

Cisco Open Platform for Safety and Security: Incident Collaboration Architecture Building Block

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 comprises six building blocks: Command and Control, Mission-Critical Network, Incident Collaboration, Sensing and Actuation, Mobile Force, and Citizen-Authority Interaction.

This paper, intended for organizations planning investments in safety and security technologies and for solutions providers, focuses on the Incident Collaboration building block:

- The *core system* provides the infrastructure and call management capabilities
- *User terminals* receive voice, video, and data over wired or wireless connections
- *Alerting and messaging services* inform emergency services personnel that an incident has occurred and provide basic information
- *Conferencing* tools enable first responders in the same or different organizations to collaborate with voice, video, and web sharing

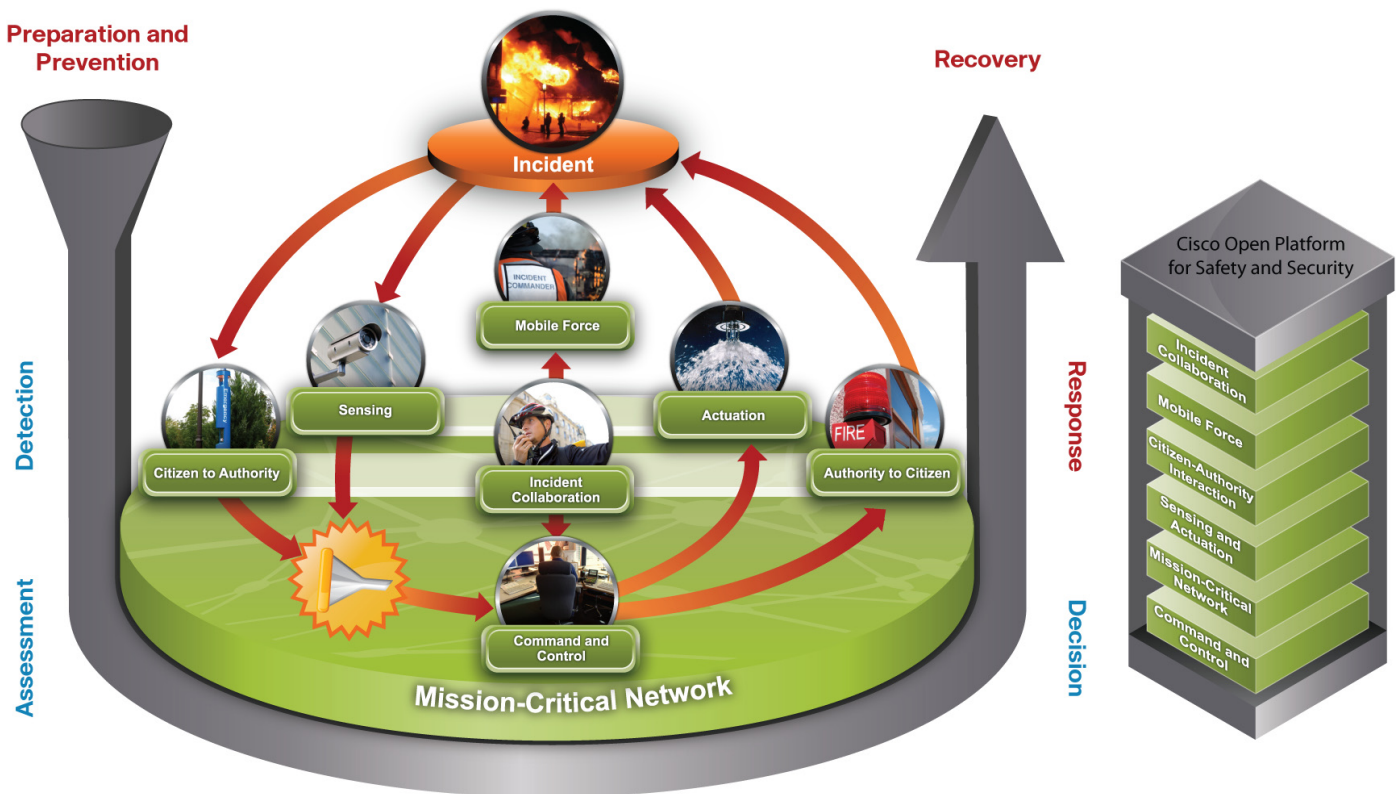
The Role of Incident Collaboration in Safety and Security

Effective incident response requires the timely exchange of accurate and up-to-date information within and between emergency service organizations. All participants need real-time communications capabilities to establish command and control at the emergency scene and maintain situational awareness. The need for incident collaboration applies during routine incidents as well as large-scale emergencies such as natural disasters or terrorist acts.

