AMAG TECHNOLOGY
A G4S COMPANY

Whitepaper Spotlight

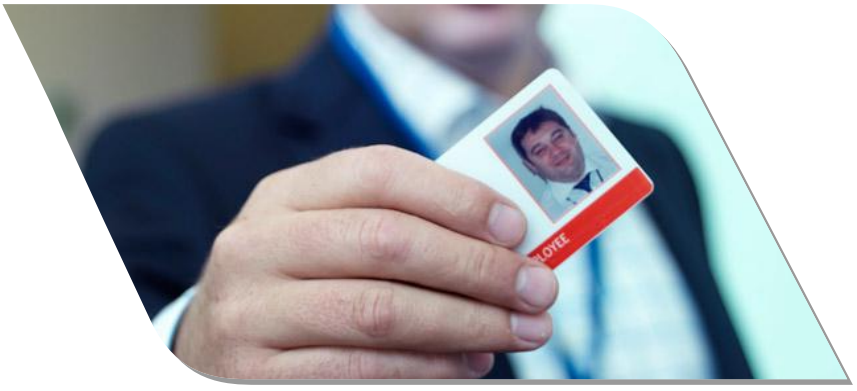
Sponsored by: NEC

SYMMETRY WHITE PAPER

Assessing "Always On" Requirements for Physical Access Control Systems

The Increasing Importance of Strong Physical Access Control

5 Nov 2015



In the past few years, there has been a dramatic increase in serious incidents due to vulnerabilities in physical access control. Failures to protect personnel against workplace violence threats, and failures to protect critical data against data thieves, have increasingly been making news headlines. Investigations have revealed that most of the large data breach incidents involve unauthorized physical access. Many more incidents don't make news headlines, yet still leave organizations with unacceptable injuries to personnel, business operations and reputation.

This is why strengthening physical access control for the protection of people and information has become paramount. As has often been pointed out, security is a weakest link discipline.

Finding the weakest link (a security vulnerability) is not as simple as it may sound, as there are usually a variety of threats to people, facilities and information—and each threat can have its own weakest link, depending upon the intent, motivation and skill of the threat agent.

Some common and easily exploited vulnerabilities in physical access control systems (PACS) are:

- ***Failure to disable access control privileges immediately when an individual becomes disqualified for access, or when a lost or stolen card is reported.***
  As a result, there is a period of time in which an unauthorized individual will be granted access without raising an alarm.

- ***Failure to establish access control duress capabilities.***
  Without a duress notification capability, someone being forced to open a door for an unauthorized individual has no safe way to alert security that there is an active threat against a person as well as against the facility.

- ***Failure to detect or prevent unauthorized tailgating.***
  Tailgating occurs when an authorized individual permits another to follow behind, without having to present an access card or enter a keypad code to gain access to a secure area.

Addressing these vulnerabilities requires a real-time PACS capability.

The Growing Need for Real-Time PACS Functionality

PACS Servers and Workstations Must Be Always-On

To keep access control privileges in an always-current state, there must be a real-time integration between the access control system and the authoritative sources of personnel status, so that changes in status update the access control system records within seconds or minutes. This is required in U.S. federal organization PACS, and is a growing trend in the private sector.

Implementing PACS duress capabilities requires a very critical real-time element—instantly communicating the duress situation to security responders or local law enforcement, and enabling a security responder to quickly lockdown potential target areas and view/forward video evidence to additional responding personnel. The same holds true for panic buttons and holdup devices.

To effectively address tailgating requires a combination of people, process and technology measures. Once multiple anti-tailgating measures are established, an unauthorized entry indicates a highly motivated attacker, and real-time detection is needed to enable threat identification and swift response. In addition, video verification of alarm conditions is a growing requirement before local police will dispatch officers to a site. Performing swift alarm situation verification requires real-time PACS/video system integration.

Evolving Security Solutions

Security technologies continue to advance in order to better meet increasing/changing threats. Most advances typically have these aspects in common:

- *They provide effective real-time detection and/or threat response capabilities.*
- *They must communicate directly to the PACS head-end, not to the field control panels that keypads and readers connect to.*
- *They extend the traditional scope of PACS integration, increasing the roles that PACS play in overall security.*

Thus PACS themselves have evolved from basic "electronic key" systems to include real time advanced asset protection functions. For example, failed attempts to access critical assets can be set to raise an alert that initiates a real-time surveillance action or an in-person security officer investigation. This can be appropriate for certain pharmaceutical controlled substances or in process food products. Casinos have begun tagging cash carts using RFID chips to track their movement and simultaneously identify the individual handling the cart, showing the activity in real-time map displays. In school campuses, PACS are being used to react to specific threat conditions, such as locking doors in facility access zones and tracking arrivals into shelter spaces and safe areas. Emerging technologies include identification of a person's manner of walking (gait), used for facility entry in high-risk areas to reduce the time to gain entry, by recognizing the approaching person while 10 feet away from the door, and unlocking the door just prior to the moment of arrival. If gait-recognition doesn't work, facial recognition is performed from a distance, and if that fails then presentation of an access card can be used. For such advanced applications, security monitoring centers need to have displays or alarms that notify when any component of such equipment is offline or in a non-functional state, so that faults can be identified and corrected immediately. The alternative is to discover such a fault by virtue of an access system failure, a completely unacceptable way to monitor the working status of equipment from a life safety perspective.

