

WHITE PAPER

Advanced physical access control security measures

Summary

One of the first systems installed when securing an organization is the access control system, which controls access into and out of one or more facilities.

Beyond installing readers, deploying door controllers, configuring software, and issuing credentials, organizations have a number of potential tools at their disposal to protect their people and assets. Written as a best practices guide for physical access control, this white paper first offers a summary of basic ACS tools and then delves deeper into advanced physical security measures and how they can be used to significantly increase safety and security.



Physical security – introduction to access control systems

Physical Access Control is about protecting people and assets. The primary focus is to keep an area secure by restricting access to unauthorized personnel. An electronic Access Control System (ACS) controls entry and exit to rooms or facilities using a wide range of credentials. Credentials can refer to tangible or intangible objects that prove the identity of an individual like a password (something they know), an access control badge (something they have) or a biometric feature (something they are). Based on the credentials presented, an ACS determines who is allowed, and where and when they are allowed to go. Basically, once credentials are verified and the ACS grants access to the authorized cardholder, an access control point—which can be a door, turnstile, or other physical barrier where access is electronically controlled—is unlocked and the transaction is recorded by the system. In addition, the system also monitors the doors and sends alarms such as when a door is forced open or held open too long after being unlocked.

Deploying readers and controllers

Used to control entry and exit, the reader and the intelligent controller—called the ‘door controller’—are two basic components of any ACS. An integral element of any access control point, the reader takes information from credentials and communicates that data to the controller that hosts all of the security functionality to make access decisions. A controller is often connected to one or more readers (one or more doors).

Issuing credentials

Credentials are claims of identity and are vital for managing who has access to a room or facility. An ACS uses credentials to identify who is requesting access through a secured access point. For access control to be operational, every cardholder must possess at least one credential, which is typically (but not exclusively) an access control card. Some of the common forms for credentials are cards and badges, clamshell cards, key fobs, stickers/tokens, and embedded chips.

Defining cardholder access rights

As the ‘who’ in any access control system, a cardholder represents a person who can enter and exit secured areas by virtue of their credentials, and whose activities can be tracked. It is often best to implement some form of role-based access control. By mapping out accessible areas and valid schedules—for instance, time periods during a day or a week—an organization can use its ACS to control who goes where and when by assigning cardholders to cardholder groups and then giving those groups certain access privileges.

In addition, an effective and secure ACS must have

- formal request and approval steps,
- record-keeping abilities to track who is making each request, who the request is for, the access control areas involved, and who is actually providing the access, and
- logs of access request approvals and denials, including who did the approving or denying.

Issuing printed badges to visually identify cardholders

To allow security personnel to visually identify cardholders and add an additional layer of security, some organizations will issue printed badges that double as picture ID badges with the cardholder’s picture printed on the badge. Printed picture ID badges also allow the average cardholder to report misuses of credentials by simply looking at a cardholder’s ID badge.

ACS monitoring and supervision

Finally, a basic ACS must supervise a variety of inputs and devices, including individual doors and readers, and provide notifications to security personnel concerning significant events and alarms, including

- successful cardholder entry to any area,

- unsuccessful entry attempts, which should be investigated to determine whether an intruder attempted to gain access,
- impossible activity, such as someone being in two places at the same time because it is an effective way to identify a cloned card,
- the tampering with or removal of card readers, and
- the malfunctioning of any device in the system.

However, an ACS can effectively protect an organization only if security personnel are continuously monitoring the status of the system or are notified in real-time of any violations.

Visitor Management to manage visitors as opposed to a sign-in sheet

Rather than relying on traditional visitor sign-in sheets or log books, a growing number of organizations leverage their ACS for electronic visitor management or deploy a 3rd party visitor management system to sign-in and track visitors. With an electronic visitor management system, a visitor is signed-in using a workstation and a temporary visitor badge is printed and given to the visitor. The major benefits of using a visitor management module or a dedicated system include

- the accurate and consistent recording of visitor information,
- the capability to quickly print a personalized visitor badge that contains the visitor’s picture,
- the assignment of a credential to a visitor and associated access rights to a facility,
- the ability to quickly create reports of visitor activity since all visitor information is stored in a database, and
- being able to pre-register visitors in the system and speed up the sign-in process upon arrival.

Advanced access control measures

The following are more advanced security measures that an organization can implement to further secure or restrict access to their facilities. By deploying each measure on its own, an organization can incrementally increase their overall level of security. But, when several measures are deployed together simultaneously, security can be significantly augmented.

