Ensuring Smart Security in Global Supply Chains and Transportation Networks

by Kathy Holoman and Aaron Kuzmeskus

Executive summary

Both supply chain and transportation environments require efficient throughput — 24/7 flow of people and goods. Smart security plays a crucial role in ensuring effective protection and business continuity. This paper examines best practices for security that apply to supply chains, airports, ports, and mass transit networks. Specifically, the components that comprise "smart security" for critical infrastructures are detailed: security master plan, security lifecycle, single command and control, integration, and open standards.

998-2095-04-03-12AR0

Schneider Electric

Summary

Executive summary

Supply chains and the transportation networks that support them reach more corners of the earth than ever before. Unfortunately, security threats that have become increasingly more sophisticated and widespread have followed suit. The implementation of intelligent security management solutions can play a significant role in ensuring business continuity, efficiency, safety and profitability. At the same time, such solutions can also deliver unanticipated business benefits that transcend the scope of traditional security.

The Introduction of Smart Security

Supply chains and the transportation networks that support them have spread far and wide. Now even the most remote corners of the earth are reached by transportation and supply chain networks. Unfortunately, just as ingenuity and imagination have enabled this expansion, the same intelligent innovation has given rise to more sophisticated and widespread security threats than ever before.

Smart security provides effective protection for people and assets at various points during transit. Intelligent security capabilities also help mitigate risk and liability, ensure regulatory compliance, and guarantee business continuity. Intelligent solutions provide economic benefits: decreased capital expenditures (CapEx) in new construction and reducing operational costs (OpEx) over time. Such solutions also deliver unanticipated business benefits that drive profitability by transcending the scope of traditional security.

How are supply chain and transport environments different?

Both supply chain and transportation environments require efficient throughput — 24/7 flow of people and goods. Smart security plays a crucial role in assuring effective protection and business continuity in each.

There is a different focus in the security needs of these respective environments, however. In a supply chain scenario, restricted areas are established and the people who interact within them are known — having already been identified and authenticated. In this case, the main variable that security management personnel monitor is objects (goods in transit).

Conversely, in a transportation network, public areas are trafficked by thousands of unknown individuals at work or in transit. Many carry luggage or personal property. Therefore, in this instance, security involves monitoring two variables—people and objects.

Let's take a closer look at the supply chain environment to better understand its specific security needs. This description, along with more information about various transportation markets, will set the stage for a discussion of the common best practices that should be employed across the entire critical infrastructure category.

Supply chain environments

In a supply chain environment, intelligent security can serve a number of crucial functions. First and foremost, it helps lower the propensity of loss or theft of goods in transit, significant contributors to increases in rising commerce costs.

Because supply chains involve goods, vehicles, points of entry, points of exit, storage and transit cycles in between, intelligent security addresses all of these vulnerability points. Supply chains that involve ground transportation incorporate measures that help protect people and goods. Fleet management capabilities keep transit vehicles, operators, and passengers “in sight” and protected at all times, for example. Mobile track-and-trace features and integrated GPS tracking enables monitoring of transit vehicles and their points along routes during various stages of the journey.

Trucks with trailers present unique challenges. Because a tractor trailer can be removed from a truck cab and installed onto hijacker’s truck, smart security often incorporates GPS systems in both trailers and cabs. The GPS systems are linked together for even greater protection.

GPS devices also provide dispatchers with critical notifications that not only protect cargo, but also can save the lives of employees. If vehicle has deviated from its prescribed route or if it has slowed considerably while in transit on a highway, the fleet management system can alert the dispatcher of this deviation. To increase safeguards and alleviate “false alarms,” many companies incorporate safety policies and procedures that mandate communication between drivers and dispatchers in the event of unscheduled route changes or slowdowns.

GPS systems also are effectively employed by many companies that transfer goods by train or by ship. Both of these environments share two unique concerns.

In rail yards and shipyards, the first consideration is loss prevention, which a combination of traditional intrusion detection and GPS systems can address. The second is perimeter security — and in the case of many international shipyards — border security. Smart security solutions incorporate biological and radiological sensor technologies or other capabilities designed to detect the potential importation of dangerous substances.