All of these factors increase the need to have an "always on" access control system.
Furthermore, when a highly integrated access control server fails—it's not just the real-time head-end access control functionality that's lost—also lost is the command and control functionality of the integrated systems. It's not possible to replace automated systems integration with independent system manual operation, without severely degrading a security center's command and control capabilities and significantly increasing operational risk.

PACS Critical Performance Factors

Assessing Current and Future Needs

When designing or upgrading access control system infrastructure (computers, software, networking and systems integrations) it is important to consider current and future critical real-time performance factors. These determine the uptime requirements of PACS servers and workstations, and the levels of network and computer fault tolerance needed. A few of the factors to examine in determining the criticality of PACS server and workstation operation are listed below. Answer these questions twice, once for current security capabilities and once for desired future capabilities.

Operations Requirements

- *Will alarms received by the access control system be monitored live, and by whom?*

- *What are the critical alarm conditions that will require immediate response?*
- *What are the most critical assets that the access control system is intended to protect? Does unauthorized access to them warrant an immediate response?*
- *Will the system be required to make email or text message notifications?*
- *What device control functions must monitoring personnel always be able to perform?*
- *What kind of real-time data transactions must the system be capable of performing? (Examples include personnel changes, access privilege changes, visitor management data, video system alarm and camera stream data, threat condition data, intrusion detection system data, outgoing pager system text or audio messages, email and phone text messages.)*
- *Is video verification of access and intrusion alarms required for police response?*
- *Will monitoring personnel respond to some alarms or situations by directing the actions of others?*
- *Does the access control system's alarm response trigger audio and/or visual messages?*

System Uptime Factors

Does the access control system include a hot standby server?
Is there a pre-configured high-end laptop computer—that is maintained to a fully current status for its operating system and security applications—on hand as a cold standby substitute in the event of a critical workstation failure?
For the network paths that critical alarm, control and integrated video traffic network data take, are there redundant network paths in place that are tested at appropriate intervals?
Are the access controls servers and critical monitoring workstations fault tolerant machines?
For software crashes (e.g. cyber attack), is there a mechanism for automatic detection and recovery in place?
Can the access control system recover quickly to a remote site in case of primary site disruption due to man-made or natural disasters?

If one or more of the Operations Requirements questions have a "Yes" answer, then ideally all of the System Uptime Factors questions would have a "Yes" answer. If not, then there should be a sound rationale for not investing a small fraction of the cost of the overall system on ensuring that the overall system is maintained in a fully operational status at all times.

Case Study Examples

Ralph L. Carr Colorado Judicial Center

Access Control System Profile:
- *Cardholders: 1,400*
- *Card Readers: 320*
- *Integrated Cameras: 285*
- *Regulatory Compliance: N/A*
- *Real-Time Integrations: Video Systems, Video Analytics Systems, Intrusion Detection Systems, Visitor Management System*

The Ralph L. Carr Colorado Judicial Center, which opened in December 2012, is a 695,000-plus square-foot complex that houses the Colorado Supreme Court, Court of Appeals, Supreme Court Law Library, Office of the State Court Administrator, Office of the Attorney General, Office of the Public Defender and the other legally related agencies serving the State of Colorado.

An effective security design is based on evaluating risks and threats, establishing design parameters, and assessing how these will affect the building, personnel, and operations of the business. Director of Court Security for the Colorado Judicial Branch, Steven R. Steadman, performed the security assessments, established objectives for the new building, and implemented an integrated access control, surveillance, visitor management and duress security system.

The Judicial Center complex's Symmetry™ Security Management System (SMS) from AMAG Technology is monitored by the Colorado State Patrol Dispatch in their offsite Communications Center. Onsite, the Colorado State Patrol also oversees the in-house Communications Center, provides the security officers and Troopers for the building and monitors the access control and camera surveillance.

Guarantee Electrical Contracting was chosen to install the access control system and all of the low voltage systems backbone. "There are many unique aspects of integrated security at work in this building," said Guarantee's Project Manager, Mike Anthony. "Using Symmetry SMS makes it easy to bring all of the functionality together on one single platform."

