveness detection methods, they do not always explain what they are or how they work. In

general, the number and type of methods a manufacturer include vary but typically fall into four different categories:

- Tissue Reflection: The most common method (sometimes called Multispectral Imaging) typically uses IR light to examine the reflected contrast of a finger's skin. This method relies on the fact that normal, healthy skin reflects IR light in a consistent way that looks different if dead or covered by synthetic material. Especially for optical based sensors, this check is done at the same time as the fingerprint is 'read', so there is no delay during the read.
- Heartbeat Detection: One of the strongest methods uses a high optical sampling rate to detect the momentary, rhythmic swelling of capillaries coursing with blood. This impulse corresponds to a beating heart, and without it present the scanning attempt is ignored. Being both reliant on hardware and software makes this particular method one of the more expensive options for manufacturers to use.
- Dermal Electric Resistance: For conductive type of sensors, healthy human skin carries a small but consistent electrical resistance. If a finger is presented and the sensor is unable to confirm typical skin resistance, it is invalidated. Even in low cost conductive strip models, this liveness check is common, but it may not be reliable in wet or cold environments that change the density of skin and blood in tissue.
- Unnaturalness Analysis: This method alone is the weakest, as it relies on software checks alone to determine authenticity. This method compares a print against typical characteristics of a fake or spoofed attempt. Based on sensor checks like blurred, abrupt or sharp edges, blank print voids, or atypical clarity of the print, if the quality of the

read falls beneath a certain 'authentic' range, the print is disregarded as fake.

Given the wide number of readers in the market, a unit without Liveness Detection can cost \$100, while a unit that layers several methods can cost 10X more. The addition of Liveness Detection is just one aspect of these units that drive price higher, along with sensor type, integration support, and environmental performance of the reader.

Liveness Methods Used

To combat the risk of fake or spoofed prints, many commercial fingerprint scanners and readers add checks to confirm they are real. Below is a list of 'liveness detection' or 'live finger detection' on access fingerprint product specsheets:

- Lumidigm/HID Global: Uses heartbeat detection and tissue reflection to validate fingers are real.
- Morpho: Depending on the reader, Morpho uses tissue reflection, dermal resistance, doubled up with unnaturalness analysis.
- Suprema: Uses a number of unnaturalness detections to determine if prints are faked by determining if they are copies.

In general, these companies implement more than a single method at once on readers- a key point in catching the wide array of potential fake/spoofed print exploits.

Beware Ambiguous Claims

Not all 'liveness detection' methods are equally effective. For example Apple's Touch ID was almost immediately fooled (upon release) by

a copied fingerprint spoof. Apple updated the sensor with 'liveness detection software and algorithms' (unnaturalness analysis) in subsequent models. However, the same spoof method proved effective again, even after these updates. In the case of Apple's fingerprint sensor, spoofed or faked prints are still a risk with software methods alone.

In general, detection methods that use hardware and software both are better performing (ie: Heartbeat, Dermal Resistance, and Tissue Reflection). Take note of which methods manufacturers cite they use, and if software-only (like Unnaturalness Analysis) or unclear, be wary.

Mobile Credentials (BLE / NFC / Apps)

One of the biggest trends in access for the last few years has been the marriage of mobile phones and access cards.

We examine:

- 4 key management problems
- 2 practical problems for users
- BLE vs NFC vs Apps Comparison

Mobile Credentials Are Slick

At a basic level, using mobile phones or tablets as credentials to open doors has a big cool factor. Take this simple demo of one setup below:

Note: [Click here to watch the video on IPVM](#)

In simple terms, instead of ringing a card, fob, PIN, or fingerprint at a reader, a user flashes a phone and the door is unlocked.

Based on the rather personal value of phones, the idea that they accompany users like keys, wallets, or ID cards and they are protected (ie: not easily lost or misplaced) items make them good potential card replacements.

4 key management problems

However, the transition is not a simple one, especially for commercial access control. A range of credential and access control management issues crop up not often issues with traditional credential methods. These include:

Cards Are Cheap

Mobile phones, even inexpensive ones, are roughly 20X - 40X the cost of a card. And the cost of maintaining a phone is much higher, requiring frequent recharges and software updates while a card remains very inexpensive and essentially free to maintain once issued. If a card breaks or is lost, the employer reissues a \$10 piece of plastic, where if a phone breaks or is lost, someone must pay hundreds of dollars to replace it.

BYOD Is Awkward

In most cases, employers will not be buying employee phones. Therefore, 'Bring Your Own Device', or the fact users leverage their personal phones for commercial uses presents numerous problems, from how enterprise network security is maintained to whether or not phone owners are willing to permit employer provisioning and perhaps management oversight on personal devices.

Ongoing Service Billing

Another fundamental issue is what happens if the phone bill is unpaid? Do service interruptions remain the responsibility of employees, even if they cannot enter work buildings as a result? Or will employers administrate service payment? Either way, the question leaves a new policy to be established not otherwise needed if mobile credentials are not used.

Physical Revocation Uncertainty

Also, unlike plastic credentials that can be turned in and physically repossessed when employees leave or turn over, mobile credentials must be remotely invalidated on a device that may remain unseen. While not a

big practical risk, uncertainty may remain for uneasy managers whether or not a device based credential is truly invalidated in all locks compared to a card that can simply be confiscated or even destroyed.

2 practical problems for users

And in contrast to 'soft' management issues, differences between plastic cards or fobs and mobile devices create 'hard' physical issues as well, including:

Awkward or No Picture IDs

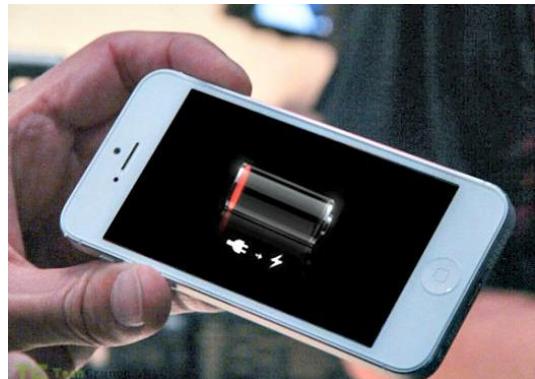
Unlike physical cards that are often printed with the user's picture, name, and other basic identity details, these are very often hidden or obscured by phones. While a user may be able to present a picture from a phone's memory on request, the simple factor of verifying identities at a glance from a picture ID card are lost.

Technology Limitations

And the range of technical issues that can go wrong with a mobile phone cannot be easily dismissed. Even problems as basic as battery life are issues with phones, and their ability to transact credentials compared to unpowered credential fobs or cards:



Indeed, battery power, operating condition, reliable function, and even multi-tasking demands are mitigated issues with cards. While users may need to discontinue phonecalls or other operations to trigger doors open with



BLE vs NFC vs Apps Comparison

In terms of formats, three common methods of mobile credentials are used in access:

- BLE (Bluetooth Low Energy)
- NFC (Near Field Communication)
- App Based Credentials

IPVM has a number of detailed updates regarding each types, frankly discussing the Pros vs. Cons of each format:

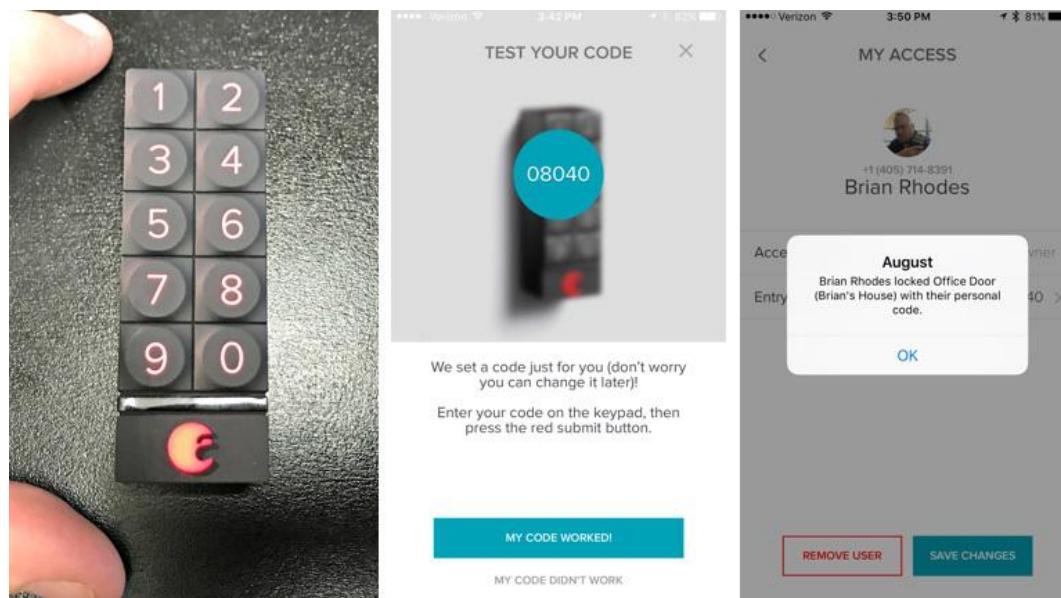
BLE (Bluetooth Low Energy)

While a relative late-arrival to the mobile credentials market, BLE is now the most common method used. The uptake is due to the relative universal inclusion of BLE in mobile phones, and therefore a near-compete compatibility with field readers regardless of phone type is appreciated.

Another key benefit is that BLE licensing costs are free or low cost compared to NFC, and manufacturers expend little money to produce BLE compliant gear regardless of volumes sold.

In terms of weaknesses, BLE requires device power to transmit, so dead phone batteries are a showstopper and mandate provision of backup credential methods.

BLE has become the most common method of remote credentialing, given reliable engineering standards definition and low/no app licensing costs. Many consumer grade products like August, Kevo, Lockitron, and other smartlocks use BLE to connect credentials, including keypads:



We outline BLE in depth in our NFC vs BLE For the Future of Access Control note.

NFC (Near Field Communication)

Once the mobile format darling, NFC was the method credentials giant HID Global elected to build out as their enterprise/commercial credential method of choice. While developments like HID's 'Twist and Go' Access Control are not limited to only NFC, HID has prioritized ways to make NFC even easier to use.

In terms of strengths, NFC has several, including sidestepping the limitation of phone power to use a credential. Once an NFC chip has been encoded as an access credential, it can be used in a passive mode and field energized by readers.

However, the cost of NFC is high in terms more manufacturer licensing to use the format. While HID appreciates significant adoption 13.56 MHz iClass formats that make licensing easier to demand/ justify, no such critical mass exists for HID NFC.

In terms of pros and cons between NFC and its closest competitor format BLE, the chart below clarifies positioning:

	NFC Method	BLE Method
Ease of Use	+	+
Range	-	+
Cost	-	+
Security	+	+
Power	+	-

The overall commitment to NFC has caused HID some trouble as success has not matched expectation. Indeed, NFC's floundering was a leading citation in the [Troubles Behind HID's CEO Ouster](#).

App Based

An emerging method is using an app or piece of software to trigger a door unlock directly rather than turn the phone into a credential. The app

method first was seen in several consumer-grade offerings like [Lockitron](#), but has crept into commercial platforms like [Kisi](#), [Brivo](#), Infinias, and others.

Using this method, phones bypass talking to door readers completely, but rather directly interface with networked door controllers. This interface requires substantial app development work that is phone OS specific, and also requires that customer networks permit remote access through firewalls to door controllers. For these reasons, we do not expect to see a strong uptake of app-based mobile credentials, but it remains a differentiator among those who offer it.



Worst Readers Ever: Keypads

One type of access control reader wins the title "Worst Choice" - the common keypad. When used improperly, keypads will let people through locked doors almost as if they were unlocked. Despite significant drawbacks, these devices are still one of the most popular choices in access today.



Operation Described

The function of keypads in access control is dead simple. The door or gate remains locked until the user enters a valid combination string, usually a sequence of numbers. Most access control applications assign each user their own number, called Personal Identification Number (PIN). Unless the user enters a valid combination, the opening remains locked.

Why Keypads?

If these input readers are so terrible, why do people use them? The single biggest 'pro' in using keypads is that no external credential is required. There are no cards or fobs to buy, fingerprints to enroll, and template records to manage. A user is given an access code that is presumably memorized or included in other documents, and nothing else is required.

The lack of external credential results in a lower operating cost relative to 'credential based' systems.

The Problems

Despite being one of the oldest and most used access readers, keypads have huge vulnerabilities. Worse still, it takes no special tools or skills to exploit these problems. While individual units may be better, or even worse, than others at these shortcomings, the biggest problems are:

- Revealing Buttons
- Snooping Eyes
- Sharing is Easy

In the sections below, we examine these issues and address how they undermine even the best access control platform and most secure locks.

Revealing Buttons: Keypad buttons wear and collect dirt over time. This is a huge problem, because only the buttons needed to gain access are the ones typically showing proof of use. Take the two examples below:



The left unit has buttons that pick up dirt and grime from user's fingers. At first glance, only four buttons show this soil, but even the most inexperienced intruder would likely associate the physical location of the

keypad with a common characteristic of the area, the US mailing Zipcode. Simple guessing and less than 5 minutes of challenges will open this 'secured' door. Soiled buttons, even when representing a 'random' number, reduce the potential combinations from tens of thousands to a few hundred, and likely combinations (address/phone/apartment numbers) may take seconds to narrow down.

Likewise, wear is obvious in the example on the right. However, instead of grime, notice the keypad is constructed of high-grade stainless steel or aluminum. Despite the extra expense of a unit built with 'cleaner' buttons, you will notice the unused buttons are dull while the buttons most often touched are shiny. In this case, guessing the combination is almost instantaneous.

Snooping Eyes: Even when evidence of prior combinations is not obvious, users can be watched entering their codes. Unless a user is deliberate in shielding their fingers and the keypad while entering a PIN, even a casual observer can note and memorize the code. A more determined intruder may even use long range optics or even 'exotic' thermal cameras to snoop out valid combinations:



PIN Numbers: Easy to Snoop / Steal / Share

Sharing is Easy: Even if 'passive' means of gaining a code are difficult, a huge vulnerability almost impossible to mitigate are users sharing codes outright. It may seem like an easy solution for an inconvenient circumstance, but sharing a unique PIN with just one other person means that 'access control' is lost.

Overcome the Weaknesses

Regardless of the vulnerabilities, keypads are installed in droves in modern access control systems. With careful attention and active management, the inherent risk can be minimized. The steps include:

Clean and Maintain Units: Wipe away oils, grime, and even 'temporary' impacts like snow. Installing keypads inside of hinged enclosures may help, but physically inspecting the buttons, keeping them clean with a mild solvent (rubbing alcohol or ammonia), and inspecting the buttons for damage and wear will go a long way in preserving security. However, all the additional effort results in a maintenance cost not needed by other credential types like contactless cards or biometrics.

Routinely Change PINs: One of the biggest failures of keypad users are that PIN assignments never change. Over time, the user's sense of responsibility to keep the number secure slips. The best and most authoritative method of remedying loose control of PINs are simply to change them on a routine basis. The frequency of changes depends on the population of users, for systems with less than 100 PINs, changing twice yearly helps refreshes the value in user's minds.

Multifactors: Another key method of beefing up keypad security are to combine them with more than one credential. For example, requiring users

carry both credential cards AND PIN combinations has the added effect of ensuring that neither lost/stolen cards OR shared codes can be individually used. However, the penalty for adding addition factors manifests itself in addition time to credential through openings and issuing/maintaining secondary credentials.

Scramble Keypads

Some keypads are more secure than others. A version called 'scramble pads' or 'random pads' do not display numerical digits in a predictable "1-9,0" orientation, but instead randomize the values every time they are used. The randomness mitigates the 'button wear' vulnerability, and evenly distributes wear among all buttons. Two common types are shown below:



Pros: Randomized orientation of digits each time a user punches in a code, cannot be viewed unless directly in front of the unit.

Cons: Very expensive (~\$900 - \$1200, compared to <\$200 for 'non scramble' types) and not always supported by the EAC system.

Hotel Access Control

Hotel access control seems to work magically. Unlike electronic access control systems used in commercial security, doors in hotels are not typically connected to a central server to confirm access.



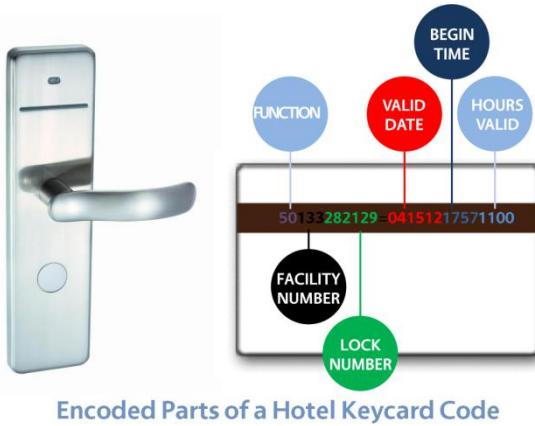
How does it work then? How can the hotel assure that cards are used properly? We cover:

- Keypad Overviews and Prices
- Keypad Magnetic Coercivity
- Hotel Door Lock Price
- Why Hotel Cards are Smart
- Protecting Against Unapproved Access
- Advantages of Hotel Access Systems
- Advantages of Enterprise Systems
- Hotel Access Security Concerns

Keypad Overviews and Prices

In the hospitality industry, 'key card' systems are typically designed using older mag stripe technology. A 'system' is composed of individual, non-networked door reader/locks, a card programmer, and encoded access

cards. The central enrollment workstation, usually at the front desk, encodes a keycard with common access data.



Encoded Parts of a Hotel Keycard Code

Among typical values are:

- Function: a number used to classify the keycard as a 'guest card', 'Master Key', 'housekeeping card', or other type of role. 'Guest cards' typically open one door, while a 'Master Key' code may open them all.
- Valid Date/Time: the time period a card is able to open a lock. This may also include a 'begin time' to calibrate lockset with system time.
- Lock Number: a unique ID value specific to the lock/room the card opens. This generally limits opening to one door per guest card.
- Facility Number: a unique code that identifies the particular property/floor/wing a card is encoded for. This prevents using the card for 'Room 123' at multiple facilities.

The door lock relies on the card itself to determine when it should unlock, so the system itself is essentially not networked and each lock is 'updated' and makes an access decision only when a card is presented.

Keycard Prices

Keycards must be cheap for these systems to make economic sense. Unlike brass door keys, keycards must be disposable or cheap enough to discard after a single use.

The most common types are CR80 size cards that cost around \$0.20 - 0.50 per card. This standard size measures 3.375" x 2.125", the same size as a credit card, and are typically made of inexpensive PVC plastic. In some cases, the cost of these cards are further subsidized as advertisement space by marketing incentive programs, local restaurants, or attractions nearby a hotel:



Keycard Magnetic Coercivity

A key trait of these credentials: the data stripes on these cards are a 'softly' encoded low coercivity mag stripe compared to more permanent types of credentials like contactless smartcards.

While this may result in the periodic 'demagnetization' of these cards if subjected to even mild magnetic sources, this attribute is often presented as a security enhancement in the form of 'short service life' of the issued credential. The physical card encoding method provides the added benefit of expiring after a short time, often a few days.



Hotel Door Lock Price

While the price of door locksets can vary greatly depending on design and finish, 'basic' units can be purchased for less than \$200 USD. Some popular models used in 'budget hotel' chains sell for less than \$75 USD. In contrast, enterprise-grade commercial electronic access control systems often cost upwards of \$1000 per door.

In general, door locks are designed to fit only the most typical door types using cylindrical or mortise cutouts. Unlike other forms of electronic access control, hospitality systems only work with a specific type of door and cannot be adapted to multiple types.

Why Hotel Cards are Smart

The biggest single difference in operation between 'hospitality' and enterprise EAC systems is the role of the credential.

In a hospitality system, the card read issues an encoded command to open the lock. A hospitality door lock has no networked understanding of how valid a credential may be, it only opens when the card being presented 'tells it' to open. The credential encoding contains all decisions and data needed to activate the lock.

In contrast, an enterprise EAC system only uses the credential to validate a request for access. The credential itself does not issue a command to open the door, it simply identifies the holder against an 'approved' dataset for entry. The networked portions of the reader confer with a central database, and then actuates hardware or denies entry based on that database. Because the door reader is networked, a credential card can be 'turned off' or disabled immediately.

Protecting Against Unapproved Access

A common question that arises with hospitality systems is "How does the door know when to deny my card?" Given a normal check in/check out interval, this answer is determined by the 'valid date range' of access encoded on the card. When the check out date is reached, the encoded data on the card is read as 'invalid' beyond a certain point. However, for dynamic situations, like unexpected early check-outs or extended stays, employee cards play a vital role. To accommodate for these situations, it is a common requirement that cards for the housekeeping staff are 'refreshed' every day, and the 'internal' rules in a hotel door lock are updated daily when the housekeeping staff insert their cards while making their rounds.

Functionally, employee cards are not constrained by the same access rules as guest cards, and can be configured for indefinite access. However, a common feature of hotel locks is the 'mechanical override' deadbolt that disables the external card reader when thrown. For these circumstances, it is common to see a mechanical, keyed door lock in the lever that allows access in an emergency.

Advantages of Hospitality Systems

The biggest characteristic of hotel cardkey systems are they are inexpensive to purchase, maintain, and operate. Despite the rather 'high tech' impression these systems give guests, programming a new card and handing it to a guest is easy enough for inexperienced clerks to manage, and because of their disposable nature can simply be thrown away rather than forcing 'key management' like traditional systems.

Other advantages include:

- Limited cardholder rules to program
- Easy to invalidate cards by reprogramming lock
- Can be completely 'turned off' by throwing mechanical deadbolt from inside room
- Mechanical override keys allow emergency access at all times
- Typically, door hardware logs up to 200 - 500 events allowing for forensic investigations as needed

Advantages of Enterprise Systems

However, traditional electronic access has key benefits for access management and user security that hotel systems generally don't:

- Multifactor authentication or biometric support
- Ability to program multiple access schedules and access locations
- Credentials can be immediately revoked or 'blacklisted'
- Doors can immediately be 'locked down'
- Credentials are used on a semi-permanent basis, and carry multiple credentials
- Hardware is not typically powered by battery packs, and is more reliable and cheaper to maintain
- Many thousands of log events stored in controllers

Hotel Systems Use Closed Resell Channels

Hospitality System manufacturers sell and install their own product, often bypassing the traditional integrator channel. This business model is justified for several reasons:

- Margins are very low, typically beneath the profit threshold an integrator will pursue.

