Transportation Security: Seven Proven Investments to Ensure the Safe Passage of People and Goods

What You Will Learn

The American Recovery and Reinvestment Act of 2009 provides funding for surface transportation programs, which include air, rail, highway, and maritime systems for both people and freight transport. Transportation agencies are evaluating investments based on their potential to increase protection of people and goods, foster economic growth, and bring about sustainable cost reductions.

This white paper is intended for transportation agency managers and government decision makers, and describes seven ways to use IP networks to enhance safety and security:

- Use IP networks for intelligent transportation systems (ITSs)
- Build advanced traffic management system (ATMS) control centers
- Automate the monitoring of rails, tunnels, bridges, and critical infrastructure
- Increase the security of seaports and ocean transportation
- Enable multiagency communication and collaboration
- Enhance motorist communications
- Secure cargo transport

For more information about these and other transportation solutions, you can refer to the Cisco Intelligent Transportation Solutions Blueprint, which presents solutions for safety and security, interoperability, citizen experience, and operational efficiencies.

Rare Opportunity for Tranportation Security Innovations

Protecting the nation's transportation systems is critical for public safety and for sustained economic vitality. The slowing or cessation of movement of goods over highways and arterials and through ports harms the economy.

Transportation agencies have a rare opportunity to advance the state of transportation security because of the following factors:

- **Roadside and highway renovation projects:** Installing fiber-optic cables and other communications infrastructure is less costly and disruptive to traffic flow when the roadside is already under construction. Broadband connectivity supports expanded ITS applications and benefits the local economy.[1]
- **Stimulus funding:** The current level of funding is unprecedented, and unlikely to recur anytime soon. Transportation agencies can take advantage of this funding to implement scalable, standards-based solutions that will continue to return value for years to come.

[1] A $5 billion increase in spending on broadband infrastructure directly creates 97,500 new jobs in telecom and Information Technology in the year in which spending occurs (source: Communications Workers of America, citing Department of Commerce and Brookings Institute models).

- **Growing adoption of IP in the transportation industry:** New IP-based video surveillance cameras, sensors, and ITS applications help to protect transportation infrastructure, people, and commerce. Transportation agencies are migrating their existing analog sensors and video surveillance cameras from dedicated fiber or wireless links to the IP network. This enables them to use the fiber for other purposes, and may open the way for more efficient radio systems.

The remainder of this white paper describes some proven investments for transportation security that take advantage of IP, can provide immediate benefits, and have been successfully deployed in state, local, and federal governments.

Use IP Networks for Intelligent Transportation Systems

Need

Today, many government agencies support multiple roadside networks for safety and security systems such as emergency call boxes, video surveillance, traffic management systems, sensors, and signage used for AMBER Alerts and traffic updates. The drawbacks of maintaining these older networks include high operational costs and their inability to support enhanced services.

Solution

A regional fiber-optic network can act as a platform for all transportation services and security systems. The IP network platform connects current assets, such as video cameras, traffic signal controllers, variable message signs, and a variety of sensing systems. It can also support future ITS applications for increasing transportation security and efficiency.

Consolidating all traffic onto one network infrastructure provides immediate operational cost savings. It also enables government to rapidly introduce new ITS applications quickly and at low cost. Table 1 lists essential network characteristics for transportation systems, and the Cisco® solutions that are available today.

Table 1. Technologies Needed for a Unified Transportation Network

Requirement	Cisco Solution
Metropolitan area connectivity	Cisco ONS 15454 Multiservice Transport Platform
End-to-end security	Cisco Self-Defending Network framework, including Network Admission Control, intrusion prevention, firewall services, and VPN connectivity for mobile workers
Quality of service (QoS), needed for excellent voice and video quality	Built into Cisco routers and switches
LAN and WAN connectivity	Cisco Catalyst® 2955 Series Switches Rugged Cisco IE 3000 Series Switches for wired and wireless connectivity Cisco 3200 Rugged Integrated Services Routers, which provide wireless connectivity in buses, trains, vessels, and first responder vehicles
Mobile networking	Cisco Unified Wireless Network, which enables secure connectivity for people on the move
Traffic Management and Monitoring	Cisco Video Surveillance Manager, Cisco IPICS, Cisco Video Surveillance IP Cameras
Transportation Security	Cisco Video Surveillance Manager, Cisco IPICS, Cisco Video Surveillance IP Cameras, SightLogix, Insight Video Net, Vigilant Video

The same fiber-optic and wireless networks deployed for traffic management can be used to meet one of the objectives of the stimulus package: providing broadband access to rural and underserved citizens.

