Infinova®
The Integrator's Manufacturer

White Paper

A Practical Trip to Effective Use of Existing and New Security & Surveillance Technology in Transport

Security and safety executives at urban mass transit, seaport and airport operations, with common and diverse challenges, using security technologies and especially video in traditional and emerging solutions and can gain from a bigger picture that compares technology approaches and their effectiveness in transport solutions.

Urban mass transit, seaports and airports have common security needs but also diverse missions, locations, regulations and requirements. This demands a firm focus on the need to move people and cargo safety and securely while supporting the business goals and regulatory needs of the operation.

In addition to the role of policies, procedures and people, myriad security technologies are in action and must be constantly evaluated for their effectiveness, need to upgrade and new approaches. Security video is one of those essential tools, both in standalone approaches and within integrated configurations where intrusion, access, facility management and communications all work in concert.

This white paper identifies the overall challenges as well as specific problems and potential solutions. These various solutions will then be viewed with an eye to contrast their individual advantages and benefits. The bottom line: A call to action to take appropriate security technology steps that keep transport safe, secure and moving smoothly.

Authors

Mark S. Wilson
Vice President, Marketing
Infinova

Ron Heil, CPP, CSC, CHS
Assistant Vice President and Senior Security Consultant
TranSystems

Todd Libengood, PSP
Senior Systems Designer/Project Manager
TranSystems

Related White Papers from Infinova

Infinova has a series of white papers aimed at helping CSOs and senior security management to make the technical and business decisions needed to manage security and surveillance installations. The previous six white papers cover:

- Coexistence strategy at the heart of a cost-effective move from analog to digital security video.
- Selecting cameras – analog to IP-based as well as megapixel and high definition.
- Fiber optics enhances the operation and business bottom line of surveillance solutions.
- Storage options and ways to determine the best for the needs of the enterprise.
- How to conduct a security site survey leading to a risk and vulnerability matrix.
- Security lighting and its deterrence as well as ability to work with security video

These white papers are available for download at www.infinova.com

In those previous white papers, readers followed the thinking and analysis of Terry Jones, chief security officer, and Helena Smith, his second-in-command, who work for a mid-sized enterprise. This presentation includes input from Ron Heil, CPP, CSC, CHS, assistant vice president and senior security consultant and Todd Libengood, PSP, senior systems designer/project manager with TranSystems, an independent architectural, engineering and consulting firm that is an industry leader in providing complete solutions to the transportation challenges of its clients.

They know the challenges in this important area: the need to move passengers and cargo safety, meeting industry and government requirements while mitigating threats ranging from theft and unauthorized intruders to homeland terrorism.

Mass Transit Moves Many People

When it comes to mass transit, it is usually defined as transportation by a conveyance that provides regular and continuing general or special transportation to the public, but does not include school buses, charter, or sightseeing transportation.

Mass transportation modes include:

- Inter-city buses
- Trolleybuses
- Subway & commuter rail
- Demand response services
- Heavy and light rail
- Automated guideway transit
- Cable cars
- Monorails

Mass transit systems provide over 9.6 billion passenger trips per year. The U.S. mass transportation fleet is comprised of 144,000 vehicles, of which 56 percent are buses. In addition, Amtrak operates a nationwide rail transport network of 22,000 miles of track, and serves 21 million passengers per year at more than 500 stations.

Several mass transit systems often share terminals and other facilities. In general, the smaller transit systems are independently owned and operated. Larger systems are typically operated by transport agencies that are owned by governmental or quasi-governmental organizations. The largest mass transit agencies are located in New York, Chicago, Los Angeles, Washington, Philadelphia and New Jersey.

Taking a Strategic Approach

Individual security executives at the various local facilities as well as the Transportation Security Administration (TSA), a sector of the U.S. Department of Homeland Security have common goals. They seek to advance mass transit and passenger rail security through a comprehensive strategic approach that enhances capabilities to detect, deter, prevent, and respond to crimes including terrorist attacks. Their common objective is to first, prevent attacks and security incidents and then respond to and recover from, any incidents that do occur. The TSA's strategic priorities for mass transit and passenger rail security are:

- Focus efforts to mitigate high consequence risk to transit assets and systems, particularly underwater and underground infrastructure.
- Expand employment of random, unpredictable deterrence.
- Build security force multipliers with technologies, training, drills and exercises, and public awareness.