- On the flip side of the coin, the manufacturer is able to control pricing. These systems depend on the 'RMR' of replacement keycard orders, and as a result they sell the door hardware and installation labor near cost.
- Hospitality chains typically treat 'keycard systems' as 'supply items', and would rather buy replacement products (cards, battery packs) from negotiated pricing programs from hospitality supply distributors, rather than security integrators.

Hotel Access Security Concerns

Several recent incidents have magnified the risks of hotel access systems compared to enterprise access. Take this example, where a careless or clueless clerk encoded every guest card with a 'Master Key' function, essentially allowing a single guest to open every door:

Note: [Click here to watch the video on IPVM](#)

The risk described in this incident can be avoided, but not completely mitigated with hotel access systems. With a fully networked enterprise access system, such an error could immediately be corrected if made, and the door lock itself configured to simply not open or remain locked to outside users until the problem is addressed.

Conclusion

While familiar to most, hospitality access control is not a market segment typically serviced by the security integrator. While exceptions certainly exist, the reasons for this are the limited profit opportunity and high service attention these systems represent. In general, the security

approach of traditional 'hardwired' access control is seen as 'overkill' and complex compared to the low cost, purpose built alternatives found in the hospitality market.

Controllers & Management Software

Access Control Door Controllers

Access Control systems may have hundreds of parts, but door controllers are in the center of them all. While these devices are often buried inside steel junction boxes or hidden inside drop ceilings, they are the central component that ties everything else together.

Which Controller Do I Pick?

Unlike mixing and matching controllers between manufacturers is not like selecting cameras and VMS software. Unlike video systems, access control systems require proprietary equipment at the door that functions with the head end panel or server. As a result, there is no selecting between different manufacturers for controllers, but a manufacturer may offer a range of controller options depending on the number of doors it is designed to control.

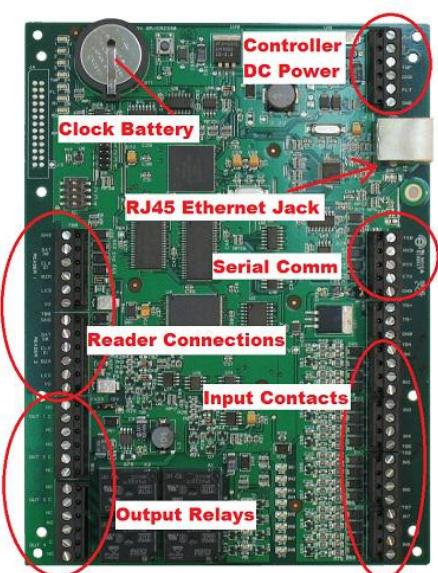
The Key to the System

Door Controllers are common to most every access system, and primarily consolidate all other devices into one spot. Every reader, sensor, and lock must be tied into 'the system' and the controller is where that happens. Whether it is called a 'controller', 'door module', or 'access computer', the controller has one function: bridge the gap between software and hardware.

While the forms the controller takes vary based from system to system, they perform the same task and are generally installed close to the door being controlled. Depending on component design, the controller may be designed in one of the following ways:

- 'Can' Enclosure Type: The 'traditional' controller a printed circuit board housed in a small electrical enclosure or 'can'. The box is typically wall or ceiling mounted above a door, and all wiring passes through knock-outs in the can to terminal blocks on the board.
- Standalone Device: A newer controller form factor, the shape closely resembles an analog video encoder or small appliance, where the terminations of all connected components are made into a self-contained box. This form factor is common with single door controllers and managed access systems.
- Combo Reader/Controller: Sometimes the credential reader is integrated directly with the door controller in a variation of the 'standalone' type. However, while offering cost savings due to decreased installation labor, this type of architecture often is a security liability, with the vulnerable controller being mounted along with the reader on the 'unsecured' side of the door.

Regardless of form factor, the features of a controller are similar. In the image below, we have marked the common 'tie-in' points between other access control components and the door controller:



In the sections below, we group and describe the primary features and common integrations of a controller, including:

- Communication: How does the controller communicate with the 'master panel' or server at the head end?
- Inputs: Which types of devices feed information to the controller?
- Outputs: Which types of devices are controlled by the controller's logic and system commands?
- Power: How is power handled by the controller, and how are attached devices powered?

Communication

Like video surveillance, both analog and IP versions of controllers are available and used. However, unlike video, the migration to IP has been much slower due to limited enhancement to move IP. Regardless of how they communicate, door controllers typically offer the same basic function, and connectivity is a simple buying preference for the customer.

- Ethernet: Like IP video cameras, controllers can be built with RJ45 ports so they can be connected to LANs like any networked device. However, even if a controller is networked, it may not use TCP/IP addressing and may not be accessible through onboard web-server. In some cases, ethernet connectivity is simply to eliminate running a redundant network. Also, while becoming more common, not all access systems offer controllers with ethernet connectivity and the feature is subject to confirmation on cutsheets.

Increasingly, '3rd Party' controllers are becoming popular. The manufacturers of these particular ethernet controllers sell their devices for

resell by access management software companies, or as single/small system standalone devices through standard distribution or even public internet distribution:



Ethernet Networked 3rd Party Controllers

IPVM has covered several of these IP controllers in default standalone configurations, including:

- [Testing Axis Access Control](#)
- [Testing HID Edge Solo](#)
- Serial: Using RS-232, [RS-485](#), and Weigand has been the mainstay communication method of access controllers for decades. Often, communication with other devices is handled through directly connecting devices to the controller by way of a dedicated 'cabling harness' that is manually punched down or terminated directly to control boards. Unlike an ethernet connected device, troubleshooting serial connections involve more than 'ping' commands, and chasing down issues often takes place with a [multimeter or continuity tester](#).

Even if an access system is installed as 'serial', it still can be configured to use LAN cabling with the addition of 'Device Servers' not unlike video



Serial Device Webserver

baluns. While these small devices cost ~\$100 per end, they can be used to bring serial-only controllers onto the LAN to communicate with 'master panels' located offsite.

Integration between the Access System and a VMS system typically takes place at the 'main controller' panel that is networked much like a DVR unit is integrated with a VMS. When an access system is ethernet networked, it often is to take advantage of existing LAN cabling, to use a cloud-based 'hosted' solution, or to eliminate running a proprietary serial-type network that cannot be maintained by in-house IT staff. We look deeper at the contrast between serial and ethernet access systems in our 'IP Readers vs. Control Panels' report.

Inputs

The purpose of inputs are to 'feed' information into the access system. The number and types of inputs connected to the controller vary, but all controllers accept the basic types listed below:

- Readers: The most exposed, public facing access control component is the credential reader. Usually the reader is mounted on the 'unsecured' side of the opening, and potentially exposed to bad weather, vandalism, and is vulnerable to damage. Aside from keeping the controller secure, a detached reader is configurable according to the type of credentials being read, the mounting surface, and the read range, and in most cases the reader is a standalone device connected by a 6-conductor style cable. For more details, catch our 'Selecting Access Control Readers' guide.
- Contacts: Anything from simple contact door closures to PIR Motion Sensors are connected to controllers to feed 'system status'

information to the controller. For example, a 'latch monitor switch' is connected to give the access system feedback on whether a door is locked or not, and door contacts are used to feedback whether a door leaf is in the closed or open position. The range and types of sensors connected to a controller may be determined by code, but functionally are limited only to opening or closing a circuit.

- Overrides: These type of controller connections include "RTE" or 'Request-To-Exit" devices, use to manually override locks in order to accommodate free egress.
- Other Systems/Devices: Any number of other devices, including video surveillance cameras, light switches, or perimeter intrusion beams can be connected to door controllers to provide input signals to access systems. The fire alarm system is typically wired into controllers so that a fire alarm condition will override the locks in an emergency.

Outputs

The purpose of outputs are connecting devices controlled by the access system. These devices traditionally are include door locks, but there is a huge range of integrations possible. We go into detail below:

- Locks: The most common output example are locks like electric strikes, maglocks, and other types of electrified hardware. An output signal interrupts the 'locked' state of the hardware to an 'unlocked' state based on a successful credential read. The controller is the device that interprets a valid read and applies logic to unlock the door.

- **Sirens/Lights:** Controllers can also be wired to chime sirens or energize strobes based on inputs. Announcer can be wired to sound when a door opens, or lights can be wired to energize as someone passes through an opening.
- **Other Systems/Devices:** Like input connections, output options are endless, and anything from gasoline pumps, high-voltage machinery, and VMS systems can be triggered and controlled by access control outputs. A common output integration is the triggering of a surveillance camera to record an opening every time a credential is read.

Power

The final system wired into controllers is power, commonly by way of individual power supply, proprietary power distribution unit (PDU), or by PoE connection. The type of power used by controllers is limited to low-voltage AC or DC, and in some cases may be passed-through the controller to power output connected devices.

Passing-through power to devices is a matter of careful consideration. Not all devices are designed to be powered by the controller, and in cases like maglocks the output power may not be sufficient or reliable enough to provide power. The 'power budget' passed through by controllers is often less than 650 mA, and a single maglock or reader can consume the entire resource.

Host Bound vs. Independent

The access control system often must be a 'zero downtime' system and doors must always function. In many enterprise-level access systems, the

controllers function independently of the main panel even when communication is lost. This advantage means that a system will operate without interruption according to current configuration regardless if the network is up or not. Most controllers are designed to hold a quantity of transaction data in memory often into the tens of thousands of records until connectivity with the main database is restored.

In contrast, 'host bound' access systems rely on constant communication with a main panel in order to operate. The 'door controller' in these systems is not a true controller at all, but rather an 'input/output' module to tie other devices into the system.

Controller Footprint

The sizing of controllers is typically determined by the number of doors they control. Common sizes are single, double, four, and eight door models. While models supporting a greater number of doors are available, they are not common due to the cost of cabling so many doors to a single device becomes costly.

The number of reader inputs a controller supports is not always equal to the number of doors it can control. Many designers can mistakenly assume 'one reader per opening', however high security applications often require two readers - a 'read in/ read out' application that still only supports a single opening schedule or range of access levels.

Controller Compatibility

In general, access control systems are steeply proprietary. It is uncommon to reuse controllers from one system to another (with notable exceptions like Axis, Mercury, and HID). Furthermore, there is a risk that existing door

controllers become obsolete during the course of system upgrades.

Reusing controllers outside their current generation of access system is not an option. While other devices like locks, sensors, or even readers may be reused, the controller itself is often relegated to the trash heap.

All-in-One Locks

While not strictly door controllers, standalone electronic access control locksets often feature the same integrations and control available to door controllers but tied into a package that includes the lock, network interface, power supply, and even door position switches.

Increasingly, 'wireless locks' are being promoted by access companies as the least expensive way of adding networked access control to doors difficult to reach with standard wired networks.



While the door controller component may be factory integrated into the lock, it essentially is still there performing the same functions (even equipped with the same firmware) as discrete door controller devices.

Access Controller Software

Properly configuring access controllers software is key to a professional access system.

These devices have fundamental settings that must be configured appropriately, including:

- Unlock times / extended unlock times
- Door Hold Open Alarms
- Request to Exit Inputs
- Card Formats
- Reader / interface type
- Input / output devices
- Tamper switches

Configuration Options Defined

The major settings that must be customized to every opening include:

Unlock Times

Given that opening sizes and spacings are different, and locks they use need to accommodate the variation, the main setting used to adjust performance is how long a lock is powered/unpowered or unlocked.

Because it takes time to register a credential and then walk to or pass-through an opening, this setting is central in making sure the opening is only unsecured long enough to allow one user to pass through before becoming relocked.

Extended Unlock Time

This variation on basic unlock time is generally given to specific credential holders based on special needs (like wheelchairs) to job responsibilities (like delivery people). Users flagged with 'extended unlock' times have a longer period to keep doors open before they are re-locked or 'held open' alarms sound.

Door Hold Open Alarms

Because open doors are not secure, access systems generate 'door hold open' alarms to notify operators when doors remain open for too long. If not configured, the system will not physically prompt operators to close or troubleshoot potentially risky situations.

Supported Card Formats

In general, controllers need specific drivers or interfaces to properly interpret information from attached readers. While controllers almost always support Wiegand or OSDP, support for other proprietary types may be available or needed by specific access systems.

Request to Exit Inputs

Some types of locks (ie: Maglocks) and some openings incorporate Request to Exit devices that allow users to override door locks without using credentials. Because these devices only need to interrupt the lock temporarily, the sensors used to manage these activities are connected to the controller and not the lock directly. The controller allows an RTE sensor to trigger an unlock, but the controller also restores the lock and opening to a normal state after a short period has expired.

Tamper Switches

In addition, a variety of nuisance and tamper detection inputs must be configured when, how, and who receives notifications when they happen. In general, controllers are useful for taking simple contact closures or openings and sending emails, SMS, or even VMS alarms when someone is disturbing access equipment.

Configuration Screen Examples

Despite the wide variety of door controllers used by access systems, the method of configuring them and even the terminology used to describe settings is generally similar. The sections below show four common controller examples:

- HID Edge EVO
- Axis A1001
- Mercury Security (EP-1501)
- Hikvision 260x Panel

These units are 3rd party models detailed in our [Axis vs HID vs Mercury Access Controllers](#) note, and while totally independent of each other, configure similar fundamental variables. In most cases, the underlying management platform can always be used to configure these settings, although some web based or standalone units let you configure them directly on hardware.

HID Edge EVO

First, an [HID Edge EVO](#)'s settings are located under the 'Door Parameters' tab:

Door Parameters

* Required

Edge Solo Door Name:	HID Edge Solo	The name of the door.
Unlock Time (1-1620 sec):*	6	The amount of time the door is unlocked during a grant access.
Extended Unlock Time (1-1620 sec):*	19	The amount of time the door is unlocked for a cardholder needing extra time.
Door Held Time (1-1620 sec):*	37	The amount of time the door can be held open before an alarm occurs.
Unlock on REX:*	<input checked="" type="radio"/> Yes <input type="radio"/> No	Specifies if the door is unlocked when the REX (request to exit) is activated.
Reader Type:	Card	The type of reader.
Keypad Type:	HID	The type of keypad connected to the Edge Solo.
Electrical Interface:	Wiegand	The electrical output type for this reader.

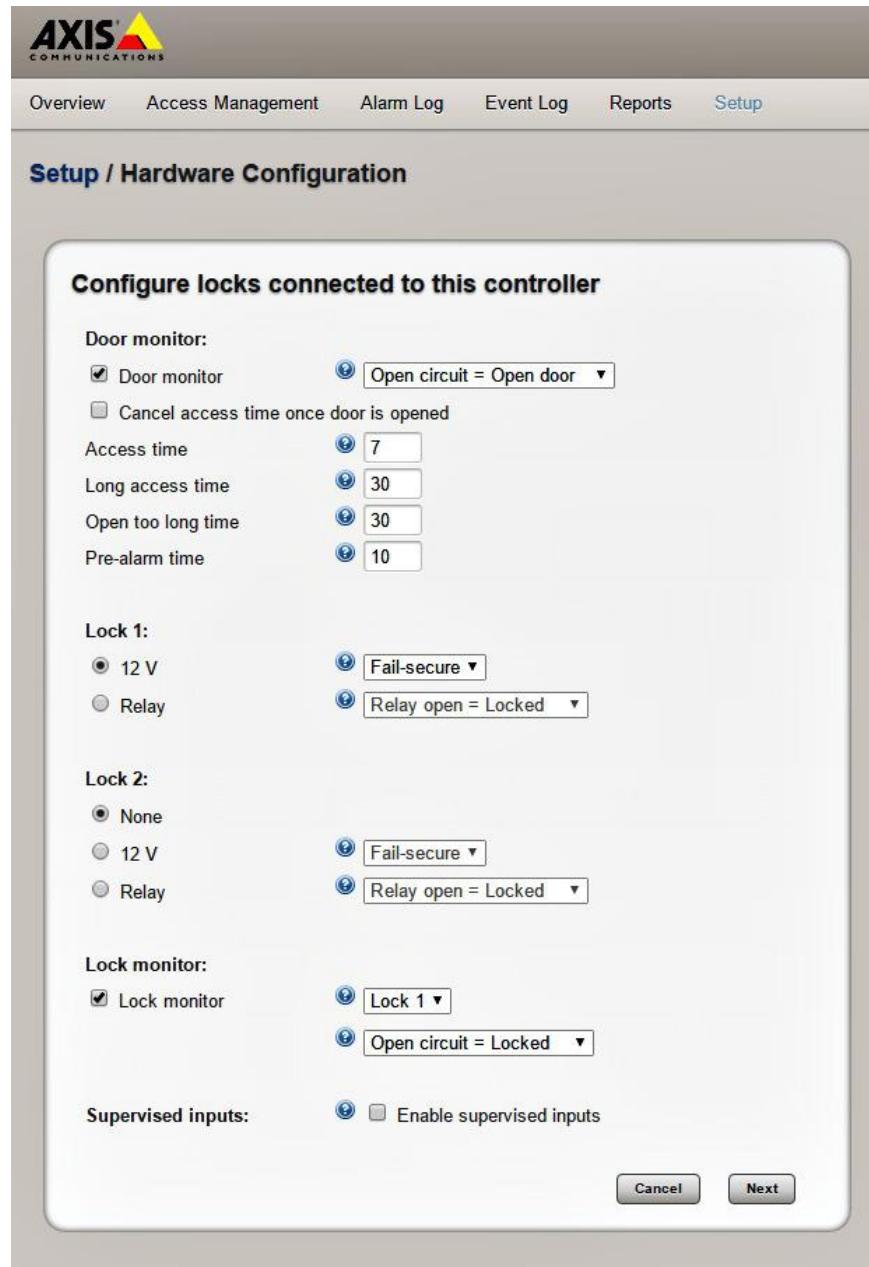
 Cancel

 Save

Note that 'Unlock' and 'Extended Unlock' times can be assigned a period between 1 second up to 27 minutes, and a brief explanation of each setting is listed beside each control. In this controller, the physical connected reader format and keypad is also configured in this screen.

Axis A1001

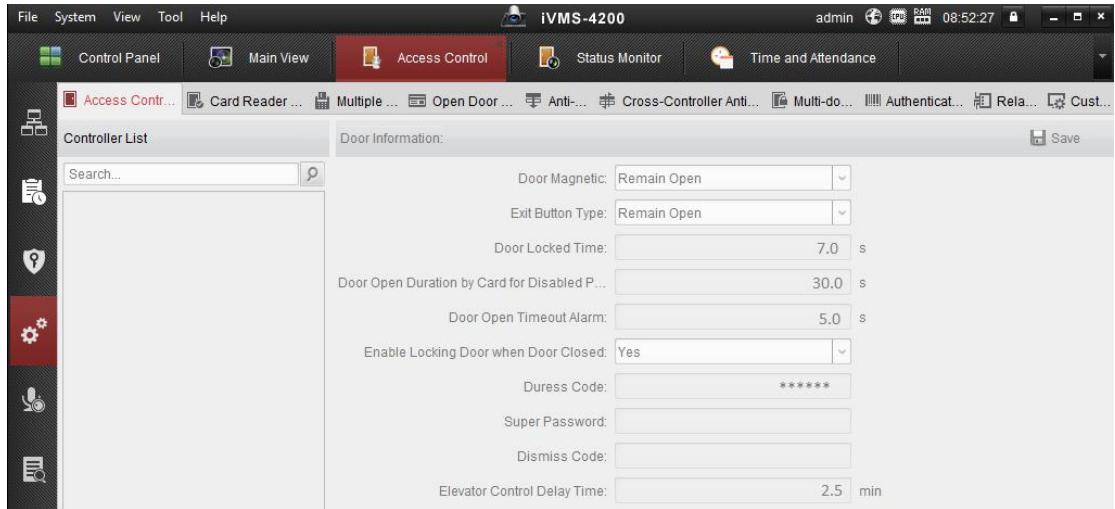
The two-door Axis controller ([test report here](#)) lists these settings under the 'Hardware Configuration' screen:



Note the same basic lock and extended unlock times are listed, but called 'Access Time' and 'Long access time' respectively. In addition, door held open (Open too long time) and nuisance (Pre-alarm time) values are also listed in this screen. Note the behavior of inputs like 'Lock Monitor' or Door Position Switches can also be configured here.

Hikvision Access Controllers

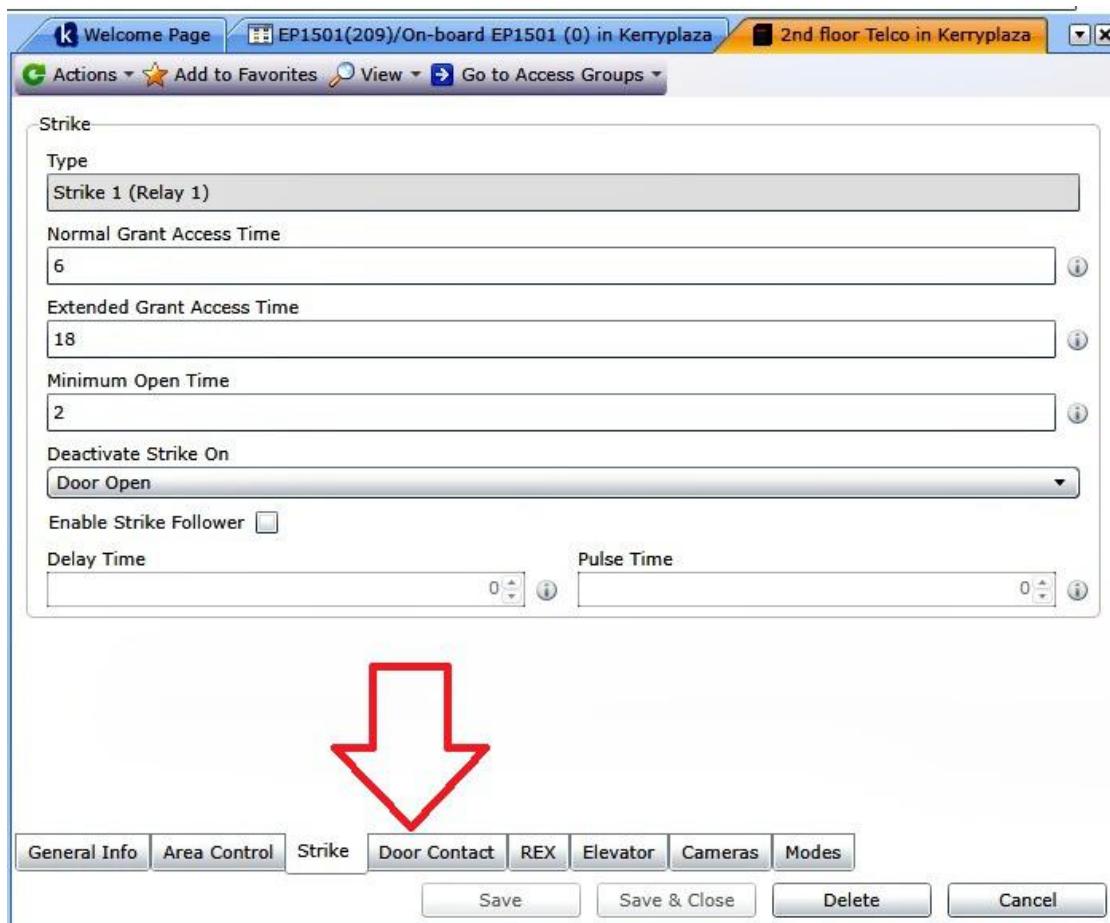
Hikvision (see: [Hikvision Access Control Tested](#)), has an interface for changing controller settings in their iVMS-4200 software:



While the label language varies, the features they control are the same as other platforms. For example, 'Door Open Duration by Card for Disabled Person' is the same as 'Extended Unlock Time', and 'Door Open Timeout Alarm' is 'Door Hold Open Alarm'.