Build Advanced Traffic Management System Control Centers

Need

The primary safety and security concerns at arterials are preventing accidents and controlling congestion. Today's traffic management systems are reactive rather than preemptive, making them less effective than they could be. When a local transportation agency becomes aware of an accident or other problem, an operator in the transportation management center (TMC) must manually change the signal patterns to ease traffic flow in other directions or create a detour. But by the time the problem has been reported, the flow of traffic has already been interrupted, affecting safety, mobility, commerce, and air quality.

Today's traffic signal controllers are also a source of recurring costs. Typically, they connect to the TMC over low-speed serial lines that the city or county may lease from a service provider. They are not likely to have the capacity to support video surveillance or other high-bandwidth applications.

Solution

With a secure, reliable IP infrastructure in place, you can quickly add new ATMS applications that improve safety and agency productivity and decrease driver frustration. For example, arterial management applications can accelerate detection of traffic problems so that agencies can take preemptive action to mitigate congestion.

The Cisco IE 3000 Series Industrial Ethernet Switches meet ITS requirements for extended temperature and high performance. The switches work with a wide range of traffic controllers, including the Naztec 2070-1B Traffic Controller, and other Ethernet-capable devices.

When the controllers are connected over IP, TMC personnel can receive immediate notification of problems throughout the system. They can remotely remedy signaling problems, optimize traffic flow by changing signal offsets and splits, and adjust signals for major events that increase traffic. They can use any web connection—at the TMC, home, or even a smartphone. Avoiding trips to intersections improves use of technicians' time and reduces carbon emissions.

Agencies can even create policies that automate responses to predefined conditions. For example, a policy might state that when vehicle counts at a certain intersection exceed a threshold, the system should recalculate signal splits and offsets and apply them without human intervention.

City of Midland, Texas Reduces Traffic Delays

The City of Midland, Texas Department of Transportation monitors and controls its arterials with 116 signal controllers at intersections, live video feeds from five IP video surveillance cameras at strategic locations, and more than 90 school flashers. Since implementing its ATMS, the city has experienced:

- 27-percent reduction in delay per vehicle
- 18-percent reduction in stops per vehicle
- 10-percent reduction in fuel consumption
- 10-percent reduction in emissions

Another proven ATMS investment is deploying wired and wireless video surveillance cameras with analytics software at intersections (Figures 1 and 2). Applications include:

- **Providing real-time traffic counts for roadways intersections, arterials, and highways:** The counts can be used to improve traffic flow and plan future construction.
- **Improving traffic enforcement:** IP video cameras can capture license plates and vehicle images—for example, to detect trucks on roadways where they are not allowed.

- **Enforcing speed limits and high-occupancy vehicle lane use, and detecting moving violations:** Automatic capture of violations 24 hours a day, plus video evidence to discourage frivolous claims of innocence, helps to encourage safer driving and increase city revenues.
- **Controlling traffic signals:** Video-based sensing systems cost less to maintain than inductive loop sensors.
- **Alerting TMC personnel and motorists of hazards:** Detect wrong-way driving and other hazards and automatically send alerts to the TMC and to digital signs connected to the IP network.

