Airports are among the most challenging environments to secure. They comprise an expansive perimeter, with numerous points of access and numerous individual buildings and facilities for which access must be provided for thousands, in some cases tens of thousands, of individuals every day.

Transportation venues must continue to protect themselves from an increase in terrorist threats. Their primary concern, in addition to getting people where they need to go on time, is to create a safe, secure and protective travel environment for their passengers, tenants and employees.

Outstanding security is not easy to accomplish and is certainly not done by accident. There is a maze of security and regulatory issues facing every transportation hub. For instance, in the case of an airport, it starts with a thorough understand of Title 49 CFR Part 1542 of Homeland Security’s Transportation Department. It covers a lot – ranging from who must be in charge, how to become compliant and airport tenant security programs to security of various locations within the airport, law enforcement and, yes, access control. The first objective is to reduce the complexity of this and all other pertaining regulations, along with the security ramifications.

Next, one needs to determine and resolve airport security and fire-safety vulnerabilities. Security could be almost perfect if everything was locked down and nobody could come or go. But, that’s not feasible. What needs to be done to assure that security is at a high level but that innocents can escape when needed? There’s a compromise and they are typically found within the regulations afore-mentioned and local codes and regulations.

The transportation security pyramid
How does one provide integrated solutions for all levels of security so that they can focus on convenient, safe travel for all? After all, there are differing products to control access at many different types of openings, from terminal perimeter points to airline clubs, retail stores, employee entrances, jet way service, and even cockpit doors.

Let’s quickly look at the levels of security, which can be best represented by a pyramid. The integration with all levels of this pyramid ensures seamless security and access control.
The complexities of securing a transportation site

At the foundation, Level 1 covers mechanical access and egress. This includes such items as exterior and interior doors, door hardware, mechanical locks, keying systems and portable security.

Level 2 is electronic access control and key management, which includes electronic key management systems and standalone electronic access controlled openings. Level 3 covers networked access control and biometrics for the management of perimeter and controlled public openings performed by biometrics and electronic access control systems. Finally, Level 4 covers facility integration, which includes the management of assets and people as well as the totally integrated facility solution encompassing access control, time and attendance, and personnel scheduling.

With all this as background, the process of protecting a transportation hub starts with a comprehensive site assessment and solution-generating task to identify the critical access openings of the transportation facility. Security needs at all levels must be acknowledged. An access security breach assessment will spot gaps between the current state of security and present and future needs.

This starts with identifying all the security stakeholders who must be involved. This will include everyone from the security coordinator at the venue including the TSA, local fire and law enforcement, union leaders, tenants, the carriers and others. They need to all be brought in up front and kept engaged throughout the process. Otherwise, any one could throw a roadblock into an otherwise “perfect” plan.

Where is access control needed?
Needless to say, the most critical openings must be identified. Since most people are familiar with them, let’s use an airport as an example. Other transportation venues are similar in nature.

When one starts researching, there are a host of openings:

- Terminals – public and private areas
- Aircraft operations areas (AOA) – tarmac, taxiways and jet ways
- Security Identification Display Area (SIDA)
- Secured area
- Employee movement – including outsourced service
- Catering service
- Air traffic control
- Aircraft – parked and active
- Passengers – screening, ticketing, metal/explosives detection
- Baggage systems – carry on, checked and handlers
- Navigation systems
- Vehicle control – automobile and cargo
- Parking lots – employee and passenger surveillance, and Cargo facilities

What are the security and safety needs of each? For instance, does Security need to capture and monitor real time events with the ability to record it if a breach occurs? There is a big difference in jarring open a door to get janitorial supplies or breaking through onto the tarmac.

Remember needing to identify all stakeholders? Here’s but one example. Does Human Resources want to combine with Security and link time and attendance recording to security to stop buddy punching? Or, how can we move passengers that have had background checks quickly to their boarding areas while still keeping security high?

Once the security needs of each opening have been decided, it’s time to perform a physical assessment of each. In other words, what type of products should we use?
The complexities of securing a transportation site

The delicate balance between security and life safety
Let's look at a couple of examples. For instance, remember how we need to balance security and life safety? A typical airport solution might use proximity card technology, monitoring switches and a locking mechanism on one side of the door and an exit device on the other. Conversely, the exit device side might uphold the security of the jet way area in terms of accessibility while the locking mechanism ensures access control in terms of the ability to lock it down on demand.