Mercury Security Controllers

For Mercury products, the settings determining these functions are located in the partner management software interface rather than on the hardware controller or board itself:



The arrangement and total number of controls depend on how deeply the parent software has integrated the hardware controller, but in general Mercury partners all include base features like lock 'Access Time', extended access duration, and common input/output components like locks and door position switches.

Practical Setting Applications

In the real world, these settings can have a significant impact on how well the access system operates.

Unlock Times

This setting usually involves a range of times, typically seconds or milliseconds. The correct setting varies widely between opening types and

even individual users. Common access controlled openings, and the typical unlock times include:

Doors: For 'standard' swinging doors where the reader is mounted immediately adjacent to or on the door frame, the unlock time generally is set between 5 and 10 seconds. This allows enough time for someone to scan a card, turn, and pull open a door before it relocks, but is quick enough to secure the door behind the user and require that user to rescan to unlock it.



Close readers equal shorter "Unlock Time"

Vehicle Gates: The range of times needed to safely open a gate and drive a vehicle through vary depending on the type of operator and style of gate. However, considering that standoff distances can be 20 or more feet, the controller may need to close relay contacts for 60 seconds or more.



Gates need more unlock time than Doors

Mantraps: When doors are installed in series, or intended to close and lock in sequence, a controller (or series of controllers) must be configured to lock and unlock based on the status of other doors. For more detail on [Mantraps, see our note](#). Because a mantrapped door often cannot be opened until the previous opening is locked, the "Unlock Time" may be 5 seconds or less.

Extended Unlock Time

Handicap or Delivery Users: When a credential carrier uses crutches, a wheelchair, or has a job that requires passing through an opening several times in a short period, an "Extended Unlock" time is often assigned to that user, to keep the door unlocked longer than typical for convenience. For example, a delivery person may not be able to transfer all packages through a door in 5 - 10 seconds, but a period of 15 to 35 seconds may be long enough to pass through without accidentally relocking the opening.



Special Needs require "Extended Unlock"

Door Hold Open Alarms

Open doors cannot keep risks out, but if alarms sound after unrealistic durations, the access control system can quickly be ignored as a nuisance. For most openings, Door Hold Open alarms should not be configured for less than 30 seconds, and not more than 3 minutes.



However, the exact duration assigned often needs to be determined by observed use.

Hardware Configuration Options

In addition to software configuration, some attributes depend on hardware selection also. The major factors include:

- Number of Authentication Factors: Related to reader type is the combination of credentials needed to open a door. For example, even basic access systems offer an option of card, PIN, or both card & PIN credentials to open a door. The decision of how many factors to use may be limited by controller support of various credential types, and may require software configuration for production use. For a deeper look, see our [Multifactor Authentication tutorial](#).
- Input/Output Devices: The 'theoretical' range of I/O options for access may be endless, but the ratings of the relay contacts onboard the controller play a big part in how they are connected. For background on [I/O connections](#), see our note. If a range of devices with different voltages and amperages are to be switched by the controller, the may need to be grouped, terminated, or installed in 'supervised' circuits where they are switched.
- Onboard Tamper Switches: In most cases, configuring a panel or enclosure tamper contact is useful for sending an alert as it occurs. Most controllers include a tamper contact or switch onboard, but setting it up for use is often optional. Software configurations, input contact configurations, or changing jumper settings are common steps required to use these tamper switches.

Controller and Reader Wiring Example

In the video below, we give a brief overview of the other common configuration work done on readers - physical connection of components

like readers. Many controllers use low voltage phoenix connectors to physically connect components that are controlled via the settings described above.

In some cases, the settings detailed above may not be detected or recognized for configuration until the physical components are wired to the controller. This video shows how wiring is typically accomplished via simple label call-outs or even contact color coding:

Note: [***Click here to watch the video on IPVM***](#)

Axis vs HID vs Mercury Access Controllers

In the access control market, there are many software platforms, but only a few companies that make non-proprietary door controllers. Historically, the most well known two have been Mercury and HID, with Axis joining the field in 2013.

We contrast the three providers, examining:

- The offerings of Axis, Mercury and HID
- How their product models compare (with chart)
- How their pricing compares
- Which of 22 notable access platforms support each of the three (with chart)

Open Controller Options

In the access market, the number of manufacturers producing door controller hardware is comparatively small to the total number of vendors writing management software. While some companies chose to produce their own proprietary controller designs, a significant portion of the market chooses to integrate with 'open' 3rd party devices manufactured by others.

For the access control market, the most widely recognized non-proprietary door controllers are produced by three companies:

- HID Global: The credentials giant also manufacturers two major series of controllers, Edge and VertX, that with a firmware update can be added to over 10 different access systems.

- Mercury Security: While strictly an OEM partner, the hardware manufacturer produces its lines of controllers and expansion modules with a common firmware framework. Over 35 companies use Mercury designed hardware, or other hardware using Mercury's standard firmware. While endusers are unable to buy Mercury direct, the resold product is 'open' and can be used without major reconfiguration in any Mercury-based platform.
- Axis: The newcomer to the group is Axis, who to date has launched just one controller: the A1001. However, this two-door controller is built using the same VAPIX API so readily adopted by video platforms and is the first (and so far only) controller to claim ONVIF C conformance - a rather weak, but clear intention for 'open' use in other platforms.

These offerings compose essentially all the 'open' controller options in the market. Of note, ZKAccess's C3 and inBio Panels are sometimes OEMed for use in other platforms, but they are not 3rd Party in the sense they can be readily added 'as-is' and are not interoperable between platforms.

Comparison Chart

When it comes to offsets, the exercise is not as straightforward as comparing low-light domes or card readers, since the controller itself can be scaled or expanded differently according to the physical location of doors in a facility. However, in general here is how a company's offerings compares to the others:

Controller Size:	 Mercury Security	 HID Global	 Axis
1 Door	EP1501	EDGE	A1001
2 Doors	EP1502	VertX V2000	A1001
2 - 4 Doors	EP1502, or EP2500 & MR51e/MR52	VertX (V1000 & Multiple V100)	--
4 - 16 Doors	EP2500 & MR51e/MR52	VertX (Multiple V1000 & V100)	--
16 - 64 Doors	EP2500 & MR51e/MR52	VertX (Multiple V1000 & V100)	--

Features: In general, the particular features of a controller is not the limiting factor is which one is more capable or better suited for a job. To what degree the underlying platform integrates with them, and which features are supported, is however.

To that end, controller options from all three vendors are IP addressable, have onboard storage for many thousands of events and cardholders, and feature pass-thru power for connected devices like readers and strikes.

However, not all products are expandable, PoE powered, or support more than a single reader. The specific features of the controller, including output linking, exact number of records stored onboard, and expandability boards are subject to the host access management integration.

Cost Comparison

While pricing varies for each controller, the hardware cost alone may also be subject to additional software licensing. However, on a hardware only basis, pricing looks like:

- Axis A1001: This two-door controller is widely available online for ~\$520.
- HID Edge EVO: The single door controller is available from distribution with a street price of ~\$350, with options for units with integrated readers for ~\$450.
- HID VertX: The base controller and two-door expansion module is available through resellers for ~\$650, but total cost varies depending on which base controller and how many expansion modules are used.
- Mercury Security: None of these products are available as direct purchases from Mercury or through distribution. Single door controllers typical range in price from \$250 - \$400, but the final cost is often heavily negotiated and drops for projects with large door counts.

Compatibility Chart

The chart below provides a look at leading access brands, and which door controllers they work with:

IPVM	HID Edge	HID VertX	Authentic Mercury Security	Axis A1001	Private Branded
Avigilon		•	•		•
BluBOX			•		•
Bosch			•		•
Brivo	•		•		•
Cbord	•	•			•
Feenics	•	•	•		
Genetec	•	•	•	•	•
Honeywell NetAXS					•
Honeywell ProWatch			•		•
Identicard			•		•
Imron		•	•	•	
Johnson Controls	•		•		•
Kantech					•
Keri Systems			•		•
Keyscan					•
Lenel			•		•
Maxxess	•	•	•		
Milestone	C	C	C	C	
NLSS	•	•	•	•	
Open Options			•		•
Paxton			•		•
RS2 Technologies			•		•
S2			•		•
Software House					•
Video Insight			•		•

C = compatible with eligible integrated system

Notice not all platforms use third party panels. For example, major providers like Tyco's Software House use proprietary controllers, which differ and are not compatible with other Tyco access products, like the distribution access line Kantech that uses it's own proprietary panels.

Takeover Exceptions Apply

While generally possible, 'takeovers', where controllers associated with one platform are switched to another, have exceptions. One example is with Lenel's NGP panels. While near duplicates of Mercury designs (even to the point of warranting a lawsuit by Mercury for patent infringement), they are not drop-in changeovers for non-Lenel systems. In other cases, like Honeywell Prowatch, physically changing chip on the circuit board may be required.

In other cases, individual platforms may not support specific part numbers, but do others. Example: One system may not support the MR51e modules connected to an EP1501 that is does support. Or individual features (like cross-linking) may be supported at the panel in one system, but not the other. The details vary, and like all integrations, they can be more complete in some platforms more than others.

While such cases are uncommon with 'open' controllers, field verification of the component builds for compatibility is prudent.

Wiegand vs OSDP

Wiegand has been the standard access communication protocol for decades. Despite advances in credentials, and the move to IP controllers, the connection between readers and controllers is startlingly unchanged. The Open Supervised Device Protocol (OSDP) aims to surpass Wiegand, but what advantages does it offer, and does it have industry support?

Key Contrasts

Comparing the two protocols is not difficult once their function is understood. In terms of a typical access system, the data link between credential reader and door controller is key. This link is where 'Wiegand' and 'OSDP' are most relevant.

The prime features of either protocol stack in the chart below:

	Wiegand	OSDP
Reader to Controller		
Controller to Reader		
Throughput	(~37b max)	(1024b max)
Data Interface	Wiegand Only	Serial & TCP/IP
Daisy Chain Cabling		

In general, OSDP offers a 'next generation' framework for data exchange between reader and controller. Before data networking was common access control had a need for it, and Wiegand gained early and widespread acceptance among access vendors for being a simple implementation.

Wiegand Limitations

However, as systems have advanced, and especially as credentials grow more secure, Wiegand has shown to have formidable limitations. Most prominent among them:

Unidirectional: Wiegand simply pushes the data it collects to the controller and does not receive information from the system at all. In terms of changing configurations, monitoring health status, or updating security keys, the reader essentially is in the dark.

Limited Throughput: Long gone are the days where a 26bit unencrypted credential is considered ample or secure. In the wave of sweeping credential changes, the amounts of data transferred by Wiegand is very limited. Due to simple interpretation of bits via voltage change, the amount of bits that can be quickly interpreted by the controller is limited to well under 128 bits, with the credential card itself typically carrying less than 37 bits. With the advent of biometrics, smartcards, and encryption exceeding 256 bits, the amount of data to push can exceed wiegand capacity tenfold or more.

Obsolete Interface: Early on, Wiegand offered a 'open' and 'simple' method of transmission. However, with even those sizable advantages, local data networking developed in other forms, eventually finding high performing analog interfaces like RS-485 serial communication and eventually digital TCP/IP ethernet.

ODSP Key Elements

The new protocol shores up those weaknesses and expands to offer:

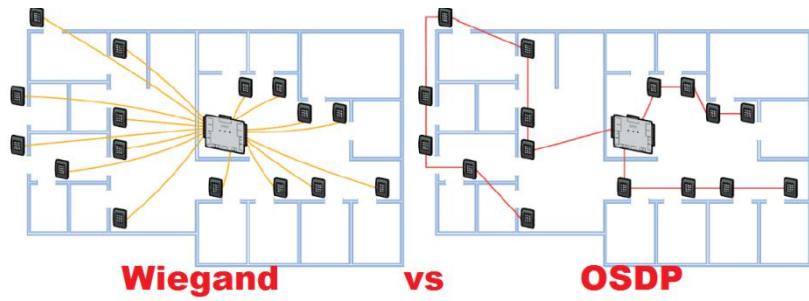
Bi-Directional: Allowing communication to travel both ways permits changes in real time, even allowing output behaviors like LEDs, Display Messages, or Sounder behavior to be changed dynamically. Depending on the reader, features like security keys or text fields can change based on the status of the system behind the reader.

Expansive Throughput: Up to 1024 bites of data can be carried by OSDP, and greater total information can be transmitted if organized in stages. This means that far more than provisional 37 bit transfers are possible as someone presents a credential (fingerprint, face, or card) to a door. OSDP not only supports a different method of transport, it organizes the information so even layered encryption can be read, only decoding the information needed to grant access, resulting in a quicker transaction.

Standard Interface: OSDP currently supports RS-485, but is poised and scalable to apply to TCP/IP as well, sidestepping obscurity and essentially using standard transmission interfaces.

Cabling Benefits?

Another notable, although not terribly useful, difference between the two is ODSP's ability to chain multiple readers together on the same cable and have them be discretely addressed. Indeed, when compared to traditional '1:1' wiring, each reader must be home run to a controller, where with OSDP strings of readers can be interconnected with a single cable back to the controller. The image below, from [SSI Magazine \(Feb 2014\)](#) is helpful understanding the difference:



This prospectively saves money on cable, although it will be a negligible difference in most situations due to discrete wiring of other inputs and outputs at the opening like door position switches or locks.

However, OSDP uses less conductors than Wiegand. Traditionally readers have been connected to controllers via 6 conductor bundles that carry power, LED behavior, sounder impulse, and ground on different conductors. OSDP only requires 4 conductor bundles and offers the same range of functions, potentially saving a marginal cost on cable.

Industry Support

While Wiegand's industry support is widespread and the 'defacto' standard, OSDP shares the backing of big players in the access market. Notably, reader and credential giant HID Global has adopted the standard, which they co-wrote with controller and interface vendor Mercury Security with support commitments from Lenel, Siemens, Brivo, Allegion (formerly Ingersol Rand) and others. The upcoming ISC West OSDP Plugfest feature several prominent access industry players:



Does It Matter?

Will OSDP replace Wiegand overnight? No, it will not. Indeed Wiegand will remain a common protocol for some systems for many years. However, with broad based support and clear operational advantages, expect to see OSDP gain traction and eventually become the basic framework used to connect readers to controllers.

Making Use of OSDP

Upgrading existing systems to use OSDP is not likely a need, unless realtime health monitoring of readers is desired. The data transmission benefits can be achieved by using proprietary, non-Wiegand formats but bi-directional communication requires additional cabling (if even supported) if not using OSDP. Some high-security deployments may find this useful but for the vast majority of systems, upgrading to OSDP is not likely compelling for the cost.

However, for new installs, using OSDP is beneficial and not likely any more costly. An increasing number of readers and controllers support the protocol and the number will likely grow in years ahead. Given the performance advantages, it makes good sense to plan systems around using the new framework rather than stay pegged to Wiegand.

Access Control Management Software

In access control, the locks, readers and credentials may be what most see but its the management software where everything is controlled.

Basic Purpose

The function of Access Control Management software is fourfold, with distinct functions and management focuses:

1. Live View: Displaying the current state of the access system; if doors are locked/unlocked, and which users are interacting with doors.
2. Door Management: Configuring every opening is critical, to ensure it opens and remains locked on schedule or depending on credential.
3. Cardholder Management: Administering all potential users for their needed access privileges, and updating those records as needed.
4. Reporting: This offers users to forensically review log details collected by the system - when and where credentials were used, and when openings were unlocked.

Essential Elements

While each management platform varies based on appearance and terminology, it contains the same basic elements. These include:

- Monitoring Interface
- Configuring Doors & Controllers
- Access Rule Creation and Application
- User/Credential Management
- Access Schedule Configuration

- Report Creator

In many cases, these elements are contained in a server or appliance separate from door controllers. System designed for smaller numbers of readers and doors may be hosted on a dedicated panel, but enterprise systems may require several servers to host the features and integrations of large numbers of doors.

Monitoring Interface

Live View allows operators to peer in to the current state of doors in real time. Exact interface features and layout vary, but most include:

- Door Events: Every time someone requests passage through a door, a lock released, or a door is opened the event is logged.
- Alarm Report: If someone holds a door open too long, forces a door open, or attempts using an invalid credential, the interface sends an alert or draws operator attention to the event.
- Lock/Unlock Controls: An operator has the option to manually unlock or lock a door remotely, often to all doors in a single 'lockdown' operation.

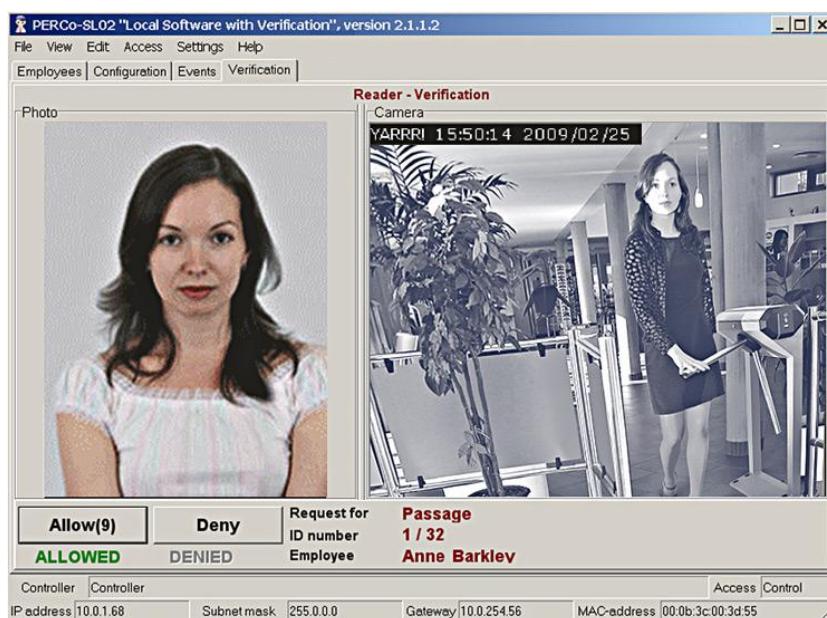
This screenshot shows how this information is typically displayed and organized, usually in a timeline of event messages:



The video below gives an overview of this element:

Note: [Click here to view the video on IPVM](#)

Video Integration usually displays live video feeds next to badge photos so operators can visually verify the person entering is valid:



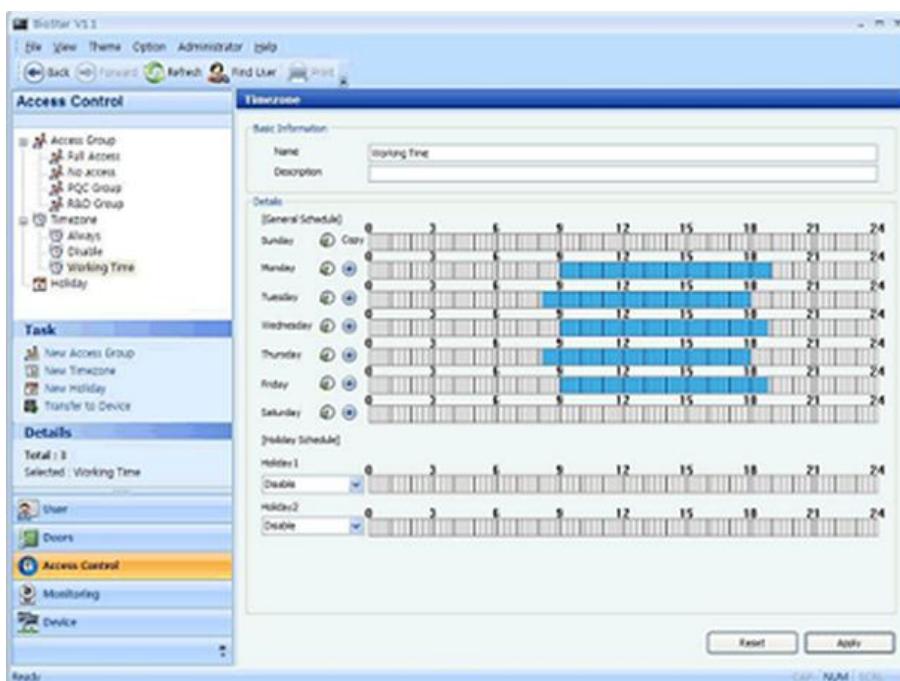
Configuring Doors and Controllers

The management platform provides the ability to add new controllers and to tweak configuration of those devices to fit each opening. Because each opening is used differently, even doors consisting of the same hardware may need to be slightly altered for efficient use. The videos below shows the 'typical' features to expect when doing these actions:

Note: [Click here to view the video on IPVM](#)

Access Rules and Schedules

The key advantage of electronic access control versus mechanical locks and door keys is the ability to restrict when and when credentials can be used. Some platforms enforce these rules against doors, while others associate them with specific cardholders. Schedules and levels are commonly configurable down to exact seconds:



Other platforms combine either option, granting a group of physical doors or cardholders enhanced security privileges. The videos below show off the basics of these features:

Access Rules

Note: [Click here to view the video on IPVM](#)

Access Schedules

Note: [Click here to view the video on IPVM](#)

User Management

Access management extends beyond just configuring doors. Every user, and the credentials they possess, are integral pieces of any system. The common user management functions headend software include:

- Adding or Changing Users
- Associating Credentials with Users
- Printing Badges

The videos below provides an overview of these features:

Adding Cardholders

Note: [Click here to view the video on IPVM](#)

Adding Credentials

Note: [Click here to view the video on IPVM](#)

System Reports

A key feature of management, querying activity logs is the equivalent to searching for recorded video. The clip below is a short overview of what to expect and how it is organized in an Access Management software:

Note: [Click here to view the video on IPVM](#)

Network & Cable

Access Control Cabling

Access Control is only as reliable as its cables. While this aspect lacks the sexiness of other components, it remains a vital part of every system.