It is important to keep in mind that not all ACS solutions support these advanced security measures. Consequently, when trying to determine the best ACS solution for an organization, it is important to determine which ACS supports specific security measures.

Emergency/duress buttons and panic alarms

Emergency/Duress buttons or panic alarms allow personnel under duress to silently, quickly, and conveniently call for help without drawing attention to themselves. Because these alarms are silent, they are ideal in situations in which personnel believe that it would be unsafe to use more conventional means of communication—such as a phone—for fear of escalating an already dangerous situation. Most organizations can benefit from duress buttons that are strategically deployed throughout a facility to trigger alarms when a threat is present.

These alarms typically consist of two components, the panic button and the communications system. Installed in locations where it can be easily reached but

hidden from the casual observer, the button is a wired or wireless device that the person activates when they need help. The communications system refers to the way in which help is called once a panic button is activated and could involve the ACS communicating with an off-site alarm monitoring center, a security command center, a mobile app, or with non-security personnel.

Readerless door management

Readerless doors provide additional oversight by allowing an organization to monitor doors equipped with only sensors and locks. Using this security measure, an organization can also automate when a door will be open and closed, regardless of the presence of an access control reader and without the need for external hardware, such as timers. Typical applications for this security measure can be found in schools, department stores, or shopping centers with automated unlock schedules.

By deploying this type of door setup, an organization can assign unlocking schedules—which determine when a door shall be automatically unlocked—and exceptions to unlocking schedules to a readerless door. In addition, it is also possible for the ACS to monitor, log door activity, and monitor usage patterns.

To manage a readerless door as part of an ACS, the door needs to be equipped with one or more of the following: a lock, a REX (request to exit) button or sensor, and a door contact (detects when a door is open or closed). Then, the ACS can use the inputs and outputs of a standard IO (input/output) module to monitor and control the door's behavior, including unlock schedules.

Antipassback—soft and hard

Tailgating, a common security risk in ACS, occurs when an individual simply follows an authorized cardholder—knowingly or unknowingly—through an access point. Although an ACS can control which cardholder has access, it cannot, once a cardholder opens a door, control how many people follow behind the cardholder through the door.

While it is possible to reduce tailgating through cardholder security awareness training, the problem can usually only be reliably solved through the use of special anti-tailgating devices, eg. turnstiles and mantraps, that permit only one person to enter or leave an area at a time. These security measures use a physical barrier that allows only one person to pass, or use sensors that detect when a person is attempting to tailgate or when more than one person tries to enter using the same credential.

The antipassback security measure prevents the misuse of an ACS by establishing a specific sequence in which credentials must be used in order for the system to grant access to personnel. This measure is ideal for protecting an organization against the use of duplicate cards since an ACS with this security measure will refuse to grant access to a cardholder who is already inside the facility.

Commonly used at employee entrances with card readers installed on both the inside and outside of the access point, this security measure requires employees to card-in when they enter an area and card-out when they leave the area. By ensuring that every use of a card at the 'in' reader corresponds to a use at the 'out' reader before the card can be used at the 'in' reader again, an ACS uses antipassback to make sure that a cardholder can only exit an access zone that they have already entered and can only enter an access zone that they previously exited. Any attempt to use a card a second time to gain access without first using the card to exit would trigger an antipassback violation.

Two of the more common types of antipassback are:

- Soft Antipassback—the ACS permits re-entry to the cardholder but logs an antipassback violation when the established sequence of use has been violated.
- Hard Antipassback—the ACS restricts entry to the cardholder and logs an antipassback violation when the established sequence of use has been violated.

By activating antipassback measures, an organization can greatly enhance its security by eliminating the deceptive use of cards and having alarms generated for each antipassback violation. It also provides an organization with an accurate count of the number of people in a particular access zone.

Global antipassback

There are two modes of antipassback, local and global. In local mode, the ACS only works to verify the cardholder's exit marking in relation to a local area or facility before allowing re-entry; this area is usually limited by the doors controlled by a single intelligent door controller. Global antipassback requires the ACS to verify the cardholder's exit markings on all areas and facilities within an organization before allowing re-entry; with global antipassback, different controllers within the same facility or across various facilities will exchange information so that they are all up to date. Global antipassback may be a key need

for multi-site or campus-style deployments when an organization wants to prevent a cloned card from being used simultaneously across sites.