There are a variety of variables to consider. Among other things, to comply with Title 49 CFR Part 1542, the mechanical locks in the Level 1 of the pyramid must be able to be operated all year long. This isn't a problem in Miami but can sure cause havoc in Detroit.

Another is key control. Key systems offer superior management when key applications are used in different locations within the airport. These systems provide an answer vital to maintaining security, the elimination of unauthorized key duplication.

In these systems, a patented “dual-locking” cylinder with two independent locking mechanisms is operated by a single specially designed key. This key has side-bit milling along the key blade, a unique feature that prevents other keys from entering the keyway. Only authorized dealers can duplicate the key for an individual designated with a special identification card.

A quick comment on credentials
Instead of keys, users can choose from a broad range of credentials for appropriate access through an opening. There are electronic access control solutions that can accommodate PIN codes, magnetic stripe cards, proximity cards, contactless smart cards, and biometrics or an integrated combination of multiple credentials for appropriate access at a variety of restrictive levels—all of which are specified as necessary components by Federal Aviation Regulations.

Unauthorized users or unscheduled users will be restricted from gaining access through an opening. To reduce the probability of unauthorized access caused by lost or stolen credentials, an airport can link access capability for higher security applications. Linked access requires multiple credentials to be presented, such as the PIN and card, similar to when accessing an ATM terminal.

Credentials can be programmed into a common database controlling the electronic locking system to provide a broad range of access authority to both online and offline locking devices. User credentials can be programmed into the locking device that:

- prevents all other users from changing the status of the opening
- allows pass through any opening at any time of day—common for VIPs
- provides one-time use and the credential is then no longer valid—ideal for contract or temporary workers
- allows for an additional user's credential to be presented in tandem before access is granted, and for higher security applications.

Moving up the pyramid
For Level 2 systems, one of the requirements is the ability to re-key and recode locks quickly. That's why so many transportation locales prefer offline or stand-alone locks for such locations. For instance, San Francisco International Airport (SFO) uses 280 of them. Stand-alone, battery-powered locks (such as the AD or CO-Series electronic locks from Schlage) are programmed using a simple software program and hand-held device, or on the lock itself to allow for time-based scheduling for restricting access and audit trail capability.

Users, access points and access privileges can quickly and easily be added and deleted from the locks. The administrator can easily control both users and access points based on time of day, day of week, credential needed
The complexities of securing a transportation site

and/or period of time. Reports show audit trails retrieved, access privileges granted and time functions established by either the user or door.

With the hand-held device, the administrator goes to the opening, plugs in the USB plug to the locking system right at the door, and quickly uploads new access instructions to the lock while downloading audits of who has been through the door and when. Programming can also be done using the lock’s keypad.

Getting people out
On the other side of the door, there’s the opposite problem, letting people get through the door to leave. In terms of exiting a building when there is a fire, earthquake or similar emergency, there needs to be a proven way to allow people to exit the building. Inchon (Korea), Jorge Chavez (Peru), Suvarnabhumi (Bangkok), Dubai International, Detroit, Hong Kong and many others do just that with electronic exit devices, which keep doors locked from the inside but unlocked during emergency conditions. This keeps unauthorized individuals from exiting the building without proper authorization when there isn’t a need for mass evacuation. Security integrators and managers can add such features as alarm horns, door position switches, delayed egress and remote monitoring signals to manage such situations.

There are actually two types of exit devices: panic hardware and fire exit hardware. Panic hardware is used on openings to allow people to get out of a building in the event of a fire or other panic situation, but fire-rated hardware must be used on fire-rated openings. While both types are listed by Underwriters Laboratories (UL) for accident hazard, fire-rated devices are capable of keeping a door latched for a specified period of time when subject to an actual fire.

When teamed with automatic door operators, electrified exit devices are playing a major role in helping to maintain security while meeting the guidelines of the Americans with Disabilities Act (ADA). Whether operated by a bollard- or wall-mounted switch or an electronic access credential, the latch must retract before the door can be opened unless it is dogged down. In applications where the outer and inner doors must open and close in order, such as in vestibules, the latch can be controlled to retract in sequence before the operator begins to open the door.

