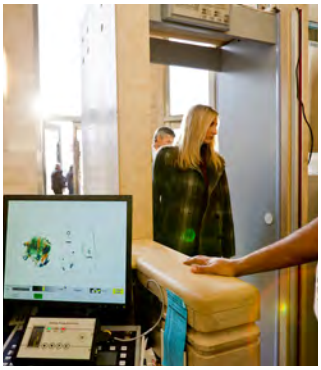
Cisco Smart and Connected Safety and Security

Solution Overview



Attracting citizens and businesses, while reducing costs

Forward thinking governments and transport providers have realized that secure communities attract more residents and businesses, while decreasing costs associated with investigating and prosecuting crime. This document explains how Cisco Smart and Connected Safety and Security—a key enabler of the Cisco® Smart+Connected Communities vision—provides government safety and security agencies and transport operators with a network-centric platform for achieving economic, social, and environmental sustainability.

Cisco Smart and Connected Safety and Security helps organizations and communities to transform the way they protect people, property, and critical infrastructure. A key focus of this approach is to enable government agencies and transport providers to handle a growing number of security incidents with fewer personnel, freeing up resources for crime prevention. Using an architectural approach that leverages rather than replaces existing IT investment, organizations and communities can improve management of day-to-day operations and emergency situations, while lowering costs.

The end goal is to create an environment that:

- Unifies operations across multiple agencies and across borders
- Ensures confidentiality, interoperability, and availability of information
- Provides effective surveillance, monitoring, and incident control
- Increases police presence on the streets

Challenges

Lack of communications and systems interoperability is one of the biggest issues facing Public Safety Answering Points, Emergency Operations Centers, Rescue Services and other first line responders. These are the organizations behind emergency telephone numbers such as '112' in Europe and '911' in the USA. Equally they could be public safety partners, such as rail and underground operators, ports, bus companies, and airports.

Today, these organizations are having to deal with increasing numbers of incidents, call volumes, and device types, with limited support from proprietary systems, multiple separate networks and analogue and legacy technology that is often both outdated and incapable of scaling. In many cases, a piecemeal approach whereby each agency or organization "farmed" its own IT estate has driven heavy investment in point technology solutions and multiple systems being deployed side-by-side.

The end result is a sprawling legacy of siloed networks[1], isolated management systems[2], and a proliferation of information systems[3] that cannot interconnect or communicate with each other because they have been built using closed or proprietary technologies. Worse still, this complex IT landscape consumes a major portion of many IT budgets.

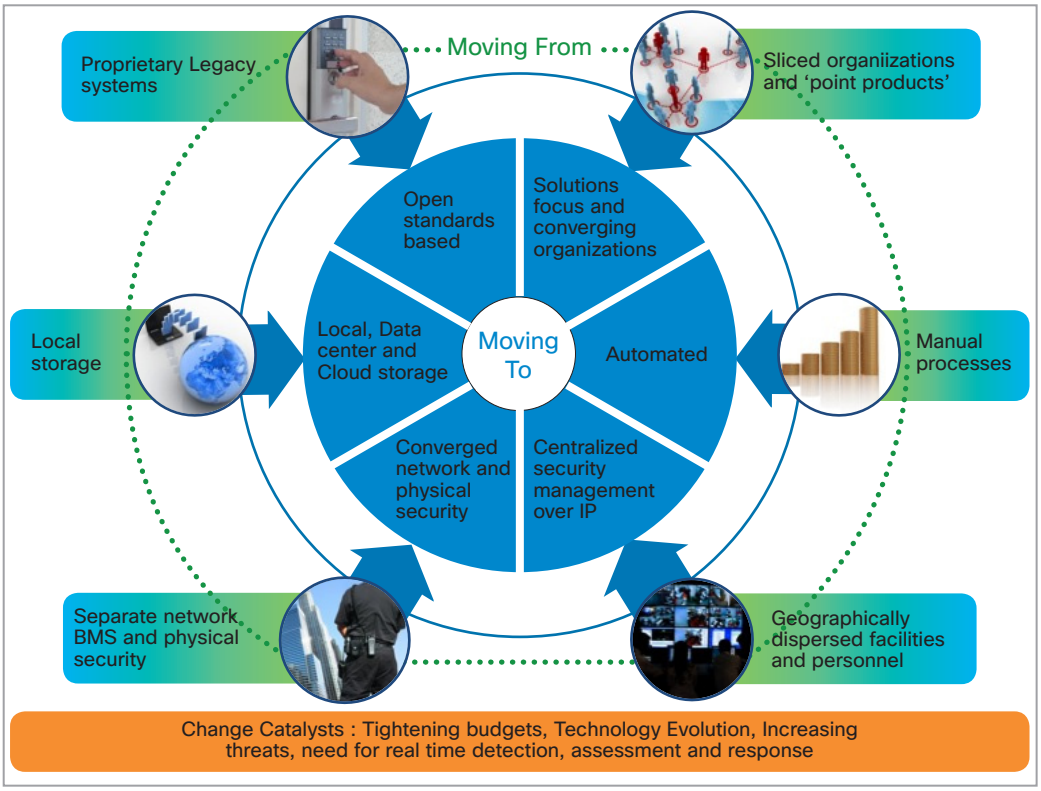
This disparate IT and communications landscape severely limits the ability to manage and share actionable information—real-time data that is accurate and relevant to the user. In turn, this hinders critical situational awareness and an effective response by slowing the speed of the decision-making loop.