Defining the Network

Access control systems use three methods to carry data between components:

- Ethernet, or IP-based Systems
- 'Hardwired', or Serial-connected Systems
- Wireless Systems

The scope of this post primarily is concerned with the first two types, although even many 'wireless' systems consist of wired components somewhere in the system. For more details on wireless systems, see our 'Wireless Access Primer' report for more details. While wireless systems continue to grow in popularity, access control is most often a 'cabled system' that used traditional stranded wire for communication.

Which Wire to Use?

Most systems specifically define which type of cabling to use, depending on which device is being installed. For example:

6 conductor cable: Typically used to connect Readers to Controllers, this bundle of connectors breaks down to where each conductor color handles a

Wiegand	Clock & Data	Wire Color
+DC	+DC	Red
Ground	Ground	Black
—	Card Present	Violet
Data0	Data	Green
Data1	Clock	White
Shield Ground	Shield Ground	Drain
Green LED	Green LED	Orange
Red LED	Red LED	Brown
Beeper	Beeper	Yellow
Hold	Hold	Blue

unique function of the reader. However, 'extra' functions (like reader beeper, or reader LEDs) may call for additional conductors, and items like power and drain wire are included apart from conductor count. The chart below details a wiring schematic for a proximity-style mullion reader:

4 conductor cable (2 pair)/ 8 conductor cable (4 pair): This cable is commonly used between the main control panel and door controller, and may cover long distances as a result. Door devices like PIR'Request to Exit' devices or closer controls are wired using this type. Unlike ethernet cabling standards that limit runs to 100 meters, these connections can span thousands of feet using the same type of cable. In most cases, while a range of cabling options will work, it is still best practice to employ whichever type the manufacturer recommends, as tech support and product warranties often depend on installing to specification:

Connection	Maximum Distance Communication (ft)	Cable Requirement
bright blue to SBB-R1	4000	18 AWG/2 Pair, Strd, Twst, Shld
SBB-NRI to Power Supply	N/A	18 AWG/2 Pair, Strd, Twst, Shld
bright blue to AD-300	4000	18 AWG/2 Pair, Strd, Twst, Shld
bright blue to Schlage VIP		
At 12 Volts DC	4000	18 AWG/2 Pair, Strd, Twst, Shld
At 24 Volts DC	4000	18 AWG/2 Pair, Strd, Twst, Shld
bright blue to PIM400-485-SBB	4000	18 AWG/2 Pair, Strd, Twst, Shld
bright blue to PIM-SBB	1000	18 AWG/2 Pair, Strd, Twst, Shld

2 conductor cable: This cable is typically used to deliver power to devices, like maglocks, strikes, or other accessory devices like illuminated RTE Push Buttons. It also is used to wire contact sensors, door position sensors, and to cameras for I/O linked functions.

Drain/Shielding Wires

Many door control devices are equipped with 'drain' wires that are included for use when a door exists in a 'noisy' RF/EMI environment. The

extra wire acts as a grounded sink for ambient interference around the bundle, and helps maintain transmission between reader/controller or controller/panel.

Which Gauge to Use?

Wire gauge, or thickness, is a key aspect determined by cable run distance, voltage and amperage draw. The manufacturer specifies the wire's specific gauge. The most common gauges chosen in access control are 24, 22, 18, and 16 AWG sizes. In general, greater voltages and longer distances call for larger diameter wire (lower AWG number). Each component may specify different wiring, and the cable specification may change according to total distance / type of voltage used.

Combining Cables

Unlike IP cameras where a single cable typically connects a device, an access controlled door require several different types of cables. For example, there might be a 6 conductor bundled with 4 and a 2. Here are a few examples of common combinations:

- 18/2: Lock Power
- 18/6: Reader Power/Communication
- 22/4: RTE Buttons/PIR
- 24/2: Door/Latch Position Contacts



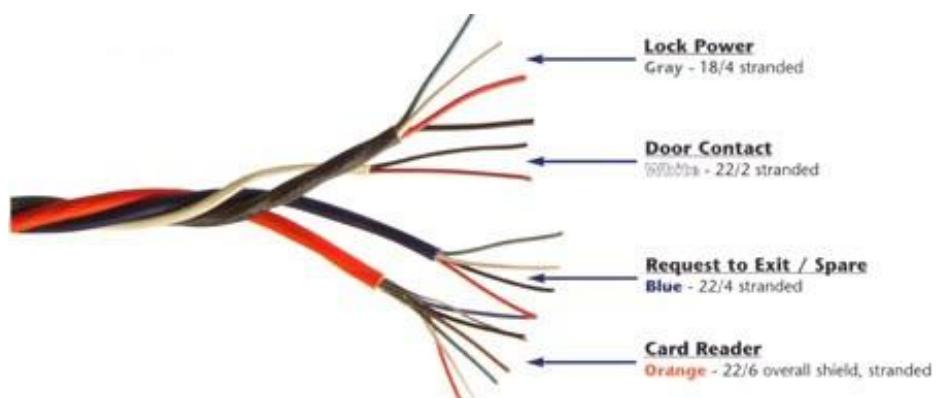
The specific configuration of cables depends on the mix of devices used at the door. However, the number of cables normally will not exceed 4 or 5

types, and in some cases multiple devices like contrats and RTE devices can be connected on the same pair.

Factory Bundles vs DIY

These combinations may be delivered as a factory bundle or combined by the installer locally.

Many cabling suppliers offer factory bundled cables composed of the common conductors and kitted at the factory wrapped together or sealed into a single jacket. The image below is an example of a bundled product and the types of cable it contains:



Bundle Pricing: While many configurations of bundle cables are available, they typically cost more per unit length than separate cables pieced together manually. Take the example below:

- 500 feet of Factory Bundled Cable @ ~\$800, or about \$1.60 per foot.

Discrete Pricing: Compare that to 500 feet quantities of individually pieced cables:

- 18/4 @ \$125
- 22/2 @ \$50

- 22/4 @ \$75
- 18/6 @ \$275

Total: ~\$525, or about \$1.05 per foot. Using individual pricing yields a savings ~\$0.55 per foot.

While straight pricing typically favors unbundled product, factory bundles reduce labor cost. A rough rule of thumb is 4 or 5 hours preparation time per 500 feet for bundling cables oneself, which saves a few hundred dollars to DIY.

Factory Bundle Pros: While more costly per unit length, factory bundled cables take no time to assemble together. Aside from improving install speed, having a single bundle of wires make hiding and protecting the cable easier than separate strands.

Factory Bundle Cons: Multiple variations of bundles are available, and proper specification is essential. Furthermore, not every door uses the same 'mix' of devices, and the bundle may change between openings. Additionally, depending on the installed location of door components, individual cables may need to be run separately from a bundle regardless.

Installation

Running cables to door and access components is frequently more difficult than standard ethernet networks. Not only are the overall number of cables greater, the locations they run to are often farther away and in difficult to access locations. Also, the construction of doors and frames vary greatly, and running cables 10 feet at the door can be more time consuming than running hundreds of feet in cable trays or raceways.

To conceal and protect door cabling, it must often be run through door and even window frames. Take the example of a common glass 'store front' type opening, composed of swinging thin framed glass doors and 'lites'. Rather than taking the shortest route from controller to components, a longer path crossing multiple panes and frames must be taken, extending overall cable lengths and installation times.

Care must be taken when drilling into frames to not break glass, and fishing cables in tight spaces is a manual and time consuming process. Take the example storefront below, and notice the cable path must cross multiple frames to reach secure mounting locations:



Other Factors

Access control cabling can encounter atypical constraints. For example, access cabling is frequently run in direct contact with metal frames, and some AHJs may require more stringent insulation specifications (e.g., thicker jacket) than standard types.

Another common issue is required penetration of firewalls to connect devices. In many cases, cabling is run to avoid drilling or cuts through a rated wall, but this is unavoidable with access control installation. Drilling through a wall may require a fire-rated connector and the use of a fire-rated sealant to backfill any holes.

Prior AHJ approval to make a penetration may be required with subsequent inspection of the final cable run. Since requirements vary by jurisdiction, checking with the AHJ is a prudent first step.

Wireless Access Control Panels

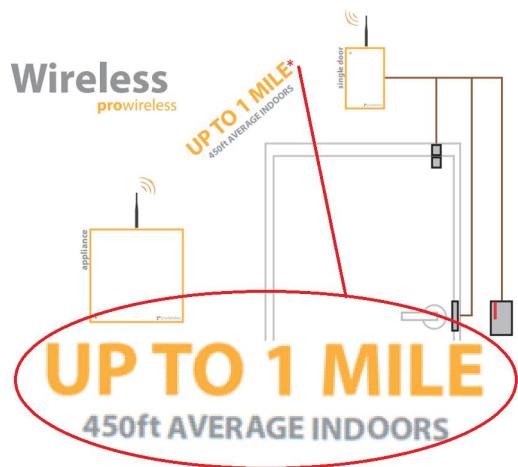
One company claims they can connect access control panels carelessly with ranges up to a mile, saving big bucks and thousands of feet of cable tying together door controllers with the main panel.



Wireless Connected

The boldest claim Prodata Key makes is all access hardware is carelessly networked together over ranges up to one mile. Additionally, each controller acts as a repeater, and the system operates using its own ad-hoc mesh network.

However, the fine print for the claim reads '450 foot average range indoors', less than 9% of the claimed maximum 1 mile range:



Why such a broad range disparity? The answer is found in the type of wireless used by the system: ZigBee. Usually reserved for home automation networks, ZigBee is a competing standard with Z-Wave that uses 2.4 GHz, low energy transmission. A significant

contributor to the range difference is the difficulty of the signal to carry through obstructions like walls and furniture. The low power and relative high frequency wavelength cannot penetrate or carry long ranges, so

indoor ranges are greatly reduced compared to outdoor, unobstructed point-to-point deployments with a clear line of sight.

Even given the fractional max range of 450 feet indoors, the distance is moderately greater than the 100 m (330 feet) limitation of typical wired ethernet networks.

Encryption Standard

With any wireless network, especially one as sensitive as physical access, security is a big concern. Prodata Key claims 128-bit AES encryption end-to-end for system data. Despite being an older encryption standard heavily exploited in whitepapers by Bruce Schneier and cryptology experts, the format still remains widely used for sensitive systems and is considered 'secure' by most standards.

Additionally, ProdataKey recommends using an optional module that writes custom encryption keys and hides door controllers from being detected by other nearby Prodata Key systems.

Technical Specifications

As far as design and installation, Prodata Key is straightforward and typical of many other systems. A main networked interface panel connects to system door controllers and bidirectional updates are synced between devices as events or changes occur. Depending on the location of the controlled doors, the system uses either single opening or eight-door controllers.

Key Details

Other notable tech details include:

- High Voltage Connectable: Prodata Key can be wired into high voltage main power without needing additional low voltage power supplies. Transforming voltage on the board simplifies power design and passes up to 2 full amps to connected devices like readers and locks.
- Limited Credentials: Prodata Key supports basic 26 - 37 bit formats, usually used by low security 125 kHz credentials. Despite the encryption emphasis for the wireless network, readers connect to controllers using weigand. More secure OSDP protocols are not supported.
- Live View Video Only: Surveillance integration is extremely limited, with management software supporting RTSP streams only. Playback or searching features are not supported by Prodata Key.
- Wired Panels Also: While wireless panels are the key differentiator, Prodata Key offers ethernet or USB connected panel options.

The management application is basic, offering fundamental controls but not advanced in terms of administration or reporting. The company's overview video below provides good detail, though notice the limited mentions of reporting, video surveillance integration, or ability to incorporate other systems into the platform:

Note: [Click here to watch the video on IPVM](#)

No licensing or maintenance agreements are required, which is pre-installed on the main panel or available as software-only for hosted or managed systems.

Price Comparison

Prodata Key's pricing and features are close to other small system platforms like Vanderbilt's BrightBlue, with the biggest potential savings coming from avoiding the cable runs between the main panel and every door. Street pricing for system components look like this:

- \$900 Main Panel
- \$450 for Single-door controllers
- \$1200 for Eight-door controllers

Prodata Key is available through national security distribution, and offers a two-year advance replacement warranty on it's offerings.

Company Profile

Prodata Key is not a well recognized access brand, and despite being founded in 2005 has not gained much traction in the access market. With incumbent access companies in business for 25 years or more, nine years is still a relative newcomer to the access market.

Moreover, Prodata Key's leadership team has limited experience in physical security. While principals do have some experience in commercial electronics manufacturing and system sales. For example, the company's CEO has prior experience at Logitech and a small physical security reseller.

However, the relative newness and inexperience of the leadership team in the access market may prove to be a disadvantage for the company's future success.

Applications

Prodata Key's wireless access panel could be a benefit where existing network infrastructure is sparse and the budget to expand it is thin,

especially where the system needs to remotely connect to far-flung doors or controllers.

The wireless panels potentially save significant costs in two applications:

- Distant Interior Doors: Running cable from main panels to remote door controllers can cover hundreds of feet. For an example door 400 feet away, eliminating this single cable run can save 25% to 40% of the total cost by cutting out \$250 to \$450 worth of cable and install labor. These savings multiply when for every controller.
- Outdoor Access Points: In the scenario of controlling parking lot gates or outdoor turnstiles, this cost saving percentage can be much bigger. Considering that direct burial cable and trenching can be \$25 to \$45 per foot, the wireless controller could eliminate \$10,000 or more for a 500 foot distance.

Prodata Key's wireless system eliminates 'extra' costs like additional media converters, conduit, physical disruption of facilities caused by trenching, or penetrating firewalls.

WiFi & Wireless Access Lock

When it comes to access control, any chance to save money on parts or install labor is attractive.

For many doors, running network cables and hanging multiple devices can run thousands of dollars. By contrast, Wireless/WiFi locks are often a simple, less expensive way to bring doors under control.

In our 2014 Access Survey, integrators noted that while still a distinct minority, use of WiFi/Wireless locks is sharply increasing, driven by ease of install and lower comparative costs. However, despite reporting growth in the segment, they also noted key downsides of using them:

- Ambiguous Network: Is it Wireless or WiFi?
- Credentials Management
- Repinning Locks
- Battery Costs
- Lockdown Feature
- Replacement Costs

WiFi/Wireless Locks Defined

By design WiFi/Wireless locks are a single major component, consisting of the a door lock, key tumbler, one or more credential readers, and an internally stored database of users and schedules in an integrated unit.

In contrast to a traditional hardwired system composed of multiple pieces that must individually be hung and wired on the opening, a WiFi/Wireless

lock can be hung rather quickly onto existing standard door lock cutouts.

The image below shows this contrast:



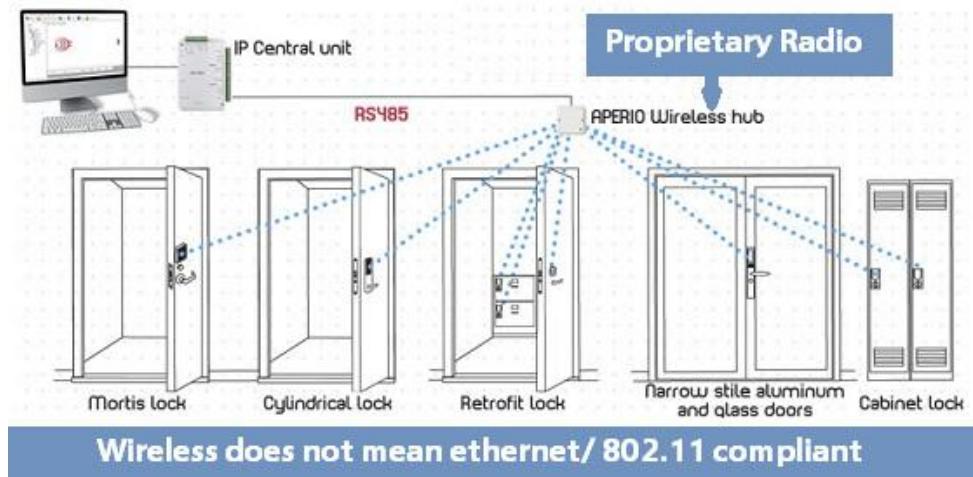
Ambiguous Network: Is it Wireless or WiFi?

However, when it comes to potential problems, it starts with defining exactly how locks are networked together. Two major distinctions are common, with units using:

- **Wireless:** Proprietary radio networks, usually in the 900 mHz range that use a MIMO style network only for lock communications and that require a system hub to be located in the range of every lock. The hubs range between \$200 - \$500 each, with coverage of about 500' in any direction.
- **WiFi:** Networks using IEEE 802.11x type connections, usually indicating a lock is given an IP address, and usually meaning a lock can use existing WiFi ethernet coverage for connectivity. WiFi access points typically range between \$35 - \$350 each, and if existing WiFi is already available it generally can be used, with the bandwidth overhead of a single lock is typically less than 15 kB per day.

Usually proprietary 'wireless' systems are less expensive per lock, but the additional cost of adding specialty radios for a separate network can

easily bring deployed cost well above WiFi cost. Twelve or more doors may be connected to a single hub provided it is within range:



Credential Management

In other cases, operations might need to visit every lock in order to reconfigure or push updates to locks. Not all wireless/WiFi system employ 'passive updating', but in the case of credential updating systems like SALTO or Hotel Lock systems, the only way to completely ensure every lock is updated and current is to visit its location with a current credential.



Non Networked Configuration Cards

Repinning Locks

In many cases, hanging a WiFi/Wireless lock also means replacing the mechanical locks in use. In order to remain useful with existing keys and keying systems, new locks need to be pinned to comply.



Pinning New Mechanical Locks to Match

While the cost of repinning a lock may be less than \$20 for most, and is likely good for years of use, this initial expense is frequently overlooked and can be hundreds of dollars for a system of a modest number of doors.

Battery Costs

In large deployments, maintaining battery power in locks can cost hundreds or even thousands per year. While most lock vendors pin internal battery life at many tens-of-thousands of cycles (ie: 90,000 for this lock), this battery life is calculated under optimal operating conditions and doors.

Even a slightly misaligned or worn door may experience some drag or binding on the door lock. This additional force to overcome can quickly drain internal batteries. Aside from alignment, the lock's distance from the radio or hub can also be a tremendous factor on battery life, with locks farther away and with a weaker signal trying to re-establish a connection or find the network more often.

Finally, the orientation and use rate of the door can greatly impact battery life, with an occasionally used opening lasting longer than one used heavily. If the interval between power draws is several minutes or longer, the battery pack has time to recover to full voltages between cycles, while one used constantly will drain quicker because of constant use, but also because the chemical recovery of cells is intermittent.

The type of battery power a lock uses may range from a specialty battery pack (as shown in the image below), or the lock may be designed to use standard commercially available replacement batteries, but in either case batteries will cost money not needed by hardwire powered locks.¹

Consider if a single lock requires a (\$50 parts/labor) battery pack replacement once per year, a system composed of just ten locks will cost \$500/year.



Lockdown Feature

A common feature with hardwired systems that often has a shaky implementation with wireless/WiFi locks is the 'Lockdown' or 'Panic All-Lock" feature. The intent of the function permits a central alarm or user to simultaneously lock all doors in a system, potentially restricting access to potential threats like active gunmen or other unauthorised users.

With any wireless system, network reliability and speed are a concern. With 'Lockdown', this concern is amplified because an unresponsive or slow lock may leave innocents at risk.

Confirming a wireless lock system includes 'lockdown' features are the first step, but also designing the wireless network and maintaining radios to the degree the command is acted on quickly is the next.

If little tolerance is allowed for a potential failure of a lockdown command on a specific door, wireless/WiFi locksets should not be used at all.



Replacement Costs

Finally, if lock parts break, will replacement of the whole lock be required?

Unlike a hardwired door with many discrete components, if an auxiliary device breaks or malfunctions, it can be swapped out. With a wireless/WiFi lock, if a routine wearing part like a keypad or deadbolt wears (costing less than \$100 normally), there is a good chance the entire unit will need to be exchanged at a cost of \$1000 or more.

PoE Powered Access Control

Powering access control with Power over Ethernet, like for IP cameras, has become increasingly common.

However, the demands for access power are greater than cameras, and the problems can be significant. Consider that, in access control, many devices may need power (e.g., readers, locks, door sensors). Plus, since access control impacts life safety, special concern needs to be taken to ensure that mistakes are not made in powering.

Where PoE For Access Is Useful

PoE is useful in retrofit access control to bring power to the door, instead of installing high voltage electrical for the system first, an expense that can often cost hundreds of dollars per door.



Without PoE, power at the door involves extending or running new circuits from breakers to openings in new conduit with new outlets, power supplies, enclosures, and junction boxes, while PoE routes power through the same cable that connects door devices to an ethernet network.

PoE Overview

Central to using PoE for Access, and undoubtedly any application, is understanding how much power is available.

Two major types of PoE are commonly used:

- 802.3af supports up to 15.4W and is used by most PoE enabled Access Controllers.
- 802.3at, 'high' PoE, supports up to 25.5W but used only by a small fraction of security equipment, generally those designed to be used in extreme weather environments. However, 'at' is compatible with equipment specifying 'af'.

In access control, 802.3at use is not common, but some controllers may offer a version using it for higher output or pass-thru ratings for powering high demand locks or readers. For example, [Paxton offers a 802.3at Net2 unit](#) that offers 1.5A/20W of output:

NET2 PLUS WITH POE+ POWER SUPPLY IN PLASTIC CABINET



	max	units
Electrical		
Output voltage	13.35	V DC
Output current (PoE+ 802.3at type 2)	1.5	A
Output power (PoE+ 802.3at type 2)	20.4	W

For more on PoE, both as a general resource and a surveillance features, see our [PoE Guide for IP Video Surveillance](#).