Most airports use a self-contained delayed exit system that incorporates all controls, auxiliary locking, local alarm, and remote signaling output. A key cylinder on the front of the device arms and disarms it. An LED indicator shows its status. It sounds an alarm and delays a person from exiting through a door for a code-regulated 15 seconds.

Not only does this discourage unauthorized use but it also provides an opportunity for a response. For instance, the security system might trigger a CCTV camera to capture a visual record of activity at the door. However, when the building’s fire alarm or sprinkler system is activated during an emergency, these devices automatically disable to allow immediate egress.

The role of biometrics at airports
How can we stop someone from sneaking onto the tarmac? They could simply use someone else’s card or key. Since 1991, SFO, the United States’ fifth busiest airport, has employed biometric hand geometry readers to secure its aircraft operations area (AOA), allowing access to authorized individuals only.

The 300 hand readers span the entire airport, securing doors and verifying the identity of more than 18,000 employees. The use of biometrics at San Francisco is airport-wide and fully integrated into the primary access control system. Not limited to airports in the transportation industry, Portos Santos in Sao Paulo, Brazil, uses hand geometry to control the movement of 75,000 longshoremen in the port area.

Biometrics and access control
Like SFO, many major airports and smaller airports use hand geometry to assure only those authorized to get through an opening can do so.
Biometrics identifies a person via a unique human characteristic, such as the size and shape of a hand or a fingerprint. If the goal of an access control system is to control where people, not credentials, can and cannot go, then only a biometric device truly provides this capability to the end user.

As a result, biometrics is used on the front doors of thousands of businesses around the world and at the entrances of other facilities where the combination of security and convenience are desired. For access control, biometrics makes sure the good guys get in and the bad guys stay out.

“We feel that hand geometry is the best and most reliable biometric technology available,” reports Yeager Airport (Charleston, WV) Director Rick Atkinson. “We have never had any problems with the hand readers since installing them in December of 2001. They work fine and are easy to administer.”

At Yeager Airport, hand readers restrict access to the control tower, which is located in the airport terminal and also to the HVAC system and other sensitive equipment. The control tower doors are opened about every five minutes around the clock. The hand readers are all networked to the airport’s central access control system. One of the hand readers is used as the master for enrollment purposes.

“It has been the consensus since 9-11 that using biometrics as an access control validation is the way to go,” emphasizes Atkinson.

**Biometrics and increased passenger convenience.**

One leading airport’s award-winning biometric system has reduced waiting times at security checkpoints from hours to just seconds. The program handles a large percent of its passengers. Travelers go through an extensive background check to first insure they are a “low risk” traveler.

To reach the boarding areas, passengers use an automated inspection identification kiosk. The user selects one of his credit cards. When entered, the credit card provides an identifying ID number to the system. Then, upon placing his hand on the hand reader, the biometric information is compared to the security database. If the information matches, the system prints a receipt and the traveler proceeds through a system-controlled gate. If the system denies passage, it sends an alert message and the traveler is referred to an immigration inspector.

**Biometrics and time & attendance**

Covenant Aviation Security, a private company that was awarded a Transportation Security Administration contract to protect SFO from terrorism, is using hand readers to verify employee identities before granting them access to their work areas.

“After Covenant Aviation Security was awarded the TSA’s private passenger screening contract at San Francisco International Airport in October of 2002, it was crucial to have a system in place that accurately and consistently identified our more than 1,200 employees arriving and departing work every day,” explains Tom Long, Executive Vice President of Covenant.

Biometrics is often the front end for time and attendance systems in all types of industries, including transportation venues. Contrary to using badges, sign-ins or other ways of tracking employees, a biometric reader assures that no employee can punch in for another, eliminating time fraud and reducing payroll costs. That’s why so many companies now employ biometrics.

A biometric time clock provides a quick, accurate, and reliable way to record In and out punches for each employee. It ensures payroll accuracy by simply requiring each employee to be present; no cards or other credentials are needed. Losses due to “buddy punching” are eliminated. As a result, some organizations report savings of up to five percent (5%) of total payroll cost. Using scheduling restrictions, unauthorized early In punches and late out
punches are eliminated. Best of all, the hardware is typically less than ten percent of the overall cost for a time and attendance system. As a result, biometric readers can be affordably placed in multiple locations.