As threats and criminal activity become ever more sophisticated, public safety organizations need to collaborate increasingly with each other and across borders. These trends are placing new demands on infrastructure interoperability, for example, to enable the efficient sharing of voice, images, video, and data.

Successful safety and security transformation (*see Figure 1*) requires a combination of end user structural and operational changes as well as technology evolution enablement.

1. Voice, data, video, fixed and wireless networks
2. CCTV and video archives as well as sensors and actuators that control traffic management, utilities metering, heating, and lighting systems
3. Geographical Information, Incident Management, planning, land registry, licensing, health, schools, homeland security, and so on

Figure 1. Transforming Safety and Security: From current to future state



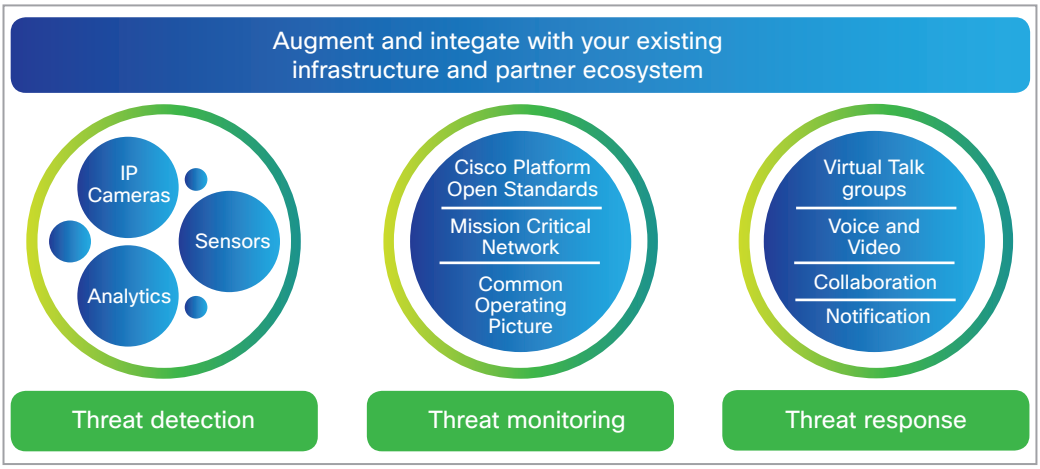
Enabling Smart and Connected Communities

Effective public safety and security is critical to the long term prosperity and success of a community. Citizens and businesses look towards authorities to prevent, prepare for, respond to, and recover from incidents. However the reality is that many cities and towns face growing threats from man-made and natural disasters These threats have a catastrophic impact on lives, property, and people's sense of well-being.

Cisco Smart and Connected Safety and Security transforms the way organizations and communities protect people, property, and critical infrastructure. It does this by providing a practical framework and proven set of integrated Cisco technologies—a Cisco Borderless Network foundation that supports Cisco Unified Communications and Collaboration tools, physical security, video, analytics, and Cisco partner solutions.

