

Integrated Safety and Security Systems: Improve Response Time and Heighten Protection

What You Will Learn

Many first-responder and government organizations have deployed advanced communications systems, video surveillance cameras, sensors, building management systems, and access controls. These systems could be more effective if they worked together rather than in isolation.

The Cisco® Open Platform for Safety and Security integrates these disparate systems, enabling them to interoperate over the IP network. Benefits include:

- Compatibility among various communications devices
- Common operational picture achieved by fusing inputs from various sources on a single screen
- Automated response based on predefined policy
- Fast time to resolution through early awareness of significant events, automated notification, and automated response

This paper is intended for safety and security personnel in first-responder organizations and government and civilian agencies. It begins by summarizing the limitations of today's isolated safety and communications systems. Next it explains the benefits of the Cisco platform and its value in common situations. The paper concludes with a brief description of the solution architecture.

Challenges of Safety and Security

National, state, and local governments, educational institutions, and businesses share a need to protect people, assets, and operations. Common barriers to meeting these goals include:

- **Siloed organizations:** When different first-responder organizations convene at an incident scene, they often cannot communicate directly because their radios operate over different frequencies and use different techniques. The consequences, underscored by recent manmade and natural disasters, are uncoordinated responses and a fragmented chain of command that can hinder the ability to save lives and prevent widespread loss of property and infrastructure.
- **Incompatible systems:** Organizations build out their sensor networks over time, using equipment from multiple vendors. Devices from different vendors—and sometimes even from the same vendor—must be monitored and managed using different interfaces. Not only do unintegrated systems increase management burden, they contribute to missed events that can compromise safety and security.
- **Manual processes:** Human involvement in event detection and response can result in missed events and delayed decisions. For example, a human operator assigned to look for sparse events on a wall of video monitors can easily overlook a significant event. And when an event does occur that requires mobilizing a team, manually dialing team members—hazmat, emergency medical services, and the safety and security officer, for example—takes valuable time that can affect outcomes.

“No longer will information remain isolated or stove-piped. Commanders at all echelons will have the information they need regarding the chemical and biological hazard and the necessary information systems tools to take the appropriate protective, evasive, and restorative actions necessary.”

Major General Stephen V. Reeves

USA Joint Program Executive Officer
for Chemical and Biological Defense

March 12, 2008 before the Senate
Armed Services Subcommittee on
Emerging Threats and Capabilities

- **Distributed workforces:** In the case of widespread disasters or pandemics, incident commanders need to manage personnel who are nationally or globally distributed. During a weather-related disaster in the mid-Atlantic region of the United States, for example, command should ideally be transferred to another region. Distributed command is impractical today, however, because each site's video surveillance cameras, sensors, and building systems can only be controlled locally. The lack of centralized control is especially problematic when government buildings need to be evacuated.
- **Security concerns:** Today, organizations that collaborate during safety incidents hesitate to share information out of concern that it will be used inappropriately. Agencies need reassurance that the information they share is viewed only on a need-to-know basis, and only by authorized personnel.
- **Budget constraints:** Government organizations have invested heavily in their sensors, video cameras, and communications technology. They want to continue using the equipment they already have rather than starting over.

Cisco Open Platform for Safety and Security Capabilities

- Cisco unified communications
- Physical security, including network-based video surveillance and access control
- Communications interoperability among radios, phones, mobile phones, and softphones
- Digital media services
- Mobility
- Sensor integration and management for a common operating picture
- Geographic information system (GIS) framework
- Physical access control
- Emergency mass notification

Solution: Cisco Open Platform for Safety and Security

The Cisco Open Platform for Safety and Security is a technology platform designed to enable government agencies, educational institutions, and businesses to protect assets, employees, and citizens using a secure, intelligent unified network. By integrating standards-based technology from Cisco and its partners, the platform helps organizations minimize risk and protect citizens, employees, and assets (see sidebar).

Following are the benefits of the Cisco Open Platform for Safety and Security for government.

