



Cisco Open Platform for Safety and Security: Meeting the Urban Security Challenges

Contents

What You Will Learn	1
The Challenges of Urban Security	1
Vision for Urban Security	3
Goal 1: Unified Operations Across Multiple Agencies	4
Goal 2: Confidentiality, Interoperability, and Information Availability	5
Goal 3: Effective Collaboration Within and Across Local Communities	7
Goal 4: Surveillance, Monitoring, and Incident Control	9
Goal 5: Increased Police Presence on the Streets	12
Goal 6: Enhanced Communication Between Government and Citizens	14
Conclusion	16
For More Information	16

What You Will Learn

The Cisco Open Platform for Safety and Security is an architecture framework for building solutions to prevent, prepare for, respond to, and recover from incidents. The framework consists of six architecture building blocks and defines architectures applicable to a variety of safety and security market domains. These include Crisis Management, Urban Security, Border Control, Mass Venues and Events, Secure Public Transportation, and Prisons and Probation.

This white paper is intended for organizations planning investments in safety and security technologies and for solutions providers. It focuses on the Urban Security domain, which addresses the following goals:

- Unified operations across multiple agencies
- Confidentiality, interoperability, and availability of information
- Effective collaboration within and across local communities
- Surveillance, monitoring, and incident control
- Increased police presence on the streets
- Enhanced communication between government and citizens

The Challenges of Urban Security

Modern cities must protect citizens and businesses from a wide spectrum of risks including crime, terrorism, attacks on critical infrastructure, natural catastrophes, and other emergencies. Following are the major challenges, extrapolated from a variety of real-life urban crises, including the widespread vandalism in the Munich, Germany underground transportation system in 2008 and the Mumbai, India shootings in 2008.

- **More sophisticated safety and security threats:** Increasingly, criminals take advantage of technology to perpetrate crime. Modern terrorist attacks, for example, are facilitated by advanced consumer electronics such as smartphones, geographic positioning system (GPS) navigators, and anonymous email accounts.
- **A move to capability-based planning:** Many emergency plans rely on the execution of explicit and documented tactics. The drawback of this approach is that it is impossible to predict all contingencies. A more practical approach is capability-based planning, or putting in place a flexible architecture with capabilities that are useful in a wide range of scenarios. This allows improvised reactions to unpredicted threats.
- **Unreliability of rarely used processes:** When personnel rarely use a system, they are more likely to make mistakes. They might even not notice an alert announced on the special emergency system, if they are unaccustomed to checking. What's more, maintaining separate systems for emergencies and everyday communications doubles the expense for training, administration, and upgrades.
- **Difficulty of monitoring and managing more systems:** The increase in the number and types of threats has led to a corresponding increase in the systems that public safety agencies must manage. Many agencies already have large existing investments in video surveillance cameras, radios, fire suppression systems, and more. Now they are adding new systems for cybersecurity, event correlation, and response to chemical, biological and radiological threats. If each system is deployed on its own proprietary network, management becomes progressively more expensive.

- **Confusion resulting from disparate emergency communication systems:** Poor information flow both within and among the organizations involved in preparing for and managing disasters is among the principal causes of failures. Costs can be measured in money as well as in lives. Typically, inadequate information distribution is the direct consequence of human error, interagency conflicts, political considerations, and lack of communications interoperability.
- **Organizational boundaries and public-private partnerships:** A variety of people from different organizations, not just traditional public safety agencies, need to share information in a crisis. These might include hospitals, clinics, schools, and housing for senior citizens. These entities ordinarily keep their information private, so they need assurance that their information will be shared only for the duration of the crisis, and on a need-to-know basis.
- **Growing dependence on privately held critical infrastructure:** Citizens depend on critical infrastructure located within or nearby urban centers. Examples include petrochemical processing/distribution centers, power plants, seaports and airports, and major stock exchanges. This further illustrates the need for urban security architectures to support information sharing with private-sector organizations.
- **Cyber warfare:** Employees can unintentionally introduce threats by bringing infected laptops to work or visiting malware-laden websites. These threats give cybercriminals an open door to the network so that they can steal sensitive information or launch additional attacks. Critical infrastructure is subject to the same risks, potentially affecting power generation and distribution, transportation, oil and gas pipelines, water distribution, and telecommunications. Disruption of this infrastructure has significant economic consequences.
- **Misinformed general public:** While law enforcements typically respond promptly to urban crises, authorities often fail to notify citizens until hours after the crisis begins. The larger the incident scope, the more carefully the information must be conveyed. Too much information can cause mass panic; too little can result in some citizens not finding out about the incident so that they can take precautions.
- **Citizen privacy needs:** Public safety agencies need to collect and apply information about citizens in a responsible way.