Within these and other types of supply chain facilities, intrusion detection systems offer layered protection against unauthorized entry. They provide inherent intelligence to minimize the potential for false alarms. Fencing and other physical barriers that can withstand tough external environments also can be included as part of an integrated security solution.

In the case of facilities, Personal Identity Verification (PIV)-compliant access control systems prevent unauthorized entry to restricted areas. Wireless transmission and remote video monitoring minimize the number of personnel needed to guard the entry points that are either onsite or in other locations.

Redundant systems are extremely useful in securing remote warehouse facilities that are part of a supply chain network. An overt system is positioned in a publicly accessible space such as a warehouse production area. This system is disarmed by workers when they arrive for the work day. Another less overt system often is used in concert with that system and cannot be manually-disarmed on-site. The second security measure typically monitors the unoccupied areas of the facility such as a roof or attic space. It cannot be turned off by an individual user, but its sensors in the occupied areas are shunted by the disarming of the primary system during hours of normal operation.

Video surveillance, intrusion detection, RFID asset tagging attached to pallets or packages and other capabilities also help secure goods in a warehouse. Pallets of merchandise may be tagged with dates as to when the goods should be moved. A motion detection alarm activates if goods are moved prior to the scheduled date and time.

Although airports are a “transportation environment,” they also are an integral part of at least three kinds of supply chains — two legal and one illegal. First, for corporations, airports serve as a transit hub in shipping goods from one location to another.

Second, airports serve as their own supply chain. Their infrastructure supports the management of goods such as food and disposables that are necessary for air travel.

Third, and much more difficult to monitor is the covert drug and other illegal export/import trafficking that winds its way through airport systems. Illegal goods are transported on—or worse yet in—travelers and in cargo.

The first two categories in airport supply chains encounter similar challenges. Statistics show that an inordinately high percentage of deliveries made to airports involve repeat visits by the same vehicles and same delivery personnel. Smart security can extend a different level of trust to accommodate repeat customers and deliveries.

In some airport facilities, vehicles used for regular deliveries are preregistered. This enables faster traffic flow and processing of goods going into the facility. Other airports have begun to designate specific entrances for certain types of deliveries. In addition, license plate and vehicle detection capabilities are particularly useful in these scenarios.

Some facilities even store X-ray images of particular pre-registered vehicles so that comparisons may be made when those vehicles reenter the property. This authentication method helps ensure that dangerous organic or explosive items are not being brought into the facility.

Goods travelling through air cargo and freight terminals also must be addressed. Today, nearly all of the cargo that is loaded on passenger planes is screened. In addition to X-ray, many other specialized technologies are used to detect dangerous chemical, biological or radiological explosives. If cargo appears questionable, then it is inspected by hand.

Illegal import/export, a third category of activity in an airport supply chain represents a myriad of detection and safety problems. With drug smuggling, money laundering, importing or exporting of controlled substances, animals, artifacts and more plaguing airports today, security personnel must rely upon many methods of detection.

Technology can alert operators of many issues. For example, thermal cameras can detect the presence of previously unnoticed animals stowed in cargo. CCTV can be used to determine movement in goods in transit. X-ray technology also can be used to detect the presence of drugs or other anomalies in goods in transit.

Detecting the presence of smuggled items on a person — or in the gastrointestinal tract of that person — can be more problematic. Technology that detects links between unusual travel patterns and points of origin or debarkation is a first line of defense. Human intervention — careful observation by security personnel — is a second. Security officers must carefully monitor behavior for unusual actions, erratic movements or certain visual signals that offer clues that a person may be attempting the smuggling of illegal goods.

Detention is a next line of defense. In the case of suspects who may have ingested illegal substances, observation (via an operator or video surveillance) provides not only behavioral information that may reveal the nature of the substances and the timing of ingestion, but also surveillance provides an irrefutable record of the incident for use at criminal proceedings.

In order to accommodate frequent business travelers who have legitimate reasons for travel, and not unnecessarily search or detain them, many airports and governmental entities are devising programs that employ smart security in the form of facial recognition and biometric access capabilities. This helps to rapidly authenticate these law-abiding individuals on entry and exit from airport facilities. It also frees operators to concentrate on unknown subjects who might be using airports as illegal supply chains.