Figure 1. Wireless Connectivity at the Intersection

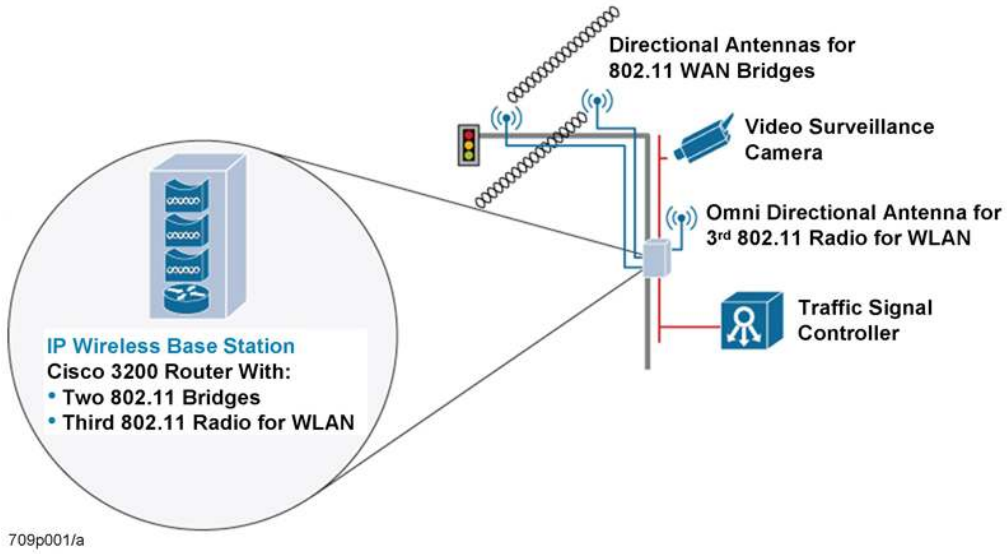


Figure 2. Signal Controller in Midland, Texas

Automate the Monitoring of Roadways, Rails, Buses, Tunnels, and Critical Infrastructure

Wired and wireless video surveillance solutions can provide early awareness of events that require intervention. They also provide evidence for forensics and prosecution. Cisco and its partners offer solutions to ensure that the evidence trail is not compromised.

Perimeter Security

Need

Public safety agencies frequently need to lock down areas and establish clear and defined perimeters, especially in areas that are bounded by open terrain. Examples include:

- Airports
- Transportation hubs
- Transit systems and waystations
- Bus and rail storage areas
- Cargo staging and storage transportation yards.

Solution

Video surveillance cameras from SightLogix, a Cisco partner, georegister all video so that personnel know precisely where an event occurred, either to prevent a crime or to support later investigation. You can protect perimeters and assets at a low cost by connecting wired or wireless video surveillance cameras at existing fencelines or anywhere you cannot or do not want to erect a fence. The cameras operate reliably in any outdoor environment, 24 hours a day, providing reliable automation over very large areas (Figure 2). Automated monitoring frees up personnel to make discretionary decisions based on actionable information.

Figure 3. A 4.6-Mile Seaport Perimeter Security Design, Created Using the SightSurvey Online Tool from SightLogix

Monitor Rail and Bus Yards

Need

Transportation safety agencies need to ensure that assets in bus and rail yards have not been sabotaged or vandalized.

Amtrak Monitors Train Maintenance Yards

Amtrak, a provider of intercity passenger rail services, has deployed a Cisco Video Surveillance solution to better protect its maintenance yards in Los Angeles and Oakland, California. Amtrak operations personnel can access video feeds from any device with a web connection, including smartphones, enabling real-time incident response, investigation, and resolution.

To protect long, exposed perimeters at the facilities' borders, Amtrak uses IP video surveillance cameras from Cisco partners, providing 1500 feet of coverage. Real-time alerts from the video analytics software allow Amtrak to stop potential threats in progress, rather than analyzing the events after the fact. The command and control platform will correlate the threat information for the officer on duty to accelerate response.

Solution

Deploy wired or wireless IP video surveillance cameras to guard against terrorism, theft, graffiti, and other types of vandalism. Operators can monitor the video from any web browser, even on a smartphone or other handheld device. Use video analytics software to recognize objects such as an unattended package and automatically notify appropriate personnel.