Vision for Urban Security

In the Cisco Open Platform for Safety and Security, the vision of the Urban Security domain is to handle a growing number of security incidents with fewer personnel, freeing up resources for crime prevention. The enabler is improved collaboration among all participants. This streamlines emergency response and speeds up reaction times, reducing the scope and impact of an incident. Within this vision, cities do not have to replace their entire existing infrastructure. Rather, they can link their existing investments to create a “system of systems.” This approach is more resilient and adaptable to today’s diverse threat environment. The Cisco Open Platform for Safety and Security architectural framework has value for day-to-day monitoring as well as major crises, lowering costs and eliminating the risk of relying on specialized emergency systems that personnel use infrequently.

The remainder of this white paper describes goals that support this vision for urban security, the capabilities required to achieve the goals, and the solutions within the Cisco Open Platform for Safety and Security.

Goal 1: Unified Operations Across Multiple Agencies

In urban environments, it is critical to reduce the time between an incident and the appropriate response. To accelerate the process, personnel need systems that can 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, and enable decision makers to assign tasks to field personnel. Achieving this goal requires the following capabilities:

- **Intelligence management:** The agency needs to gather information from different sources, including citizens, first responders, and various sensors.
- **Process management:** Converting data into actionable information requires tools to analyze, correlate, and consolidate data. Emergency operations personnel need a role-based view of the information.
- **Common Operational Picture:** All participating organizations must be able to share information from their own systems and access information as appropriate to their role. The Common Operational Picture (COP) makes the commander's physical location irrelevant. Everybody participating in the emergency process can access and distribute information from anywhere.

Figure 1 shows the solution, which is based on the Command and Control architecture building block in the Cisco Open Platform for Safety and Security. Solutions from Cisco and examples of partners that deliver these capabilities appear in Table 1. For details, visit www.cisco.com/go/copss.

Figure 1 Multiple Agencies Can Unify Operations Using the Capabilities in the Command and Control Architecture Building Block

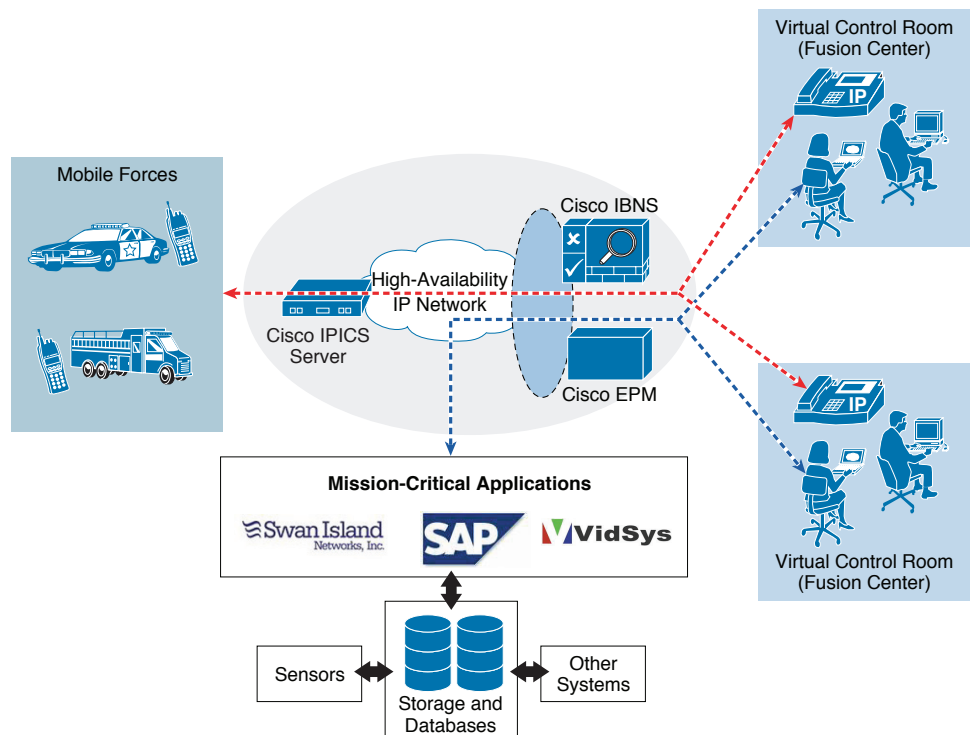


Table 1 Solutions in the Command and Control Architecture Building Block

Vendor	Solution	Description
	Identity Based Networking Services (IBNS) and Cisco Enterprise Policy Manager	Allows organizations to define granular rules controlling who can access the network, information, and applications. Rules can take into account real-time information such as network load.
	Cisco IP Interoperability and Collaboration System (IPICS)	Enables personnel in the same or different organizations to communicate directly using disparate communications devices, including any type of radio, traditional phone, IP phone, mobile phone, or softphone. Cisco IPICS can apply policies to enforce compliance with formal command hierarchies.
	Public Security Solutions	Increases operational awareness, preparedness, responsiveness, and ability to recover following an incident. The solutions combine risk and intelligence management, identity resolution, investigative case management, and command and control with resource deployment.
	Situation Management and Video Management Applications	Provides a web-based interface to monitor all physical security assets and to quickly identify and resolve real-time security violations. Used for the surveillance and management of borders, unmanned remote locations, valued assets, and buildings and campuses. Operations personnel can work from anywhere.
	TIES	Creates an online virtual watch center, bringing together diverse data such as local, national, and global incident maps; emergency-number feeds; weather data; flood maps; health advisories and alerts; and traffic information. TIES disseminates alerts and notifications of potentially disruptive events to web-based and mobile clients.

