SECURING AVIATION FACILITIES

Enhancing Security and Accountability at Perimeter Access Points

CyberLock

CyberLock, Inc. 1105 N.E. Circle Blvd., Corvallis, OR 97330
541-738-5500 • Fax 541-738-5501 • www.cyberlock.com • sales@cyberlock.com • support@cyberlock.com

SECURING AVIATION FACILITIES

Enhancing Security and Accountability at Perimeter Access Points | *by CyberLock*

Of the 16 critical infrastructure sectors defined by the U.S. government, the Transportation Systems sector arguably attracts the most attention from the public at large. Disruptions in this sector can unfortunately end with traumatic results that leave indelible marks on our society. Consequently, the Transportation sector employs some of our nation's most extensive safety and security measures. Countless aspects of our daily lives rely on the efficacy of these measures.

The Transportation sector comprises seven subsectors, or modes, including Aviation, Highway and Motor Carrier, Maritime Transportation, Mass Transit and Passenger Rail, Pipeline Systems, Freight Rail, and Postal and Shipping. Of these modes, Aviation has undoubtedly played the most prominent role in shaping our collective expectations for securing public spaces. Following the September 11th terrorist attacks in Pennsylvania, Virginia, and New York, the Aviation and Transportation Security Act of 2001 established the Transportation Security Administration (TSA). TSA's mission is to "protect the nation's transportation systems to ensure freedom of movement for people and commerce." In addition to creating the TSA, Section 106 of the Aviation and Transportation Security Act directed airport operators to strengthen access control points for certain areas to ensure the security of passengers and aircraft. These secured areas encompass a significant portion of airport facilities, including catering delivery, baggage handling, and maintenance, among others. With a multitude of businesses and organizations operating independently within a single facility, managing access for thousands or even tens of thousands of employees is an ambitious undertaking.

MANAGING ACCESS FOR THOUSANDS OR EVEN TENS OF THOUSANDS OF EMPLOYEES IS AN AMBITIOUS UNDERTAKING.

In its two decades of existence, the TSA has continued to refine the security procedures for airport operators. To comply with the myriad regulations concerning secured areas, airport operators must select from a broad assortment of access control technologies. While the desired outcome for each of these technologies is practically indistinguishable—permit access to authorized individuals while restricting access by unauthorized persons—the infrastructure and administrative demands differ significantly across the various systems. In this paper, we explore why certain access control solutions are not suited for the unique demands and strict security protocols of Aviation facilities.

Unique Challenges

Among the most demanding requirements for airport operators is the responsibility, under 49 CFR § 1542, to prevent and detect unauthorized entry of individuals and vehicles into their air operations area (AOA). Notably, an airport's AOA includes aircraft movement and parking areas, meaning that operators must secure perimeters extending well beyond terminal buildings. For many airports, this means securing hundreds of remote access points and, for each of those points, managing access for a dynamic group of key holders. To add further complexity, these access points may be situated at perimeter gates, exterior doors, and other peripheral locations that are difficult to integrate with an airport's primary security and network infrastructure.

IT'S ESSENTIAL THAT OPERATORS CAREFULLY EVALUATE THEIR SECURITY DEVICES TO DETERMINE IF SUCH SYSTEMS ARE CAPABLE OF HANDLING THE EVOLVING NEEDS OF THE AVIATION SECTOR

In addition to threats of violence and other malicious attacks, insider theft represents yet another layer of concern for airport operators. Even areas that fall outside the purview of TSA regulations may nonetheless present an easy target for unscrupulous employees and contractors. Shrinkage from storage areas and equipment sheds can lead to elevated operating costs and siphon resources away from critical operations. While most, if not all, airports have some measure of access control in place, it's essential that operators carefully evaluate their security devices to determine if such systems are capable of handling the evolving needs of the Aviation sector. Independent from its regulatory and enforcement activities, the TSA has prepared extensive guidance to help airport managers identify security concerns and tailor appropriate security solutions to their unique environment.

Best Practices for Aviation Security

In 2017, the TSA released its second edition of *Security Guidelines for Aviation Airport Operators and Users*. The revised guidelines, developed jointly with General Aviation stakeholders, provide a set of community-endorsed best practices for Aviation security. Within the 56-page document, the TSA recommends an extensive selection of security enhancements. These guidelines are particularly important for those facilities that have scored poorly on an Airport Security Assessment. Locks are an important security enhancement recommended for use on both indoor and outdoor assets. With thousands of access points dispersed across such a vast area, airports have unique needs to consider when selecting from the wide range of available locking devices.

WITH THOUSANDS OF ACCESS POINTS DISPERSED ACROSS SUCH A VAST AREA, AIRPORTS HAVE UNIQUE NEEDS TO CONSIDER WHEN SELECTING FROM THE WIDE RANGE OF AVAILABLE LOCKING DEVICES

Although mechanical locks and keys are satisfactory for basic access control needs, TSA recommends that such locks be re-keyed, replaced, or discarded regularly. This can quickly become cost prohibitive, which may encourage some airport operators to ignore or abandon best practices for mechanical systems. Additionally, lost or stolen keys represent a serious risk if they fall into the wrong hands.

A variety of mechanical and electronic cipher locks are commercially available. Also called code locks or push button locks, cipher locks typically require a dedicated power supply and expensive door hardware. Cipher locks also have a number of weaknesses, namely the fact that codes can easily be shared with unauthorized individuals. In fact, the TSA recommends that cipher locks only be used in manned areas to limit their exposure.

CyberLock solutions for remote access control

Combination locks are another potential security solution, primarily for outdoor gates and other peripheral access points. As with cipher locks, airport security can easily be compromised if the access codes are shared with unauthorized individuals. If exposed to freezing temperatures and harsh outdoor conditions, many versions of these locks are rendered inoperable. Combination locks can also be time-consuming to operate, causing frustration among frequent users.