Unlike the large airports and, to a degree, seaports, urban mass transportation systems face fewer federal security regulations and requirements. The only regulatory authority that the TSA has exercised in the mass transit industry was the 2004 Security Directives RAILPAX-04-01 and RAILPAX-04-02. These required rail transportation operators to implement certain protective measures, to report potential threats and security concerns to the TSA, and to designate a primary and alternate security coordinator.

TSA surface transportation security inspectors, from the TSA Office of Security Operations, conduct on-site inspections of mass transit and passenger rail agencies and maintain collaborative working relationships with industry representatives. They work closely with the TSA Mass Transit Security Division for support and program direction. The TSA, in coordination with its federal partners, has the Transit, Commuter and Long-Distance Rail Government Coordinating Council (GCC) to bring together the Federal entities with responsibilities that affect the transit security.

Getting Everyone Involved

Outreach to stakeholders in the mass transit and passenger rail community established a modal coordinating council. With the American Public Transportation Association (APTA) as the Secretary to the council, the Mass Transit Sector Coordinating Council has been organized around an existing body of the APTA Security Affairs Steering Committee. Participating entities include:

- APTA
- Community Transportation Association of America
- Amtrak
- Amalgamated Transit Union
- Individual transit agencies representative of the community in system size and geographic spread
- Business organizations providing support services to the public transportation industry

The councils meet independently to set their priorities and positions to jointly develop and implement security strategies and programs. The Critical Infrastructure Partnership Advisory Council (CIPAC), established by Homeland Security to cover all critical infrastructure sectors, provides the process that enables consensus-based engagement among the councils. Intermodal issues are addressed by the Transportation Sector GCC under this process.

The TSA has also established the Transit Policing and Security Peer Advisory Group. The TSA works with transit agency security professionals to harness the application of resources and the development of programs to maximize the impact in enhancing security. The advisory group brings together the expertise of numerous transit police chiefs and security directors from systems as a consultative forum with extensive experience to facilitate development and implementation of effective security programs.

Seaport security is a different kettle of fish.
The U.S. maritime transportation system is vital to the global economy. Over 95 percent of non-North American trade enters the country through U.S. seaports. These seaports handle over $740 billion and 2 billion tons of domestic and international freight annually with foreign vessels making 50,000 port calls annually.

Coast Guard Sets Seaport Security
The seaports and maritime transportation infrastructure face multiple threats from the vessels, people, and cargo that move through them. Seaport security calls for a layered defense that starts far beyond the U.S. mainland. At the facilities themselves, the U.S. Coast Guard, Homeland Security, and state and local rules and regulations are in force. Most seaports include portions of the facility owned and operated by private concerns inside of a publicly-operated facility.

Seaport challenges include:

- Ensuring security before cargo ships reach port as covered by the Maritime Transportation Security Act of 2002 (MTSA). This initiative enables the Coast Guard to develop, review, and approve vessel and facility security plans, ensure foreign vessels are meeting security standards, enhance its intelligence capacity and provide underwater detection capability.
- Improving information and intelligence. The Coast Guard's maritime domain awareness programs spotlight on understanding what transits through or near the nation's waters. MTSA regulations require commercial vessels to install automatic identification systems, which broadcast certain vessel information that helps identify and locate vessels in the U.S. maritime domain.
- The container security initiative (CSI) allows DHS to pre-screen cargo before it reaches a U.S. seaport.
- Radiation detection monitors are used to screen passengers and cargo coming into the United States.
- In the United States, the customs-trade partnership against terrorism (C-TPAT) leverages public/private partnerships to improve security along the entire supply chain, from the factory floor, to foreign vendors, land borders, and seaports, while expediting border processing for legitimate shipments.
- The transportation worker identification credential (TWIC) is a vital security measure that is designed to prevent individuals who pose a threat do not gain unescorted access to secure areas of the nation's maritime transportation system.