Goal 2: Confidentiality, Interoperability, and Information Availability

To respond early in the crisis, cities need ubiquitous, instant, secure, and reliable access to information. That information can come from centralized databases, sensors, or 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. Required capabilities to achieve this goal include:

- **Resilient infrastructure that can survive adverse conditions:** Redundancy and resiliency mechanisms help to ensure the network remains available despite partial outages of the underlying infrastructure.
- **Interoperability:** Personnel need the ability to transmit voice, video, and data, including rich-media like building floor plans, over wired or wireless networks. This requires communications devices and networks that support open standards.
- **Cyber Security:** To protect sensitive information, including private citizen data, public safety agencies need to protect the network from unauthorized access and from internal and external attacks.

Figure 2 shows the solution, which is based on the Mission-Critical Network architecture building block in the Cisco Open Platform for Safety and Security. Cisco solutions that deliver these capabilities appear in Table 2. For details, visit www.cisco.com/go/copss.

Figure 2 Confidentiality, Interoperability, and Information Availability Are Enabled by the Mission-Critical Network Architecture Building Block

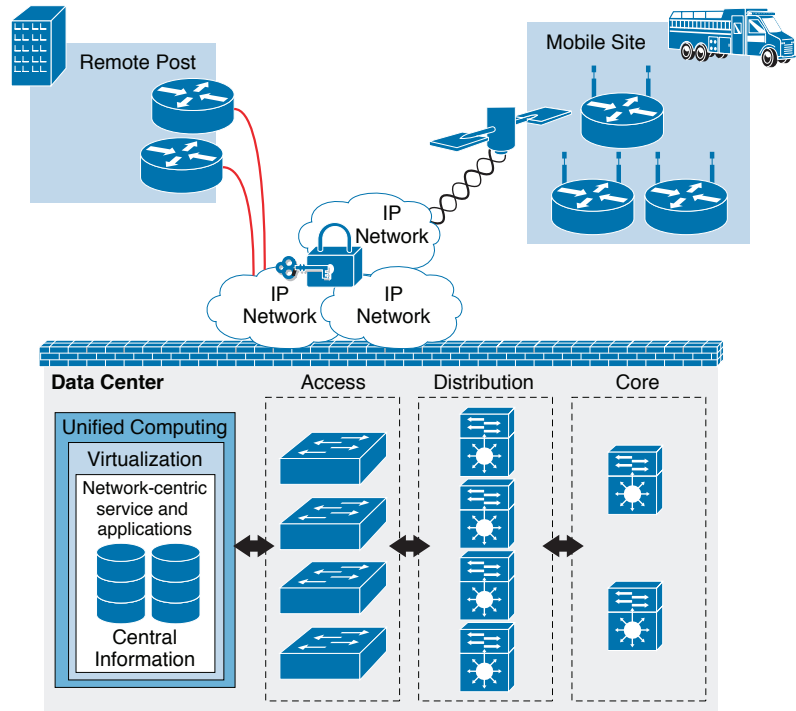







Table 2 Solutions in the Mission-Critical Network Architecture Building Block

Vendor	Solution	Description
	Cisco Outdoor Wireless Solutions	Enables public safety organizations to build cost-effective outdoor wireless networks, even in moving vehicles. For urban security, wireless networks are useful to connect mobile users to headquarters and to each other, and also to provide location-based services such as locating assets and personnel.
	CiscoWorks	Enables centralized administration of all Cisco components deployed within the network. Capabilities include network discovery, topology views, centralized configuration, monitoring, and real-time fault analysis.
	Data Center 3.0 Solutions	Helps prevent unauthorized access while making it easy to grant access to new or temporary users and devices. These solutions automatically check devices for required software and configuration when the devices attempt to connect, and automatically perform remediation if needed. Other solutions in the suite monitor for anomalous behavior to protect against unknown, or day-zero, threats.