Now let's examine the needs of several specific transportation environments. Airports, ports and mass transit networks each have unique security challenges.

McCarran International Airport,
©Kathy Holoman 2011.

Airports

Every corner of an airport is vulnerable. Passenger terminals, check points, cargo areas, fenced perimeters, runways, parking areas and control towers each represent windows of opportunity for security threats. The constant flow of passengers, employees, contractors, visitors, and vehicles makes protecting these areas even more challenging.

A smart airport security solution integrates systems designed for each area of vulnerability. These systems all can be integrated and managed from a consolidated control platform. Terminals, gates, turnstiles, keypads, cameras, analytic software and other security mechanisms alert operators of unauthorized entry, objects left behind, anomalies in various airport zones and other situations that might represent possible threats. When a breach does occur, an integrated smart solution can alert operators, automatically summon first responders and trigger emergency notification systems to announce an incident.

On airport grounds, badge access control and credentialing systems limit access to those with the appropriate job function or role hierarchy. Card readers, keypads and/or biometric readers limit access to the jet bridges that lead from boarding gates to tarmacs and airplanes.

The airport personnel who manage the issuance of credentials also represent a significant risk factor. In order to decrease the predisposition for unauthorized access, smart security solutions typically authenticate these individuals with at least three levels of technology (card, fingerprint, and pin number) before they can be granted the authority to issue credentials to others. The credential issuance process also must be carefully designed to vet and authorize only ‘trustworthy’ individuals.

Smart airport solutions incorporate video analytics to monitor hangars, runways, and fuel farms. Intrusion detection systems automatically alert security staff about unauthorized entry into these areas. Traffic management measures such as bollards, wedges or fences, integrated radar and advanced video analytics protect the perimeter. Tracking systems monitor vehicle direction and speed and pinpoint anomalies in passenger pick-up and drop-off zones and in cargo loading areas.

Process — adherence to globally-established levels of security — also plays a key role in preventing incidents. Intelligent security systems can incorporate a threat level management capability that allows security settings to be adjusted from the consolidated control platform when necessary. Smart security systems typically provide more than one way to activate a lockdown to limit movement after an incident or after a change in global security levels. Security managers have the ability to make changes centrally, via the Web, or remotely from personal mobility devices.

A smart security solution can deliver even more value in an airport setting. For example, security solutions can be used to monitor baggage conveyor belts to minimize lost baggage claims or alleviate baggage pileups. Security capabilities can be used to alert operators of traffic flow issues around terminals. Integrated solutions can also ensure employee productivity and proper adherence to established policies and procedures. All of these functions transcend the traditional role played by security in a transportation facility. They represent business value that can be monetized.

Smart security solutions for airports can include the following capabilities:

- Intelligent video surveillance
- Credentialing and badging systems
- Intrusion detection capabilities
- “Direction of travel” software
- “Object left behind” software
- Card readers, keypads, biometric capabilities
- Adjustable threat level management
- Lockdown measures
- And many more capabilities.

Ports

Ports represent another unique transportation environment that includes a constant flow of cargo, vessels and people. A smart security solution must provide visibility and protection not only for the facilities, cargo containers, vehicles and other things that comprise land operations, but also to water, to incoming vessels and to seaside areas that contribute to port operations.

Centralized control, elaborate surveillance, access control, video analytics, sonar and radar, biometrics, and perimeter control comprise a best of breed solution that keeps a port safe without hindering the flow of cargo. All of these security components must comply with government rules, regulations and initiatives and meet local law enforcement agency requirements.

Wireless intelligent video surveillance can monitor activity on land. This ranges from tank farms and rail yards to equipment storage areas and loading docks. Surveillance helps reduce cargo theft and pilfering. Video also helps secure the seaside, protecting ships on waterways.

Radar, sonar, and thermal imaging help control the seaside perimeter, while anti-vehicle controls protect areas on land. License plate recognition helps operators monitor parking areas and vehicular movement in and out of the premises. “Object left behind software” provides alerts from the video management systems of potential threats or suspicious behavior.