Part of the need to identify, authenticate and constantly check people against federal databases, TWIC was established by Congress through the MTSA and is administered jointly by the TSA and the Coast Guard. TWICs are tamper-resistant biometric credentials issued to workers who require unescorted access to secure areas of ports, vessels, outer continental shelf facilities and all credentialed merchant mariners. More than 1.5 million workers including longshoremen, truckers, port employees and any others requiring unescorted access to a port area now have a TWIC. To obtain a TWIC, an individual must provide biographic and biometric information such as fingerprints, sit for a digital photograph and successfully pass a federal background check.

Airline Security
With its tragic 9/11 history, and recent shoe and underwear bombing attempts, airline and airport security has special security needs. The biggest U.S. airports handle a lot of cargo as well as 618,415,203 passengers on domestic flights in 2009.

Airports are divided into landside and airside areas. Landside areas include parking lots, public transportation train stations, tank farms and access roads. Airside areas include all areas accessible to aircraft, including runways, taxiways, ramps, hangers and tank farms. Access from landside areas to airside areas is tightly controlled at most airports. Passengers on commercial flights access airside areas through terminals, where they can purchase tickets, clear security screening, check or claim luggage and board aircraft through secured gates. Secure Identification Areas, or “SIDA” (pronounced See-da) are further restricted to only authorized and properly credentialed personnel.

Airport and airline security is diverse and complex and includes multiple layers of security and multiple systems that operate to implement different security objectives. There are perimeter systems to alert of unauthorized vehicles and people, door monitoring, access controls for airport and airline employees, cargo screening, passenger screening, and security video within the facilities, among other systems. There continues to be advances, enhancements and new technology, most often instituted or directed by the TSA and Homeland Security.

Technologies, Applications Continue to Evolve

Systems, procedures and requirements often change and evolve in this sector of transit. Most recently, DHS Secretary Janet Napolitano announced that the TSA will begin implementing new enhanced security measures for all air carriers with international flights to the United States. This effort will strengthen the safety and security of all passengers, superseding the emergency measures put in place immediately following the Detroit attempted terrorist attack on Dec. 25, 2009.

These new, more flexible security protocols—tailored to reflect the most current information available to the U.S. government—will apply to all passengers traveling to the United States. “These new measures utilize real-time, threat-based intelligence along with multiple, random layers of security, both seen and unseen, to more effectively mitigate evolving terrorist threats,” said Secretary Napolitano. “The terrorist threat to global aviation is a shared challenge and ensuring aviation security is a shared responsibility. I commend our many partners around the world who have taken steps to increase their own security measures through deployment of new technology, enhanced information sharing and stronger standards to keep air travel safe.”

Within U.S. airports, security solutions are diverse but fall into one of three categories: passengers, cargo and facility/perimeter security.

Security technologies include

- Active and passive millimeter wave screening systems
- Smart surveillance camera solutions
- Hostile intent (behavioral Pattern) and facial identification software integration into video surveillance
- Explosives trace detection equipment to supplement informed random screening of passengers and bags, including hand-held systems
- Table top baggage screening systems
- Document scanners to screen tickets or fare cards handled by passengers.
- Integrated monitoring and control software for a holistic view of safety, security and logical controls

While passenger screening is the purview of TSA, airport facility security falls under the local security director.

Policies, Procedures Play Crucial Role

But, no matter what the location – urban mass transit, seaports or airports – security technology ranging from intrusion to card access to security video is only one tool. These security executives also employ policies and procedures which are the heart of most programs, according to Ron Heil, CPP, CSC, CHS, assistant vice president and senior security consultant with TranSystems, an industry leader in providing complete solutions to the transportation challenges of its clients. Heil works on the non-technical side that includes risk, threat, and vulnerability analysis; emergency planning; emergency response; security forces; policies and procedures; and site design. Colleague Todd Libengood, PSP, senior systems designer at the firm, gets into designing systems, selecting integrators, and construction management.

Heil emphasized the “big target” that is transit and transportation. “It’s a matter of the movement of people and cargo from point to point” in a safe and secure manner and with a business bottom line. “You have to keep things and people moving while balancing operational requirements,” added Heil.