PoE Into Controller and Out to Access Devices

The typical access architecture is for PoE to directly power the [door controller](#), with the controller powering attached low voltage access control devices like readers and in some cases, locks. The controller consumes some of the PoE power as overhead for its own operation, but then passes on portions of what is left to companion pieces. Usually this power is divided up to the different ports based on the device type connected to it.

PoE Controllers Frequently Limited to 4 Doors Or Less

Controllers with four or more openings using PoE are uncommon, for the simple fact that while the controller itself is powered, the remainder amount available 'passed thru' to field devices divide in four partitions is too weak to power the locks and readers.

Unlike IP cameras, where a single device draws power from a PoE source, with access control, controllers supporting PoE are just the first device in a chain. Most PoE sourced power is exhausted just from the controller and devices composing one or two doors. As a result, PoE options are common for single or double door IP based controllers like Mercury EP-1501, HID Edge EVO, and the Axis A1001.

Field Powering Attached Devices

Three main types of devices receive power from the controller - readers, locks and door sensors. How much power these devices need total is critical in determining whether PoE will be sufficient for each opening.

- Readers: The most common device receiving direct power, most keypad or card readers are specified to operate on steady power sourced only from the controller.
- Locks: Depending on lock types, using controller pass-through power may not be optional. For example, while Strikes may be able to operate off of PoE power budgets, Maglocks typically cannot as they draw significantly more current.
- Door Sensors: In some cases, other sensors may draw power from a PoE supplied controller for door position or even RTE, but this is not commonly needed or used.

In many cases, the total power needed for all these devices will exceed what PoE is able to provide. As a result, totaling up all the individual power requirements and reconciling against the supplied power is critical for every controlled opening.

Three Steps to Calculate

First, check what type of PoE the door controller accepts (e.g., 802.3af or 802.3at). Next, verify how much output power max the controller provides. Then compare to the total power consumption needs of all devices being powered from the control.

Workable Scenario

In our first example below, more than enough power is available:

A door is controlled by a Mercury Security EP1501 supporting 802.3af PoE, and passing through a max of 650 mA to field devices. To that controller, a HID 6005 Prox Reader requiring a max of 75 mA of power, and a HES 8300 Strike needing 240 mA on a continuous duty basis are connected and draw power.

The total power demanded by the reader and strike is 315 mA from the controller, compared to 650 mA provided, which is more than enough.

Failed Scenario

However, in this second example below, notice how insufficient power is available.

A door is controlled by a Mercury Security EP1501 supporting 802.3af PoE, and passing through a max of 650 mA to field devices. To that

controller, two Aptiq MTK15 readers (for a read in/read out application) drawing a max 230 mA each, and a Folger Adam 310-4 Strike needing 510 mA on a continuous duty basis are connected and draw power.

The total power demanded by the readers and strike is 970 mA from the controller, exceeding the available power by over 300 mA despite no warning or connection obstacles otherwise.

Available Field Power

Check the specification sheet of the controller to determine how much power is available. For example, this HID controller spec sheet lists the following power values:

Output Power (MAX) for individual field devices, DC Input = PoE	
Wiegand / C&D Reader	7.1W (580mA @ 12.25VDC)
Wet Output (@12VDC)	6.9W (580mA @ 12VDC)
Wet Output (@24VDC)	8.6W (360mA @ 24VDC)

According to this chart, the maximum available field power for particular devices vary by port. For example, the 'Reader' connection offers up to 580 mA for a device using 12.25VDC, or about 7.1W.

For 'wet outputs', or contacts that provide pass-thru power to control a lock, notice the desire output voltage affects the output amperage and wattage as a result. While this particular controller offers either 12 or 24 VDC selectable outputs, not all controllers do. Neither will all controllers divide up or limit pass thru power to a particular port. In many cases, the controller portions max power between reader and output ports, but other controllers simply assign a controller max field power output for all ports.

Max Power Varies

Another key point is how field power amount varies based on power source type. Typically when using PoE for power, overall available power is less than what is possible with separate low voltage power supplies:

Output Power (MAX) for total system (all field devices)	
DC Input @ PoE	9.6W
DC Input @ AUX +12VDC	14.4W
DC Input @ AUX +24VDC	28.8W

Note that the total power available with PoE (9.6W) is 33% less than 12VDC (14.4W) and 66% less than 24VDC (28.8W).

Code Impact

Many designers avoid using PoE to power locks outright, even if adequate power budget indeed is available. Building codes may complicate using PoE for power. Perhaps the most common issue is found for "Request to Exit" Pushbuttons that release door locks when pressed. The most applicable code, IBC 1008.1.4.4.3(2015) defines:

"A manual unlocking device (push button) shall result in direct interruption of power to the lock – independent of the access control system electronics. When the push button is actuated, the doors must remain unlocked for 30 seconds minimum. The push button must include signage stating "Push to Exit" and must be located 40" to 48" vertically above the floor and within 5' of the doors. Ready access must be provided to the push button."

This code basically prohibits controlling lock power by way of contact closure on the controller, and mandates a direct break in lock power through interruption. At the very least, a push button must be installed in

series between a PoE source and a door lock, but many AHJs reduce this to 'full power must be cutoff', even at the supply source as to be fully 'independent of the access control system electronics'.

For those looking for formal code citations online, see [Free Online NFPA](#), [IBC](#), and [ADA Codes and Standards](#) for area relevant versions and actual code language.

Cost Savings Significant

Using PoE to power doors often save ~\$200 - \$250 per door, given the elimination of extra cable, power supplies, and labor. For example, one could eliminate:

- 500' of 18/2 Power Cable: \$90
- 4A 12/24VDC Power Supply: \$50
- Installation Labor for Above: \$60 - \$100

Compared to an average door cost of ~\$1,000, this savings can be quite significant.

Potential PoE for Access Problems

Even when properly applied, PoE can present operational issues that separate power supplies do not. For example:

- Low-Draw Strike Bind: Many low power strikes, especially those marketed for PoE use, are vulnerable to misalignment jamming and binding that full power, high draw models can simply power through. While PoE is not the root cause of these issues, systems using PoE locks often require more frequent adjustment and are more sensitive to typical wear.

- Maglocks: Because maglocks require continually duty power and are relatively high-power locks, many PoE controllers are not built with contacts rated for continuous use. Intermittently powering strikes or deadbolts are within design limits, but continually issuing amperage at supply limits are not. Warnings against powering maglocks directly from the controller, by way of PoE, are commonly stated.
- Backup Power Drain: In addition, if PoE is used, the demand and subsequent drain on battery backups can be substantial. If the doors fall unlocked when power goes out, then specific high-availability backup power may be more prudent than a general resource used network wide. In many cases, breaking out access control PoE devices from other general networked devices is too complex for backup power management, and physically separate power supplies may simpler and less costly to manage.
- Reboot/Updating PoE Switch Kills Power Supply: A member explains "When doing a switch firmware update, PoE power is lost. When it is a camera system, the inconvenience is merely lost video during the upgrade. When it is access control panels, the penalty can be unintentionally unlocking or locking doors." The problem is caused by the system falling dead during <routine> firmware updates, but also then not negotiating PoE again when the update brings the switch back up. To mitigate the risk, PoE UPS devices can be applied, often for ~\$200 per opening to bridge the 'power gap' while a switch is temporarily offline.

Quiz Yourself

Take the [PoE Powered Access Control Quiz.](#)

[UPDATE: This tutorial was originally published in 2015 and substantially revised in 2017]

System Design & Special Conditions

Access Control Specification

Specifying Access Control correctly can be tricky, because every opening has quirks and are prone to outside factors that impact system performance. Not only this, but what you don't specify can be just as problematic as what you do.

Most access RFPs have serious problems. While they comprehensively spell out contract conditions and business terms, they are typically scant on relevant details about the system. Not only do they tend to be a random smattering of technical points, pulling them together into a cohesive system is often needlessly costly or may even be impossible to build.

The Big Mistakes

Most of the trouble specifying access has a root cause in one of the three areas below:

1. Incomplete details, where things you don't know can ruin your budget and system goals.
2. Difficult to build, where details that sound prudent may actually limit selection and significantly drive complexity to integrate.
3. Proprietary, where even generic boilerplate writes in choices that lock you into one vendor.

We address the best strategies to avoid these problems.

Doing It Right - 18 Key Specification Areas

The good news is that you do not need to be an expert to specify great systems. In the sections below, we cover the right details to include, how to include them, and how to avoid common traps through addressing these 18 areas:

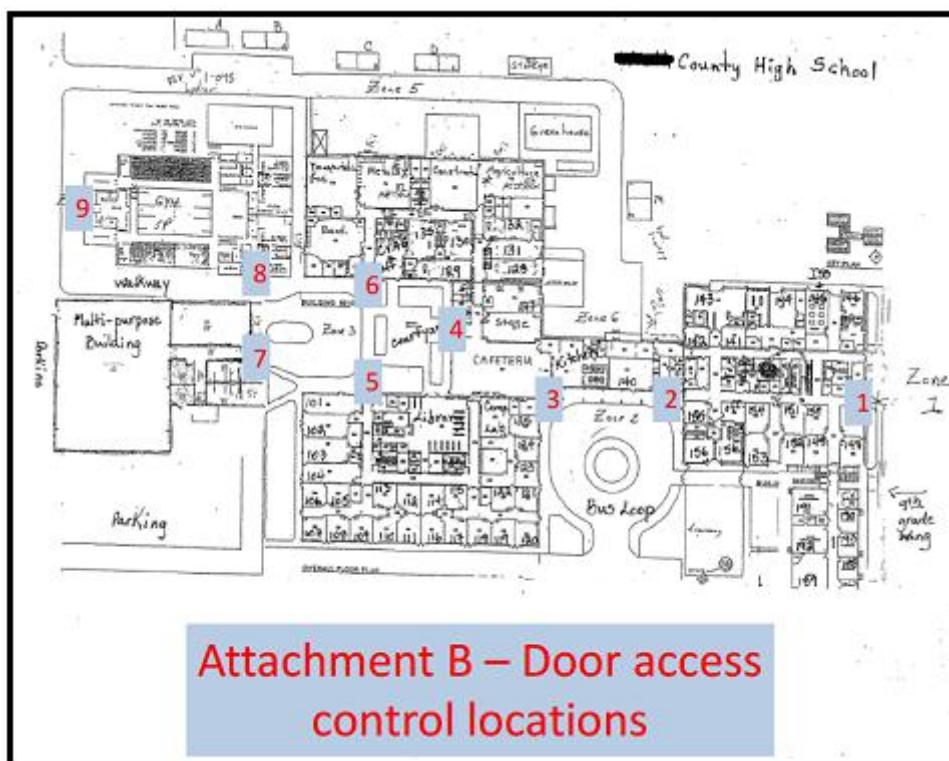
- Is This An Expansion or New System?
- Determining Access Security Goals
- Establishing Monitored, Managed, or Forensic Use
- Identifying Other System Integrations
- Which Credentials To Use
- Defining Doors/Opening Detail
- Defining Turnstile Use
- The Importance of Door Position Switches
- Defining Existing Locks/Hardware
- Specifying Readers
- Deciding to Use IP or Serial based Controllers
- How To Use PoE For Powering Systems
- System Edge vs. Centralized Architecture
- Is System Networking Wired or Wireless?
- Considerations For Using Existing Databases
- Evaluating User Management Features
- Using Special Features Like Time and Attendance & Mustering
- Establishing System Maintenance Expectations

First take a look at how common mistakes appear:

Common Examples

RFPs for access control might be well intentioned, but that does not mean they will get the job done. Look at these examples we pulled from recent RFPs:

Not Enough Detail: With any specification, the risk is including too many particulars that potentially drive cost. However with Access Control, the opposite is more typically true. Take this example from the Specifications section of this school's access solicitation:



Woeful Specifications

The bulk of details to build a quote from are found in the map above. No details regarding door/opening type, existing hardware, how many people need to have access or what credential types they carry, or when the openings should be unlocked are noted. Not to mention that descriptions

of how and who the system will be used, or which other systems will need to integrate with the access platform.

Granted, all these details may be released or discovered after a job walk, but not all respondents may have a fair crack at using them to build a bid.

Careless Specification: Another regrettable trait is the inclusion of specs that sound smart or economical, but prove to essentially limit choices to just one or two bids. Take the example from a Police Department RFP:

This system will provide physical security and control, access management and tracking, and reporting, and interoperability with current physical security equipment. The vendor will provide comprehensive, expandable solution including hardware, software, installation, acceptance testing, integration, training, and ongoing support of the access control system.

Physical Locations and General Requirements

- [REDACTED] Florida **Limits selection**
 - 4 Exterior Doors
 - 1 Door currently has standalone Motorola Flex Pass reader and door contact
 - 12 Interior Doors
 - 6 Doors currently have readers and door contacts controlled by iStar Door Controller connected to C-Cure 9000 installed on an agency server.
 - 1 Door currently has standalone Motorola Flex Pass reader and a door contact
 - 1 Door currently has door contact operated with a push button we prefer to keep functional
- [REDACTED] Florida
 - 5 Exterior Doors
- [REDACTED] Gainesville, Florida (South Location)

One Specification Excludes Most Choices

Overall the spec includes good detail including door descriptions and locations, and is non biased. However, due to the ambiguity in defining 'interoperability' and the listing of a single proprietary type of door controller essentially limits quotes to expansions of that existing system.

Whether this is intended or not is difficult to guess, however it would be much more efficient for both the solicitor and the bidders to state this requirement plainly up front. In the author does not realize the proprietary nature of access systems, they may think they are economically trying to use existing hardware for another system. However, the lack of detail defining 'interoperability' dooms this option.

Technical Specification

Here are 18 technical aspects to include in every access specification:

Is This An Expansion or New System?

Is this system new, or will it be a scaled addition to an existing system? Divulging this upfront will clarify for all involved what kind of work is being scoped. Due to the proprietary design of most access systems, interoperability is essentially non-existent, and if a system is already in place and satisfactory the best path is likely expanding that platform. This is likely the least expensive option since redundant equipment like servers and software may be avoided and not needed.

Also making this plain potentially avoids mistakenly buying two systems that cannot incorporate each other's equipment. Even if the goal is abandoning an existing system, recovering or reusing some of the existing components is a goal that should be made clear from the start. Special labor or software tools may be needed to transfer existing cardholder information, a point our "[Replacing Access Control Systems](#)" note elaborates in more detail.

Determining Access Security Goals

Harder to define, but essentially important, is to give a concise explanation of the goals for the access system. Stating "With this system, our facility wants to restrict off-shift staff from entering the premises, and keep all but certain individuals from entering <specific areas> at any time" will greatly assist those designing a system in knowing the important features to build around.

Specifically, when access control is confronted by the issue of "Tailgating", knowing where the most sensitive openings are located is key when specifying equipment to offset the risk. For deeper definition and detail on this risk, see our "[Access Control Killer: Tailgating](#)" note.

Even when specialty design or equipment is not needed, establishing the rough groups that get access and when/where they need it is the foundation of access control. Making these basic goals clear will help bidders select the right platform with the proper level of assignable features for the stated need.

Restating and examining these goals when expanding an existing system is still essential, as the areas of control and vulnerabilities can change over time. Including a short statement describing 'security goals' can refresh the effectiveness of a system even decades old.

Establishing Monitored, Managed, or Forensic Use

Next is to define how the 'control' aspects of the system will be managed. Is the goal to set everything up initially, and then only access it when absolutely necessary? Will an onsite guard staff actively monitor and

respond to events 24/7/365? Or is it better if system oversight and monitoring is active, but farmed out to a central station facility?

Defining just how the system is going to be used and by whom can control costs by avoiding unused features, or by making sure the right people can manage the system at the right time.

Identifying Other System Integrations

Do you want your access control to be combined with video surveillance or intrusion alarms? Do you have a fire alarm system? Making a point to state these goals, complete with the current make/models/versions of the systems to be integrated help drive design and installation labor requirements.

Which Credentials To Use

If the system is new, important decisions should not be answered by the lowest bid response. If an expansion of an existing system, the answer might already be made. However, in either case explicitly defining which credential type is desired prevents it from being a purely economic decision.

In terms of technology, most access systems use contactless credentials. In the past, 125 kHz credentials have been the mainstay, but due to security concerns (lack of encryption) and limited storage capacity, they have been superceded by 13.56 MHz types. From a cost standpoint, the more advanced credentials are the same price or cheaper than older formats.

If no credentials already exist, deciding the right product is as much security design as an economic one. How many people will be credentialed?

Should photo IDs double as badges, or is a more durable option needed? What other systems use credentials, and should they be combined? What about biometrics? Does risk mandate multiple factors are used?

Additionally, if existing facility codes are in use, they should be noted as a specification of the future system. Not all systems are able to work with dynamic codes, and this minor detail may drive significant cost if not made clear.

For more details, read our reports on:

- [Access Credential Form Factor Guide](#)
- [Popular Formats](#)
- [Fingerprints for Access Control?](#)
- [Multiple Factor Authentication Guide](#)

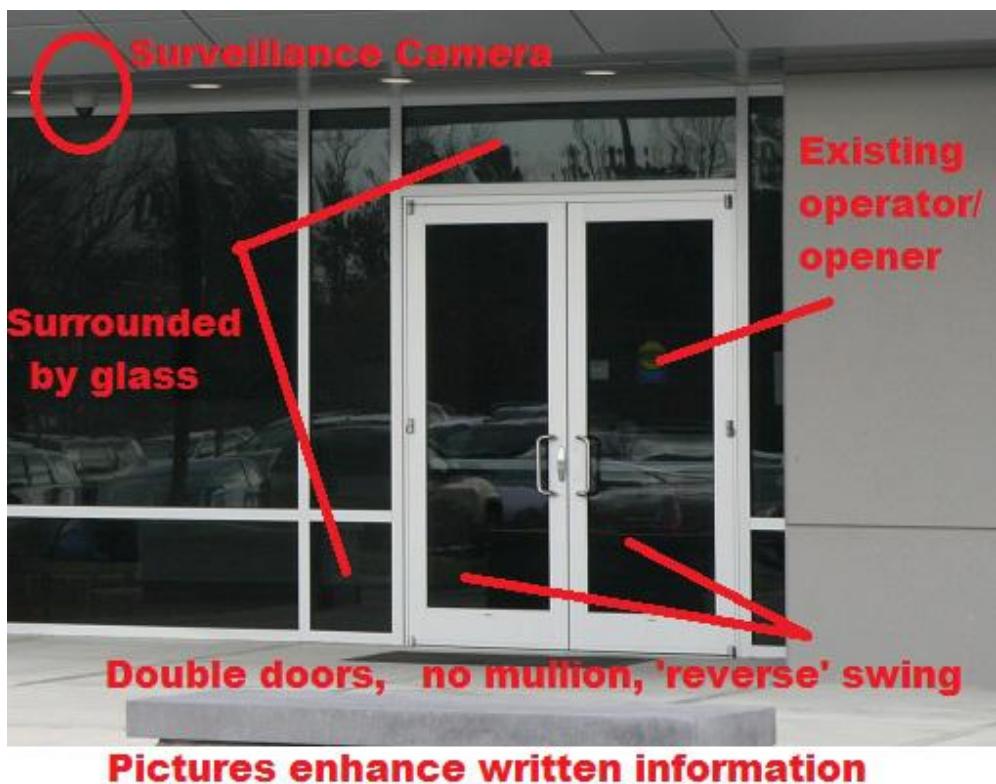
Defining Doors/Opening Detail

Describing the openings to be controlled is helpful not only from a design perspective, but also from potential management changes. No two openings are alike or used the same way, and a short description or picture of the opening and it is used goes far in designing good controls.

For example, the 'main entrance to an office building' is better described like this:

"The main entrance is a set of glass double doors that both swing out. These doors are handicap accessible, and the right side automatically opens and closes when a nearby button is pressed. A nearby security camera should be integrated into the system so that all potential users are recorded as they

enter. This entrance is typically used by the public during business hours, but should be locked and only accessible by approved users from 7pm - 6am overnight. Approximately 30 people may need access during a typical night during those hours, including cleaning staff and delivery people. This picture shows the opening:"



Note: Photos need no annotation, just a good clean shot of the opening to be useful.

While not technical, the information provided gives great insight that cannot be observed during a quick job tour and includes door type, door function, security goal, user volumes, and secondary system integration (video). While expert knowledge is not needed, passing on basic details mitigates guesswork.

For more detail on how to properly describe openings, whether they are doors, gates, or even turnstiles, catch the readings below:

- [Door Swing Primer](#)
- [Glass Doors and Access Control](#)
- [Turnstiles Guide](#)
- [Gate Access Control](#)

The Importance of Door Position Switches

One of the most useful, yet most neglected aspects of access control are the sensors that indicate whether the door is shut or open. While many view DPS as an 'extra', there remains no more effective or inexpensive way to monitor the current state of the opening than these sensors.

Since they are viewed by some as 'optional', solicitors should explicitly state they want these sensors included. Catch our "[DPS Tutorial](#)" for more detail. For insights on the biggest barrier to successful use of DPS switches, read "[Combating Door Prop Problems](#)" to catch the subtle behavior that totally undermine the access system.

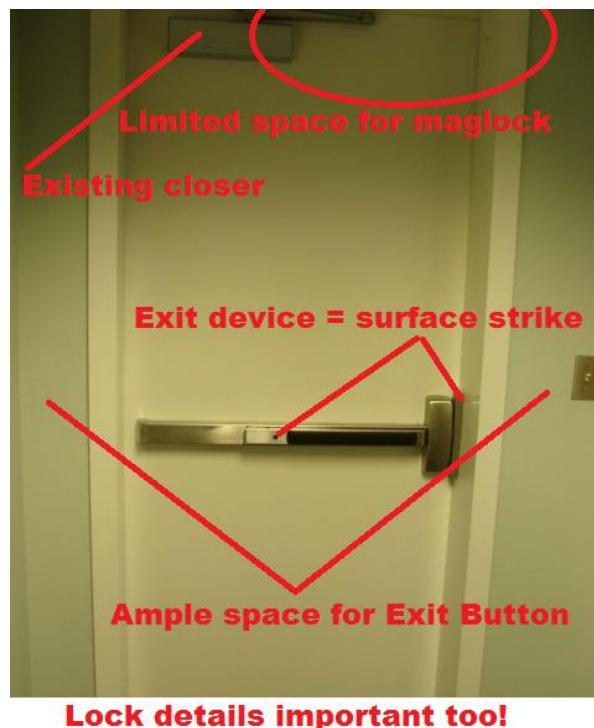
Defining Existing Locks/Hardware

Like doors, expert level detail is not required, but basic observations are useful. Often access control interoperates with existing mechanical locks, and quick inventory of how each opening is appointed is invaluable to choosing the best method of control.