Employ Automatic License Plate Recognition

Need

Transportation security agencies and other public safety agencies need to locate and apprehend people suspected of crimes.

Solution

Highly accurate automatic license plate recognition (ALPR) systems can be integrated into the Cisco 3200 Series Rugged Integrated Services Router, reducing solution footprint and cost. An example is Vigilant Video's CarDetector. Video surveillance cameras with ALPR can be deployed in patrol cars and city buses as well as high-traffic parking areas and high-crime intersections. Captured license plates can be transmitted wirelessly to a regional repository throughout the day, making it easier for neighboring jurisdictions to share information. ALPR repositories capture the date and location of scanned plates so that law enforcement officers can view a vehicle's past locations and predict where to find it.

Video Capture in Vehicles, Trains, and Buses

Need

When security incidents occur on public transport, early detection and complete situational awareness contribute to an effective response. Currently, bus drivers and train engineers can only communicate by radio, providing a limited picture. In some situations, they cannot communicate at all, and transportation security authorities don't find out about the incident until it is too late to prevent harm or mitigate the situation.

Solution

Trains and buses equipped with a Cisco 3200 Series Rugged Integrated Services Router can transmit live video to a command center for continuous monitoring. Transportation security officers can capture video evidence from their vehicles using MARvista, an in-car video management system from Cisco partner Insight Video Net. Video captured from cameras on buses or trains is stored digitally on an in-vehicle Cisco 3200 Series Router, usually stored in the trunk. This same solution is currently in use by several law enforcement agencies, providing a rugged and compact in-car video solution. The router can also replace in-vehicle laptops when it is configured with a single-board computer, integrated cellular communications, and video encoder boards.

MARvista works in conjunction with Insight Video Net's Central Management System (CMS) software to capture video, audio, and other event metadata from the vehicle to create a rich evidentiary record. The ability to integrate metadata such as bookmarks, snapshots, GPS data, and triggered events provides the evidence needed to present

a true story of events, and helps to prosecute or exonerate. CMS also provides an effective way to manage terabytes of critical information and prevent improper release to the media or Internet.

Increase Security of Seaports and Ocean Transportation

Need

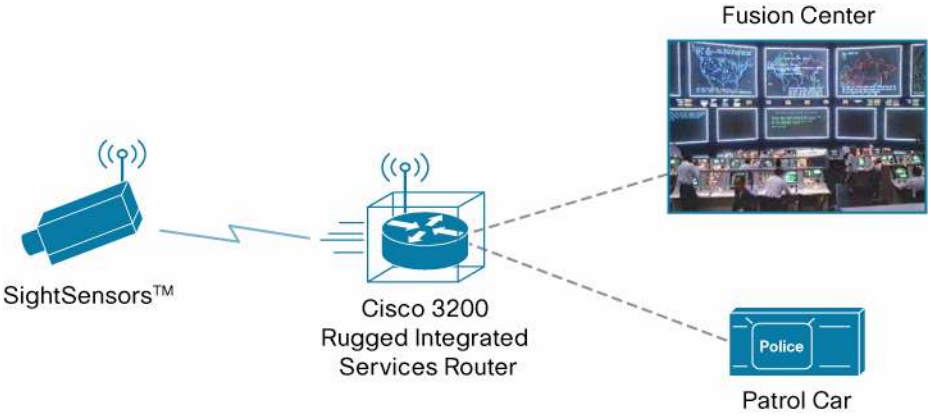
Securing the protection zone around vessels presents unique challenges. Bad lighting, variable weather conditions, visual occlusions, and large operational teams increase the frequency of nuisance alarms. Linking proprietary sensors and incident response systems to quickly marshal people and assets is often time-consuming and expensive.

