

Networked security has arrived

– a real departure from stovepiped systems

Transportation agencies around the world are using advanced communications capabilities to improve operating efficiencies, enhance safety and security, and contribute to a better experience for passengers.



BEFORE HIS RECENT RETIREMENT, Mark Forare, the assistant director of security for the Miami-Dade Aviation Department, reminisced with Ericsson about how it felt to take on security responsibilities at Miami International Airport shortly after the terrorist attacks of September 11, 2001.

Forare was a Miami-Dade Police Department (MDPD) lieutenant, a critical incident response expert and liaison with the US Federal Aviation Administration. With that experience behind him, it wasn't what he didn't know about his new Aviation Department job that kept him up at night. He knew all too well that he was stepping into a security operation tasked with the safety of more than 30 million passengers traveling through the airport every year.

He also knew he would be responsible for completing the "New Security System," a project with a name that was innocuous and ambitious at the same time. Part of the airport's USD 5.2 billion capital improvement program, the New Security System was planned prior to 9/11, and underscored after the terrorist attacks occurred. Among the objectives: increase passenger and personnel safety, increase surveillance capacity, and reduce overall incident response time.

Forare told Ericsson that given the circumstances – taking on a high-profile position at a major transportation operation with the assignment of building a system that was "new" and "secure" – he couldn't shake the thought that this New Security System was going to be one of those projects where he spent his time trying to get his contractor, subcontractors and internal departments to play in the same sandbox. In other words, he dreaded the chaos he was sure would ensue.

However his story has a better ending than you might suspect. Today, Miami International Airport has an access control and alarm system that secures more than 1,000 points of entry, as well as a video surveillance system that is synchronized with two-way, simultaneously transmitted audio intercoms. All this data travels in real time over a converged communications network that is flexible enough to support transactional information from con-

course shops and restaurants, and scalable enough to accommodate the sensors and biometric applications that the airport and federal government are testing. What's more, the entire operation is monitored and managed from centrally located security-officer workstations.

It is an entirely New Security System. And it's "tightly pulled together and something we're proud of," Forare said, smiling, as he left the system to his able successor and headed off to relax in the Florida sunshine.

Secure communications: keeping you moving

Like Miami International, many transportation facilities around the world are undergoing major overhauls. Billions of dollars are invested annually to modernize current transportation hubs or build new transportation capacity for economic development and to enhance business and commuter travel, as well as tourism.

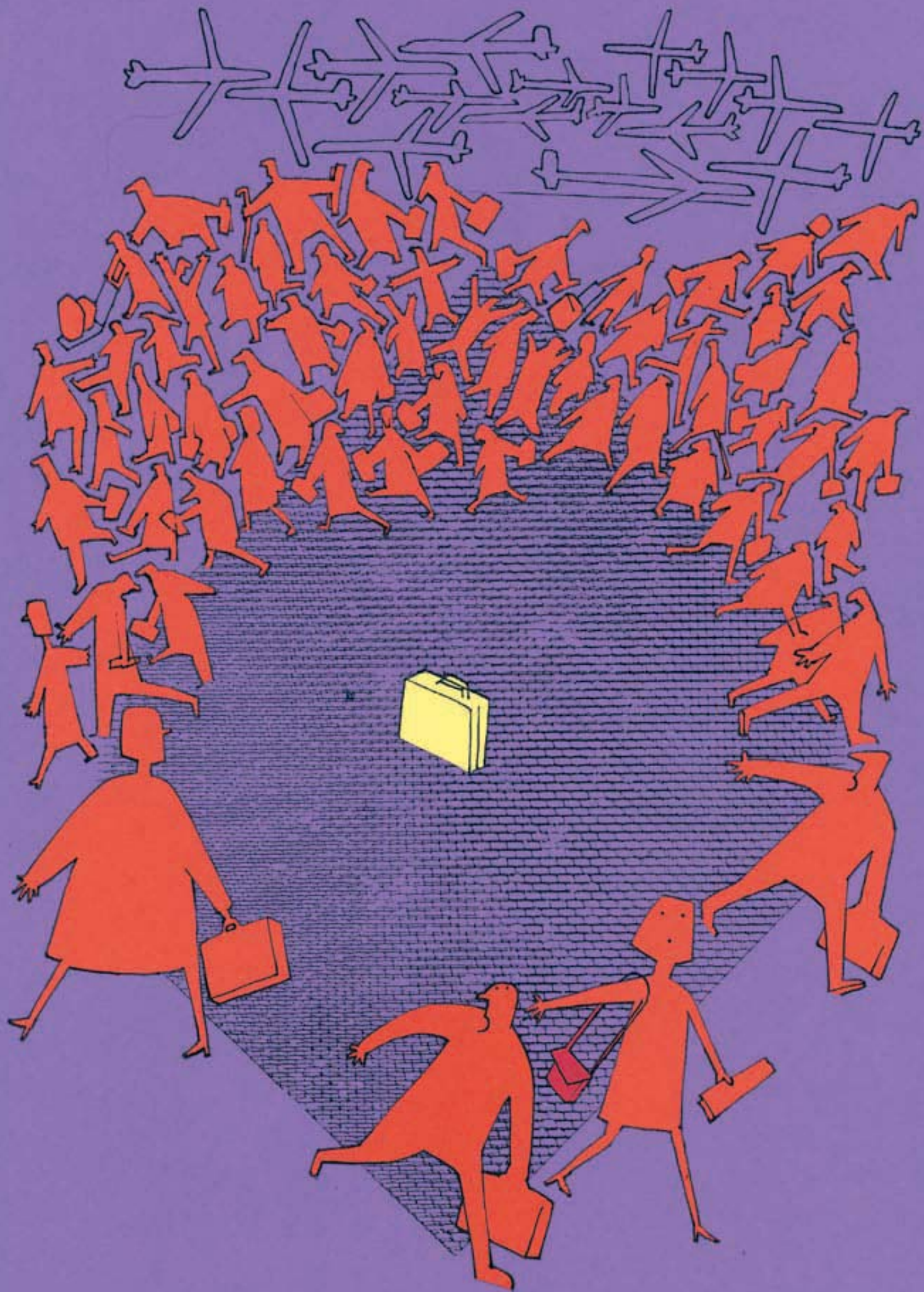
In addition to the capital improvement efforts, transportation officials responsible for the smooth, daily operation of airports, public transit systems, roadways and seaports face growing economic and environmental challenges. The costs of operating and maintaining modern, efficient transportation systems are rising. Increasing fuel costs, stricter environmental regulations and higher demands on capital improvements coupled with downward pricing pressure – all place stress on the transportation industry.