Interlocks and mantraps

Interlocking is a security measure which prevents multiple doors from being opened at any given time to access a given area or room. Usually seen in higher security or restricted environments, interlocking ensures that only a single door is open at a time.

Similar to an interlock, a mantrap is also used to ensure that only a single door is opened to access a room. A mantrap consists of a passageway with a door at each end; after using their credentials to open the first door, the cardholder enters the passageway, closes the door behind them, proceeds to the second door, and then uses their credentials to enter the room. On occasion, mantraps will be equipped with sensors—including electronic beams, weight detectors, intercoms, and video cameras—that detect the total number of people present. If the mantrap detects that there is more than one person in passageway, an alarm sounds and access is denied.

While these security measures have traditionally been handled through programmable logic controllers (PLC) or dedicated devices, an organization that deploys an ACS that natively supports interlock and mantrap capabilities

- can leverage their existing ACS hardware,
- can configure and monitor all security measures from a single solution,
- can avoid deploying specialized equipment such as PLCs, and
- can eliminate the need to establish links between their ACS and interlock/mantrap devices.

Directional flow control

Based on the layout or specific security concerns at a facility, an organization may want to control the flow of traffic into and out of a particular area or

building. There are several security measures that can be used to achieve directional flow control:

- access gates, which allow an organization to control and canalize the flow of people into and out of a particular area or building,
- deploying entry-only readers on a set of doors and exit-only readers on another set of doors, thereby preventing a door from being used for both entry and exit,
- sensors, which detect when someone is moving against the intended flow of traffic and sound an alarm.

First-person-in rules to prevent the activation of an unlock schedule

To provide greater levels of safety and security or to protect unattended facilities, some organizations do not want people to gain access to certain areas unless a designated supervisor or employee has entered first or is actually present on site.

Typically deployed in schools and retail locations, the First-Person-In rule ensures that an access point configured to unlock on a schedule remains locked until a designated supervisor enters the area. At this point, the access point unlocks according to the defined schedule, allowing other users to enter. For example, using First-Person-In rules, the main entrance to a retail location that usually unlocks during store hours would remain locked until the manager or another employee is present.

First-person-in rules with ACS credentials and access rights

First-Person-In Rules can also be used to activate standard cardholder access rights. In this instance, employees can gain access to certain areas only after an authorized person is on site.

By enabling the First-Person-In rule for access rights, an organization can ensure that an access point remains restricted, preventing authorized cardholders from gaining access while an area is unattended. Once the supervisor is on site,

standard access rights are enabled and cardholders can use their credentials to navigate an area or facility.

Two-person rules for access to highly restricted areas

Access to certain highly sensitive areas that contain valuable assets, including server rooms, cash rooms, and areas with such sensitive data as intellectual property, should not be permitted to any single individual. To protect these assets, an organization can enforce Two-Person access rules to those areas. When implemented, this security rule ensures that entry to a restricted area is granted only when two authorized personnel jointly use their credentials.

An access point configured according to the Two-Person rule functions as follows: Two authorized cardholders are required to present their access credentials to the card reader within a specified time. Once access is granted, the door unlocks and the individuals are prompted to enter and close the door.

In some systems, after two authorized individuals have been admitted into the secured area, additional individuals can also enter but must still verify their entry. Many access control systems will monitor the number of persons in the secured area and display the occupancy total. Ideally, Two-Person rules should be flexible enough so that they can be enabled at entry points, exit points, or both.

Visitor escort

The needs of an organization with regards to visitor management will vary depending on the level of security required. While many organizations issue paper credentials to visually identify a visitor, others issue working credentials to visitors with unescorted access.

In the case of heightened security requirements, some organizations issue functional credentials and assign limited access rights, but still require escorted access to various areas. If an ACS supports Visitor Escort mode, then a visitor is able to use their credentials to gain access to an area but only when their escort—an employee—gains access at the same time. Functioning in a manner

similar to Two-Person rules, this guarantees that visitors are never alone when they enter certain areas and also ensures that their movements and their escort's movements are tracked at all times.

Security clearances and threat level management

To respond effectively to a growing array of potential threats, a security team may need to lock down a facility at a moment's notice, restrict access to affected areas, or prevent an intruder from reaching people or critical assets. To achieve this level of preparedness, an organization must have the tools and capabilities to change the status of its security system in real-time and in response to specific types of threats. Some vendors are addressing this need by offering what is known in the security industry as Threat Level Management.