Solution

Advanced sensors can be connected to Cisco wireless networks to augment human scrutiny with analytics software. SightLogix provides a wireless, thermal-infrared SightSensor that works well over water, regardless of daytime reflection or nighttime darkness. The SightLogix solution operates in conjunction with Cisco Video Surveillance Manager to detect, track and identify targets 24 hours a day. The solution can be used in:

- **Naval vessel protection zones:** SightLogix thermal sensors consider the size, speed, location, and direction of a target over water at distances of one kilometer or beyond, day or night. You can use the sensors to create a naval protection zone that automatically sends alerts whenever an unauthorized watercraft approaches a vessel in port or within a shipping channel. This solution was demonstrated during Operation Golden Phoenix 2008, a four-day exercise led by the U.S. Department of Homeland Security Customs and Border Protection; the County of San Diego, California; the City of San Diego; and the U.S. Marine Corps Aircraft Group 46. The demonstration included both land and sea borders to represent a typical seaport environment.
- **Cargo storage and staging areas:** Seaports often store large amounts of costly and potentially volatile cargo in staging facilities, which typically have large perimeters. Automated video surveillance can detect unauthorized traffic or people at specific times of day or night, and send alerts for further investigation (Figure 3).

Figure 4. Streaming Video and Alarm Information to Security Operations Centers or Port Police



IP-based video technology can also accelerate the processing of port workers when they check in for their shifts. When someone swipes a Transportation Worker Identity Credential (TWIC) in an unattended card reader, that person's image is sent to a central command center, where a worker can compare the person's image to the photograph on file. The port authority can easily program the video surveillance cameras to send an alert if workers enter certain areas after allowed hours.

Enable Multiagency Communication and Collaboration

Interoperable Communications

Need

Transportation agencies collaborate in response to events ranging from train accidents to weather-related disasters. Today, when different government organizations convene at an incident scene, their radios are incompatible because they operate over different frequencies and use different techniques. The consequences are uncoordinated responses and a fragmented chain of command that can hinder the ability to save lives, property, and infrastructure.

Solution

With Cisco IP Interoperability and Collaboration System (IPICS), transportation agencies and other government and private-sector organizations can communicate directly instead of through a dispatcher. They can use any type of radio, phone, cellular phone, IP phone, or a laptop with client software to join radio talk groups.

Auckland International Airport Enhances Emergency Response and Operational Efficiency

New Zealand's largest airport, Auckland International Airport Limited, serves more than 12 million passengers annually. Its operations center is staffed 24 hours a day and handles an average of 7000 calls weekly, including maintenance matters, security breaches, medical emergencies, car accidents, and aircraft emergencies.

In the original operations center, each desk had multiple radios and up to three telephones. To perform a certain job, such as coordinating a response to aircraft emergencies, a staff member had to be sitting at a certain desk with the appropriate communications equipment.

Now, Cisco IP Interoperability and Collaboration System (IPICS) enables operations center staff to use a headset to communicate from any location in the operations center. Using the Cisco Push-to-Talk Management Console (PMC) software on their PC, security personnel just click once to select the radio channel that they want to monitor, eliminating the need to work at a desk that has the physical radios. An emergency operations center can be set up without delay, providing interoperable communications among staff, police, fire, ambulance, and the air traffic control tower.

Collaboration

Need

TMC personnel need to communicate and collaborate with mobile operations teams, field personnel, first responders, and state and local city agencies.

Solution

Transportation safety personnel in multiple locations can collaborate face to face over the network using a variety of Cisco voice, video, and web collaboration solutions, on the desktop or in conference rooms. The ability to collaborate across distance accelerates decision-making and reduces travel time and expense.

Improve Motorist Communications

Need

Traveler safety improves when transportation agencies can provide early alerts about detours, accidents, approaching weather threats, occupancy of rest areas, and other information. This information helps travelers make decisions that reduce congestion and improve their experience. Current methods for motorist communications include highway advisory radio (HAR) and satellite radio. Some agencies use variable message signs, but they have to transport the signs on trailers, which is a labor-intensive process.

Solution

Traffic authorities can use the same IP network for ITS applications and to connect dynamic digital signs. In areas without wired connectivity, Cisco IE 3000 Series Industrial Ethernet Switches can connect the signs without the expense of trenching and cabling. Disseminating messages over the network helps to decrease congestion, increases the number of people on the lookout for vehicles matching a description, and frees up operators from having to drive signs to roadways and highways.