Figure 2 shows how this network-centric approach provides an intelligent fabric that optimizes all stages of the public safety and security process: detection, assessment, and response.

Figure 2. The network: An intelligent fabric accelerating detection, assessment, and response



In this highly responsive and adaptive IP environment, disparate communications and information silos no longer exist. Legacy PBX systems, radios, and servers are transformed into a single intelligent network. The right information is securely delivered, to the right person, in the right format, at the right time.

Incoming calls and video streams can be distributed via a variety of sources: cellphones, IP phones, smartphones, tablets, and so on. Unlike a traditional network, a Cisco Borderless Network intelligently recognizes the type of end device and delivers the video stream in the most optimal format for that device—whether that is pushing content from a smartphone at the scene to a screen at the incident control room, or vice versa.

Cisco's architectural approach to Safety and Security

Cisco Smart and Connected Safety and Security offers a practical roadmap for accelerating public safety and security transformation by using proven enterprise architectures and a structured approach that is both "top-down" (because it takes a holistic view at the problem definition, and does not try to fit pinpoint solutions ignoring the broader perspective), and "bottom-up" in nature (because it leverages real-life customer experiences to develop its solutions). *Figure 3* shows how Cisco's SOFT (Strategic; Operational; Functional; and Technical) approach meets the interests of stakeholders at four levels within an organization.

Figure 3. Cisco's SOFT framework for implementing Cisco Smart and Connected Safety and Security

Perspective	Type of Stakeholders	Main Objective
Strategic	Srategic decision makers, e.g. political leaders, regional governors, chief executives, etc.	Provides the vision and goals of the organization (its reason for being) and encompassing context for copatibility planning
Operational	Operations managers, heads of departments, etc.	Defines the missions, the use case scenarios, agents and processes, information flow, and requirements on systems
Functional	CIO, ICT Directors, Project Managers, etc.	Designs functional systems and derives specifications from operational requirements
Technical	ICT Managers, Engineers, etc.	Defines the solution (usually an ecosystem) and implementation

Strategic

Cisco Smart and Connected Safety and Security provides government agencies and transport operators with a pragmatic approach for accelerating transformation on several fronts, including:

- Reducing costs, for example, by reusing existing infrastructure and extending security systems for other purposes
- Improving situational awareness, real-time collaboration, and decision making
- Lowering training costs
- Accelerating incident detection
- Automating responses
- Using predictive modelling and data-mining techniques to look for patterns and process improvements
- Lowering risk by helping to ensure that IT investments align with long-term vision and goals
- Providing an open, interoperable platform for integration so budget can be used to enhance, not replace

Operational

The focus here is on working with department heads and operational managers to capture relationships and information exchange between logical entities. The end goal is to develop a plan for improving the effectiveness of people, applications and processes – for example, by providing more information at the fingertips of users, and introducing some of the new capabilities discussed within the later sections of this document.

Key milestones in the operational planning phase are to create an organization chart with clearly defined responsibilities as well as a sustainable financial model. Use case scenarios, similar to the examples shown in the later sections of this brochure, also help to explore and establish desired outcomes.

Functional

Working with the CIO and senior team, the next step is to describe the logical systems and services that support the operational requirements, and provide the long-term technology roadmap to support the strategic vision and goals.