Heil and Libengood both agree that much of the security for transit and transportation are driven by government requirements and regulations. They also see a coming together of security and operations. “That is where there

are better results for a more balanced approach," said Heil. Libengood added that in testing technology and systems, "it is essential to run drills and table top exercises. It's more than just security; there are operations, maintenance, unions and fire departments. And communications is often where things may break down."

On the performance side, security executives need to look at what best would control access to a given area. "It's a matter of designing solutions that meet transit and transportation requirement," said Heil. Added Libengood, "Regarding video, IP is here and will stay. It's a matter of scalability with a network that supports video and supports the information that the images create." He added that video is better than humans for detection and record retention if current technology is applied.

While card access control and perimeter intrusion are important elements of a total security plan, security video has become crucial for deterrence, monitoring, identification and after-event forensics.

Security Video Covers Facilities

When it comes to urban mass transit, security video is on rail platforms, in bus stations and even on buses and rail cars. With seaports, cameras guard the perimeter, on the property and even are in aerial and underwater drones that patrol the facility. At airports, intelligent security video can provide alerts to objects left and people walking the wrong way in a corridor.

While there are many security technologies in this sector, a growingly important one is security video. As with commercial and corporate video surveillance, legacy systems are analog based but the strong trend is to digital or IP-based video. The overall transition strategy is coexistence of analog and digital as end users move to higher level megapixel and high definition cameras, more processing and intelligence at the edge, better compression, a variety of transmission means including fiber optics and diverse storage ranging from the camera and local digital and network video recorders to in the cloud services.

Intelligent network-based video surveillance technology based on Internet protocol (IP) can transform yesterday's analog CCTV system into tomorrow's feature-packed security management tool. Yesterday's analog cameras can be replaced by the latest intelligent digital cameras that offer features including multiple megapixels of resolution. These cameras are the "edge devices" on a digital network that takes advantage of all the standards and functionality of the same advanced networking technologies. Cable costs are lowered by the use of Cat-5 unshielded twisted pair (UTP) cable instead of coax. With networked video, there is remote access anywhere, anytime. Non-proprietary hardware is easily accommodated, and computer technologies such as distributed recording servers and networked storage, increase capabilities.

Diverse Cameras, Software, Analytics

Today, transit security executives can choose from an existing array of intelligent cameras and edge devices, including content analytics-enabled cameras, which themselves can supplement the content analytics software that resides at back end.

Especially attractive to transit security, capabilities include:

- Motion detection (the size/shape, speed and direction of a moving object)
- Non-motion detection, such as stalled vehicles or an abandoned object
- Behavioral analysis, such as tailgating at entry points or loitering
- Accurate optical character recognition (OCR) for applications such as license plate recognition.

The combination of IP with the latest video client devices – whether a desktop, hand-held device, the Internet/wide area network or a command center video wall – makes remote access available anywhere, an essential feature for mobile transit security executives.

When an incident happens, intelligent video is a useful investigative tool. Advanced megapixel cameras expand capabilities, whether digital pan-tilt-zoom of live or recorded images, or fixed high definition cameras with virtual PTZ patrolling.

Security video is also a crucial tool with an integrated system, where the combined data from all of the systems (safety, security, surveillance) can be accessed instantly based on time, motion or event, and can be more efficiently analyzed and acted upon.

Specialized Use of Video

For mass transportation systems, a unique application is video recording on a moving bus or train. There can be local storage or video streaming often through wireless mesh networks. For seaports, unique applications may include megapixel or high definition cameras that cover large amount of territory as well as specially located cameras that can cover sea-side environments without false alerting to changes in the water levels and waves. At airports, often perimeter security video is differently designed than inside cameras while there is increased experimenting with advanced analytics beyond typical motion detection and license plate recognition.

Whatever the application, bringing together video systems, first responders, police and transit administrators is a worthy situational awareness goal. For example, as with other underground rail systems, the Shanghai Metro System management was very concerned with what could happen if there was an accident. With so many people using the system, responding to the calamity and getting the injured rescued could be a major problem.