Nuclear detection and x-ray scanning are employed to monitor cargo and protect against terrorist activity. In highly secure areas, advanced biometrics provides heightened access control. In addition, badge and credentialing systems enable operators to limit individual access to secured areas based on job function or hierarchy in the organization.

Integration of various disparate security systems provides the possibility of a single control platform. From this dashboard, operators can access real-time actionable information and make informed decisions based on facts.

Best of breed security solutions for ports typically include:

- Wireless intelligent video surveillance
- License plate recognition software
- “Object left behind” software
- Access control with advanced biometrics
- Integrated nuclear detection and x-ray scanning
- Radar, sonar, and thermal imaging
- Anti-vehicle controls
- Badging and credentialing systems
- Command/control center systems
- And many more capabilities.

Mass Transit Networks

Mass transit networks include bus, rail, bridge, and tunnel systems as well as commuters, employees, and facilities. Many of these transit systems cover miles of territory and serve as the primary entry and egress routes for all major metropolitan centers. Therefore, the variety of security threats that can be encountered is vast -- from violence, vandalism, graffiti, and theft to personal robberies, car theft, hijacking and terrorist activity. Smart security solutions for mass transit networks address problems such as these and provide the capability to scale as the reach of the networks grows.

A best of breed solution employs wireless mobile video surveillance to monitor activity inside vehicles, as well as fixed systems under bridges, in tunnels, in parking areas, and on platforms. Security cameras serve not only as a deterrent, minimizing the potential for graffiti, theft, and other illegal actions, but also as a mechanism to record incidents when they do occur, and aid in the identification of the perpetrators.

Integrated analytics detects incidents, records the events, and can even automatically dispatch police and emergency services. Mobile video and DVR archives enable access and documentation to surveillance history for research, evidence, and compliance purposes.

Intelligent traffic systems quickly detect traffic jams, accidents or even traffic violations. Such systems also can be integrated with license plate recognition applications for a greater level of protection.

Emergency response capabilities are also crucial in a mass transit environment. Intelligent security solutions leverage state-of-the-art technology to alert passengers and personnel of emergencies and provide evacuation orders. Call stations, fire/smoke/CO detectors, alarming/dispatch capabilities, mass notification systems (digital signage) and emergency response systems all play a key role in keeping patrons and employees out of harm's way in the event of an emergency.

Intelligent security solutions for mass transit include:

- Wireless mobile video surveillance
- Integrated analytics
- Mobile DVR
- Intelligent traffic system
- Integrated GPS tracking
- Access control
- Intrusion detection
- Chemical threat detection
- Emergency response capabilities
- And many more capabilities.

These diverse environments should share common (smart) best practices

While each of these environments — supply chains, airports, ports and mass transit networks — have unique characteristics that demand specific security capabilities, some common best practices apply to all of them. Smart security solutions for critical infrastructures should incorporate some basic components and several key characteristics. Read on to find out more.

Smart security for critical infrastructure—the basics

What are the components that comprise smart security for critical infrastructures? To answer that question most effectively, consider this list:

- Security master plan: A security master plan assures that each stakeholder knows his/her role in the event of an incident.
- Security lifecycle: Viewing security management in terms of a security lifecycle guarantees that learning occurs on an ongoing basis and stakeholders all play a role in process modifications based on their experiences.
- Single command and control capability: Smart security management enables security operators to be more effective and efficient in several ways: they have shorter learning curve, they employ technology that is easier to operate, and they manage a sophisticated integrated solution that provides situational awareness and actionable information in real-time.
- Integration: Disparate security systems share a single technology infrastructure. This enables those systems to be managed via one consolidated control platform.
- Open standards: Vendor-neutral smart solutions facilitate flexible expansion and growth.

A security master plan synchronizes people, processes and technology

A security master plan for transportation or supply chain environments is a crucial foundational element for effective protection and higher return on security investment. It is necessary to ensure that security stakeholders of all types — internal and external — have immediate access to intelligent actionable information at the right time about any given threat or incident. A good security master plan outlines standard processes and procedures and includes the input from all key stakeholders.