	<p>Cisco Trust and Identity Management Solution</p>	<p>Provides a web-based interface to monitor all physical security assets and to quickly identify and resolve real-time security violations. Used for the surveillance and management of borders, unmanned remote locations, valued assets, and buildings and campuses. Operations personnel can work from anywhere.</p>
	<p>Cisco Integrated Services Routers and Cisco Catalyst Switches</p>	<p>Combines multiple services on one platform, such as voice, video, wireless, and firewall. This simplifies management and ensures that security and wireless, for example, apply to voice, video, and data.</p>

Goal 3: Effective Collaboration Within and Across Local Communities

Interagency collaboration is often thwarted by incompatible communications systems. Comprehensive communications interoperability requires the following attributes:

- **Multimodal:** First responders and background personnel need the flexibility to communicate with whatever device is available, including analog or digital radio, cell phone, traditional phone, IP phone, or laptop.
- **Cross agency:** Public safety personnel need to be able to collaborate with people in other agencies.
- **Ad hoc:** Organizations involved in urban security must be able to instantly join their systems into a “system of systems” for the duration of their collaboration.

Figure 3 shows the solution, which is based on the Incident Collaboration architecture building block in the Cisco Open Platform for Safety and Security. Solutions from Cisco that deliver these capabilities appear in Table 3. For details, visit www.cisco.com/go/copss.

Figure 3 Effective Collaboration Within and Between Communities Is Enabled by the Incident Collaboration Architecture Building Block

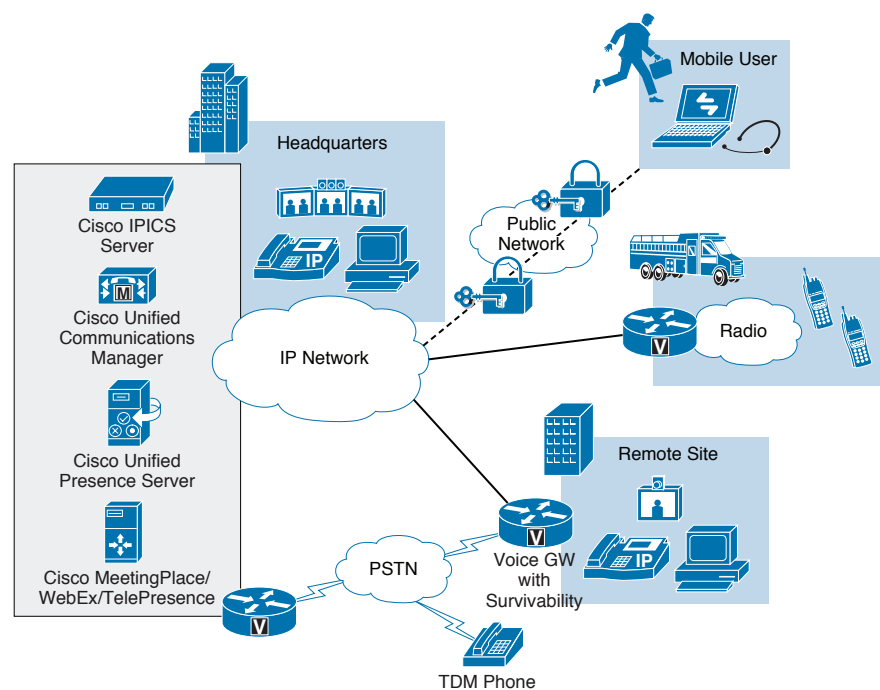









Table 3 Solutions in the Incident Collaboration Architecture Building Block

Vendor	Solution	Description
	Cisco Unified Communications Manager	Provides centralized or distributed call processing. In the distributed model, each location needs only a Cisco Integrated Services Router and Cisco Unified IP phones, reducing costs.
	Cisco Voice Gateways	Links Cisco Unified Communications Manager with traditional TDM voice systems. If the network connection between the branch and the centralized Cisco Unified Communications Manager becomes unavailable, the Cisco voice gateway automatically connects to the public switched telephone network (PSTN) for the duration of the outage and then automatically restores the IP network connection when the link becomes available.
	Cisco Unified Operations Manager	Helps administrators monitor and troubleshoot the Cisco Unified Communications System. Administrators can use the test capabilities to identify potential issues before they cause problems.
	Cisco Unified Provisioning Manager	Saves time for moves, adds, and changes to voice and voicemail accounts.
	Cisco Unified Presence Server	Shows whether other people are available and how they prefer to be reached, saving precious time otherwise spent dialing multiple numbers and leaving voicemail.
	Communications Devices	Includes wired and wireless Cisco Unified IP phones, with and without video, and Cisco IP Communicator, a feature-rich softphone. Cisco Unified Personal Communicator includes a softphone as well as other collaboration applications, including presence, voicemail, instant messaging, and unified messaging. All Cisco devices can be used to deliver XML applications, such as status of incidents, visual and audio paging, information access, and more.
	Cisco IP Interoperability and Collaboration System (IPICS)	Enables personnel in the same or different organizations to communicate directly using disparate communications devices, including any type of radio, traditional phone, IP phone, mobile phone, or softphone. Cisco IPICS can apply policies to enforce compliance with formal command hierarchies.
	Cisco TelePresence, Cisco WebEx, and Cisco Unified MeetingPlace	Enables remote meetings combining voice, video, and web sharing. Cisco TelePresence provides an in-person experience, with life-size images and very-high-quality of audio and video. Scheduling and joining meetings with any tool is just like scheduling or joining an ordinary conference call.