In the Cisco Open Platform for Safety and Security, the Incident Collaboration architecture building block enables communication and collaboration between first responders and with their commanders, which we call Authority-to-Authority communication. Citizen-to-Authority communication is a separate architecture building block.

Communication is integral to all aspects of emergency operations. Therefore, the Incident Collaboration building block is tightly integrated with all other building blocks in the framework (Figure 1).

Figure 1 The Incident Collaboration Building Block Integrates with All Other Building Blocks in the Framework



Note that the Incident Collaboration does not replace an organization's existing communications infrastructure and collaboration tools. Rather, it augments existing investments with new tools and enables collaboration with other organizations that use different network technologies and tools.

The remainder of this white paper describes the components of the Incident Collaboration building block: core systems, user terminal, alerting and messaging, and conferencing.

Core Systems

The core system component provides the infrastructure and call management capabilities required for Incident Collaboration:

- **Call processing:** Manages, monitor, and controls calls between two or multiple people.
- **User and device provisioning:** Automates the process to save time and eliminate human errors.
- **Communication provisioning:** Provides dial plans, call control, bandwidth allocation, and APIs for service creation.

- **Monitoring:** Allows the organization to quickly detect problems with communications systems.
- **Interoperability service:** Enables communications interoperability between different organizations' disparate push-to-talk (PTT) radio systems, traditional phones, mobile phones, IP phones, and PCs.
- **Security services:** Protects the infrastructure, applications, and access, and provides a unified management interface for all security features.
- **Presence services:** Indicates whether colleagues are currently available and how they prefer to be reached.
- **Interoperability gateways:** Provides interworking between different networks or media, including public switched telephone network (PSTN), Global System for Mobile Communication (GSM) terrestrial trunked radio (TETRA), Project 25 (P25), and others.

“From [Hurricane] Katrina, we learned that we cannot rely on any specific infrastructure: PSTN, radio tower, or other. We need the option of reconstituting communications from a disaster recovery site.”

—Kevin Ross
New York State Emergency
Management Office

Technology Highlight: Cisco IP Interoperability and Collaboration System

Cisco IP Interoperability and Collaboration System (IPICS) is an easy-to-use, scalable, comprehensive solution for communications interoperability. It sends radio traffic over IP networks, which allows people to join radio talk groups using any kind of radio handset as well as telephones, mobile phones, and laptop and PC clients. Cisco IPICS can facilitate coordinated, incident management response for emergencies and day-to-day operations across multiple agencies, jurisdictions, or departments. Commanders outside of radio range can join virtual talk groups using telephones or laptop clients. Cisco IPICS costs just a fraction of replacing the entire radio system. It allows organizations to upgrade to new P25 radio systems gradually, as the budget permits, rather than all at once, providing interoperability between the old and new systems for as long as needed.

Case Study: Georgia Forestry Commission

Georgia Forestry Commission (GFC) has been tasked to be a logistical stronghold for the state's emergency plan. When GFC collaborates with other agencies in incident response, dispatchers can quickly set up a virtual talk group that personnel can join using their various radio systems or laptops with Cisco Push-to-Talk Mobile Client software. When the talk group is activated, broadcasts from each of GFC's two radio systems are automatically relayed across both networks, enabling two-way communication. This arrangement avoids the need to manually set up two radios side-by-side or have a dispatcher verbally relay what each party is saying. Virtual talk groups take only a minute or two to create on Cisco IPICS, and they avoid the overloading that can occur on mutual aid channels.

Case Study: Boulder County, Colorado

In Boulder County, Colorado, Special Weapons and Tactics (SWAT) teams use Cisco IPICS to facilitate negotiations with suspects. They can patch the suspect's PSTN phone or cell phone into an operational or tactical radio channel, and the negotiator can communicate using either a radio or cell phone.