To prevent hackers from gaining control of the signs, Cisco Self-Defending Network technologies can be used to protect all applications deployed over the IP network. You can also monitor the area around digital signs using Cisco Video Surveillance IP Cameras.

Another way to improve motorist information is by adding a 511 phone service as part of an Advanced Traveler Information System. You can cost-effectively introduce 511 services using the same Cisco Unified Communications infrastructure that your department uses for IP telephony, conferencing, and roadside telephony services.

Secure Cargo

Need

Many government transportation and commerce agencies cannot confirm that trucks arrive with the same cargo they started out with. Criminal activity flourishes when people can add and swap cargo in between weigh stations without detection. Visually inspecting every container is costly and interrupts commerce. A secure cargo solution must be cost-effective and scalable, and must require little human intervention.

Solution

Transportation agencies can take advantage of the Cisco Unified Wireless Network, RFID sensors, and commercial software to detect cargo anomalies. An official affixes an RFID tag or bar code to the cargo at the point of origin. This information plus the truck weight is sent wirelessly to a central repository. At the destination, the wireless network reads the RFID tags and transmits the vehicle weight. The software confirms that the cargo is the same, and that the truck weight matches expectations after factoring in fuel weight and tire rubber loss.

Why Cisco

Cisco offers the solutions, expertise, services, and partner ecosystem to help you make the most of your investments in transportation security solutions:

- **Stability and ongoing R&D investment:** Cisco invested more than $5.2 billion in R&D in 2008, contributing to innovations that contribute to transportation security and other government initiatives.
- **Preintegrated, end-to-end solutions:** Cisco solutions are based on open standards, giving you the flexibility to use components from multiple vendors. Using Cisco solutions for the network as well as for video surveillance, sensor integration, and access controls eliminates interoperability concerns, accelerating deployment and reducing ongoing costs.
- **Expertise with government and transportation customers:** Cisco provides solutions for hundreds of transportation customers, including the New York Port Authority, the U.S. Department of Transportation, and many of the world's leading airlines.
- **Compliance with government standards:** Cisco switches and routers have been IPv6-ready since 2004. More than 70 Cisco products have received certifications for FIPS 140-2 and Common Criteria.
- **Extensive partner ecosystem:** Cisco has partnerships with leading systems integrators such as Accenture, ARINC, Booz Allen Hamilton, Desca, IBM, Lockheed Martin, Northrop Grumman, SAIC, and Transcore. Cisco solutions are interoperable with Aeroscout RFID solutions, Intermec handheld computers, L-3 Communications Praetorian solutions for situational awareness, Naztec ITS applications, and others.

Conclusion

A single investment in a reliable, scalable IP network pays large dividends for transportation security:

- Converging multiple networks onto one network platform reduces ongoing capital and operational expenses.
- The network adds intelligence to existing assets, such as video surveillance cameras and signal controllers, increasing their value.
- You can flexibly add new ITS applications as they're introduced, continually increasing government's effectiveness at ensuring the safe passage of people and goods.

For More Information

For more information about Cisco transportation solutions, visit: http://www.cisco.com/web/strategy/transportation/index.html

For more information about Cisco solutions for terminals, trains, buses, and trackside, visit http://www.cisco.com/web/strategy/transportation/rail.html

To read case studies about Cisco customers that have made roadways safer and more efficient, visit: http://www.cisco.com/web/strategy/transportation/roadways.html

For more information about Cisco Physical Security, visit: http://www.cisco.com/go/physec

For more information on the Cisco 3200 Series Rugged Integrated Services Router, visit: http://www.cisco.com/go/3200

For information on solutions from Cisco partner SightLogix, visit: http://www.sightlogix.com/whitepapers.html

For information on solutions from Cisco partner Insight VideoNet, visit: http://www.insightvideonet.com

For information on solutions from Cisco partner Vigilant Video, visit: http://www.vigilantvideo.com

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C11-555028-00 08/09