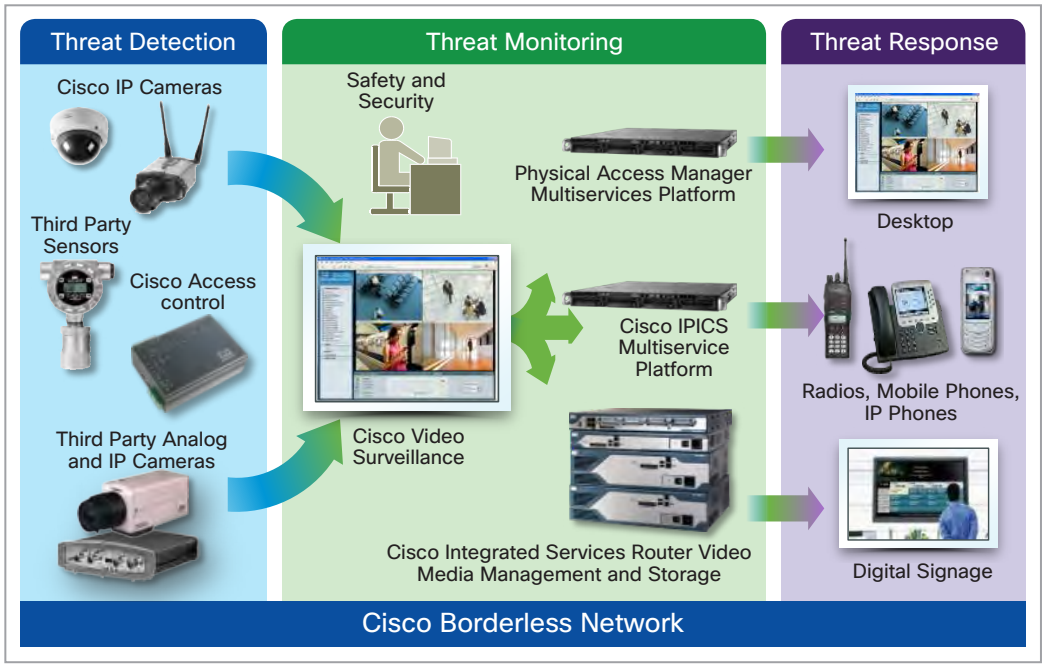
Technical

The focus here is on reducing risk, cost, and time to market. Cisco's methodology includes combining horizontal solution blocks to form vertical solution blueprints, for Cisco and ecosystem partner technologies, along with adapted detailed designs and pre-validated configurations and templates.

Solution Overview

The key components of Cisco Smart and Connected Safety and Security (*see Figure 4*) are part of a wider portfolio of Cisco Public Safety and Security solutions. These solutions have been, and continue to be, adopted worldwide by Cisco customers involved not just with the security management of cities and municipalities, but also key organizations operating within the energy, healthcare, education, and physical security sectors.

Figure 4. Key components of Cisco Smart and Connected Safety and Security



Key components of Cisco Smart and Connected Safety and Security include:

Threat Detection

- Cisco IP cameras / Video Analytics: A broad range of wired and wireless cameras, including high-definition picture quality, designed for both indoor and outdoor use, combined with decentralized on-board / in-cam(era) or centralized video analytics.

Threat Monitoring

- Cisco Physical Security Operations Manager: Provides a scalable command and control-style operator console by unifying incident management and operation of Cisco VSM, PAM, and IPICS solutions (described within the following sections).
- Cisco Video Surveillance Manager (VSM): Distributes, stores, and manages video from thousands of legacy analog cameras, while also allowing this video to be integrated with analytics applications to alert operators of predefined events.
- Cisco Physical Access Manager (PAM): Improves access control by providing the ability to configure Cisco Physical Access gateways and modules, monitor activity, enroll users, and integrate with IT applications and data stores.
- Cisco IP Interoperability and Collaboration System (IPICS): Speeds up dispatch and incident response by enabling public safety teams to consolidate incident-related information– whether in voice, video, or data format– and instantly share it with any device type– IP phone, cell phone, walkie-talkie, mobile device, or PC.
- Cisco Integrated Services Router with Video Media Management and Storage: leverages the video management and storage system module for the intelligence of video management through Cisco Video Surveillance Manager and the integrated storage system module for extended video storage.

Threat Response

- Digital Media Suite: End-to-end digital signage system that can be used both as a display for safety and security guidance and pre-recorded video content, or to centrally broadcast situational updates as an incident develops.
- TelePresence: Provides a powerful in-person, HD-quality video collaboration platform, which can also be integrated with Cisco WebEx and video endpoints, to rapidly engage responders and key decision makers.
- Media Experience Engine: Removes two barriers traditionally associated with video—accessibility and ease of use—in turn accelerating the transition to pervasive video by connecting people and media across any device or application.
- Unified Communications and Collaboration solutions: A wide range of voice, video, and web conferencing; messaging; mobile applications; and enterprise social software solution that empower people to work and collaborate— anytime, anywhere, and on any device.