Using Threat Level Management, an organization can automatically lockdown a room, an area, or a building simply by triggering a specific and pre-defined threat level. Activating the right threat level will usually be based on the type and severity of the identified threat. A threat level may be created to restrict access to everyone, authorized cardholders included, but still allow access to the security team or local law enforcement. This works to limit the intruder's movement while also preventing cardholders or visitors from walking into harm's way. By assigning individual security clearances in advance, the change in access rights can be virtually instantaneous as long as the capability is supported by the ACS.

Another important capability to consider is whether threat management is limited to the ACS or whether it can be linked to other security systems, such as the video surveillance, communications, or intrusion systems. More advanced systems can unify the simultaneous response of multiple systems, generating a comprehensive response to threats as opposed to piecemeal or system-by-system responses.

Multi-factor authentication

Multi-factor authentication is a highly effective way to ensure that the person presenting their card at a reader is the same person to whom that card was initially issued. This measure is ideal when an organization is concerned about protecting highly sensitive areas from unauthorized access, including when someone uses a stolen access card to enter restricted areas.

This approach increases the level of security by requiring personnel to use a combination of the following factors:

- something they have, eg. a credential,
- something they know, eg. a password or a keypad PIN,
- something they are, eg. a biometric feature like a fingerprint.

Human interaction could also be used in some instances to provide the second factor, such as verifying the cardholder's identity by using video cameras before manually unlocking a door.

For the greatest level of secured access, multi-factor authentication works best when three factors are required, but adding just one additional factor to a basic system can also be effective. A password or PIN is a relatively inexpensive second factor of authentication that can be implemented using card readers with built-in keypads. In addition to minimizing the threat of card cloning, readers with a built-in keypad minimize the likelihood that a lost card can be picked up and simply used to enter a facility. Taking it one step further, biometric readers ensure that the person presenting the card is actually the same person to whom that card was issued.

Security-of-security

Security-of-Security is a newer concept that is of great interest both to the physical security department and the IT department. Security-of-Security actually refers to the overall accessibility and security of the ACS platform itself: how administrator and operator (users) access is authenticated, what users

are authorized to do, and how stored and transmitted data is protected and kept private. One vulnerability that is often overlooked when talking about the security of a platform is encryption in an ACS. Even if some ACS data is encrypted, the system remains vulnerable when the entirety of the system does not leverage the latest encryption standards. A truly secure ACS is protected at all levels by using encrypted data and communications from the credential and reader, to the door controller and software.

While card and reader technologies are becoming increasingly secure, the larger vulnerability in many ACS deployments is the link between the reader and the door controller. Wiegand has been the common standard for most access control card readers since the early 1980s. Wiegand-based readers are largely unsupervised devices, in that they can be compromised without security personnel knowing. Readers can be vandalized, become defective, or even get stolen with no notification to the system administrator. That is why it is never recommended to equip perimeter doors with Wiegand readers because the organization is exposing the integrity of their premises with an unencrypted one directional protocol.

With Open Supervised Device Protocol (OSDP) Secure (V2), encryption is a standard, not an option. Using a two-way communication protocol, an OSDP reader is supervised meaning that if the reader is tampered, the security system administrator is notified so that action can be taken. One of the forms of encryption used in OSDP is AES-128 bit encryption, which encrypts and decrypts data in blocks of 128 bits using cryptographic keys thus preventing man-in-the-middle attacks.

Smart cards and readers

An organization can deploy smart cards and readers that offer additional security features and help prevent the misuse or illegal reproduction of credentials. Traditional ACS credentials, eg. proximity or prox cards, were invented in the 1980s, are still widely used, but offer little in terms of security against a

growing number of attacks. They use a very limiting frequency range, lack the additional security features of more advanced smart card technologies, and does not transmit their data in an encrypted format, making it more susceptible to sniffing and card cloning.

With an embedded microprocessor, applications, and additional security features, a smart card is like having a miniature computer on a card. Contactless or contact smart card technology offers an organization the highest level of security and interoperability through mutual authentication and cryptographic protection mechanisms with secret keys. For example, access control data in a contactless card may be protected using 64-bit diversified security keys based on a unique card serial number. This security can be further customized by the end-user with a card programmer. In addition, smart cards, because of their extensive memory capacity and ability to securely store any kind of information, can serve as multi-application credentials that may also include biometric data and more.