If these challenges are not complex enough, government-mandated security requirements add to the stress.

To take on these challenges, transportation officials must continually find ways to enhance safety and security, improve operating efficiencies and contribute to a better experience for passengers. What they're realizing is that voice, video and data communications, racing in real time through a converged fixed-mobile network, can improve all of the above.

It takes a leap of faith to upgrade a communications network for a transportation operation that probably runs non-stop or close to it. But improve it we must. Unfortunately, that's one of the lessons learned since global terrorists chose the transportation





▣ ...Networked security has arrived

industry as a target. Most governments stipulate that transportation authorities must develop comprehensive security plans that include:

- facility protection systems
- perimeter security systems
- redundant critical operations and control systems
- chemical, biological, radiological, explosive detection systems;
- video surveillance equipment
- communications equipment
- emergency response equipment
- fire-suppression and decontamination equipment
- global positioning or automated vehicle-locator systems
- evacuation improvements.

A clear picture of the entire operation

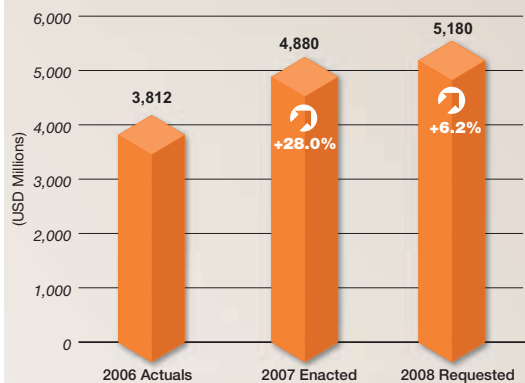
Most transportation authorities look beyond the mandates for even more sophisticated answers: systems that can deactivate wireless devices identified as threats, biometrics for smart access and applications that trigger system-wide lockdowns during threats.

Getting there

There are four major steps to improving your security operation. And no single company does all of it. A communications provider such as Ericsson is typically involved in steps three and four, and works with your security team or partners for steps one and two.

1. Risk and threat assessment
2. Site survey and security system design
3. Communications system design
4. Installation, technical assistance, and staff training (on-site maintenance and operations where desired).

Homeland Security IT budgets on the rise



Source: President's fiscal year 08 IT budget, May 2007

The good news is that a converged communications network can accommodate or enable these systems, as well as the voice, data and administrative traffic that is typical of any business operation. Even better from a return-on-investment perspective, the right converged communications network may even accommodate legacy systems that operate just fine today. At Miami International, the thinking behind the New Security System was to use as many legacy analog CCTV cameras as possible, provide an open architecture to allow for new technologies to be added to the system, and reduce the number of separate IT networks (and administrative and maintenance functions) that it took to operate stand-alone systems.

What Ericsson has discovered is that formerly stovepiped systems often need a new infrastructure to give them new life. An example is a major metropolitan transit authority that still uses the same magnetic system it used in the 1950s to monitor headway spacing and telemetry. The transport authority uses the system because it still works. The difference is that the telemetry data now runs over the same network that supports digital video feeds for security and surveillance.

As a result, the transit authority's command center (which receives, monitors and acts upon all this information) has a clearer picture of the entire operation, which leads to enhanced situational awareness, improved security and the potential for fewer delays for passengers – all because central command connects the dots more quickly to determine that something's not quite right on the commuter train.