Reduced Capital and Operational Expense

An open platform reduces costs in the multiple ways:

- **Lower capital expense:** Organizations can continue to use elements of their existing systems, including analog and digital sensors and analog or IP video surveillance cameras. Sensors and cameras become even more valuable when connected to the IP network because they can be centrally monitored and controlled. In addition, their output can be fused and correlated with other sensors to enhance situational awareness and minimize missed events (false negatives) or erroneous events (false positives).
- **Automated monitoring and response:** Instead of assigning multiple people to visually monitor video banks or disparate systems, an organization can use video analytics software to identify events of interest and then automatically invoke policies such as notifying safety personnel or activating other sensors to gather more information. Automated incident response enables the organization to reassign personnel to functions where people add more value.
- **Lower infrastructure management costs:** The IT staff can manage one converged IP network, relieving other organizations from having to manage their own separate infrastructures for video surveillance, communications, building management systems, and physical security.
- **More efficient facility and safety and security operations:** The agency can automate time-consuming manual notification processes. If gas sensors indicate a chemical spill, for example, the emergency operations center does not need to locate someone in the facilities department to report the situation. Instead, the system invokes a predefined policy to automatically contact the appropriate person based on the nature of the incident and time of day.

- **Fewer emergency operations centers to maintain:** An IP-based platform for safety and security eliminates the real estate, personnel, and energy costs of maintaining a separate emergency operations center for each location. Instead, all safety and security systems can be monitored centrally over the resilient, scalable, and secure IP network.

Faster Speed to Decision and Response

The faster that safety and operations personnel can assess an incident, decide on a response, and act, the better they can mitigate damage. The Cisco Open Platform speeds time to decision by fusing input from multiple sensors of different types to provide a complete operational picture. For example, in a location with gas pipes, the platform can be set up to fuse inputs from pressure, heat, and infrared sensors to enable earlier and more accurate detection of incipient leaks. Another type of sensor can indicate the type of leak—poisonous or explosive—giving personnel more time to plan an effective response. Another way that the Cisco Open Platform accelerates response is by simultaneously notifying all personnel in the response team, on any communications devices—phone, pager, radio, or smartphone—instead of notifying them one by one. The policy can also include actions such as remotely locking down buildings by activating network-connected building access controls.

Using the Reliable, Scalable Network as the Platform

Using the IP network as the platform provides safety and security capabilities not available when solutions are isolated:

- **Common platform for real-time multimedia services:** Information from video surveillance systems, sensors, building management controls, and other applications is available on a common interface. Agency personnel do not need to use separate applications and user interfaces that report on only one aspect of the situation.
- **Intelligence to assign priority to different traffic based on business rules:** For example, time-sensitive traffic such as video from surveillance cameras is given priority over non-time-sensitive traffic such as email. During crises, any traffic originating from or destined to specified individuals can be given priority.
- **Access control:** The Cisco Open Platform can be layered atop the secure information-sharing architecture (SISA) that Cisco designed to support multiagency or coalition collaboration services. Role-based access control enables each organization to decide which information it wants to share, when and with whom, and to track the content that each individual views.
- **Pervasive security:** Government organizations have already invested in security technologies for their data network. The Cisco Open Platform lets them capitalize on the same investments for their communications systems, sensors, and video surveillance cameras. The network can detect signatures and patterns in network traffic to automatically detect and optionally stop suspicious activity.
- **Mobility:** Field personnel can use suitcase-sized tactical kits or mobile command vehicles to rapidly establish all safety and security capabilities over a satellite or broadband cellular network connection. Rapidly deployable communications capabilities are useful for disaster response in areas where telecommunications infrastructure has been severely degraded or destroyed or never existed. Organizations can also use permanent wireless networks to deploy wireless sensors and video surveillance cameras, avoiding the costs of trenching for wired lines.

Use Cases

Following are sample scenarios illustrating the value of the Cisco Open Platform for Safety and Security.

Mobilizing Response Teams and Base Recall

An incident occurs that requires mobilization of a tactical team. Upon detecting the condition through network-attached sensors, the notification system simultaneously alerts all team members on their preferred communications device, depending on the time of day. Notification methods include phone calls, instant messages to PCs, Short Message Service (SMS) to smartphones, and radio notification. The system tracks recipients' acknowledgements of the alert, ensuring accountability. Simultaneously, the system establishes a virtual talk group that first responders can join using any type of radio as well as phone, cell phone, IP phone, or softphone. The event is then handed off to the incident response system.

Implementing Force Protection

On a military base, the live display provides continuous confirmation that the camera is monitoring the perimeter. For additional protection, video analytics software is used to identify intruders or suspicious vehicles or objects and activate other sensors according to predefined rules. If a person crosses a video tripwire, for example, automated actions might include:

- Displaying video from the camera of concern on the Security Operations Center display.
- Storing archive clips of adjacent cameras in nearby zones so that activity before and after the incident is readily available for further investigation.
- Signaling the emergency communications systems to automatically alert all personnel of a lockdown by sending SMS messages and publishing alerts to consoles.
- Pushing video to multiple locations, including PCs, smartphones, and digital signage.
- Establishing a radio virtual talk group and notifying first responders so that they can collaborate on a security response.
- Fusing sensor information and public sources on a single screen to provide a common operating picture.