A great security master plan not only does these things, but also it evolves over time, becoming a "living" communications mechanism that includes regular meetings, constant communications and informed process modifications that are made as new and relevant information is learned. Stakeholders can share incident reports, data about emerging threats, procedural successes or failures and more. The net result is that over time, the organization's security management discipline becomes stronger, more cohesive and much more proactive.

A case in point is a major international airport that serves passenger, cargo and port traffic. At this particular entity, a security master plan is well orchestrated and has been in place for more than a decade. This particular airport authority has painstakingly honed the process and procedure side of security management while at the same time, continuing to constantly update and perfect its integrated security management solution's technology infrastructure.

For this team, each day begins with a security meeting that includes a large number of stakeholders -- from airport management to other entities contained inside the airport such as the Transportation Security Administration (TSA), specific airline and freight carrier representatives, ground personnel, vendors who rent space in the airport, the facility's police force and more. Third party police and fire fighter organizations, emergency responders, and other relevant government agencies also are included as stakeholders that play a key role.

Through open and regular communication between constituents, daily incidents are reviewed, successes are analyzed, failures are dissected, and processes are modified in order to drive continual improvements in how security is managed. All stakeholders contribute to the safety of the airport and its extended network. Everyone is informed and each individual is an agent of change. These collaborative owners of the security master plan ensure that the needs of travellers, shipping customers, tenants, vendors, emergency responders, ground crews, and other constituents are all known, respected, accommodated and safeguarded.

In this example, the security master plan provides clear collaboratively-determined guidelines that support the collective goals and missions of the entire team. Security is woven into this organization's DNA.

What is a security lifecycle?

In making security an essential part of a critical infrastructure entity's DNA, executives must consider the synergy between people + process + technology. When all three work together in an intentionally designed symmetry, an organization can realize the highest possible performance improvements and reap significant benefits across many business operations. Viewing the discipline of security as a process-driven lifecycle highlights how this synergy works.

(See Illustration 1).

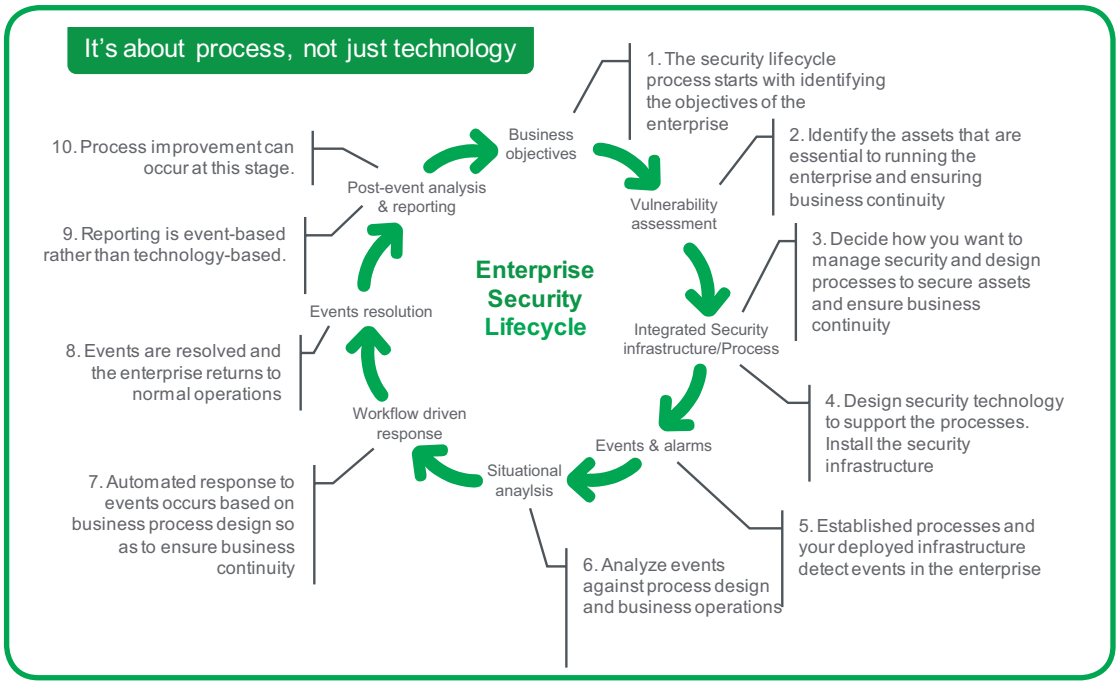

Illustration 1: The Security Lifecycle: incorporating processes to ensure business continuity