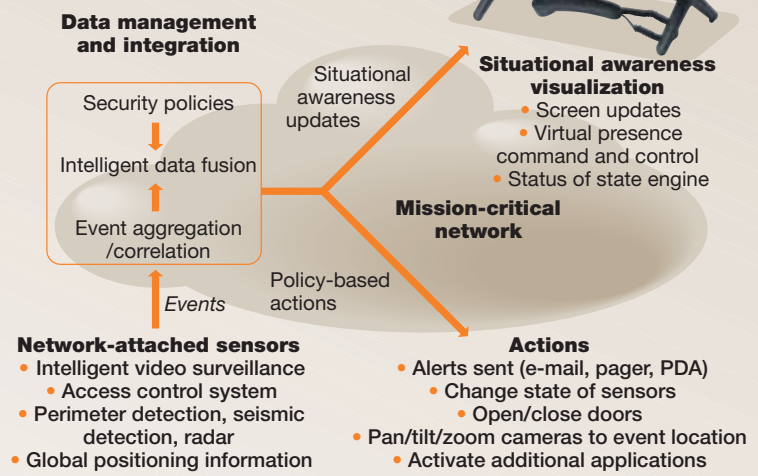
A converged network is a breakthrough for security

Security professionals are continuously striving for better situational awareness; they need to know what's going on in their environment in order to accomplish their mission. Situational awareness is derived from contextual information delivered in a timely fashion. For years, each major electronic security system in operation has provided a piece of the overall situational picture. This requires security professionals to assimilate multiple informational inputs from a variety of sources, before developing a response decision.

By taking advantage of advanced technologies, security professionals can automatically integrate the information from a variety of security systems, and then couple it with real-time capabilities to realize the promise of their investment in communications technologies. The figure on the next page shows how the trend in the integration of security applications, coupled with advanced communications technology, results in the next-generation electronic security system.

- Situational awareness is a function of contextual information delivered to decision-makers in a timely manner
- Contextual information is derived from the integration of previously stand-alone security applications
- Video content is the cornerstone element of contextual information
- Current security system communications capabilities are not designed to transport large amounts of video traffic, let alone integrated video with audio and data traffic

Leveraging advanced communications



The end game: plug-and-play

At Miami International, there is the potential to someday integrate fire-detection systems, fire alarms and other life-saving systems into the network. And biometric devices for fingerprints should be relatively simple additions to the system. However, “plug-and-play” is what security professionals expect from a network of this scope. The network should not have to be redesigned just because new technology becomes available.



- Real-time decision-making is based on video-based, contextual information and real-time communications capability
- A scalable network environment provides room to grow with advancements in security applications

It is also good for business

And then there's the enormous promise of mobile communications in this environment: the ability of security and operations personnel to access digital video and other critical data on any screen, any place, at any time.

From a business perspective, a converged network can be a pleasant surprise. Depending on the size of the transportation operation, converging legacy and next-generation systems into an advanced communications infrastructure could save millions or billions of dollars in operating costs.

Beyond operating efficiencies, agencies such as the Miami-Dade Aviation Department are generating revenue from their new networks. Passenger transportation hubs usually have retail tenants who need a network for transactional data. By carving out a portion of the network that is completely separate from the secure operations in the airside terminal, an airport can, with very little effort, become a service provider for its shops and restaurants. A port authority with warehouse and cruise-ship tenants and a train station with adjacent retailers are other examples of this business model.

How it could all go wrong

A transportation system that serves the public is arguably one of the most complex environments to network. Safety and security are paramount. Safe, affordable transportation for the citizenry is the remit. It takes an experienced communications partner to help transportation officials (and often their general contractors) create a safe and secure operation while minimizing the impact on the smooth flow of people, goods and services through the system. Asking the right questions could mean avoiding the selection of the wrong communications partner. Does the vendor have in-house capabilities to provide an end-to-end fixed and mobile infra-

structure? Does it have strong relationships with technology partners, including digital video providers, sensor manufacturers and access control specialists? Does the vendor have experience in integrating legacy systems with next-generation applications? Does the vendor have experience in this sector, period?

As with any complex operation (and as any transportation official will tell you), plenty can go wrong in this environment. However, when you get communications right, the entire operation benefits.



the authors

Shane McClelland (shane.mcclelland@ericsson.com) is responsible for identifying global growth opportunities at Ericsson's Data Networks and planning initiatives to win new business in new markets. Before Ericsson, he worked with Marconi, Fore Systems, and as a lieutenant in the US Air Force. McClelland earned his Bachelor of Science in electrical engineering from the University of Denver and his MBA from Southern Illinois University.

Lori Wirth (lori.wirth@ericsson.com) is a marketing communications specialist for Ericsson's Business Unit Networks. She began her telecommunications career in 1998 as a copywriter for Fore Systems, then for Marconi, and joined Ericsson when the company acquired Marconi in 2006. She holds a Bachelor of Science in public administration and a Bachelor of Arts in journalism and communications from Point Park University.

Bret Park (bret.park@ericsson.com) currently works with portfolio marketing for Ericsson's Government Solutions unit. He earned his Bachelor of Science in mechanical engineering from the University of South Alabama. After graduation, he worked with 3M and ICI Americas before joining Ericsson in 1990. Park is completing his MBA from Keller Graduate School of Management, concentrating on finance.