User Terminal

User terminals are the devices that emergency services personnel use to communicate and collaborate. Fixed user terminals, like PCs and IP phones, have a physical connection to the network. Wireless user terminals, like smartphones and wireless laptops, can connect over a variety of popular wireless standards, including WiFi, GSM, TETRA, P25, and WiMax.

Important user terminal features for incident collaboration include high reliability and support for voice, video, web access, and presence services. In addition, the interface must be easy to use for first responders in chaotic environments.

Technology Highlight: Cisco Unified Presence

Cisco Unified Presence enables first responders and commanders to collaborate using instant messaging and presence. The presence engine collects user presence information (available, busy, on the phone, idle, or away) and device capabilities (voice, video, instant messaging, and web collaboration). A first responder can see which people at headquarters are currently available and just click to send an instant message, for example.

Case Study: San Diego Country Sheriff's Department

When a series of severe wildfires swept across Southern California on October 20, 2007, multiple local, state, and national agencies coordinated their response. Ordinarily, San Diego County Sheriff's Department deputies can communicate with other county agencies on a shared frequency, but cannot communicate with state and national first responders, which use incompatible radio systems. During this fire, the Sheriff's department took advantage of Cisco's traveling Network Emergency Response Vehicle (NERV) to collaborate with federal agencies. Using the Cisco IP Interoperability and Collaboration System (IPICS) in NERV, the Sheriff's Department was able to establish direct radio communications with a U.S. Customs and Border Protection helicopter, whose pilot was looking for flare-ups. The pilot had a much better perspective than spotters on the ground. By communicating directly with the pilot, the department was able to call for fire resources to protect a threatened residence even before the fire department was aware of the danger.

Alerting and Messaging

Alerting refers to an attention-getting signal, such as a page or audible alarm. Often, first responders are expected to respond to an alert so that command can confirm that the response will be adequate. Messaging refers to asynchronous communication, such as Short Message Service (SMS) or instant messaging. Asynchronous communications can be sent to one person or a group of people.

The Alerting and Messaging component provides the following technologies:

- Pager systems
- SMS
- Instant messaging
- Email

Technology Highlight: Berbee Software

Berbee InformaCast allows emergency organizations to simultaneously send an audio stream and text message to multiple IP phones, IP speakers, desktops, and overhead paging systems. You just push a button on the IP phone or click with the PC mouse to send a live, recorded, or scheduled broadcast to one or more paging groups.

Conferencing

Conferencing tools allow emergency responders to collaborate from any location and establish an effective response plan. The Conferencing component of the Incident Collaboration building block includes the following components:

- Audio
- Video
- Data
- Web, including slide presentations, application sharing, co-browsing, annotation, and file sharing
- Cisco TelePresence

Technology Highlight: Cisco WebEx

Cisco WebEx Virtual Emergency Operation Center connects first responders and headquarters personnel into rich media conferences. Participants can:

- Exchange documents and files
- Collaborate using any public safety application
- Share desktops and remotely control another participant's desktop
- Feed video from one or more points
- Record the interaction for later analysis and reporting

Case Study: Broward County School District

Broward County School District uses Cisco Unified MeetingPlace to coordinate command, control, and recovery efforts after hurricanes and other disasters. During the 2004 hurricane season, the school district made the Cisco Unified MeetingPlace system available to the National Guard and Florida State Emergency Operations Center, which used the system to coordinate with 65 counties after the storms. National Guard personnel saved time by remaining in the field and presenting their findings in voice and web conferences. The ability to collaborate and have direct discussions enabled the county to resume normal citizen services seven to ten days earlier than usual for this type of disaster. The voice and web collaboration sessions helped to ensure that everyone had consistent information on which roads and electrical towers were still out of service, and where water, food, ice, and other supplies were needed.

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. The Incident Collaboration building block provides:

- Basic and advanced call management services that enable collaboration within and between emergency organizations
- Wired and wireless user terminals with the capability to exchange voice, video, and data
- Alerting and messaging services for asynchronous communications
- Interactive conferencing services to prepare for and plan a response to emergencies

For More Information

To read more about the Cisco Open Platform for Safety and Security, including partner profiles, visit:
www.cisco.com/web/strategy/government/national-open-platform.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 HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, 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, 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. (0812R)