For each door, a picture or basic written description is useful: "The back door is a metal (steel) door currently kept closed with a panic bar. The door swings out and has an 'Exit' placard above it. The door can be locked or

unlocked from the outside of the door by a key only issued to managers.

See picture for details:"



For further details on describing locks or how to choose the right type for securing your access door, see these posts:

- [Understanding Lock Functions](#)
- [Specifying Door Locks](#)
- [Maglock Selection Guide](#)
- [Electric Strike Selection Guide](#)

Specifying Readers

Selecting the right reader is the result of which credentials are used and where the opening is located. From the written descriptions and photos of the doors/locks, good decisions can be made what type to include and where.

Clearly indicating the openings where Multiple Authentication

Factors should be used help ensure the right reader is specified to support all credentials needed at that spot.

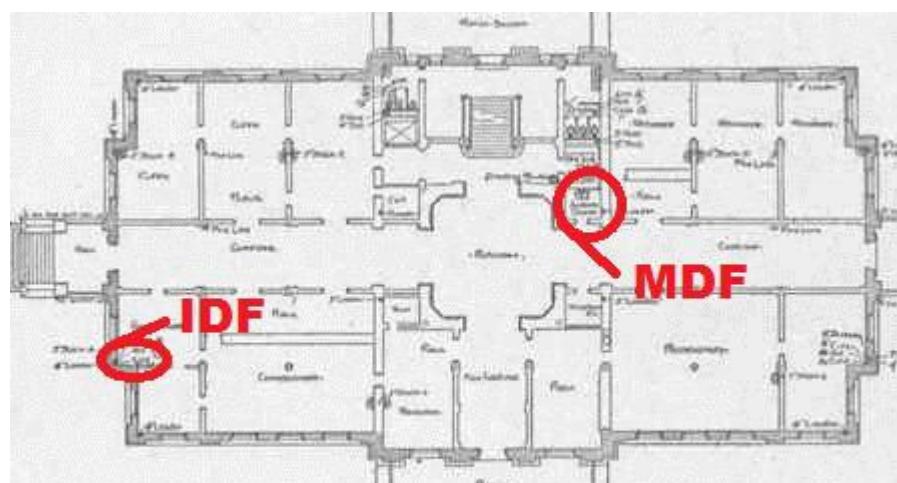
For general background and more detail on choosing readers, catch our guides below:

- [Access Reader Selection Guide](#)
- [Keypad Reader Concerns](#)
- [Proximity Readers Tutorial](#)

Deciding to Use IP or Serial based Controllers

The network that ties a system together should be mentioned if existing cabling or LAN should be used. Hard specifying one type over the other can be costly if preference is not strong, although many modern systems use IP networks as the primary option, a trend that will continue.

If existing networks are to be used, making the locations of existing switch rooms clear avoids guesswork or expensive redundancy. Marking a set of floorplans that include these positions part of your specification is vital:



Network /Server Room Locations

If new or dedicated networks are needed, making note of any raceway, main cable trays, or access panels confirms that new cable will run concurrent with existing.

System Edge vs. Centralized Architecture

To a lesser extent, specifying where door control takes place is important.

Most modern systems use a form of door controller mounted near the opening, and specifying centralized location of system components could significantly drive cable costs or result in older systems being bid.

Even if 'edge' systems are used, all equipment can be installed behind locked closets or secured enclosures. However, making sure enough space is allocated for those devices is commonly overlooked and can drive costs if not properly considered during spec writing. These reports include more detail the subject:

- Controllers or Control Panels
- Securing Access Control Systems

How To Use PoE For Powering Systems

In many cases, standard 802.3 af/at PoE can be used to inject power to edge controllers and subsequently connected devices like readers and strikes. Using PoE is generally more convenient and offers online management when separate, stand alone power supplies typically do not.

However, using PoE may limit the range of connected devices based to 'total pass-through' power available, which is usually 750 mA or less, and the max number of doors on a single PoE powered controller are limited to two. Other factors to consider include the rating of the controller contacts,

and disclaimers against powering maglocks on a constant basis from a PoE controller are common.

Our [PoE Powered Access Control Guide](#) includes an in-depth look at the subject.

Is System Networking Wired or Wireless?

When it comes to controlling cost, hard specification of wired systems can cause prices to skyrocket for remote or hard to reach openings. Especially if those doors are not heavily used, but electronic control and logging is essential, consider using wireless and 'stand-alone' styles of locks.

While the unit cost may be high for a single wireless lock, the overall cost of connecting multiple devices together via a long network run could be more expensive. While the overall price and maintenance associated with wireless locks (ie: replacing batteries) could be prohibitive for entire systems, they could prove an economic fit in lieu of significant wired network expansion. For more on these applications, see our "[Wireless Access Primer](#)".

Considerations For Using Existing Databases

Especially for larger, multi-site systems, the database can bring significant cost. Assuming the most economical choice will be made is foolish unless the specification explicitly states which database platform may already be available. Our "[Hidden Cost of Access: Database](#)" posts covers this point, and the common options, in depth.

Evaluating User Management Features

Defining user's needs are a critical aspect of the specification, and one where presuming features will be available is dangerous. Spelling out expected 'Live View' and management control helps designers specify can configure the right platform. If operators need to lock/unlock doors in real time, weekly activity reports are to be created, or if the access system should integrate with the video surveillance system, these requirements should be clear.

Even for systems that are not actively managed, if items like 'remote access' from smartphones or inclusion of 'ID Badge' creation modules, it should not be assumed it will be included unless stated.

Also, if specific workstations are to be used for running clients, description of their location and build specifications should be listed so deploying the system to operators is confirmed. For more details on the software management piece and explanations of the typical features desired, see the following posts:

- [Access Management Software Guide](#)
- [Maintaining Access Records](#)

Special Features: Access control is useful for more than just unlocking doors. Many systems include options for 'Time and Attendance' logging that essentially replaces a time clock, or 'Mustering' that grants you special reporting that provide a roster of occupants in a particular area.

If these features are desired, or any other integrations falling outside the core access control functions, effort should be spent defining the desired result in specification documents. These posts will help clarify what to ask for and how to note the requirements:

- [Time and Attendance Tutorial](#)
- [Mustering Tutorial](#)

Establishing System Maintenance Expectations

Finally, specifications should spell out any ongoing annual software maintenance costs and any additional ongoing expenses required to keep the system current and operational. Some platforms have no ongoing maintenance plan, while others require a yearly plan and may not prioritize service or tech support if not current.

The cost of this maintenance should figure into system selection, as a system may be thousands less when initially installed, but add thousands in unrealized costs in subsequent years.

Access Control Specification Form

The following section provides a summary of each requirement and common options to consider. We recommend you copy and paste this into your own documents and use it as a starting point in defining the requirements for your access systems.

Opening/Door Type: Often best depicted in a picture. If not permitted, a short written description describing: Steel, wood single or double door? Right, left, or swing ‘reverse’. Glass opening? Turnstile?

Users per Hour: Average number of users during busy times, so that cycle times of locking hardware can be sized accounting to the busiest period the door permits access.

Opening's Security Goals: The high-level purpose of access control: “Restrict unapproved users from entering during overnight hours” or “Only

residents with current rent payments should be allowed to use gym facility.”

Other Equipment on the Door: Often best expressed in a picture, a snapshot or written description of the other hardware devices hung on the opening. Examples: “Closer on upper hinge side, vertical rod on upper strike side, and an exit device hung on the inside. Outside keyed access.”

Reader Type/Mounting Position: On the door frame (mullion), or on an adjacent wall? Are mounting surfaces suitable? Are they protected/sheltered from ice and snow? Can someone in a wheelchair or with limited range of movement reach the reader, per ADA (or similar)?

Credentials to Use/Multiple Authentication Needed: Common Choices: 125 mHz, 13.56 MHz contactless. HID format, MiFARE/DESFire? 26,33,34,35 bit cards? Facility code needed? Is more than one credential needed at the door to verify the user?

Intercom Needed?: If a user cannot enter the door, or if a visitor request entrance, can they page help or an attendant? Two two-way conversations need to be supported?

Lock Type Needed: Choices- typically electric strikes or maglocks, but dictated by building code, AHJ preference, and type of hardware existing on the door.

System Network Type: TCP/IP, Serial hardwire, wireless, or stand alone locks? If IP, are existing LAN segments available? Are cable pathways and data closets marked? If wireless, the signal strength at doors verified?

Controller Types: Choices- Edge or Centralized? Standalone or host dependent?

Critical User Management Features: What real-time features required? What type of reporting is needed? Will users need access from a browser or mobile devices? Are client workstations available?

Server Space/Preference?: Do you have available resources in the server stack? Are they physical or virtual? Do you need your servers to host access locally or remotely? Including this ensures no ugly incompatibilities happen at the last minute. If a new server is used, will local IT resources be familiar with configuration and support?

Database Platform Needed: Does your enterprise already use a standard database platform like SQL? If so, make note so the access system can plan to make use of existing rather than purchasing new or using a proprietary platform.

Special Features: Do you need Time & Attendance or Mustering? If so, does your hardware design support those features? Make note of the 'other systems' you would like access control to feed into or use like video surveillance or intrusion alarm.

Mustering

Access control can be used for more than just securing buildings. Among these powerful 'other' functions is mustering, which immediately accounts who is where in a building. However, a system has to be designed properly and carefully to use this.

Mustering's Two Approaches

First, one must select / differentiate between the two types of mustering, depending on how much administrative oversight is required:

- Area tracking
- Checking In

Area tracking: The concept of mustering uses access control to generate a roster of occupants in a certain area. Every time an occupant scans a card to enter and leave an area, the access system logs the time, date, and credential holder of the credential. This data can be used to determine who is in the area at any given time, including emergency situations.

Checking In: Alternatively, mustering can be implemented in some systems as a 'opt-in' control, where a credential reader located at an evacuation point is scanned as cardholders reach that location. Then that list of names can be compared against the assigned list of evacuees who should scan into that reader during emergency. The report screen below is an example output screen from a 'mustering reader':



In either use case, the goal of mustering is to account for specific individuals, so if they are not confirmed present within an area, then additional action can be taken to investigate where they are. In an emergency situation, the resources to search for the unaccounted are limited, and having an accurate list of who is present helps bring focus to those efforts.

Where Is Mustering Used?

Aside from 'Emergency Roll Calls', mustering functions can be applied in several ways. In industrial or mining facilities, mustering can be used for 'Lock Out/ Tag Out' situations, where machinery should not be restarted or an area reoccupied until all maintenance personnel are accounted for. If even one maintenance person has scanned in to an area, but not yet scanned out, all machines are de-energized until everyone can be accounted for.

Likewise, in facilities where frequent headcounts are important, like prisons, daycares, or passenger manifests, mustering can be configured to ensure that all members of a group are present in an electronically logged system.

Depending on how mustering is implemented, it can send notifications or print reports to predefined locations. Not only can 'absentee reports' be

sent to nearby printers within an evacuation area, it can send emails or text messages to current occupants alerting them to emergencies (ie: severe storms, bomb threats, or other emergency circumstances).

Additional Design Required

Depending on how a system implements mustering, additional software configuration and hardware may be required. If 'mustering readers' are used, then configuring this function may be no more than selecting a few checkboxes. This configuration often requires cross referencing other readers in the system to confirm occupants are not elsewhere in the system, or may even cross-reference shift or vacation schedules to confirm occupants are gone.



However, other forms of mustering may require additional readers. In order to take an accurate inventory of who is present in an area, occupants must 'scan out' when they leave. Most access controlled openings simply require 'scanning in' for access, so the addition of an out reader, even when hardware is not linked to it, adds cost and complexity to a system.

System Examples

Implementation of the feature varies by access control software, but is typically supported by enterprise level offerings. For example:

- CCURE: Older versions of CCURE support mustering by way of designating specific readers as "Evacuation Points", however current

versions include exception reporting that generate a list of names in an area on demand.

- DSX: This system supports mustering readers, as well as input/output linking that can be used to create 'muster reports'. When 'Time & Attendance' readers are used, mustering reports can be filtered by who is currently present in a facility.
- LENEL: OnGuard supports both reference readers and exception reports method in all versions, and can be integrated with other systems.

If mustering is important to you, make sure to check carefully check how it is implemented in your access control software as approaches and availability vary greatly.

Tailgating - Access Control

Despite costing thousands of dollars per door, electronic access control systems are vulnerable to an easy exploit called 'tailgating'. Unless this threat is recognized and addressed, even a friendly gesture compromises one's security investment.



We take a look at 'tailgating', the most common causes / risks, and contrast 4 options to address / minimize tailgating:

- 'Hold Open' Alarms
- Turnstiles/Revolving Doors
- Mantraps/Airlocks
- Piggybacking Detectors/Analytics

The Problem

'Tailgating', also called 'piggybacking' by some, describes the situation when a credentialed person opens a door allowing one or more individuals to immediately pass through while the door is open. The effect of this simple action can render an entire facility insecure.

The situation can benignly occur when holding a door open for someone. It also happens accidentally, typically when someone is focused on hurriedly making it through an open door. Rarer, but most risky of all, is when someone commits a malicious act by purposely sneaking behind a valid card holder to beat the security system.

Common Courtesy The Biggest Enemy

In many cultures, holding the door open for people is a warm, kind expression. Likewise, explicitly slamming the door shut behind you can create ill will between neighbors or co-workers.

The most common tailgating risk is that many credential holders do not consider how they are undermining an access control system with their own 'good manners'.



Indeed, many cultural objections to not holding a door often circulate.

Countless articles decrying the failure of civility are popular, like:

- [Holding The Door Open For Women](#)
- [A question of etiquette: do you hold the door for others?](#)
- [Here's The New "Holding The Door Open For People" Rule](#)

However, the aspect these articles fail to recognize is that the only way a door is protective is when it is closed and locked.

Security Awareness Is Key

Most people do not deliberately seek to undermine physical security of a room or building, but they fail to recognize just how potentially risky or damaging their behavior can be.

The best method to balance 'politeness' with 'security' is simple awareness of why, or if, a door is a security point. Not all facility doors, not even those frequently used, are necessarily part of the security access controlled perimeter. But if a door is kept closed and locked, or if it is equipped with telling devices like readers or keypads, it should never be held open and politely kept closed after authorized entry.

For these openings, user training and door signage is often necessary to reinforce authorized users of the security importance. Training people and hanging signage is a 'low tech', but often most broadly effective way of dealing with this risk.



Other Contributing Factors

There are a variety of other tailgating root causes. Understanding the 'why' of each door threatened helps to determine the best defense against it:

- **Bad Weather:** Especially in rainy and cold climates, holding the door open offers a welcome shortcut to those seeking the warm and dry environment of a facility. In these cases, sheltered entries, windbreaks, or awnings help diminish the tendency to hold open doors out of environmental harshness.
- **Misaligned/Worn Doors:** Over the course of thousands of open/close cycles, even commercial grade doors, hinges, frames and closers sag or become worn over time. If left unchecked, doors may not fully close when opened or may take a long time to close, therefore allowing many people entrance from a single card read. A regular and discipline door maintenance schedule for access controlled openings is critical to prevent the issue.
- **Inconvenience/Laziness:** There are a variety of simple ways to keep a door from latching after it has been opened. Doorstops, rocks, bunched-up rugs, and hardware tampering are all commonly employed to eliminate the task of presenting a credential for access, often seen as onerous by employees. For this reason, consider embellishing 'smoking area' doors or delivery entrances with cameras and intercom systems to mitigate tampering and provide other communications paths for outside access.
- **Malicious Intent:** Preventing untrusted or dangerous people from entering an area is often the primary goal of access control. Often, readers and locks alone are not enough to mitigate this risk despite the occurrence being minor. To properly prevent undetected entry, often additional engineering controls like sensors, analytics, or even turnstiles are needed.

The Solution

The risk of tailgating is widespread and almost every access controlled facility is vulnerable. Fortunately, a host of engineering controls are available to combat the problem. In the section below we take a look at the major types:

- 'Hold Open' Alarms
- Turnstiles/Revolving Doors
- Mantraps/Airlocks
- Piggybacking Detectors/Analytics

'Hold Open' Alarms

Many access control systems have the ability to monitor door contacts - simple switches that check whether a door is closed or not - and can be set to alarm if a door is held open for too long. Alarming occurs on doors open longer than a few seconds, thereby indicating that multiple people are passing through a 'held open' door. However, while this is a low-cost or free measure for combatting tailgaters, it also is the biggest source of nuisance alarming when implemented. Unless a facility actively monitors its access control system, this solution is likely to be (promptly) dismissed as irritating and ineffective.

Externally fitted alarms usually cost between \$500 - \$1,000 however many access control systems can be configured to sound a local alarm via reader beeper and door position switches as a 'free' configuration setting.

Turnstiles/Revolving Doors

In recent years, turnstiles have moved from massive, noisy mechanical devices to sleeker, quiet, architecturally styled access control points. This

type of equipment restricts entry to a single person at a time, and eliminates the ability to hold a door open for unauthorized access.

The promotional video below provides an example of an 'office turnstile' designed to restrict access into an interior space, and features 'tailgating' detection:

Note: [**Click here to watch the video on IPVM**](#)

We covered this particular unit in our [Free Flow Turnstile \(dFlow\)](#) post.

The cost of turnstiles and revolving doors can range from \$1,000 to \$25,000+ and are frequently core access features, not retrofitted afterthoughts. For more, see our [Turnstiles Guide](#).

Mantraps/ Airlocks

These installations are entryways that feature two sets of controlled doors. Usually sized just large enough for one occupant, the doors are configured to open one set at a time. This means the interior set cannot be opened until the exterior set has been closed and is locked. Because the physical space inside a mantrap is tight, only one person per card read is permitted through the doors. Mantraps can be configured for wheelchair access, as shown in the example below, where an additional room is unlocked only when a wheelchair-credentialed user scans in to a door:



These installations have a variety of operation uses beyond security; in some cases the function as airlocks to segregate 'clean room' environments

from outside contamination, or they are used as inspection checkpoints for contraband. These installations are substantial, and because they use multiple sets of doors and have large physical footprints, they are among the most costly anti-tailgating measures.

The cost of mantraps and airlocks are generally very expensive, routinely costing more than \$20,000 to construct. Like turnstiles and revolving doors, these physical perimeters are core access features, not retrofitted afterthoughts. For more, catch our [Mantraps Examined](#) note.

Piggybacking Detectors/Analytics:

This option, usually based in sensors hung on the frame of a door, or nearby analytic-enable surveillance cameras, are configured to detect individual movement through an opening. The movement profile of a single individual is compared against the actual movement measured as it credentials into an opening. Based on movement anomalies (ie: the pattern is atypical of 'normal'), the unit or camera will alarm. Sometimes the unit itself is built to sound an alarm,

One example of the door-based piggyback detector show in the promo video below:

Note: [Click here to watch the video on IPVM](#)

The cost of these solutions vary, but generally range from \$300+ for a camera analytic (less camera), to <\$2,000 for a single 'light curtain' sensor.

Solving The Problem

While solutions abound, the 'best' option is an tough matter to decide.

Many security managers faced with tailgating simply rely on repeated instructions and signage to remind credential holders about the issue. Lacking the funding or organizational will to eliminate the issue, the vulnerability (and subsequent risks) of tailgating remain.



In those cases where tailgating must be prevented, the use of turnstiles and manways is common. However, due to the cost of these solutions, many end users find them too expensive and instead opt for less costly (and less-effective) options like Piggyback Detection or Video Analytics.

The Passback Problem

Every security system has flaws, even high-tech ones. While Electronic Access Control helps keep sensitive areas safe, it is not without weaknesses.

One of the most troubling vulnerabilities is called 'Passback' - the practice of using someone else's credentials to gain entry. We take a look at the problem and how designers can minimize vulnerabilities, looking at:

- Passback vs Tailgaiting
- Basic Software Solutions
- Other solutions
- Ignoring it



Passback vs Tailgaiting

'Passback' is the colloquial term for 'sharing credentials', taken from the example of two people passing through an access-control turnstile.

Suppose 'Person A' scans their badge and passes through normally, but 'Person B' is not allowed access into the area. 'Passback' occurs when 'Person A' hands their badge to 'Person B' so that person can gain access.

This practice is roughly equivalent to slipping a door key through a mail slot to an outside person, or sharing your password with someone else. At best, it means that the system is not controlling access in the way it was designed, and at worst it could mean the system has no knowledge of a potential threat.

Less Risky Than Tailgating, Still A Problem

In terms of security threats, Tailgating is a 'killer' risk, while Passback is generally less intense. Many passback events occur when people try to find ways to undermine the access control system, while Tailgating typically flatly ignores it. So in general, Passback is easier to manage with 'soft' methods or with direct reminders to users to avoid sharing credentials.

Simply defined, 'tailgating' means that once a door has been opened by a credential, it is left open so that more than one individual is allowed to pass-through. In contrast to 'passback', 'tailgating' simply bypasses the requirement to scan individual credentials. However 'anti-passback' controls, especially those of the 'Pattern and Flow' variety, may be able to combat the 'tailgating' problem.

For more, see our [Tailgating - Access Control Tutorial](#).

Basic Software Solutions

To counter the risk, Access Control systems often feature 'anti-passback' controls, which generally describes a set of barriers applied to credential use. For example:

Time Limit: A card cannot be used at the same reader twice within a certain amount of time. While this represents a decidedly 'low-tech' solution, it is the easiest to implement. Simply limiting a card to be read on the same reader for a period of 3 to 5 minutes discourages the convenience of improperly 'passing-back' a credential. However, this type of control can be inconvenient to users, on the occasion they accidentally drop something after reading a card, become distracted by a conversation, or have some other legitimate reason for quickly re-credentialing through an opening.