Infrastructure

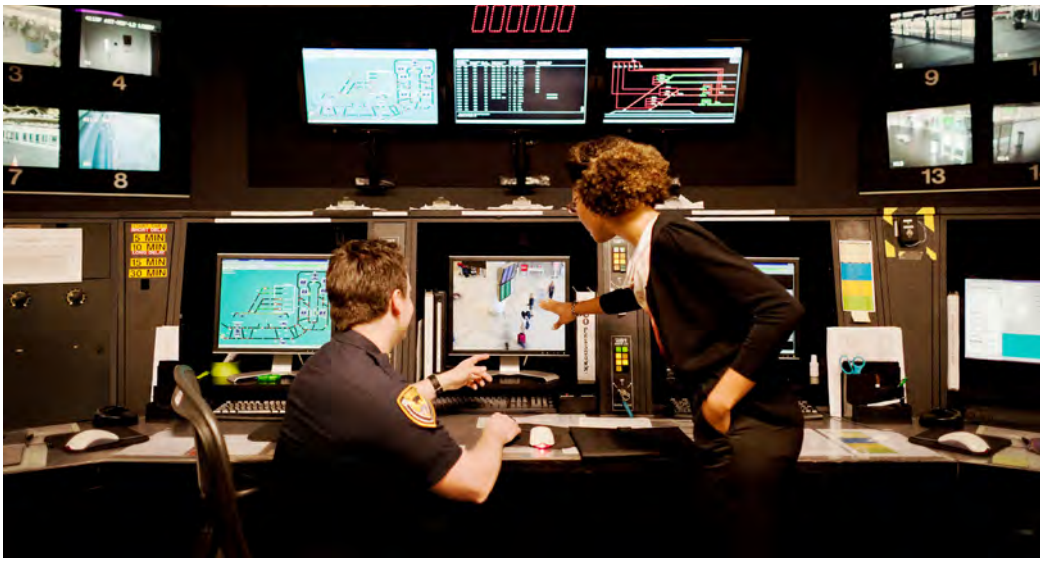
- Cisco Borderless Network: The foundation for Cisco Smart and Connected Safety and Security. Unlike a traditional network, a Cisco Borderless Network introduces new innovations, such as SecureX, Medianet, EnergyWise, AnyConnect, CleanAir and Clientlink that enable new methods of connecting, working, and collaborating.
- Cisco Integrated Services Router: Delivers highly secure broadband, Metro Ethernet, wireless LAN connectivity, and business continuity in a mobile environment (police car, ambulance, fire truck, …).

Mobile Command and Control Center

- Cisco Network Emergency Response Vehicle (NERV): A self-contained vehicle in which all technology travels together as a preconfigured package that can be up and running in 15 minutes.

Third Party solutions

- A guiding principle of Cisco Smart and Connected Safety and Security is to design solutions that avoid a 'rip and replace' approach and instead allow authorities to integrate and leverage existing assets, including technologies from other vendors.



Use Case Scenario 1

Using Cisco NERV to manage a natural disaster situation

Adam is the head of the city's emergency planning unit. As an impending tornado hit gets upgraded in severity, he realizes that the situation on the ground is rapidly deteriorating as events unfold and resources become stretched.

By calling out a Cisco Network Emergency Response Vehicle, Adam and his team immediately set up a mobile command and control center at the precise location it is needed.

Disparate voice communications, previously only limited to personal cell phones and radios, receive an instant boost as Cisco specialists use Cisco IPICS so that emergency services can talk to each other and collaborate as a virtual work group using IP communications.

Local forces have IP connectivity via the wireless hotspot provided by the vehicle

Also, by using the vehicle's satellite link and in-built Cisco TelePresence system to deliver live video streams, the command team can now see and fully assess the situation, before directing first line responders as appropriate.