Case Study: Piedmont Region, Virginia

Several independent jurisdictions in Virginia wanted interoperable communications. Replacing each department's radios would be cost-prohibitive. Instead, the jurisdictions deployed a Cisco IP Interoperability and Collaboration System (IPICS). Personnel can join talk groups using any radio system, as well as traditional phones, IP phones, and mobile phones. According to a report co-authored by Major Dean Hairston of the Danville, Virginia police department, "The ... project validates an exceptional model to improve local and state public safety response effectiveness through the use of IP technology. For the first time ever, these organizations are able to communicate in ways that they never thought possible. We recommend that all sovereignties look into taking full advantage of their existing IP network infrastructure to improve both inter- and intra-jurisdictional communications."

Goal 4: Surveillance, Monitoring, and Incident Control

Effective response to large-scale disasters requires that all participants can rapidly access all available information, including sensor data. They also need the ability to take action remotely, without having to rely on deployed human forces. To meet this goal requires the following capabilities:

- **Ubiquitous sensor system:** 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.
- **Distributed analytics:** Video analytics software looks for predefined events and then takes an action, such as sending an alert, when the event is detected. It is preferable to perform video analytics in the cameras themselves instead of in centralized servers. This conserves network bandwidth and reduces hardware cost and space requirements.
- **Asset and people tracking and tracing:** Urban security sometimes requires tracking the location of people and assets. Safety agencies can accomplish this by affixing RFID tags to objects, and providing people with bracelets or badges containing the tag. The tags can be read by fixed or handheld RFID readers.
- **Remote actuation:** Actuators remotely move or control mechanisms such as airflow control vents and fire sprinklers. They can be triggered by a human or a sensor. For example, if a gas sensor detects a leak, the supervisor can remotely shut the valve. Alternatively, the alert can trigger an action to automatically shut the valve.

Figure 4 shows the solution, which is based on the Sensing and Actuation architecture building block in the Cisco Open Platform for Safety and Security. Solutions from Cisco and examples of partners that deliver these capabilities appear in Table 4. For details, visit www.cisco.com/go/copss.

Figure 4 Surveillance, Monitoring, and Incident Control Are Provided by the Sensing and Actuation Architecture Building Block

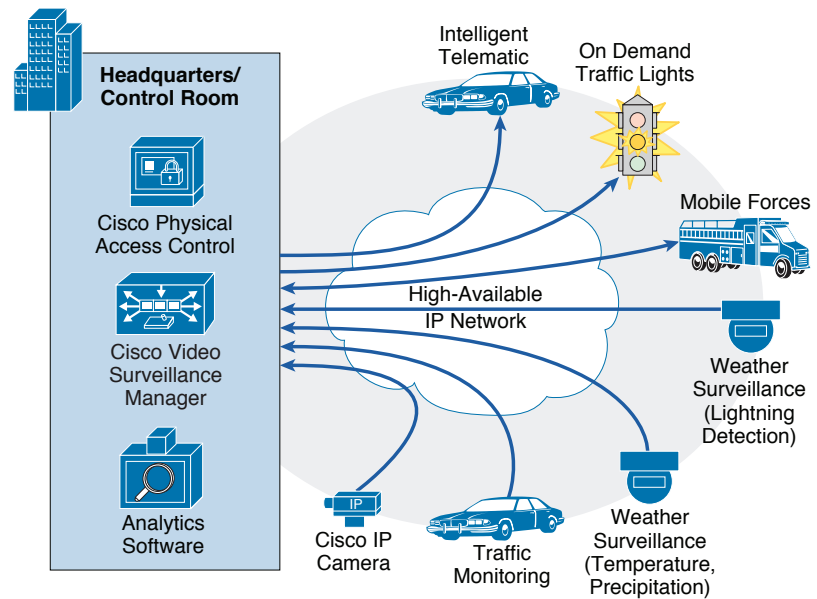







Table 4 Solutions in the Sensing and Actuation Architecture Building Block

Vendor	Solution	Description
	Cisco IP Video Surveillance Cameras	Captures standard-definition or high-definition video, in MPEG-4 or H.264 formats. The cameras integrate with microphones, speakers, and access control systems—for example, to begin streaming video if someone swipes an access card.
	Cisco Video Surveillance Manager	Enables organizations to manage, replicate, distribute, and archive video streams. Provides a web-based interface to authenticate and manage access and manage solution components. The included Cisco Video Surveillance Virtual Matrix allows operators to select which video stream to view.
	Cisco Physical Access Control	Enables security personnel to remotely lock and unlock doors, either according to a predefined schedule or on demand. Access privileges can vary based on time of day or day of week. Integrates with the Cisco Video Surveillance solution.
	Wireless Sensor Networks	Enables emergency organizations to rapidly develop and deploy wireless sensor networks, often in just one hour. Leverages IETF RFC4944, the standard for IPv6 communication over low-power IEEE 802.15.4 wireless radio.
	FaceVACS	Recognizes faces to help prevent identity fraud, secure borders, and support physical access control. An open system architecture simplifies integration with other systems.