Custom card formats

An access credential or card stores data and the structure of the binary data stored in the card is known as a card format. Historically, organizations deployed credentials with card formats that were either owned by the card or reader manufacturer, by the ACS vendor, or by the systems integrator. In most cases, the format was not specific to the end user and was likely shared by many, and some card formats are so widely used that their specific format and description is publicly available.

With custom card formats, an organization has the option to define its own card format instead of having to deploy standard or well-known formats, such as the standard 26-bit format. Custom card formats can be found both with basic proximity credentials and smart cards, with the latter offering far greater flexibility and security. Smart cards with credential numbers leveraging advanced encryption algorithms, end user defined encryption keys, and extended card numbers offer more security than ever before.



In fact, using cards with custom card numbering and a card format that is longer than the standard 26-bit number—such as 256-bit formats—can add another layer of security. Custom cards may also provide additional provisions for the non-duplication of card numbers, and some manufacturers' readers can be set to ignore cards not completely conforming to the proper format. But it is important that an organization verify that its access control hardware and software have the ability to manage custom or nonstandard card formats.

Microsoft active directory or LDAP integration

This advanced access control measure involves integrating an organization's ACS with its Microsoft (MS) Active Directory (AD) server or with an IT directory server.

MS Active Directory is the directory service that Microsoft developed for Windows domain networks. Included in most Windows Server operating systems, MS Active Directory employs an AD domain controller to authenticate and authorize all users and computers in a Windows domain type network. Advanced access control systems can automatically link to AD and enable automated synchs from the AD server. Data entered in AD can be used by the ACS, avoiding duplicate data entry while also ensuring that the ACS is always up to date, which guarantees that physical access reflects employee current status.

AD integration allows an organization to link Windows security groups to ACS cardholder groups, leading to more efficient access control management. Not only are accounts automatically created or deactivated based on synchs from the AD server, but cardholders can be automatically assigned their physical access rights throughout a facility. As a result, any changes to a Windows security group leads to automatic changes to cardholder groups and their access rights. This ensures the ACS is updated in real-time and accurate.

Integrating ACS with Active Directory facilitates the immediate propagation of any changes, saving time and reducing instances of human error because IT and security personnel do not have to manually create or delete a cardholder

in different systems. Another benefit is the elimination of gaps in time before physical access is revoked following a change in AD.

Operator notification and remote review

Operator notification

An ACS can effectively protect an organization only if security personnel are notified about tampering and critical events in an efficient and timely manner. Therefore, in addition to deploying physical measures to prevent security breaches, it is also important for an organization to consider how security teams and operators are notified when exceptions to established access control rules occur or when threats arise.

Security teams and operators must instantly be notified in the case of critical events and emergencies that warrant a response. Although not an exhaustive list, some of the most critical events that require immediate response include the following:

- High priority alarms
- Threat level triggered
- Door Forced Open
- Access Denied
- Antipassback violation
- Door opened too long
- Hardware tamper (reader or controller)
- Offline unit, controller or reader
- Manual station activated

Notifications can take many forms. Some examples of automatic notifications include:

- Audible and/or visual alarm in the monitoring application
- Color change in operator display
- Text message or pop-up in the monitoring application
- SMS text message send to a mobile phone
- Push notification send to a mobile app on a smart phone or tablet
- Email with attachments

Remote accessibility to review

An ACS that supports remote access allows operators to monitor and manage the ACS from anywhere, no matter their location. Not only can they receive alarms or see the changing state of the security system, but they can also take action and respond to threats. Two important features that should be part of any ACS for remote management are support for a Web Client and access to a variety of Mobile Apps.

Beyond access control – how unification with 3rd party systems can enhance physical security

By implementing an Internet Protocol-based (IP) ACS, an organization can more easily operate, expand, and customize its physical access control infrastructure. In addition to being able to incorporate the advanced security measures mentioned above, an organization can also leverage IP technology to

- standardize their access control infrastructure,
- reduce the number of failure points and streamline system monitoring and management by moving intelligence to the door, and
- realize significant savings in the Total Cost of Ownership (TCO) through the simplification of future infrastructure expansion and modification.

An open architecture IP ACS should also unify with multiple 3rd party security systems, including video surveillance, communications, and intrusion, to provide greater situational awareness and heightened levels of security.