The lifecycle chronologically follows a progression through the eight stages that occur in most security environments — from determining business objectives at the beginning -- to events resolution and post-event analysis and reporting at the end. Each of these stages provides a mechanism for continuous improvement on the part of the critical infrastructure's security management team. At various points along the stages in the lifecycle, security professionals can answer basic questions that are crucial to guaranteeing effective protection of the organization:

- What needs protecting: people, property or data?
- How are the people or assets potentially vulnerable?
- What forces are likely to threaten the organization?
- How would such a threat be executed?
- How would such a threat be detected?
- How should our organization respond to a threat or disruption to business (e.g., in the case of natural disaster)?
- What reports are required to meet regulations or protect the organization from legal liability in the case of an adverse event?
- How should security technology be deployed to support this?

Notice that the technology question is the last one. This a key point. The reason for this is that security effectiveness is as much about process as it is about technology. The investment in technology is made to support the processes that are established to govern how security functions are carried out in the organization.

Now let's take a closer look at the security lifecycle and how its logic can be applied to the business of managing security. The lifecycle progression helps professionals in

- identifying and articulating the objectives of the critical infrastructure entity;
- identifying the assets that are essential to running the critical infrastructure and ensuring business continuity;
- deciding how to manage security and designing processes to secure assets and ensure business continuity;
- designing security technology to support processes and installing the appropriate associated security infrastructure;
- establishing processes and deploying infrastructure to detect events in the enterprise;
- analyzing events as compared to process design and business operations;
- reviewing automated responses that are based on the business processes design;
- resolving events and returning the enterprise to normal operations;
- reviewing event-based reports;
- implementing continuous improvements to processes.

In the security lifecycle, technology serves as a crucial enabling tool that can be designed in concert with the needs and goals of the critical infrastructure entity. It provides situational awareness; automates processes; provides a platform for establishing rules that automatically analyze what is happening in the business; and flags anomalies as events. Technology helps security teams respond in a planned and effective manner. Technology also enables reduced costs to be realized over the long-term. With the right technology, a security team can increase the effectiveness and efficiency of security and the quality of protection provided for the organization.

The security lifecycle guarantees that learning occurs on an ongoing basis and that all security stakeholders play a role in process modifications based on their experiences.

Integration enables consolidated command and control

In a critical infrastructure, a smart security environment integrates disparate security systems onto one IP-based IT backbone and enables the solution to be managed by a single control platform. One platform is easier to learn and less problematic to operate than multiple disparate systems. Therefore, a new operator will experience a shorter learning curve than he would with multiple disparate systems. A shorter training cycle saves costs for the business. Given the fact that the security industry sees high employee turnover, having the ability to ensure a short learning curve is crucial.

An integrated security solution is easier to operate on a day-to-day basis than many disparate security systems, so long-term cost containment is achieved. System redundancies and infrastructure overlaps are eliminated.

An integrated system for critical infrastructure applications can provide a host of powerful capabilities. Among them are the following:

- intelligent video surveillance and analytics
- analog, digital, thermal, and infrared observation
- intelligent video analytics and monitoring/recording
- redundant video recovery
- hot redundant systems
- alarm and event monitoring
- intrusion and incident detection
- remote command center/notification
- alarm management system
- event audit trail
- integrated fire safety
- emergency notification and evacuation systems
- fire detection
- suppression systems
- identity and personnel management
- smart cards
- capabilities that enable compliance to governmental regulations
- advanced biometrics
- database integration
- extensive reporting capabilities
- comprehensive access control
- interior, exterior, and perimeter protection
- dual and triple verification
- high encryption
- area lockdown
- intercom and paging
- IP/analog/hybrid systems
- emergency call station
- video integration
- mass notification
- perimeter and barrier protection
- crash-rated anti-vehicle protection
- virtual fences with video analytics

- ground-based radar
- traffic and baggage/cargo monitoring
- flow control
- parked car surveillance
- vehicle and personnel tracking
- direction of travel and speed detection
- abandoned baggage or pileup monitoring

Because integrated systems are displayed on one consolidated control platform, analytics can filter all of that data and alert operators to potential anomalies that fall outside the range of normal operations. This enables the right people to take appropriate action immediately and possibly avoid an incident. Integrated security helps minimize impact when a threat or an incident does occur.