Protecting Assets During Events

An agency issues a severe tornado warning using a Common Alerting Protocol (CAP) feed. Receipt of the incoming message triggers a set of actions, such as displaying the message on the Security Operations Center common operating picture and sending the alert to safety and security staff in the affected region using voice, SMS, and email. After initial assessment, the Security Operations Center commander can activate the incident response team to meet for a voice, video, and web collaboration session that the system set up automatically. If needed, the team can use the web interface to invoke the platform's emergency communications and mass notification systems—SMS, email, phone, digital signage, and loudspeakers—to notify people to take cover.

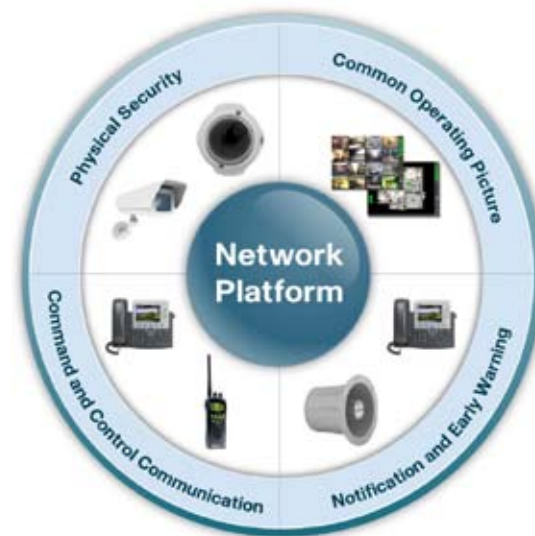
Activating Multi-Agency Response Plan Based on Pandemic Assessment

Potential pandemics are likely to be identified in animal populations before they become widespread in human populations. Agencies worldwide can use the Cisco Open Platform to collect and centralize laboratory pathogen information gathered from far-flung agricultural centers, game and wild life management offices, and other facilities. IP-enabled testing instrumentation from these facilities becomes part of a global network of automated sensors. In response to the pathogen, the platform invokes policy-based actions such as notifying specified healthcare agencies and decision makers using email, phone, and SMS. The policy might include establishing a live web collaboration session to facilitate discussion of an emerging health crisis.

Architecture

Figure 1 illustrates the Cisco Open Platform for Safety and Security Architecture. The comprehensive architectural approach helps organizations protect employees, communities, and mission-critical processes by using commercial, off-the-shelf (COTS) products that are integrated by the resilient IP network. The platform combines voice, video, data, and physical security systems to create a holistic, common operating picture. Use of COTS products reduces costs and enables agencies to integrate more capabilities from different vendors as mission needs change.

Figure 1 Open Platform Architecture



Solution components, which can be mixed and matched, include:

- Communication
 - Command and control
 - Emergency notification and early warning
 - Collaboration and virtual emergency operations
- Physical security
 - Video surveillance cameras and video analytics software
 - Sensors
 - Physical access controls
- Common operating picture
 - Geospatial displays
 - Fusion, filtering, and correlation of data feeds from sensors and cameras
 - Decision support and policy-based response

Conclusion

As safety and security threats increase, public and private sector organizations are striving to empower the workforce by delivering the right information at the point of need to protect citizens and critical assets. The Cisco Open Platform for Safety and Security addresses this requirement by integrating isolated systems to create a common operating picture. Benefits include:

- Improved employee safety and security during emergencies through early warnings and employee accountability
- Enhanced risk management by facilitating continuity of operations, crisis management, and all-hazards incident response
- Protection of facilities and critical infrastructure using network-connected physical access controls and sensors
- Reduced operational costs by using technology to make existing resources more effective
- Interoperable communications regardless of device or location
- Strengthened interagency coordination and collaboration made possible by real-time data, video, and voice on location

For more information about the Cisco Open Platform for Safety and Security, visit:

<http://www.cisco.com/web/strategy/government/national-open-platform.html>

To learn more about how Cisco Open Platform for Safety and Security can benefit your agency, visit:

www.cisco.com/web/strategy/government/coe_index.html




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, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store 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, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, 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.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0807R)