Benefits

With Cisco Smart and Connected Safety and Security, organizations can:

- **Unify operations** across agencies, in-country and across borders, in turn reducing the time between an incident and response. This is achieved by:
  - **Empowering support teams** and first responders with the tools they need to instantaneously receive information from different types of sensors and different agencies, process the information to detect anomalies, present it in an easy-to-understand fashion tailored for the person's role, to their device of choice, and enable decision makers to assign tasks to field personnel.
  - **Improving intelligence management** by enabling personnel to gather information from different sources, including citizens, first responders, and various sensors.
  - **Making processes more effective and efficient**, for example, through the use of tools that analyze, correlate, and consolidate data into roles-based, actionable information.
- **Ensure confidentiality, interoperability, and availability of information by:**
  - **Improving and streamlining the flow of data** from centralized databases, sensors, and first responders on the scene. Access to information should not be restricted by the user's location, type of network, or device. Rather, it should be governed by policies related to the user's role and factors such as time of day.
  - **Enabling any-to-any communications** so that personnel can transmit voice, video, and data, including rich-media like building floor plans, over wired or wireless networks.
  - **Building in extra redundancy and resilience** so that the network remains available despite partial outages or attacks on the underlying infrastructure.

Use Case Scenario 2

Workforce enablement for city operations

It is a hot day in the Smart City. Through video surveillance and citizen reports received from calls, texts, and tweets a break in a major street water pipe is identified.

Operators assess the situation with nearby video cameras and the operations manager initiates an action plan. First responders, including fire, police and water repair teams are instantly notified.

Live video and situational information, including infrastructure plans and traffic data, are shared so all parties have an identical view and understanding. Alternate travel routes are posted on digital displays to help ease congestion.

At the scene, Cisco technology allows field crews and remote experts to work seamlessly together via effective voice, video, and data exchange.

The police install traffic diversions allowing the water supply to be turned off and repair work to start in complete safety.

The intelligent traffic management system senses secondary congestion caused by the diversions and notifies the control center and traffic police nearby.

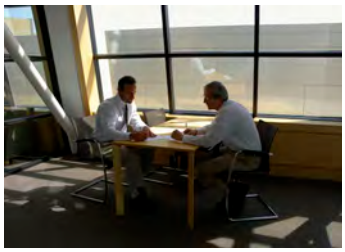
Officers take manual control of several traffic lights. In the meantime, the water pipe repair has been completed, leaving citizens to go about their business without further disruption or inconvenience.

- **Improve surveillance, monitoring, and incident control by**:
  - **Enabling access to voice, video, and data, on the move and remotely**. An example is precipitation and frost sensors, which can help identify conditions leading to traffic accidents. Public safety agencies can use this information to reduce speed limits or close roads. Similarly, traffic sensors can trigger intelligent traffic control systems to avoid jams. Gunshot detection systems can be placed in areas with high crime rates or in busy public areas. And video surveillance systems have been shown to deter crime, and collect valuable forensic evidence when crime does occur.
  - **Integrating video analytics software** to search for predefined events and send alert notifications. There are typically two deployment models: Performing video analytics in the cameras, or using centralized servers. Cisco has solutions for both approaches.
  - **Introducing asset and people tracking solutions**, such as RFID tagging:
  - **Using remote actuation**, for example, to move or control mechanisms such as airflow control vents and fire sprinklers. For example, if a gas sensor detects a leak, the system would automatically close down or alert a supervisor to shut the valve.
- **Increase police visibility and presence by:**
  - **Reducing the administrative burden of policing** so that officers spend less time in the office and more time in the community reducing crime and fear of crime.
  - **Improving mobile communication and real-time access to data** such as video, maps with satellite imagery, and GPS tracking, and global databases.
  - **Establishing incident area networks** (typically a highly mobile network housed in a van) that connect personnel at the incident scene with colleagues in the control room and headquarters.
  - **Using location-based services**, for example, to provide up-to-date information on positioning, or conditions, such as temperature, humidity, or heart rate.

Partner ecosystem

A key element in the implementation of Cisco Smart and Connected Safety and Security is the partner ecosystem. The specific role of Cisco and Cisco partners will vary depending on the complexity of each project. Typical roles are,