Finally, the combination of integration and open standards enables a critical entity to leverage as much of its existing investment as possible. A discussion of open standards follows.

Integration for security effectiveness

Integrating multiple disparate security technologies onto a single comprehensive IT network drives more effective security protection and ultimately results in lower capital expenditure (CapEx) costs in new construction and in decreased operating expenses (OpEx) over time. Integration ensures security effectiveness.

The promise of security effectiveness -- protection against disrupted operations, compromised assets, and bodily injury -- represents the most basic reason why executives invest in security management solutions for critical infrastructures. This level of security is exemplified by common and visible systems that are installed in buildings, in rail stations, in airports and in areas occupied by people or goods in transit. Cameras, access control solutions and the other tools may be integrated with these systems.

In critical infrastructure environments, disparate security systems may be integrated not only for the ease of operators, but also to ensure that many separate law enforcement and security entities can economically maintain video surveillance and other capabilities. Integrating these disparate security systems onto one common security platform enables sharing of actionable data between the agencies. This reduces overall costs not only for the agencies themselves, but also for the critical infrastructure entity. This strategy also delivers highly-effective security monitoring protection so operators can be extremely responsive and quick to address potential threats.

Open Standards

One of the hallmarks of an intelligent security management system is open standards. A solution based on open standards enables the integration of security components and systems from various vendors and provides the flexibility to accommodate the inevitable growth and change that occurs in a critical infrastructure environment.

An open standards-based solution makes it easier for a critical entity to upgrade to IP-enabled security at its own pace. An airport authority or mass transit network has equity in its existing security equipment, for example, and may not be ready to commit to the purchase of all new systems. A smart security management solution enables executives to leverage current security equipment and legacy analog systems. Smart solutions support both technologies and offer a future-proof path to IP.

A second level of protection: risk mitigation and business continuity

Smart security can be used to improve the overall travel environment. Intelligent video surveillance, comprehensive access control, smart alarm and event monitoring, and PSIM add intelligence that helps mitigating risk and decrease the potential for liability.

Intelligent video surveillance can track and locate people and vehicles. An integrated system can automatically pinpoint suspicious behavior or activity and alert personnel about it. Video recording can capture irrefutable proof of what occurred. The reach of video cameras with analytics can be extended even more by integration with other systems such as radar or thermal imaging. Vehicles, equipment, terminals and storage areas all can be monitored so all activity inside or out can be viewed and assessed. Even traffic flow and movement of baggage or cargo can be monitored to improve operational efficiency and guests' travel experiences.

Identity Management Systems facilitate the issuance of credentials and badges that comply with governmental regulations. Integration with a consolidated control platform provides single-click access for making modifications to permissions. Required credentials can be modified or permission can be disallowed if security levels are increased.

Smart alarm and event monitoring combines access control and alarm systems with video recording and archiving capabilities. An alert status can automatically be adjusted if security levels change. The incorporation of advanced biometric access control adds even more protection. Video surveillance, intercom and paging capabilities, and fire and safety systems also can be integrated to speed response times and optimize damage control efforts.

PSIM (physical security information management) is a relatively new technology information platform that provides real time situational awareness and situation management capabilities. PSIM integrates and analyzes information derived from traditional physical security devices and systems, presenting it to the operator for real time problem resolution. PSIM helps connect and manage many of the technologies found in critical infrastructures such as video surveillance, life critical systems, radar, analytics, GPS tracking and GIS mapping. PSIM aggregates the actionable information it derives from these systems. Using a common operating picture (COP) and following the guidance from alerts and alarms, PSIM provides operators with complete situational awareness, situation management capabilities and a greater ability to comply with security policies.