	Location-Based Services	Locates and tracks people and equipment using small AeroScout RFID tags. The solutions can also locate any 802.11-enabled wireless device, including laptops. Use the solutions to prevent theft and issue automatic alerts when equipment or people move outside of defined locations.
	ObjectVideo Software	Analyzes video to detect events of interest, such as perimeter breaches, loitering, unauthorized entry or exit, and theft. When user-defined rules are violated, ObjectVideo immediately generates an alert or initiates another user-defined action, such as recording video with Cisco Video Surveillance Manager.
	Customized Cisco Integrated Services Routers	Provides customized, rapidly deployable Cisco ISRs for emergency response; telemedicine, oil, gas and mining infrastructure protection; border security and surveillance; and enterprise safety and security. The solution is preintegrated with solutions from Cisco and other partners for CBRNE sensors, access control devices, physical security devices, radars and video surveillance systems, and more.
	SPM Sensor Policy Manager	Combines inputs from multiple networked sensors of any type, from any vendor, making the information available from any web browser. ViaLogix SPM creates a real-time operational picture and reduces false positives and negatives. It can also initiate user-defined actions in response to sensor inputs, such as notifying emergency personnel.
	EdgeFrontier™	Enables organizations to build and manage solutions that integrate data from all edge assets, including existing sensors as well as Cisco Video Surveillance Media Server, Cisco Access Control Manager, and end-user applications. Using the existing network for remote monitoring and data sharing reduces total cost of ownership.

Case Study: State of Texas Disaster Response Tracking System

Texas state officials wanted to ensure the safety of evacuees who are vulnerable because of special needs. They met the requirement by installing GPS tracking devices in buses that are used for evacuations, and providing bracelets with embedded RFID tags to people needing assistance. The state Homeland Security Director says the system allows responders to “track assets and people in real time across the state.” The program is a collaborative effort spanning law enforcement, recovery workers, cities, counties, and the state.

Goal 5: Increased Police Presence on the Streets

Police visibility reduces crime and fear of crime. And the less time that police spend in the office looking up information, the more time they have to spend in the community. Achieving this goal requires the following capabilities:

- **Mobile computing:** Police officers need access to real-time video, maps with satellite imagery, Global Positioning System (GPS) tracking, and global databases. They need mobile computing devices that can run such applications and can withstand harsh environmental conditions. In addition, the incident scene must provide wireless connectivity such as Wi-Fi, satellite, or GSM/UMTS for instance.
- **Incident Area Network:** Established for the duration of a particular incident, the Incident Area Network (IAN) connects all personnel at the incident scene and also connects them to the headquarters network. IANs can move, as when they're deployed in vehicles.
- **Location-based services:** Personnel and equipment need to be equipped with RFID tags providing up-to-date information on their position and perhaps other conditions, such as temperature, humidity, or heart rate.

Figure 5 shows the solution, which is based on the Mobile Force architecture building block in the Cisco Open Platform for Safety and Security. Cisco solutions that deliver these capabilities appear in Table 5. For details, visit www.cisco.com/go/copss.

Figure 5 Communities Can Increase Police Presence Using Capabilities in the Mobile Force Architecture Building Block