Unification with video

Unifying ACS with a video management system (VMS) would provide security operators with more information—visual information in the form of correlated video—to assess current and past situations. Unification with video would provide live monitoring of access and would make it possible for operators to validate a cardholder's picture against live or recorded video.

Operator notification and remote review in an ACS also becomes more effective through unification with video. As a result, an operator will instantly have more information about a critical event, including door forced open or tampering, and can make more informed decisions. For instance, after receiving a notification, an operator can immediately monitor video cameras on the system and view the scene. This can be a key factor in helping security operators identifying false-positives and responding in a timely manner.

Unification with communications

Unifying an IP-based ACS with an advanced 3rd party communications system increases security and efficiency by simplifying how an organization responds to day-to-day ACS request, including emergency calls and lost cards, how it manages threats, and how it responds to security breaches. For instance, ACS and communications unification would allow an organization to add another layer of security to their operations by adding intercom communications within a high security environment, thereby allowing security operators to grant or deny access to highly secure rooms or areas by validating audio and access control information at the same time.

And, by further unifying ACS and advanced communications with video, an organization would make it possible for operators to answer incoming emergency

calls, view live video while responding, and take the right action to address situations—such as whether or not to activate threat levels—as they arise with visual information on hand. This would also streamline how operators respond to employee lost card requests. Because intercom call stations would be linked to access-controlled doors and video cameras, operators could accept incoming calls, confirm caller identity through live video and their cardholder profile, and grant access quickly from a single unified security application.

Unification with intrusion

Another way to protect resources and assets is through the unification of ACS with an intrusion monitoring system. Because of the valuable information forwarded by the intrusion system, security operators can make decisions based on a more comprehensive understanding of the current situation. Such unification would also enable real-time monitoring of the status of alarm panels (whether armed, disarmed, or in alarm) and more advanced arming options, such as setting up automated actions to arm based on time or system events.



Overview of Synergis and security measures it offers

The Synergis™ IP Access Control System from Genetec™ is the ideal ACS solution for any organization looking to increase the safety and security of its personnel and facilities.

The Synergis system is a fully-featured solution with embedded badge design, cardholder and visitor management, and advanced reporting that allows an organization to effectively and efficiently meet its everyday security needs. And, Synergis also offers the advanced security measures required to protect people and assets during critical situations, including

- Threat Level Management
 - › Quickly select the right response to perceived threats and restrict access with pre-built threat levels based on organizational security policies.
- End-to-End Encryption
 - › Ensure communications are secured between client apps, server apps, and door controllers with encryption enabled through Synergis.
- Microsoft Active Directory Integration
 - › Simplify user and cardholder management with automated synchs between the IT directory and Synergis and guarantee that user and cardholder access rights to the Synergis ACS are up-to-date.

- Global Cardholder Management
 - › Deploy independent Synergis systems that synchronize cardholders and credentials automatically between locations, a feature that allows larger organizations to issue one card across all sites and use global antipassback to further secure their sites.
- Additional capabilities include the support for smart cards and readers, custom card formats, Two-Person and First-Person-In rules, and much more.

Alongside the Synergis system, an organization can also deploy the Genetec Security Center unified platform to consolidate and run all of its security activities, including access control, video, intercom, and intrusion systems, from a single application. By unifying Synergis with video surveillance, intercom, asset management, and intrusion systems, an organization can make clearer and timelier security decisions based on more information when compared to traditional, standalone access control systems.

Table listing the security measures, when to use them, pros and cons

The table below summarizes the security measures introduced in this white paper and provides direction when each measure is best used along with some advantages and possible disadvantages of the security measure.


Security Measure	Overview	When to use it	Pros	Cons
Emergency/Duress Buttons and Panic Alarms	Allow personnel to silently and quickly call for help	When personnel believe that it would be unsafe to use more conventional means of communication	Call for help without escalating an already dangerous situation	These devices do not function pro-actively to prevent emergencies or dangerous situations
Readerless Door Management	Allows the monitoring of doors equipped with only sensors and locks	Facilities with automated unlock schedules, such as schools or retail stores	Automate when a door will be open and closed without the need for external hardware or access control reader	Unlocking doors in response to unscheduled events can be difficult if not support by the ACS
Soft Antipassback	Antipassback events are registered but access is granted	Need to identify when cardholders are not using their credentials to access a facility as per company policy	Instantly identify misuse of credentials Non-intrusive as cardholders are not impeded from gaining access	Difficult to change behavior because it does not prevent access