The access control system integrates with HID Global's EasyLobby® Secure Visitor Management (SVM™) system to register visitors and give them access to predetermined floor levels or areas where they are allowed to go. The visitor management system reads the magstripe on a person's driver's license, which pre-populates the input fields and provides the name and address of the person, expediting the badge creation process. Tenants can easily pre-register guests using its web page. Pre-registered visitors show up in the visitor management system's grid view and badges can be pre-printed from the system's software. A photo is taken when the visitor arrives.

A temporary barcode badge with photo is issued and the visitor is granted access to the designated floor and lobby of the tenant they are visiting. The barcoded visitor badge is activated through the visitor management systems integration with the access control system to allow for specified access, such as provisional access in which the badge should remain active. Eight HID Global multi CLASS® readers stationed in the office tower and elevators contain a barcode reader as well. Visitors must swipe their barcoded visitor badge in the designated readers to gain access to the pre-determined areas or floors. Once the visitor enters the lobby of the tenant they are visiting, they are escorted throughout their space.

"Without question, this is the most advanced security set-up in any court building in Colorado, perhaps in the country," Director Steadman said. An NEC Fault Tolerant (FT) server ensures the Ralph L. Carr Colorado Judicial Center's access control system is up and running continuously. The fault tolerant server is designed to provide extreme availability by using fully redundant system components (CPU, memory, motherboards, I/O, hard disk drives, and cooling fans) and thus can provide continuous availability even in the event of a computer hardware failure. Fault tolerant systems can provide up to 99.999% uptime which equates to just a little more than 5 minutes of downtime per year.

National Grid

Access Control System Profile:

Cardholders: 25,000
Card Readers: Approximately 2,000
Integrated Cameras: 2,500

Alarm Points: Over 4,000
Regulatory Compliance: CTFAT, NERC CIP, TWIC
Integrations: Video Systems, Video Analytics Systems, Intrusion Detection Systems

National Grid is an international electricity and gas company with 95% of its activities in regulated businesses. It is the largest utility in the UK and the second largest utility in the U.S. It delivers gas to 11 million homes and businesses in the UK. In the U.S., National Grid delivers electricity to approximately 3.3 million customers and distributes natural gas serving 3.5 million customers in Massachusetts, New Hampshire, New York and Rhode Island.

"We have a large number of intrusion detection systems and we tie those systems into AMAG's Symmetry for the purpose of monitoring alarms," said Wendel Steenbuck, National Grid's Manager for National Grid Global Security in the Security Technical Support Unit. "Symmetry provides centralized alarm handling and reporting making it easy to manage alarms from different sources." "When we have an intrusion alarm, our cameras react and move so security operators can see what caused the alarm," said Steenbuck. "Symmetry's trigger commands automatically control the cameras and give them that direction." "All integrations are working seamlessly with Symmetry," said Thomas Palermo, President of Alliance Systems Integrators, Inc., the company who installed and integrated the security systems.

With having so many cardholders, alarms and alarm points, National Grid's Steenbuck chose to install an NEC Express FT server to use in conjunction with NEC ExpressCluster software, to provide remote hot standby server functionality for the access control system. The NEC FT servers are designed to provide extreme availability by using fully redundant system components and can provide continuous availability even in the event of a computer hardware failure. Fault tolerant systems can provide up to 99.999% uptime which equates to just a little more than 5 minutes of downtime per year. The NEC ExpressCluster software provides continuous monitoring and fully automated recovery of target applications and data to local or remote standby system within minutes from hardware, software, network and site failures.

Springfield-Branson National Airport
Access Control System Profile:

Cardholders: 25,000
Card Readers: Over 115
Integrated Cameras: Over 150
Regulatory Compliance: TSA
Integrations: Video System, Perimeter Intrusion Detection System, Intercom System, Pager System

Springfield-Branson National Airport, located in Springfield, Missouri with a metropolitan population of over 436,000, recently underwent a large expansion project. Its six gate terminal was no longer supporting the increasing air traffic from its four airlines. The airport recently built a brand new terminal on the opposite side of the airfield. The new terminal currently has 10 gates with the capability of expanding to 50-plus gates.

The airport chose to install AMAG Technology's Symmetry™ Enterprise Security Management System (SMS) with Symmetry Video for its security platform. Symmetry access control system is integrated with several third party vendors to provide a sophisticated, yet easy-to-use system that met the strict TSA requirements. The access control system secures the main terminal building, its seven satellite buildings, the perimeter fence and 10 vehicle gates via a fiber optic cable intrusion detection system that surrounds the entire airfield.