- Thought leadership and planning for large-scale projects such as city redevelopment, new city build-out, and large-scale sporting events. Cisco ecosystem partners include Accenture and AECOM
- General contractors that take these plans to the development stage and act as the contract lead responsible for executing service delivery. Examples include companies such as SKANSKA, Honeywell, Bin Laden Group, and Schneider.
- Technology Partners providing specific vertical solutions that will be part of the larger Smart Connected Community.
- System Integrators interconnecting the various technology components of the solution on behalf of the customer. Examples include EADS, IBM, Thales, Raytheon, GD, and LM.
- Operators delivering services or operating services for the customer as part of an outsourced / managed service model. These partners can be governmental-owned (full or partly) such as Airwave in UK, or private companies or service provider organizations.
- Financial Partners such as Cisco Capital or other funding entities such as the World Bank or European Union.
- Cisco Safety and Security Advanced Technology Partners with the training and experience to install all the Cisco elements of the solution






Case Studies

Transport for Greater Manchester

Transport for Greater Manchester (TfGM). is responsible for overseeing public transport services throughout Greater Manchester in North West England. It also owns Greater Manchester bus stations, funds essential bus and train services, and owns the successful Metrolink tram network.

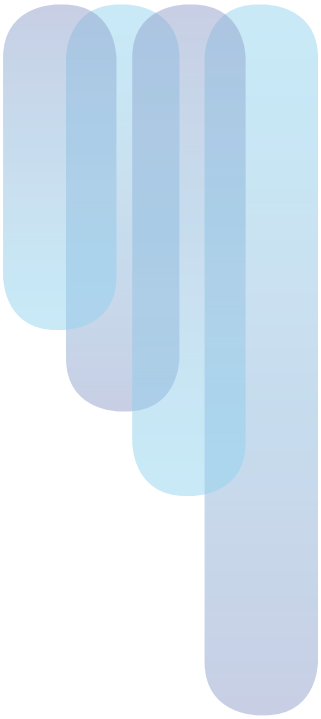
Centralized storage and management means that TfGM will no longer need to purchase and maintain video surveillance storage and management servers at each station, reducing equipment costs and power consumption. The only technology that each station needs is cameras and a web browser. TfGM saved more money, because Cisco Video Surveillance IP Cameras receive power over Ethernet, from the station's Cisco Catalyst® Switch. This feature eliminated the expense of bringing power cables to each of the cameras.

Authorized station personnel and police can view video from any camera, from any web browser. "The web-based interface for Cisco Video Surveillance Manager enables us to view video from any location, not just the station, and saves the cost of client software for each station," Wharton says. Operations personnel at the station were able to begin using the Cisco Video Surveillance Solution with minimal formal training, using the intuitive interface to view real-time and archived video from different cameras.

Situated in North Central Mexico, San Luis Potosí is home to about 700,000 people. It wanted to improve physical security of citizens, significantly increase situational awareness of police, and enable fast, real-time response. The city has invested in an advanced video surveillance solution, integrating video analytics and other applications, running over a wireless network.

The video surveillance solution has significantly increased the city's ability to spot incidents and react quickly to them. Not only does the new solution deliver far more useful forensic evidence, the combination of higher quality images, analytics, and the way in which the information is displayed, means that operators can send resources to an incident as it is happening. In some cases, they can even anticipate crime before it happens. Ricardo Galindo Ceballos, Public Safety, IT director for San Luis Potosí, says: "They allow the optimization of police resources. A visual verification can be made without putting the officer at risk, and operations can, therefore, be carried out more securely. They also assist in assessing how many and what kind of support personnel are required on the scene and with what equipment."

The solution has also helped to save lives, such as when a Command Center operator was able to help direct emergency services to a young woman very seriously injured in a road traffic accident. Not only were the emergency services given the best route, based on what was happening on the streets, the operator was able to brief them better about the accident and what they might find there. Wireless devices, such as handheld, personal digital assistants, can also link directly to the network, its applications, and the Command Center



Technical components

Key components of the Cisco Security solution include:

- Cisco Video Analytics
- Cisco Physical Security Operations Manager
- Cisco Video Surveillance Manager
- Cisco Physical Access Manager
- Cisco IP Interoperability and Collaboration System
- Cisco Integrated Services Router with Video Media Management and Storage
- Cisco Digital Media System
- Cisco TelePresence
- Cisco Media Experience Engine
- Cisco Unified Communications and Collaboration applications
- Cisco Borderless Network infrastructure

Next Steps

For additional information or to speak with someone regarding Cisco Smart and Connected Safety and Security, please contact your local Cisco office / partner or pss-as-support@cisco.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.**