There were many challenges in creating such as system. First of all, because the system is so vital, it needs to stay in either semi-automatic or full automatic mode all the time. Thus, the video system itself must be monitored continually to ensure that all aspects of it are running in real-time and that recorded video is always available to the surveillance center as well as the police at all times.

Adding to the challenge, a huge number of cameras are deployed. To date, the system uses more than 1,000 cameras and approximately 60 networked matrix switchers. Another problem is that as trains go over the rails, they create electromagnetic interruptions that can impact the video cameras and other surveillance devices. This presented a tough challenge for the transmission design.

In a metro system, camera positioning is paramount. If the person can't be recognized, the system is of no value as a deterrent. Therefore, in any one visit to a Shanghai metro station, a passenger will be viewed by four different cameras, all from the front, and will appear in six different surveillance images.

Passenger Safety and Operational Needs

For instance, both the entrances and exits of metro stations have fixed cameras, each capable of viewing a person from the front as they enter a ticket-check station. In each of the metro halls, an integrated high-speed dome camera surveys the entire facility. Secluded corners also have additional fixed cameras so that these areas are not out of sight to the surveillance system. Cameras are also on the platforms to give rail system administrators an overview of passenger flow and help train drivers make sure that all passengers are on or off the train before the train is put into motion.

Although complex, the system is easy for operators to run. For instance, a control center operator can call up and control video in each station via one of the keyboards connected to the Ethernet network. However, they can't do anything solely at will because control procedures and priorities are managed uniformly by a sole management server within the network.

The business bottom line for mass transit, seaport and airport security is that intelligent application of security video and other systems when married with policies and procedures can provide protection such as the one in Shanghai and also can aid operations and maintenance.

By helping channel partners provide their customers with complete, affordable, best-in-class, large and small video surveillance solutions, Infinova helps integrators generate more business more profitably. Leveraging a manufacturing process certified to ISO 9001:2000 standards and over 250 engineers with a list of video industry firsts, Infinova channel partners provide their end-users with industry-acknowledged product reliability and technical leadership.

So that Infinova channel partners can create complete solutions, Infinova provides IP surveillance cameras and components, CCTV analog cameras, DVRs and components, camera accessories, monitors, power supplies and fiber optics communications devices. Infinova also has the technical ability and manufacturing flexibility to let integrators propose customized solutions. In addition, Infinova will partner with other manufacturers making other surveillance equipment and software to help its channel partners create turnkey solutions. Contrary to most other companies, Infinova will back-up their partners' products as well as its own to assure both the integrator and its customers that one call – to Infinova only – takes care of everything.

Infinova works diligently to assure its channel partners can provide cost-conscious solutions. With Infinova's hybrid systems, channel partners can propose systems that protect a customer's investment in its already-installed analog surveillance system but that also put them on a dynamic migration pathway to IP systems.

Infinova is lauded for its exceptional maintenance programs. A major highlight is the company's 24-hour advanced replacement policy in which a substitute product is shipped immediately upon notice of a problem.

With such customer focus, Infinova is often referred to as "the integrators' manufacturer."

TranSystems is focused exclusively on the vital transportation component of the economy. Our passion is to bring solutions directly to each client in each of the market sectors. Our technical depth within each sector is matched by our consulting expertise delivered across all sectors:

- Architecture, Engineering and Planning
- Management and Supply Chain Consulting
- Real Estate Consulting
- Security

Global Contact Information

Infinova®
The Integrator's Manufacturer

United States
Infinova
51 Stouts Lane
Monmouth Junction, NJ, 08852
United States
Phone: +1 732-355-9100
+1 888-685-2002 (toll-free)
Fax: +1 732-355-9101
Email: Sales@infinova.com

Latin America
Miami: +1-954-990-0787
Mexico: +52-55-5392-1735
Venezuela: +58-212-336-0661
Brazil: +55-11-7479-5640
Email: Sales-LAR@infinova.com

Europe
Phone: +40 2 6841 5582
Email: Sales-EUR@infinova.com

Middle East
Phone: +965 247 5678
Email: Sales-ME@infinova.com

India
Sales: +0091 9980728579
(South and East India)
Email: Sales-IND@infinova.com

Hong Kong
Phone: +852 2795 6540
Email: Sales-HK@infinova.com