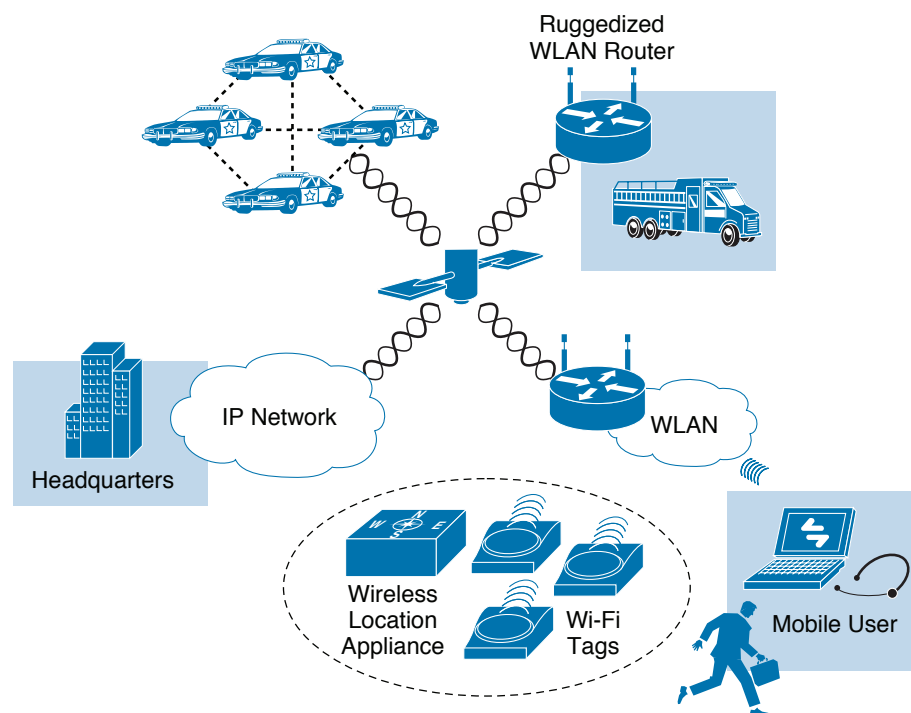


Table 5 Solutions in the Mobile Force Architecture Building Block

Vendor	Solution	Description
	Cisco Unified Wireless Network Solution	Provides secure outdoor Wi-Fi mesh capabilities with the 802.11a/b/g standard. Includes route optimization, self-healing capabilities for interference or outages, resiliency, and dynamic re-optimization when new sectors are added. Communities can easily expand the coverage area because no on-site configuration is required, a capability called zero-touch configuration.
	Cisco ESR 5900 Series Rugged Integrated Services Router	Extends the IP network from wired premises to the areas in and around first-responder vehicles. Personnel can stay connected while in motion. The modular, industrial-grade design is optimized for use in harsh environments.
	Cisco Outdoor Wireless Mesh Network Solution	Eliminates the need to wire every access point in the network, making it easier and more cost-effective to extend the reach of the network. Access points discover each other automatically and continuously communicate with each other. If a link is degraded, the access point determines whether a better path exists and then takes it.
	Cisco Wireless Location Appliance	Simultaneously tracks the location of thousands of wireless devices as well as objects or people that have RFID tags. Enables organizations to keep track of personnel and high-value assets, provides location-based alerts, and records historical location information that can be used for to discover trends.
	Cisco 3300 Series Mobility Services Engine	Enables organizations to deliver the same application across Wi-Fi, Ethernet, WiMAX, and cellular networks while preserving security and manageability. Personnel who use dual-mode phones or laptops can roam between cellular and Wi-Fi coverage areas without service interruption. The engine comes with Cisco Context-Aware Software, Cisco Mobile Intelligent Roaming, and Cisco Adaptive Wireless IPS.
	Cisco Context-Aware Mobility	Provides applications for real-time location tracking, presence detection, chokepoint visibility, and telemetry on mobile assets.

Case Study: Zurich City Police Department

Previously, Zurich City Police officers had rely relied on radio for information about suspects and cases. Access to photos and databases would require a trip to the office, taking them off the streets. Now officers in their vehicles can access federal, regional, and local databases and the Internet. Vehicles are equipped with Cisco 3200 Mobile Access Routers, which establish the best available wireless connection:

- Wireless LAN at police headquarters
- Universal Mobile Telecommunication System (UMTS) High Speed Downlink Packet Access (HSPDA)
- Global System for Mobile Communications (GSM) Enhanced Data Rates for GSM Evolution (EDGE)

The connection is maintained as the vehicle roams between different coverage areas. With access to information from their vehicles, officers are free to spend more time in the community.

Goal 6: Enhanced Communication Between Government and Citizens

Cities need to give residents defined ways to report security incidents and ask for help. For example, citizens expect to be able to communicate with authorities using newer devices such as video-capable phones or Short Message Service (SMS). Adding multimedia information to an emergency conversation can provide valuable information useful for planning a response. The other side of the story is that government needs effective ways to communicate with the public. Required capabilities to meet this goal include:

- **Distributed emergency call system:** When citizens experience or notice an emergency, such as a street accident, a fire, crime, or a medical emergency situation, they need a reliable way to report the emergency and ask for help. A call to a public safety answering point must never get lost.
- **Emergency calling devices:** Citizens should be able to report an emergency using mobile phones or from ordinary phones with VoIP accounts. Alarming points can also be installed in vehicles to send an alert in the event of an impact. The European Commission and the industry have agreed to equip all new vehicles with eCall alarm systems beginning in 2010. When an accident occurs, the module automatically calls a 112 PSAP and transmits details about the accident and the vehicle's location, using a built-in geographic positioning system (GPS) and an integrated subscriber identity module (SIM) card or a connected cell phone. The PSAP then forwards the location information to an emergency vehicle by satellite. The U.S. has a similar service called OnStar.
- **Public Alert Notification:** These systems quickly disseminate warning messages to specific individuals, communities, or organizations in response to an imminent or oncoming emergency or hazardous event. The message describes the event and the affected areas, and provides instructions. For instance, if toxic fumes are emanating from a chemical factory, the agency might need to inform neighboring citizens to seal their windows and doors and wait for further instructions. When confirmation of receipt of the message is required, the system can keep trying until receiving acknowledgement, or else repeat the message at regular intervals for the duration of the incident. Technologies include: Emergency Telephone Alert System (ETAS), Cell Broadcast (CB), voice alert (Public Address), digital signage, and mass media.