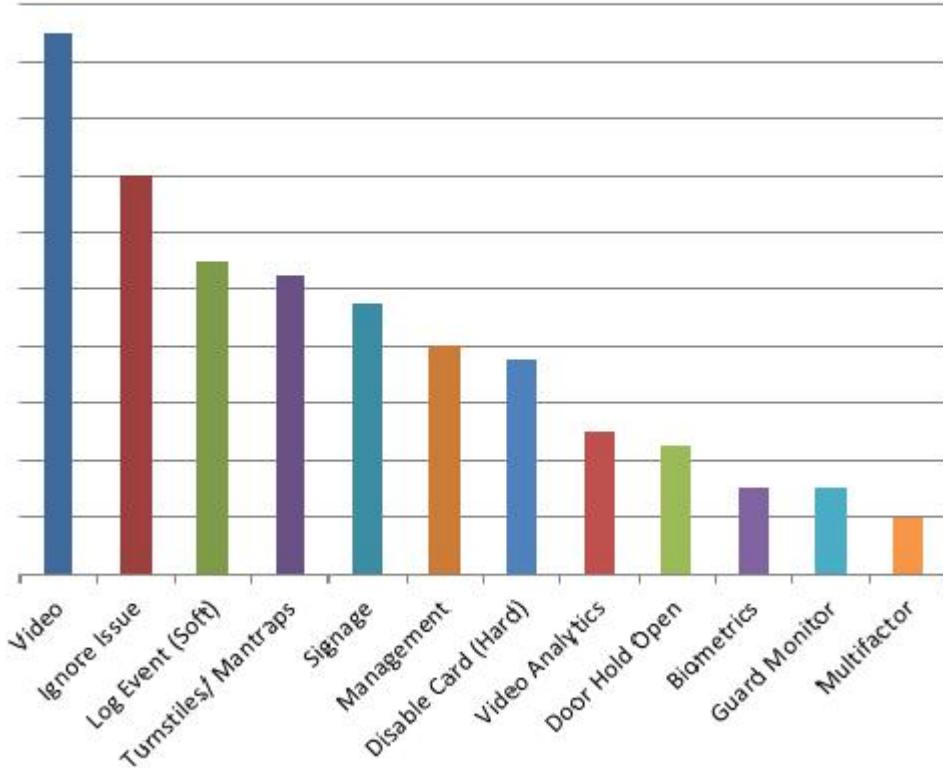
Reader Pattern and Flow: This type of control requires credential reads follow a logical pattern within a system. For example, a credential must be used at an 'OUT' reader before it can be used for an 'IN' function. Likewise a credential cannot be used to enter 'Building B' if 'Building A' has not first been exited. This method of anti-passback is the most comprehensive at controlling the problem, but it requires the most configuration and places an emphasis on having all doors controlled within a facility, even doors that are infrequently used.

Time Limits and Reader Patterning are software features that some, but not all, access control management software supports. For other, more strict solutions, additional hardware sometimes costing thousands is required.

Other Solutions

Conclusively battling passback typically involves more than only software. For example, in our [Practical Solutions To Piggybacking and Tailgating](#) survey, more than 10 solution types were voted, and more than 80% of those responses mentioned using more than one solution method:

HOW DO YOU DEAL WITH TAILGATING & PASSBACK?



The most common 'other solutions' besides basic software cited:

- Biometrics: A sure way to prevent passback is to credential based on biometrics instead of 'shareable' credentials. Tying access permissions to unique physical features generally stops most sharing.
- Cameras: Another common approach involved using surveillance cameras to record and verify no misuse was happening at access points.
- Turnstiles: The most common 'strict' method were using turnstiles, revolving doors, or mantraps to physically prevent more than a single person entry at any time.

- Signage: The most common 'soft' measure of those that indirectly or passively address the risk was the use of signs to remind people that misusing the system invites danger or undermines security controls.

Ignoring it

However, another key trend identified in the results was ignoring the issue. About 15% of responses said they simply do nothing, because addressing it is too costly, or it is not enough of a risk to warrant countermeasures.

Choosing to ignore the threat may seem prudent for some, but doing so introduces the opportunity to undermine and even invalidate the power features that justify using electronic access control versus traditional mechanical keys and locks.

Delayed Egress Access Control

Is it ever legal to lock people into a building?

The answer is: Yes... under specific situations.

With so much of access control driven by life safety codes, and a predominant focus of 'free egress' during an emergency, 'delayed egress' may run counter to common sense.



Major Codes Allow Delayed Egress

Surprisingly to some, both IBC and NFPA 101 codes permit delayed egress, if done in a manner that meets specific safety requirements.

While the approved occupancy classifications differ between the two authorities, they both allow for exit from a building to be delayed up to 30 seconds, but typically 15 seconds. In practical terms, this means when someone approaches a delayed egress opening and pushes on the exit bar, an alarm sounds but the door remains locked for a short period before unlatching and allowing them to exit.

The specific citations defining delayed egress include:

- IBC: 1010.1.9.7 (2015), 1008.1.9.7 (2012)
- NFPA 101: 7.2.1.6.1 (2015 and 2012)

For those looking for formal code citations online, see [Free Online NFPA, IBC, and ADA Codes and Standards](#) for area relevant versions and actual code language.

But Some AHJs Forbid Regardless

However, not all AHJs are accepting of this method even when it is code compliant. Locking people behind closed door for any period of time is deemed too risky and potentially deadly, regardless of code acceptance.

Several municipalities prohibit or heavily restrict use of delayed egress for specific occupancies. For example, [Maricopa County / Phoenix, Arizona](#) limits use of these locks in most situations, contrary to IBC and NFPA 101.

The jurisdiction only allows delayed egress is one specific occupancy type, and prohibits it in education, retail, and high-security commercial applications:

425.4.2.5 Delayed Egress Locks. In R-4 Condition 2 occupancies, delayed egress locks shall be permitted in accordance with 1008.1.9.7, Items 1,2,4,5 and 6.

Limited Applications By Code

The IBC does not allow delayed egress locks on Assembly, Educational, or High Hazard occupancies, but does on certain educational, healthcare, and group areas. In contrast, the more accepting NFPA 101 includes limitations specific to each individual classification.

In general if allowed, every delayed egress door must be readily operable from the egress side without keys, tools, or special knowledge or effort, and without tight grasping, tight pinching, or twisting of the wrist. One operation must initiate unlatching the door from the egress side, and operable hardware must be mounted between 34 inches and 48 inches above the floor.



In addition, a permanent sign needs to be affixed to the opening notifying users that unlatching may be delayed after a specific period.

Fire Alarm Override

Another requirement: even if delayed egress is used, all doors must be made to unlock immediately when the fire alarm is pulled.

This override is included in order to mitigate the stampede or crushing risks for those trapped behind a locked door during a fire event or other emergency.

However, some authorities recognize that many emergency egress situations unfold without involving fire alarms. Active shooters, severe

weather, and bomb threat evacuations can be hindered by delayed egress locks. AHJs often object to any delayed egress because of these concerns.

Nuisance Delay Optional

Depending on which code authority is accepted, the person exiting may need to press on the exit bar for three continuous seconds. This time period, called the 'nuisance delay' helps mitigate accidentally triggering a delayed egress door by simply bumping the exit bar. If no delay is allowed by code, then 'pranking' the door by bumping the bar and running is a potential irritant and reduces the effectiveness of the annunciation to supervising staff.

Real-World Delayed Egress Applications

Delayed Egress is valuable in certain niches. Take the following examples:

Retail Stores: Modern 'big box' retail stores are expansive facilities that require multiple emergency exit doors throughout the building. In the past, shoplifters have taken advantage of these openings, simply loading up with expensive merchandise and crashing through these doors to waiting vehicles for a quick getaway.



Delayed Egress helps counter this problem. If someone attempts to crash through an opening, an alarm sounds for 15 - 30 seconds before unlatching, allowing for store associates to apprehend the shop lifter before escape is possible.

Daycare/Nursing/Convalescent Homes: Another valuable place to use delayed egress is where the risk of occupant escape is high. For daycare and elderly care facilities, ensuring that clients are secured indoors is a high priority, and use of delayed egress on unsupervised openings is an invaluable tool.

How It Is Implemented

The list of components needed for compliant delayed egress varies according to how it is implemented, but public notification signage is required to be hung on the door regardless of the method.



Panic Bar: Delayed Egress can be installed on any opening, even if it is the EAC system does not control it. However, in most cases, substantial specialized hardware is required. Most exit device manufacturers offer a delayed egress equipment package that can be retrofitted to an existing opening but the installed cost of these packages range between \$2500 - \$5000 each opening.

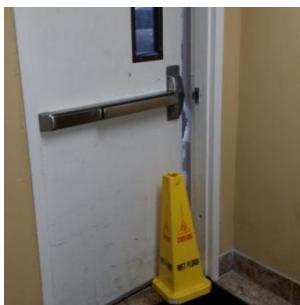
Access Control Systems: Many access control systems can be configured to release locking hardware after a timed delay. However, some forms of controlling hardware are able to be overridden by mechanical hardware (ie: electric strikes), so additional door mounted devices, like an 'exit check' may be required. The installed cost of delayed egress on an access controlled door can range between a few dollars for a sign (\$2) to \$2500 to integrate an delayed egress lock and annunciation sirens.

'Exit Check' Device: Often a modified type of maglock, this device is tied into an exit bar or senses opening force to begin a timed countdown. After that period expires, that maglock releases, and the door freely opens. The installed costs of this option range from a few hundred (\$400) to several thousand dollars, depending on the amount of extra equipment required to bring a door compliant with codes. See our note [Delayed Egress Maglock Claims to Save Thousands](#) for an example of this type of product.

Propped Doors Access Control

Doors should keep 'bad guys' out.

One of the most basic problems with doors is people propping them open:



Even worse, door propping undermines significant investments in electronic access control. The issue is especially frustrating to building security because it is so common and easy to pull off. We examine:

- Convenience vs Security
- Common reasons for doing so
- Eliminate the means for door propping
- Adding signage and education
- Installing specialty equipment
- Using door closers

Convenience vs Security

Propping doors is not a difficult issue to describe. Whether it happens because of wood wedges, kickdown hardware, or even rocks, trashcans, or kicked rugs, preventing a door from closing makes passing through it easy.

The classic 'convenience versus security' problem is clearly demonstrated by a propped door. Whatever the reason a door is held open, it cannot lock or secure the space within. When this takes place on perimeter openings, like the main entry for buildings, any stranger can walk in and perpetrate

crimes. Making sure that doors get closed when opened is an age-old problem with seemingly no easy solutions.



Granted, door propping is not an issue with every door. Propping doors that divide rooms, offices, or closets may not cause security problems, but propping a facility's access controlled openings is a nasty issue. When a door is used as a 'layer of security' to segregate access, keeping it held open can compromise an entire facility.

Common Reasons For Doing So

Since propping is so common, what are the root causes?

- Convienence: Closed doors are a barrier. Not only does it takes effort to swing open, needing to lock it with a key or credential card is especially a hassle. Especially when passing through an opening many times, or carrying a load with both arms, keeping the door propped open is a welcome alternative to contantly fighting a shut opening.
- Climate: Doors are propped when the room inside is too hot, cold, or air circulation is stale compared to outside spaces. Keeping a door open provides some relief, but at a big expense to area security.

- Hardware Malfunction: Not all doors are deliberately propped open. In some cases, faulty hardware like worn hinges or maladjusted closers can keep a door open and unlatched through neglect.

The Solution

Solving the problem does not require exotic solutions and can be done by:

- Eliminating the Means
- Adding Signage/Education
- Installing Specialty Equipment

Eliminate the Means For Door Propping

This simple step often yields the most effective result. Uninstall kick-downs, throw away door wedges, and move items like floor rugs and trashcans away from doors.

People seldom give much thought or effort to propping a door, so making it more difficult to use trash or common items to hold doors open has a big effect. The image below gives a few examples of how doors become propped:



Kick-Downs



Strike / Latch Tampering



Door Stops

Adding Signage/Education

Making a point to emphasize keeping doors closed also is inexpensive. By hanging signs and (vigilantly) reminding occupants of the important security purpose of closed doors, the propping problem can be significantly resolved.



Installing Specialty Equipment

When more stringent action needs to be taken, or when the problem needs to be eliminated, specialty devices or access control systems can be configured to alarm. Regardless of the device used, the operation of anti-propping equipment uses a set of contacts and a timer. When the door opens, the contact break open, and a timer begins to countdown. If the door does not shut within a range of time (typically 15 or 30 seconds), an alarm sounds alerting occupants to the open door.



If for no other reason than to avoid the nuisance of alarm sirens or the attention of security guards, occupants learn to keep doors shut.

Some basic ways to do this:

- EAC Integration: Many Access Control systems support an 'anti-prop' function that works in conjunction with door position contact and the door controller to send an alarm when doors are open too long. However, this feature may have no 'local annunciation' or audible siren at the door, and instead sends an alarm to the access control management console for attention. Addressing the 'prop alarm' falls to guards or operators working with offenders to stop the problem. Configuring this alarm on a door already installed with access control hardware is a no-cost solution.
- Auxiliary Alarms: For doors without access control, secondary powered devices can be installed. Designs vary from door-mounted timers to wall mounted alarm boxes. These solutions typically employ a siren at the door, and can be mounted as battery powered or hardwired units. Cost, including installation, range between ~\$150 to ~\$250.

Using Door Closers

The importance of the door closer is overlooked in door prop problems. Most often, these devices use a spring or hydraulic arm to pull doors automatically closed after they are opened.

Note: [***Click here to watch the demonstration on IPVM***](#)

Door closers are specified according to pull strength, the type of door they are fixed to, and how rapidly/slowly they must operate. For more, see our [Door Closers: Critical Security Hardware](#) post.

The surrounding environment, like predominant direction of wind or balance of the HVAC system may also play a role in specifying and adjusting a closer to properly shut the door.

Quiz

Finally, after reading, take our 5 question quiz.

Visitor Management Systems Examined

"Who are you, and why are you here?"

Facilities that implement Visitor

Management Systems hope they never need to ask that question to anyone, ever. While access control goes to great lengths to make sure only approved personnel are able to enter approved areas, they hardly ever handle



'temporary access' well. For that, Visitor Management fills a niche, and claim to do a better job than the old, proven clipboard sign in sheets.

Three Goals

For every visitor management system, there are three basic goals for the system:

- Accountability: No one is allowed to enter the site without first logging it. This guarantees that no unidentified person is wandering around a potentially dangerous or sensitive site, but it also matches that visitor with a specific sponsor, typically a permanent employee. This makes sure that the visitor's business is directly tied to a meaningful task and often results in a fully escorted visit while onsite, increasing site security.
- Visibility: While ID Badges and access credentials may only be issued to permanent employees, most visitor management systems include temporary badging, good for printing inexpensive labels worn for a few hours that make it clear someone is indeed a 'Visitor'. If

someone is observed onsite that has neither a permanent ID or temporary visitor badge displayed, they very quickly can be identified by guardstaff as potential intruders.

- Quickness: Large facilities may be faced with handling hundreds, even thousands, of visitors per hour. Especially for high-security facilities like military bases or critical infrastructure sites, quickly processing valid large volumes of visitors is essential for timely visits, reduced service costs, and keeping tight appointment times.

Additionally, most visitor management systems keep logs of visitor activity and the scope of why they visit. Because of this, a variety of other systems, including physical access control, accounting, and vendor performance, might be integrated although fairly uncommon because of cost.

Common Components

While the exact mix of hardware and software needed for the system vary, most systems use these basic components:



Here is an overview of each one:

- **Workstation:** The central software is PC based or network server based, and most enrollment stations center around the data entry workstation.
- **ID "Mugshot" Camera:** A camera provides visual record of a visitor, and even paper badge labels generally include a small black and white printout of the credentialed visitor. Some platforms use purpose built 'ID cameras', while other systems use common webcams or even surveillance cameras to collect mugshot images.
- **Paper Badge Printer:** The end result is a temporary credential printed on a label marker. (See example below.) The composition of the badge makes the wearer's identity as visitor clear, and may include

barcodes for provisional logical/physical access and include the expiry date.

- **Barcode Scanner:** If the barcode printed on visitor badges need to be enrolled in other systems, the enrollment station includes a reader to scan the badge into information or asset tracking systems giving the wearer provisional privileges to use access protected systems.
- **D/L or ID Reader:** In some systems, an optical or magstripe reader that can read general ID badges, like Driver's Licenses (D/L) or Government Common Access Cards (CAC) contain values that can be pulled into the visitor management system.

The 'temporary' paper label visitor badges often resemble the example below:



System Costs

In general, the cost of a visitor management system includes software, hardware, and supply items like labels and ink. The actual costs vary on the exact configuration and level of integration with other systems, but ballpark costs range about ~\$3,000 - \$5000 per enrollment station including all software, licenses, and peripherals/supplies. Some common platforms include:

- HID's EasyLobby: The most commonly used system, its cost ranges from ~\$3000-\$8000 per station (typically one per building). Price depends on level of integration with mobile readers, cloud servers, and asset scheduling programs (meeting rooms, vehicles) or physical security systems like access control.
- Jolly Technologies 'JollyPro' is a budget alternative: a ~\$3500 kit includes software, readers, cameras, and scanners, but does not include the workstation and does not integrate with other systems, a reason why larger users choose HID EasyLobby over this.

Other options are available as extensions or modules of ERP or Subcontractor Management systems, but the needed basic components are the same.

Applications

Not everyone needs a Visitor Management system. Even facilities with aggressive access control may not need to implement visitor management beyond a well-policed clipboard system. However, the buildings that stand to benefit most from Visitor Management include:

- Large Visitor Volume: Where booking visitors requires devoting labor hours to the task, a Visitor Management system can gain efficiency. With simplified data entry, sponsors doing 'pre-checkin' paperwork, and stored record access, sites can significantly speed up the process of getting visitors onsite quickly without compromising other security policies.
- High Security: Anywhere that places a premium on knowing the identity/business of EVERY individual onsite could use Visitor Management to make administration of the policy easier, and use

the temporary ID badges to reduce the cost of credentialing every user.

- High Liability: Many sites contain dangerous locations. Furthermore, any visitor onsite may need to file proof of insurance or be recorded onsite to be covered by existing policies. Visitor management creates or manages these records.
- Repeat Visitors: In some cases, visitors are frequent guests. Rather than spending time every visit manually entering repetitive information, visitor management retains the information and can mean recurring visitors are able to conduct their business more efficiently.

Up Next - The Industry's Best New Product?

A visitor management system won ISC West's best in show award. In our next post later this week, we will examine their value and potential relative to traditional systems.

Time & Attendance

Access Control is useful for more than unlocking doors. One of the best features is also rarely used: Time and Attendance logging. However, selecting the 'same old' door readers for can open several vulnerabilities to abuse.

Time Logging is Central

One of the most powerful features of EAC is the time/date stamp associated with every event in a system. Not only do systems log when door opens, they also record whose credential was used to open them, typically down to the second.

Time Logging makes it possible to 'track' a user's movement through a system, and provide a concrete record of where a person was at a given time. These logs have even been used to solve murders and otherwise establish presence at certain times with high precision.

Time Clock Function

With relatively minor adjustments, most EAC systems can use 'time logging' with time clocks.



Many workers are paid an hourly wage. Clearly establishing when they start their job and when they stop working is crucial, as 'time' is indeed 'money'. Capturing this time has traditionally been the function of precise clocks, where workers insert cards to have the time indelibly punched out on a given day. Indeed, "punching the timeclock" is a common saying.

However, the method is not problem free. First and foremost, abuse is a risk, where an employee punches more than only his/her card. This type of fraud is at the forefront of many HR and Corporate issues. Many seek to eliminate this risk/temptation entirely. While time clocks are primarily intended to protect the employer, the employee also benefits from having a clear record of attendance to lean on when calculating paid vacation days, sick days, or overtime pay.

Using the EAC system for Time & Attendance often means setting aside separate readers for the sole purpose of recording 'In' and 'Out' entries in the system. Once a pay period closes, a report is created listing activity on these two readers, summing the 'In' periods and subtracting the 'Out' intervals leaving an accurate record of attendance.

Multi Factor Makes Sense

In order to avoid the pitfall of 'buddy punching' (a risk EAC systems normally call 'passback'), Time and Attendance readers should feature multiple authentication factors, including fingerprint or palm readers. This 'extra authentication' ensures that no one can casually misrepresent themselves as another person.

Most modern EAC Time & Attendance readers feature biometrics, typically resembling the examples below:

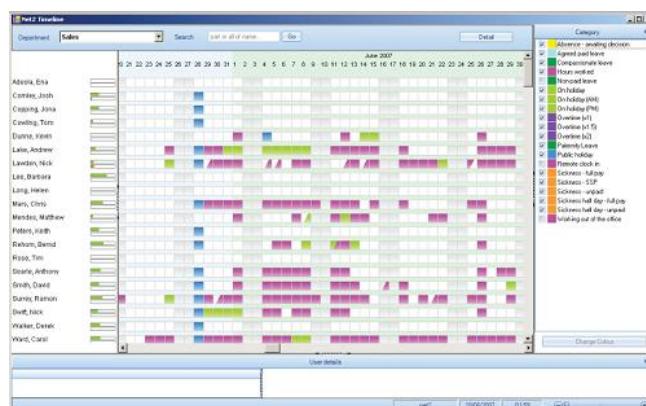


Multifactor 'Time & Attendance' Readers

These style of readers are sometimes sold as 'standalone' timeclock systems that require no EAC system interface, but this increases cost when connecting them with access headends. EAC systems simply need an interface to collect this data. General biometric access readers can be used in this role successfully (e.g., see our [3M/Cogent's MiY Touch](#) note for example).

Payroll Integration

When EAC platforms market 'time and attendance' function, this is frequently more than generating custom reports. Many EAC systems will format data so it can be manually exported into payroll systems like [Kronos](#) or Sage. However, this is typically a manual process, and accounting or payroll staff require instruction on the access platform to collect reports. The screenshot below shows [Paxton's](#) default export screen of Time and Attendance data:



In other cases, 'Time & Attendance' function may be based in the Access Platform, but an additional 'payroll module' is added to the platform for direct integration. This additional software becomes the default payroll platform, so adoption in large systems may need approval from 'non-security' stakeholders.

Common enterprise-grade platforms offer additional 'software module' solutions, including:

- [Lenel](#)
- [AMAG](#)
- [Software House](#)
- [Continental](#)
- [Honeywell](#)

Costs

Readers: You could simply use a regular card reader but if you want to avoid buddy punching, time and attendance biometric readers range between ~\$300 and ~\$2000 each, with high-accuracy optical fingerprint readers costing around \$700 each. (See our [report on fingerprint readers](#) for more detail.) Multiple readers may be required for large sites, and expanding the EAC system often includes adding controllers or interfaces to support those readers.

Basic Software: General costs to add a Time and Attendance module range from 'free' upwards of ~\$3000. Many platforms offer a '[no additional cost](#)' timeclock functionality to their basic system, but the data must be manually incorporated into a payroll platform.

Advanced Software: 3rd Party software / integration module provides more automated interface, but typically costs between ~\$500 and ~\$3000, generally depending on the size of a company's employee roster and number of sites data is collected. For most enterprise access systems, these modules cost about ~\$1,000 each.