The TSA acknowledges that electronic locks and keys provide significant benefits to airport security. Importantly, a key-centric access control system provides airport management with the ability to immediately disable missing keys, minimizing the risk of lost or stolen access credentials. These systems also provide a detailed record of personnel movement throughout airport facilities. In addition to the aforementioned security benefits, electronic locks and keys are an easy, affordable upgrade. Key-centric systems enable airports to quickly retrofit their existing door hardware, padlocks, and other enclosures with electronic locks, eliminating the need to hardwire each access point with network or power cables.

A KEY-CENTRIC ACCESS CONTROL SYSTEM PROVIDES AIRPORT MANAGEMENT WITH THE ABILITY TO IMMEDIATELY DISABLE MISSING KEYS, MINIMIZING THE RISK OF LOST OR STOLEN ACCESS CREDENTIALS

Rigid Infrastructure

Most airports already feature hardwired, card-reader systems at their high-traffic interior doors. However, the infrastructure required to extend hardwired access control devices to perimeter fences, gates, cabinets, or seldom-used entrances is simply not feasible. The permanent nature of hardwired systems can also create administrative headaches if airports need to modify or reconfigure a secure area, for example to accommodate seasonal traffic. For airport operators seeking to enhance security and ensure compliance with TSA regulations, deploying versatile electronic locks alongside a hardwired access control system is the ideal solution, particularly if both systems can be managed under a single software platform.

Multifaceted Access Control

The CyberLock system is the only access control solution that offers both hardwired and key-centric technologies within one software package. With the CyberLock Flex System, an airport can retain card readers at high-traffic locations while affordably securing hundreds of remote access points with CyberLock electronic cylinders. CyberLock has developed over 400 cylinder designs that retrofit into nearly any application. With all of the power for the system provided by the key, airports don't need to manage periodic battery replacements for locks scattered throughout their immense facilities. CyberLock's IP68-rated padlocks can secure remote gates and perimeters in the harshest of airport climates. From lever sets to server racks, CyberLock is suitable for deployment almost anywhere. And since every access attempt is recorded in both the lock and the key, airports can regain accountability at locations that were previously impossible to monitor.

WITH THE CYBERLOCK FLEX SYSTEM, AN AIRPORT CAN RETAIN CARD READERS AT HIGH-TRAFFIC LOCATIONS WHILE AFFORDABLY SECURING HUNDREDS OF REMOTE ACCESS POINTS WITH CYBERLOCK ELECTRONIC CYLINDERS.

Flex System is comprised of a series of exchangeable access control modules, each offering different capabilities. The modules are controlled by a Flex System Hub, which connects directly to the CyberAudit-Web management software. The Hub's onboard memory stores access permissions and caches audit trail information, enabling continuous operation even if the network connection is interrupted. Like CyberLock's electronic cylinders, Flex System is designed to meet the needs of diverse facilities. For high-traffic doors, Flex can trigger an electric door strike when authorized credentials are presented at a card reader. Mix and match Flex System's versatile modules to create a custom access control system, tailored to meet the specific needs of small, medium, and large-scale facilities. Input modules such as card readers and Keypad Displays can be combined for dual-credential door access. In addition to supporting traditional RFID credentials, the new Flex II FlashReader provides efficient keyless entry via a web-enabled smartphone. For outdoor use, weather-resistant key vault modules can be installed in the field to securely store CyberKey smart keys for convenient employee access at remote locations. Flex System also supports additional inputs and outputs that can control relay devices such as alarms, speakers, cameras, or sensors. Finally, Flex supports compatible third party Wiegand devices such as HID readers and biometric scanners, providing the ultimate flexibility for airport management.

FOR ADDED SECURITY, IF A CYBERKEY IS LOST OR STOLEN, AIRPORT MANAGEMENT CAN SIMPLY FLAG THE MISSING KEY IN THE SOFTWARE. INSTEAD OF UNDERGOING A COSTLY RE-KEYING PROCESS

The nucleus of the CyberLock system is the CyberAudit-Web management software. From its intuitive interface, airport administrators have complete control over the access rights of airport personnel. For access points that don't support a hardwired device, CyberLock's industry-leading range of connected smart keys still gives management near-real-time control over CyberLock cylinders in padlocks, storage cabinets, and other remote locations. To minimize key control risks, expiration dates can be set to prevent keys from operating beyond their authorized life. For added security, if a CyberKey is lost or stolen, airport management can simply flag the missing key in the software. Instead of undergoing a costly re-keying process, CyberLock lets airports quickly distribute lost key instructions to their locks, ensuring any lost keys are rendered harmlessly inoperable.

CyberLock solutions for remote access control

Conclusion

With CyberLock, airport operators are equipped to address the many challenges posed by their immense security perimeters and strict TSA regulations. CyberLock's versatile electronic cylinders offer precise control over each and every access point, enhancing airport security and improving accountability throughout the organization. Detailed audit reports generated via the CyberAudit-Web software show a time-stamped access record for each location, helping airports quickly recognize potential security issues and take preventative action. By combining hardwired access control with the versatility of a key-centric system, CyberLock provides benefits that no other system can match. With over 20 years of proven success, CyberLock is built exclusively in the U.S.A. to meet the unique needs of the Aviation sector. ◎

DETAILED AUDIT REPORTS GENERATED VIA THE CYBERAUDIT-WEB SOFTWARE SHOW A TIME-STAMPED ACCESS RECORD FOR EACH LOCATION, HELPING AIRPORTS QUICKLY RECOGNIZE POTENTIAL SECURITY ISSUES