Figure 6 shows the solution, which is based on the Citizen-Authority Interaction architecture building block in the Cisco Open Platform for Safety and Security. Solutions from Cisco and examples of partners that deliver these capabilities appear in Table 6. For details, visit www.cisco.com/go/copss.

Figure 6 Communities Can Enhance Communication with Constituents Using Capabilities in the Citizen-Authority Interaction Architecture Building Block

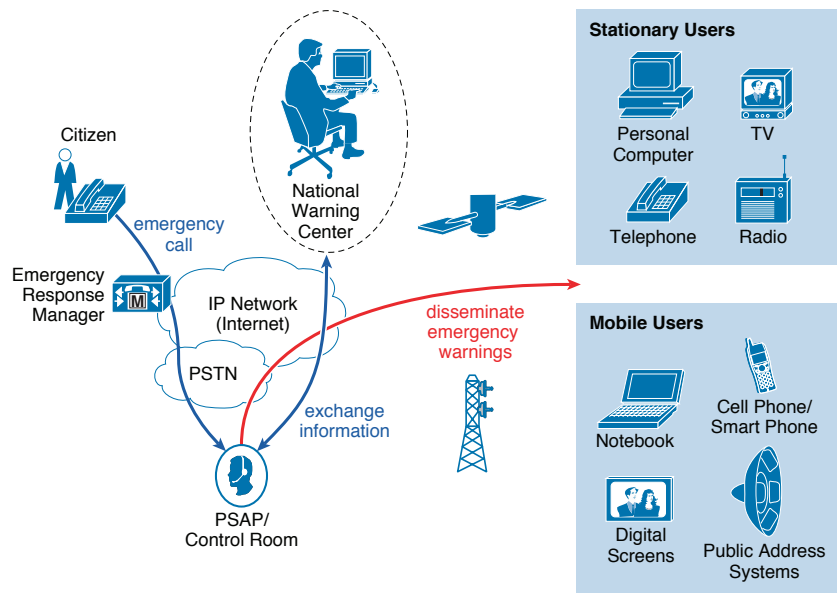








Table 6 Solutions in the Citizen-Authority Interaction Architecture Building Block

Vendor	Solution	Description
	Cisco Emergency Responder	Tracks the physical location of callers within a Cisco Unified Communications environment, even if the phone was moved. This ensures that the Public Safety Answering Point (PSAP) dispatcher can direct first responders to the right area of the building and return the call if necessary.
	Cisco Digital Media System	Enables authorities to inform people about emergencies by sending text, video, images, animation, and web content to network-connected digital signs. Authorities can centrally create, store, and schedule content.
	Integrated Communication Control System	Enables PSAPs to capture information from callers using a variety of devices and media types and forward it to responders on their way to the scene. London's Metropolitan Police Service is using ICCS to enable 23 boroughs to communicate using the national Airwave digital radio system. Boroughs can also share CCTV images, increasing situational awareness for officers.
	Emergency Communication and Collaboration Platform	Integrates with Cisco Unified Communications Manager to enable PSAPs to accept citizen communications by VoIP, video, email, or SMS messaging.

	<p>InformaCast</p>	<p>Enables organizations to simultaneously send an audio stream and text message to multiple IP phones, IP speakers, desktop notification systems, and overhead paging systems. With the push of a single button on an IP phone or a single click from a PC, public safety organizations can send a live, recorded, or scheduled broadcast to one or more paging groups.</p>
	<p>IWSAlerts</p>	<p>Transforms the IP network and connected devices into a unified emergency notification system, delivering alerts to thousands of people using PCs, mobile phones, IP phones, public address systems, all within minutes. Public safety organizations can use IWSAlerts to provide detailed instructions to affected citizens and receive feedback to help ensure a safe response.</p>

Conclusion

Public safety and security is a complex and rapidly evolving discipline, and a single vendor cannot provide all pieces of an architecture. Therefore, it is vital for the industry to develop and adopt open interfaces that enable best-of-breed solutions to work together. The Cisco Open Platform for Safety and Security provides a framework for solution providers to jointly create and implement solutions.

Organizations involved in crisis response can refer to the Urban Security domain to ensure they have the needed capabilities. It meets the following goals:

- Unified operations across multiple agencies
- Confidentiality, interoperability, and availability of information
- Effective collaboration within and across local communities
- Surveillance, monitoring, and incident control
- Increased police presence on the streets
- Enhanced communication between government and citizens

For More Information

To read more about the Cisco Open Platform for Safety and Security, including partner profiles, visit: www.cisco.com/go/copss.



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.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flip Video, Flip Video (Design), Flipshare (Design), Flip Ultra, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.