Business Benefits Beyond Security

Many of the same integrated capabilities that mitigate risk and decrease liability —intelligent video surveillance, comprehensive access control, smart alarm and event monitoring, PSIM and more -- can provide a third level of security. This category transcends traditional security by delivering pure business value that can be monetized. This level of security enables executives to clearly show return on security investment (ROSI) in critical infrastructure environments.

Let's review some relevant examples discussed previously:

- Using security solutions to monitor baggage conveyor belts and minimize lost baggage claims results in fewer loss payments
- Employing security to alert of traffic flow issues around terminals reduces the time required for goods to enter facilities and decreases the cost of service
- Ensuring employee productivity and proper adherence to established policies and procedures by using video surveillance reduces the number of operators required to manage a facility
- Using security to provide irrefutable proof of accident situations or theft incidents reduces investigation time and lowers the number of potential lawsuits that might be levied
- Employing security capabilities to spot anomalies that could disrupt 24/7/365 operations ensures more business for the facility and its vendors.

In each of these cases, integrated security solutions provide value that improves customer service, helps maintain a pleasant travel environment, ensures a productive supply chain, decreases the possibility of costly litigation, or protects against an expensive business shutdown. Security delivers business efficiency and business value. This can ultimately add to the bottom line.

Conclusion

In evaluating security management solutions for critical infrastructure entities, the list of considerations that defines smart solutions is straightforward. First, it includes striking the right symmetry between people, process and technology. People (employees and stakeholders) should be governed by a security master plan and a security lifecycle. They should have the ability to onboard quickly and learn the security management solution rapidly thanks single command and control capability enabled by integration of disparate security system components onto a IP-based IT infrastructure. The solution should feature open standards to facilitate flexible expansion and growth.

In a critical infrastructure environment, a best-in-class security solution should deliver three levels of security: 1) efficient protection, 2) risk and liability mitigation, and 3) business value that transcends the scope of traditional security.

This brings us to the bottom line. In critical infrastructures, security protects us. It decreases the likelihood for bad things to happen. It ensures continuous operations. It reduces liability. And it has the ability to enhance the customer experience, guarantee continuity, protect brand reputation, thwart costly litigation, make processes more efficient and positively contribute to the entity's bottom line.

Smart companies continue to find new innovative ways to use intelligent security solutions to deliver business value. This business value has the potential to lower costs and increase profitability. These things are what managing the bottom line is all about.[1]

[1] Some parts of this white paper are derived from the white paper "The Evolution of Return on Security Investment," by Kathy Holoman and Aaron Kuzmeskus, Schneider Electric Integrated Security Solutions, January 2012.

About Schneider Electric Integrated Security Solutions

Schneider Electric will help your company realize significant economies of scale by integrating disparate security systems onto one highly flexible, IP-based platform. Security system integration increases operational efficiency by providing stakeholders such as security personnel, government agencies, and first responders with immediate access to actionable information. This ensures that the combination of people, process, and technology works together as efficiently and effectively as possible to avoid costly security incidents.

Pelco by Schneider Electric is a world leader in the design, development, and manufacturing of video security systems that are ideal for any industry. As a pioneer in data center infrastructure, APC™ by Schneider Electric ensures high availability and reliability in security technology. These brands are integral parts of the Schneider Electric buildings portfolio.

About Schneider Electric

As a global specialist in energy management with operations in more than 100 countries, Schneider Electric offers integrated solutions across multiple market segments, including leadership positions in Utilities & Infrastructures, Industries & Machine Manufacturers, Non-residential Buildings, Data Centres & Networks and in Residential. Focused on making energy safe, reliable, efficient, productive and green, the Group's 130,000 plus employees achieved sales of 22.4 billion euros in 2011, through an active commitment to help individuals and organizations make the most of their energy.

www.schneider-electric.com

Schneider Electric

One High Street,
North Andover, MA 01845 USA
Telephone: +1 978 975 9600
Fax: +1 978 975 9698
http://www.schneider-electric.com

This document has been printed on recycled paper

WP-SEC-INTEGRATED GSC TRANSPORT SECURITY-A4.BU.N.EN.03.2012.0.01.CC

March 2012 ab