The airport employs a police department that monitors security in the Airport Operations Center (AOC). Inside the AOC sit two workstations that include three large monitors. One monitor graphically shows an overview of the entire airport. The police can see the whole building and zoom in on areas that are in alarm while a rolling count of who is swiping their access card throughout the airport is displayed in real time. The second monitor displays camera views using the Symmetry video matrix. The third monitor is for alarms. When an alarm sounds, the camera associated with the alarm zooms in on the area. A trigger is set up in the access control system so that a pop-up screen appears on the monitor to provide a closer look. That pop-up screen will also appear on a 50" wall monitor, normally used to display flight information, to provide a larger look at the area in alarm.

"The camera view is automatically tagged to its alarm," said Randy Riley, Airport Information Systems Supervisor. "If the police want to go back and review the video, they can pull up the video on the screen to instantly view it."

C&C Group installed the comprehensive security management system for the Springfield-Branson National Airport. "If an alarm sounds in a jet bridge, the security staff can see two viewing angles," said Martin Dowman, C&C Group's Operations Manager. "They can see views from a fixed and PTZ camera. A person in the control room can move the PTZ to get a better view or follow someone throughout the terminal."

Indoor PTZ cameras are also positioned to view outside activity. "At the end of a jet bridge in the turret is an emergency exit door," said Dowman. "That door leads to the tarmac and pilots walk through it to perform plane inspections prior to take-off. If someone passes through the door that does not have access or someone breaks through the door, a delayed egress alarm will sound and a PTZ camera will swing around and begin recording through a glass wall to catch what's going on outside."

The access control system's integration includes an interface to the police department's paging system. When an alarm sounds, all officers on duty are alerted through a page, including the sergeant. The airport found it beneficial to have all police officers notified simultaneously. Everyone is up to date, and the officer closest to the alarm can respond. In an emergency situation, all officers can respond and call for backup if necessary.

The flow of traffic on and off the airfield is managed by 10 vehicle gates around the airfield. Each vehicle gate requires a card swipe to enter the airfield. For a service truck that needs to gain access, TSA requirements demand a positive identification as is required of all people entering the airfield. An integrated Stentofon intercom provides a fast way for officers to speak with drivers. When the intercom is activated, it alerts the Airport Operations Center via the access control system and a camera zooms in on the vehicle's driver. An officer can speak to the driver as well as verify identity and allow access.

In support of their security round-the-clock operations requirements, the airport chose to establish continuous uptime for their access control system by using a NEC Fault Tolerant (FT) server that mirrors its standard access control system server. In the event of a failure in the standard access control server, the automatically

switches over to the redundant server and reports the failure to the police, for component replacement. "The system runs on the primary set of computer boards," said Dowman. "If a board or component fails, they can change the board or component out and it starts working immediately. Thanks to NEC's FT server, the Symmetry system is capable of never losing control. The hot swappable capability is valuable; the IT Staff can handle a server failure and still continue to run the Symmetry system."

Affordability and Performance of "Always On" Solutions

The overall computer and network technology trend regarding pricing and performance is that prices decrease while capabilities advance, both at an increasing rate. The result of this trend is that today's fault tolerant servers can provide up to 15-times or more performance improvement, depending on the model used, of their minicomputer predecessors and at a fraction of the cost.

A Windows server operating system can be installed in under 45 minutes, and standard off-the-shelf Windows applications can run on the fault tolerant machine. Similarly, a Linux OS or VMware can be installed and can run off-the-shelf software. Thus technical support is a fraction of the time and cost it was with earlier technologies.

The modern-day ROI from fault tolerant servers makes them well worth considering for access control systems that have any real-time functions for which continuous operation is a requirement. In fact, according to an Enterprise Strategy Group (ESG) Validation Report Summary, NEC Express fault tolerant servers cut costs in half compared to VMware fault-tolerance. Additionally, compared to traditional high availability solutions, NEC Express fault tolerant servers eliminate the need for expensive and complicated SAN-attached storage; reduce the number of servers that need be purchased and maintained; reduces the network resources required for cluster monitoring; and provides 99.999% availability for virtualized applications with no performance penalty.

ExpressCluster, NEC's high availability and disaster recovery software, enables fully automated recovery of critical application and data systems from hardware, software and site failures within minutes to avoid serious operational disruption and damage with ease and flexibility. Unlike, traditional solutions, ExpressCluster is an easy to use and self-contained HA/DR software solution that flexibly supports industry standard server and storage hardware running common operating systems (e.g. Windows, Linux, VMware, and Hyper-V) and applications.

About NEC

NEC offers a full line of Express5800 fault tolerant servers that offer up to 99.999% uptime and ExpressCluster software that enables fully automated local high availability and remote disaster recovery within minutes from failures. We are a leading supplier of server technology to the access control industry. If you would like more information, call 866-632-3226 or visit www.necam.com/ft and www.expresscluster.com.