The benefits of such biometric-based systems are many:

- No badges to issue, replace when lost or stolen, or recover when an employee leaves or is terminated because their hand is their badge
- No more problems of employees “buddy punching” for their friends. After a biometric reader is installed, many companies are stunned to discover how much “buddy punching” was costing them
- No more data entry errors when calculating payroll or recording attendance
- No timecards or badges yield a “green” solution
- A “plug and punch” feature enables some readers to be installed in less than 15 minutes

For instance, at Miami International Airport, biometric terminals facilitate time and attendance for the janitorial services.

**Bringing it all together in levels 3 and 4**

In today’s environment, it is most likely that the airport’s access control system will be governed by management software. Software needs to dynamically link individual work schedules to access authority – not just the physical areas of the airport, but to cabinets and storage areas, vehicles, fuel supplies and equipment. The features and benefits of the airport’s software are equally as important as the hardware that it will manage.

What is needed is an integration of technologies and products throughout the airport environment that consolidates information, data and security devices into a common database. This enables airport security personnel to monitor every individual in an airport – from pilots and flight crews, to baggage handlers, to aircraft technicians, to vendors – and simultaneously provide customized access for each to only those areas where they are required to be, and only when they are required to be.

Transportation software must be secure from access by unauthorized operators. At the very least, it must be password protected. It must also be flexible enough to manage the various user groups within facility, from managers to airport personnel to delivery services to passenger. Because different levels of staff will use it, the software must be user-friendly and easy to learn. Lastly, the software must provide a management hierarchy, perhaps allowing others to manage certain elements, such as adding or eliminating a user. The C-level managers must be at the top, able to approve and/or cancel what others have modified.

However, it’s no longer enough to use an access control system that only controls and monitors cardholder activity. Tracking transactions such as someone attempting entry at Door X with an unauthorized card at 1:00am is a basic element of access control, but coupled with alarm and video management, this event could trigger a variety of responses. For instance, the alarm management system can simultaneously route an alarm to a monitoring station, send a command to a PTZ camera to change position to focus on the alarm location, and send text messages to security guards via their cell phones.

With an integrated alarm monitoring and video recording system, airport officials can view live images from cameras associated with alarm events, control PTZ functions, and view live video. They can also search stored video clips by time and date with established parameters for pre- and post- alarm event recording. Alarms can also be triggered by video motion detection or camera saturation. With the inception of video analytics, alarms can be triggered by a variety of conditions including non-motion and missing object detection and human behavior such as running or falling.

For optimal control, the ability to integrate alarm events and required actions with the access control and other security management systems is essential. With many enterprise security systems, you can also incorporate
The complexities of securing a transportation site

graphical or pictorial displays with alarm events, thus allowing responders to quickly map the alarm location and trigger the appropriate response and reporting system.

**The clock is ticking...**

Airport access management is a world of unlimited possibilities. Unfortunately, too many systems in existence today are either underutilized or based on antiquated technology. There is a new generation of security management systems, incorporating electronic access control devices from wireless to wired locks and sensors and a wide variety of video and alarm management solutions. The key is to do your homework. Learn about all the options available and specify systems that are multifaceted and designed for interoperability. By doing so, the systems you deploy today will be considered a security asset, built to evolve and grow with the airport for many years to come.

While nobody will argue that it is good to plan and test, searching for the best and most viable solutions to protect the world’s traveling public, security professionals can put as much or more stock in what’s been successful. Those venues already employing successful security systems provide the roadmap on what steps should be taken next.

Learn more about transportation venue security

For more information about security at airports and other transportation sites please contact a professional security consultant in your area by calling **888.758.9823** or fill out the Contact Us form on our website at [allegion.com](http://allegion.com).

About Allegion

Allegion (NYSE: ALLE) creates peace of mind by pioneering safety and security. As a $2 billion provider of security solutions for homes and businesses, Allegion employs more than 7,800 people and sells products in more than 120 countries across the world. Allegion comprises 23 global brands, including strategic brands CISA®, Interflex®, LCN®, Schlage® and Von Duprin®.

For more, visit [allegion.com/us](http://allegion.com/us)