What are the Risks?

While using EAC to host time clock function can be advantageous, it is not without risks:

- **Clock Drift:** In effect, the EAC system clock serves as the payroll clock. While a variety of solutions for syncronizing/standardizing time exist, such as NTP Servers and central data clocks, differences between EAC and other timepieces can create significant problems. When EAC is used for Time and Attendance, keeping system time in sync with the local standard time is vital.
- **Single System Breakage:** Or rather 'Putting all your Eggs in One Basket'. As a matter of redundancy, if your EAC system drops offline, so does your Time Clock. Why hiccups in granting access through offline doors can often be solved by issuing mechanical keys, no simple solution exists for Time and Attendance failover. You might want to have an older manual timeclock as a backup, just in case, and for the time the system is offline, manually reconcile the timeclock entries.
- **Passback Conflicts:** For access systems using 'Anti-Passback' controls, logic discrepancies can cause low-level conflicts with Time Clock readers. If an employee 'scans In' to the timeclock, and then immediately 'scans In' to a normally secured door, the EAC system

may generate an alarm or deny access unless the timeclock reader is isolated from passback rules. Given the large number of doors across multiple sites, or large populations of employees in a single system, these sort of errors can be common and hard to troubleshoot.

What are the Benefits?

However, it makes good business sense to use EAC to host 'Time and Attendance' function, including:

- **Less to Buy, Maintain:** While a single system can be a weakness, it can also be efficient. Many facilities prioritize the upkeep of facility access systems, and issuing a credential for access also means it can be used for payroll. The investment in one facility system can be leveraged by another.
- **Expanded Security Controls:** In normal use, if an employee has a security credential revoked in an EAC system, they immediately become invalid in the payroll system. In addition, tying the two systems together can prevent an unauthorized employee from gaining access to an 'Time In' reader before an allotted shift and help manage overtime payouts, and payroll hour allocations are enforceable by physical access controls.

Access Control Job Walk

Significant money can be saved and problems avoided with an access control job walk if you know what to look for and what to ask.

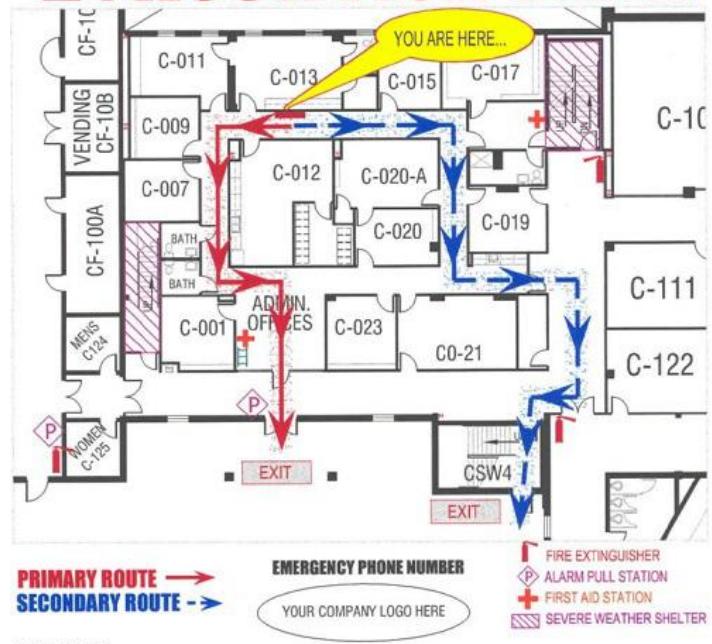
By inviting interested parties onsite for pre-bid job walks, many of the site conditions inadequately described in solicitations can be examined firsthand. Indeed, in some cases, the most costly parts of the design are not covered in bid documents.

Four Tools Needed

Having the right tools makes work more efficient and effective. A job walk's main purpose is essentially to gather as much information as possible in a short amount of time. At the least, each job walk participant should carry:

- Floorplans: In order to take detailed notes about the facility being controlled, a key document to have is a scaled drawing of the site. If not provided in a bid package, a common source for workable drawings are in commonly posted 'Fire Evacuation Routes' in many buildings. If no drawings are available, images from [Google Maps](#) can sometimes provide a good start for drawing design sketches. In any case, having these before the walk begins helps recording important details a quick process.

EVACUATION PLAN



Evacuation Plans Useful as "Maps"

- Tape Measure: Physical distance and dimensions should not be guessed, as access designs often cover hundreds of feet and fractions of inches.
- Flashlight: Often access control ties into utilities or spaces not in plain view. Being able to clearly see into dark crawlspaces or attics is critical for paths to run cable or install controller panels is crucial.
- Camera: Perhaps the most useful tool is a camera with plenty of storage for snapshots. Not every customer will permit pictures to be taken, so prior approval should be given, but when allowed there should be no reservation in photo documenting a site. Both sides of a door (secured/unsecured), adjacent structural details like walls or windows, the area immediately surrounding the door including ceiling types, and any important details like closets or server rooms should be photographed, as being able to refer to those details during bid development can be critical. When in doubt, take more

pictures than you may think you need, as it is typically hard to go back yet there is little cost for having extra pictures.

Five Door Details To Look For

During the walk, every future controlled location should be visited and notes taken about how it is situated. Paying attention to how they have been designed and assembled at key points can greatly affect design.



Most often, swinging or rotating doors are the points of access control in a building:

- Device Install Locations: Access Control typically adds Readers, Locks, Controllers, and Cabling to a door. Stepping through how and where each of these elements is installed is foremost in making the visit a success. Having at least provisional knowledge of how installation tasks work and flow are helpful in understanding how site conditions impact system design. Taking careful notes and photos of how the opening is built means the best choice can be deliberated afterward and is not a snap decision.
- Door types: For every door, the exact configuration and composition of the opening varies. Taking note of existing door hardware, special ratings like fire ratings, and the alignment/maintenance of the

opening is important because it likely is not reflected in bid documents. Our [Installing Door Hardware primer](#) offers good basics for evaluating the condition of a door.

- Special Use: Is the door an Emergency Egress? Can it be modified to accept access control if it is a fire door? In these common cases, the options to control access through them is constrained.
- User Accessibility: How will installed access equipment affect accessibility? Will a user on crutches, in a wheelchair, or with limited use of hands be able to gain access? If not, how will they be accommodated for? The answer may affect where equipment is located, but also which type of equipment is used.
- How is the door used? Are you controlling a main entry, or is it delivery access? Will the door need to be opened and unlocked many times per hour? [Mechanical lock grades](#) typically grow more expensive the heavier they are used, and hardware that wears, binds, or breaks should be avoided for busy access points.

Three Cable Details To Look For

Next, planning how the doors and devices should be networked together is needed:

- Network Design: Establishing utilities like cable trays, wire raceways and access panels typically make the job of designing networks easier. Instead of guessing where cable should be run, the decision has already been made but may not be clear in bid documents.

Pull locations: Efficiently staging cable boxes/reels for minimum number of pulls can shave thousands in labor costs from a design. Accessibility is key, but planning cable pulls so that bends, turns, or terminations/connections

are minimized ensures that overlooking a significant installation cost does not lose the bid. If staging cable reels or boxes in a hallway, will they block normal traffic? Or if the shortest cable pull runs overhead of an office or breakroom, will disruption be a concern? Being mindful

- of where cable should be run may also influence when it can be run, potentially impacting cost.



Cable Pull Labor drives Cost

- Wireless: Even if no cabled network is installed, is wireless strength sufficient to reach and connect all wireless locks? Most wifi lock manufacturers offer a wireless survey toolkit that allows a quick check of signal strength at all doors. Logging readings at every location helps identify the gaps early before it becomes an operational issue.

Panels/Power Supplies/Servers

Finally, checking to make sure that everything has enough space to be installed and is secure in those spots should be reviewed:

- Mounting Real Estate: Checking for open wall or rack space, or empty spaces above the door means no ugly surprises during install.

Finding that there is not enough room to mount central equipment can be an expensive oversight, and ultimately it may affect with type/form factor of hardware is selected. In the image below, seven doors worth of hardware takes up ~50 sq. ft. of wall:



Real Estate Needed

- Keeping it Secure: Keeping security equipment behind locks, alarmed, or hidden should not be left to chance. Stepping through potential locations with system security in mind will protect the entire facility.
- Power Tie-In/ Locations: Confirming both availability and location of electrical service at the door or closets are important. While distance often can be addressed by cabling, the material and labor costs, and potential code restrictions are important to note before work begins. If approvals are needed to tie-in to existing utility, this should be done promptly rather than assuming permission exists.

Upgrades And System Takeover

While not as common, some may be called to walk access systems slated to be changed or significantly upgraded. Taking inventory of which parts can be reused or which ones must be changed can account for thousands of dollar per door.

Door Controllers

One of the costliest parts of an access system is the board or panel used to coordinate activity at the door. In many cases, the hardware used is proprietary to a particular system. However, the use of 3rd party hardware products is common, and even if not marketed that way. If controller equipment is sourced from Mercury Security, HID Global Edge/VertX, or Axis, there is a high possibility of connecting the opening in its current configuration to another 3rd Party Compatible management system. Check our [Axis vs HID vs Mercury Access Controllers](#) post for more on potential reused controllers.

Typically Reusable Parts

Other common components are typically reusable when connected to new access controllers. While the cost of reterminating these devices into new devices should not be assumed as a 'zero-cost' activity (new cable may need to be run), these devices are typically compatible with access systems in default formats:

- Readers: Card, PINpads, or even biometrics are often reusable if connected to controllers in Wiegand or OSDP formats.
- Locks: Basic low-voltage rate power supplies and relay contacts make lock almost always reuseable.

- Door Position Switches: Simple sensors that monitor NO/NC circuit conditions are typically compatible with access systems.
- User Credentials: And finally, if the companion readers are compatible, then existing credentials often are as well, however confirming the format types with new system providers is a prudent step.

Converting Databases

Finally, another substantial portion of access systems can often be partially reused, if not also requiring rework.

The underlying user database can often be exported and then imported into other access systems, preventing the manual data re-entry of thousands of records. The process varies, and in some cases specialized database translation tools must be used, but spending a few hours configuring a conversion process can save hundred of hours rekeying the same data into new systems.

How to Use the Findings

Developing project estimates is a substantial topic all its own. However, for most jobs having multiple skillsets examine the collected findings is helpful to determine the best plan of action or installation path to address them.

Even the most experience designer benefits from a roundtable-style post walk meeting where the exact system design is established. Having multiple sets of eyes with different responsibility viewpoints means glaring mistakes and bad assumptions are less likely to end up quoted.

Also, having the full scope of trades review the data collected during the walk allows a clear understanding of where labor gaps exist. If advanced skills like finish carpentry or locksmithing is needed to pull off a job, reviewing the findings of the job walk get them out in the open as soon as possible.

Quiz

Finally, after reading, [take our 5 question quiz.](#)

Hazardous & Explosion Proof Access Control

Controlling access to hazardous environments require equipment meeting specific ratings that certify they will not start fires. Understanding those ratings mandate careful selection. We explain:

- Where is explosion proof access equipment required?
- What are the three considerations for Hazardous rated access control?
- Hazardous rated access equipment including Assa, HID, Interlogix, and others.
- Typical product cost
- What are the ratings? Including NFPA 70, EX, Division 1, Division 2, and ATEX directives 95/137
- What do the ratings mean?

Explosion Proof Surveillance

For a companion piece detailing explosion proof camera systems, and the specific requirements of that equipment see our [Hazardous & Explosion Proof Video Surveillance](#) note.

Where is Explosion Proof Access Equipment Required?

In general, any location where ignition of fumes, vapors, or any flammable material is kept or processed may fall under a 'hazardous area' restriction. In general, fire potential is the concern, as locations with high radiation risk or toxic material exposures are less common and classified differently.

Examples of common hazardous area locations are petroleum based chemical storage areas, like gasoline tank farms, chemical processing and refining sites, or any locations where airborne dust may be ignited common to manufacturing plants or agricultural storage granaries.

Automobile fueling stations are not typically classified as 'hazardous areas' requiring special equipment, however, care should be taken to confirm or investigate if a location requires rated access control equipment.

What are the three considerations for Hazardous rated access control?

Access controlled openings, unlike video surveillance cameras, typically require multiple components all installed together within dangerous areas. Therefore, all hazardous area access needs to be installed observing three basic rules:

1. All devices located in the hazardous area, like readers and locks, need to meet explosion proof ratings of the area.
2. Any data or power cabling for those devices need to be made intrinsically safe when it enters the area.
3. Wiring connections to devices like readers and locks should not be capable of causing a fire.

These requirements generally can be accomplished by using rated equipment with the approval of an AHJ. Options for meeting specific ratings can be readily found, as we detail in the next section.

What equipment satisfies this requirement?

In general, access control inside hazardous areas locates as many system devices as possible outside of the rated area. Accordingly, components like

access controllers, panels, low-voltage power supplies, and network switches are installed in safe zones and require no special ratings.

However, not all devices can be moved and must be hung immediately adjacent or onto openings within a hazardous area. The most typical components needing to be certified are detailed below:

Readers

Because credential readers and keypads are typically hung immediately at the opening, it is common that these devices must carry a rating.

A number of options exist that depend on specific rating and credential format support, but include examples from large manufacturers including:

- [HID Global/Class 1 Div 2 Mullion \(~\\$300\)](#)
- [Honeywell Class 1 Div 2 Keypad/Gate Interface \(~\\$1200\)](#)
- [Sentry/ Class 1 Div 1 Enclosure Mount \(~\\$800\)](#)



Hazardous Location
MiniProx shown with
incorporated junction box
rated for use in hazardous
locations.

Door Position Switches and RTE Devices

Another device typically hung onto doors in hazardous areas are Request to Exit devices and door position switches and contacts.

Rated examples include:

- [Assa Explosion proof RTE Pushbuttons \(~\\$1100\)](#)



- Interlogix Magnetic Contact (~\$125)
- Falcon EX Rated PIR (~\$900)

Locks

Interestingly, maglocks are the most common type of hazardous rated lock available, despite other types of locks like electric strikes being preferred for traditional openings. Maglocks are used because their typically potted, solid state, and enclosed construction is easier and less costly to manufacture as explosion proof compared to the basic inductive coil/solenoid driven operation of strikes and exit devices.

Rated maglocks include:

600 lb bond 12/24 DC, Class 1 Div 2 unit (~\$1000)

However, special order products from manufacturers like Securitron are available.

Integral Door Locks

In many cases, the explosion rated door or gate itself will be designed with a mechanical security lock, and the access system will integrate to it via controller or relay contacts.

However, other elements of the door may be responsible for keeping a door closed, or even open, as in the case of explosion rated Door Holders and Door Operators. These devices are application and opening driven, and may cost \$5000 or more.



Airlocks/Mantraps

In many cases, aggressive forms of controlling access are physical elements of opening design for hazardous areas. Features like door interlocking systems or elevator interlocks designed to allow only strictly controlled and verified personnel into the rated room.

As we note in our Mantraps Examined note, these features typically involve using a series of doors and separate rooms to segregate hazardous areas from general populations of people.

Explosion Proof Enclosures

In some cases, non-rated equipment must be installed in hazardous areas, and elements like cabling or power wire must be run into a rated area.



For this, a variety of general purpose enclosures, junction boxes, and wire seal compound is available. However, the rating and degree of protection needed from these general items are subject to AHJ approvals:

- Rated Enclosures
- Wire Termination Seal Compound
- Rated Junction Boxes

Prices for these general items can range from a few hundred to ten thousand dollars or more depending on dimension, rating, and whether or not being filled with inert gas or sand is required.

Explosion Proof vs Blast Resistant

For openings, two different rating systems are often cited as 'special conditions' and may even appear together in the same door. However, these ratings indicate two distinct properties:

- **Explosion Proof:** Doors and related equipment will not introduce or sustain potential ignition in a hazardous environment
- **Blast Resistant:** Doors can sustain an explosion or pressure load and still retain their structural properties

It is important to not munge these requirements together and assume either preserves proper ratings.

How do I know when to consider special rated equipment?

If you are an integrator, security manager, IT manager or manufacturer, you should not be deciding yourself whether or not special rated equipment is required.

Typically, the 'AHJ', or 'authority having jurisdiction' makes this determination. The AHJ might be a Fire Marshal, an operational risk assessment engineer, occupational safety authority, or even an insurance underwriter. That individual will classify the hazardous area based on risk criteria. It is the best interest of the owner/operator of such an environment to realize, control, and mitigate any potential risks in the hazardous area – including the installation of electronics equipment like surveillance cameras. Installers are typically asked to provide appropriate certification of the furnished equipment.

In general, a key indication that hazardous access gear is required comes from observing occupational protective equipment or process equipment in the area. For example, if all area workers need to wear electrical grounded clothing or if area forklifts have an EX rating, the area likely requires explosion-proof access equipment. However, it is important to base equipment specifications upon solid confirmation of the area, as the cost of equipment certified as 'safe for use', or 'intrinsically safe', is significantly more expensive than non-certified equipment.

What does a particular 'hazard rating' mean?

Worldwide, a variety of hazardous area certification marks exist, and it is appropriate to furnish equipment that satisfies whichever prevailing standard applies to your application.

United States

In the US, the widely adopted "National Electrical Code or 'NFPA 70', defines environments by flammable volatility. The classification is segmented in three (3) classes, with a Class 1 environment being the most volatile typically including sites that handle gasoline and chemicals. An accompanying clarifier (the Division) denotes the default danger 'type of condition', being Division 1 – normal, or Division 2 – abnormal.

In this manner, the risk of fire or explosion in a hazardous location can be qualified. For example, portions of a fuels transfer facility may be designated as a 'Class1/Division1' area, while a wood pulp storage facility may be designated as a 'Class3/Division2' facility. Both classifications denote some risk, but certainly the risk is qualified as being more significant in the area with the lower rating.

Globally

In the EU, a rough equivalent for the NEC's Class/Division rating is noted by the 'ATEX directives, 95/137'. While technical definitions of hazardous areas differ (and may not overlap) among standards, the ATEX directive seeks to quantify hazardous areas in the same manner.

In South America, especially Brazil, the INMETRO risk classification system performs the same function as the bodies listed above.

While independent of each other, these ratings all seek to explicitly define hazardous areas

"Future-Proofing" Access Control

It's one of the most misused phrases around: "Future-proof". However, even without the crystal ball and wizards, designing access control to be "future proof" is much more practical than the concept implies.

The features we tag as 'future proof' are:

- OSDP
- Smartcard Frequencies
- Door Controllers
- Third Party Controllers

While we explain why these products or features should be avoided:

- ONVIF C
- 125 kHz Cards
- Combo Readers and Controllers
- Mobile Credentials

Adopt

First, here are the technologies to use in your access system, and why you should:

- OSDP: A new approach that resolves longstanding security vulnerabilities between controllers and readers is OSDP. The protocol is billed as a replacement for Wiegand by offering advantages like encryption, two-way communication, and accommodates more credential data, faster. (For more detail, see our [Wiegand vs OSDP note](#)) Moreover, while the protocol is still

new, adoption by industry majors has been widespread with leading companies on both the reader and controllers side already adopting it.

- 13.56 MHz Credentials: While not new, the market has been slow to migrate to the higher frequency, more secure 'smartcard' frequency format. However, as time progresses, the availability of older formats becomes more difficult and expensive, security risks aside. With mainstream vendors like HID building new readers that primarily use 13.56 MHz formats, avoiding costly changeovers mean adopting the format now.
- Decentralized Controllers: In the past, the most common architecture for access was to use one panel to control four or more doors, sometimes as many as 32 in one enclosure or even eliminating door controllers entirely (see our Eliminating Control Panels? Viscount review for one example). However, with the emphasis and availability of IP networks within modern facilities, adding a 'smart controller' at the edge is not a challenge and offers savings to endusers in reducing cable and installation labor to a few feet rather than homerun to central closets.
- 3rd Party Hardware: While 'proprietary' cannot be eliminated outright from access, restrictions can be lessened by adopting hardware controllers that can be used in multiple systems. Options for interoperable devices are limited to the three major providers and controllers we list in our Axis vs HID vs Mercury Access Controllers note. An enduser with hardware from one of these providers typically has multiple management platform options to chose from if the current choice is failing to get the job done or goes out of business.

Avoid

And here are the technologies to steer clear of and the reasons why:

- ONVIF Profile C: Despite grabbing attention early, ONVIF's access interoperability guideline has fizzled with no significant adoptions since Axis released their A1001 two years ago. The current outlook for ONVIF and other interoperability standards is grim with little market traction, detailed in our [Access Interoperability: Going Nowhere](#) note.
- 125 kHz Credentials: Steer clear of older, much exploited, unencrypted contactless credentials using the 125 kHz frequency. Despite YouTube being full of videos revealing how to use \$50 cloning kits widely available online, many endusers and integrators still are adopting it is the key to their systems. In our most recent [Favorite Access Control Credentials](#) survey, a whopping 36% still call the type their preferred option. However, with costs for 125 kHz cards and readers typically equal or more than 13.56 MHz products, there is little reason to continue using them.
- Combo Controllers: While decentralized controllers make good sense, the idea can be taken too far, as is frequently the case by combining the controller with the reader. The major weakness of the approach is the vulnerability when hanging the units on the unsecured side of the door leaving the opening - and subsequent area security - at great risk to intrusion threats. We detail the risk in our [Access Control: Combo Reader / Controllers Tutorial](#) note.
- Mobile Based Credentials: Few access technologies have gotten the hype of smartphone credentials. The slick imagery of access users waving their smartphones in front of a reader instead of a stale,

boring ID card may make for great tradeshow buzz, but shifting to mobile is expensive and raises big operational problems, like how willing smartphone users will be letting employers manage device settings, how credentials are provisioned, and whether or not users need to carry cards anyway for picture IDs. We examine these major issues in our [NFC: Not Ready for Primetime](#) note, but they also apply to [BLE \(Bluetooth Low Energy\) for Access](#) as well.

Cost Savings

The exact dollar figure impact of these decisions is substantial, and savvy designers and end users can save thousands by 'buying right' upfront.

For example, a 'forklift upgrade' of proprietary controllers instead of reusing existing 3rd Party Hardware can amount to over \$1000 per door when costing the additional controllers and installation labor. The cost of upgrading a reader to work with 13.56 MHz smartcards can be \$200 per reader and \$10 per card for each user when existing 125 kHz options are [discontinued by the vendor](#).