Security Measure	Overview	When to use it	Pros	Cons
Hard Antipassback	Antipassback events are registered and access is denied	Need to identify when cardholders are not using their credentials to access a facility as per company policy	Instantly identify misuse of credentials Help modify cardholder behavior	Can be a nuisance to cardholders because it prevents access
Global Antipassback	Controllers across various facilities exchange information to verify cardholder's exit markings before allowing re-entry.	Need to identify across multiple sites, such as on a university campus, when cardholders are not using their credentials to access a facility as per company policy	Instantly identify the misuse of credentials across multiple sites	Can be a nuisance to cardholders because it prevents access
Interlock and Mantraps	Prevents tailgating—when an intruder follows an authorized person through an access point	In high traffic areas where safety and security can be compromised by tailgating When access to an area has to follow strict policies	Greater security by controlling the flow of individuals through access points	Can cause congestion by slowing down the flow of individuals through an access point
Directional Flow Control	Allows the control of the flow of traffic into and out of a particular area	To control or canalize the flow of traffic into and out of a particular area To prevent an access point from being used for both entry and exit	Greater security by controlling the flow of individuals through access points	Can cause inconvenience to cardholders who need to move against the flow of traffic

Security Measure	Overview	When to use it	Pros	Cons
First-Person-In Rules	Grants access to individuals or cardholders only once a designated supervisor or employee has entered first or is present on site.	Unprotected or unattended facilities with doors on unlock schedules, such as schools or retail stores	Greater level of security since the access point remains locked until the supervisor or authorized employee is on site	If something unexpected happens to the supervisor or authorized employee, the access point remains locked, which can interfere with normal business operations
Two-Person Rules	Grants access to a restricted area only when two authorized persons use credentials within a specified time	Ideal for highly sensitive areas that contain valuable assets, including server rooms and cash rooms	Greater level of security since two authorized personnel must jointly use their credentials before access is granted	Can slow down business operations
Visitor Escort	Visitors are given functional credentials but require escorted access to various areas	Ideal for facilities with highly sensitive areas that contain valuable assets	Visitor is never alone in certain areas Ensures that visitor and escort movements can be tracked at all time	Can become cumbersome for both the visitor and the escort to travel together, especially when there is more than one visitor per escort
Security Clearance and Threat Level Management	Capability to automatically lockdown a room, area, or building by triggering a pre-defined threat level	For organizations that face a growing array of potential threats to personnel and facilities	Greater level of safety and security by being able to respond quickly and effectively to potential threats	Can cause inconvenience by restricting personnel access to specific areas once a threat level has been triggered



Security Measure	Overview	When to use it	Pros	Cons
Multi-factor Authentication	Ensures that the person presenting their credentials is the same person to whom those credentials were issued	For any organization interested in increasing safety and security at its facilities	Effective and often an inexpensive way to increase security	Can impede the flow of traffic
Smart Cards and Readers	Prevent the misuse or illegal reproduction of credentials, leverage encryption	For organizations concerned about the misuse of credentials by employees or potential intruders	Offer higher level of security and interoperability Offer greater security by leveraging advanced encryption algorithms and end user defined encryption keys	Some types are susceptible to cloning and wear and tear
Custom Card Formats	Allows an organization to define its own card format, making the fraudulent duplication of cards more difficult	For organizations interested in the option to define their own card formats	Offer greater security by leveraging both custom and extended card numbers	Can impede the flow of traffic
Microsoft Active Directory or LDAP Integration	Links Windows security groups to ACS cardholder and administrator groups, providing more efficient access management control	For any organization interested in saving time and reducing instances of human error associated with establishing and changing physical access rights for cardholders	Accounts are automatically created or deactivated based on synchs from the Active Directory server Cardholders can be automatically assigned their physical access rights throughout a facility	Some types are susceptible to cloning and wear and tear



Genetec™ develops open-platform software, hardware and cloud-based services for the physical security and public safety industry. Its flagship product, Security Center, unifies IP-based video surveillance, access control and automatic license plate recognition (ALPR) into one platform. A global innovator since 1997, Genetec™ is headquartered in Montreal, Canada, and serves enterprise and government organizations via an integrated network of resellers, integrators and consultants in over 80 countries. Genetec™ was founded on the principle of innovation and remains at the forefront of emerging technologies that unify physical security systems. For more information about Genetec™, visit: genetec.com

—