



Cisco Open Platform for Safety and Security: Understand the Crisis Management Domain

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 Prison and Probation.

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

- Unification of operations
- Resilient and ubiquitous infrastructure
- Interoperable collaboration
- Environmental monitoring and control
- Effective deployed units
- Enhanced communication with the victims

The Challenges of Crisis Management

The practice of crisis management involves taking steps to avoid technology failure and establishing formal communications processes to avoid or manage crisis situations. While crises vary widely, the challenges are common. Following are those challenges, illustrated by the Mont Blanc tunnel disaster of 1999:

- **Rapid decision-making:** Crisis management teams often have no time for preparation or discussion. Of the 41 individuals who died in the tunnel disaster, most perished within 15 minutes of ignition. The response team had to very quickly make choices such as properly activating the ventilation system and effectively deploying emergency personnel.
- **Accurate and timely identification of threats:** Initially, the fire escaped detection because of the tunnel's location deep underground and the absence of properly operating sensors. Early warning and assessment are essential to implementing an effective response. Deploying more resources than needed increases costs, while deploying too few resources can result in loss of life and property.

- **Rapid dissemination of critical information:** During the Mont Blanc disaster, the control centers on each side of the tunnel, their own responders, and emergency personnel from France and Italy needed precise information to save lives and the tunnel itself. During any crisis, most requests for information require immediate response.
- **Re-establishing a feeling of control:** People affected by a crisis often feel that they have lost control, causing them to panic and make less-effective decisions. Neither the French nor Italian command center had the information, preparation, or network infrastructure to respond effectively to the fire. People in the tunnel lacked the means to communicate with people outside because the emergency lines were unavailable.
- **Restoration of normal activities:** The Mont Blanc had to be completely shut down during and after the fire, disrupting the commute for thousands of commuters. Crisis response teams need to minimize disruption in routine activities when responding to crises as diverse as terrorist attacks, industrial chemical accidents, and cyberthreat.
- **Communications management:** Throughout a crisis, responders need to be able to convey the right information to the right people, at the right time. During the Mont Blanc crisis, a disabled network infrastructure inside the tunnel prevented different participants from interacting. These included the two command centers, rescue personnel, outside agencies, and people trapped in the tunnel.

Vision for Crisis Management

Although every crisis situation is unique, the responses share common elements. First, every organization needs an infrastructure to collect, analyze, and disseminate real-time data before, during, and after the crisis. Second, they need a plan for training and human resource management. Finally, they need interoperable communications with all participants, in the same or other agencies. The vision for the Cisco Open Platform for Safety and Security is to enable organizations to develop a customized crisis plan that combines all of these elements to mitigate harm from unexpected events.

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

Goal 1: Unification of Operations

Traditionally, public safety agencies such as police, fire brigades, and emergency medical services maintained their own control rooms, which were not connected to the others. Effective crisis management requires fusing information from multiple sources to create actionable intelligence. Achieving this goal requires the following capabilities:

- **Unified situation awareness and control:** Operations centers must be interconnected, not isolated islands of disjointed information. The main priority of the operations center is to assess the situation at the disaster scene and create a Common Operational Picture that increases situational awareness for emergency personnel.
- **Process planning:** The emergency plan should include an accurate risk assessment, implementation of a safety and security policy, continuous reassessment of the plan, a procedure to regularly check equipment, and force training.
- **Role-based view:** When an abnormal situation is detected, operators should automatically be presented with information that is appropriate for their role and relevant to their location. During the Mont Blanc tunnel disaster, the role-based view might have included the type of event, number and types of vehicles inside the tunnel, availability of access passages, and controls for traffic control and ventilation systems.
- **Training:** Careful planning can mitigate the effects of confusion during crises. Regular full-scale exercises help to ensure that all teams know what to do.
- **Automation:** Automation increases the speed of emergency response. Examples of actions that can be automated include activating sprinklers in the event of a fire, notifying public safety organizations, redirecting traffic, activating ventilation systems, and displaying instructions on networked highway signs.

These capabilities are addressed by the **Command and Control** architecture building block in the Cisco Open Platform for Safety and Security.

Download a detailed white paper about the **Command and Control** architecture building block on: www.cisco.com/go/copss.

Goal 2: Resilient and Ubiquitous Infrastructure

First responders and rescue teams on the front line depend on the network to share information needed for an effective response. Required capabilities to meet this goal include:

- **Data recording:** Effective crisis recovery and post-event analysis require a review of event communications, video, sensor information, and more. Therefore, all relevant information must be captured and stored.
- **Redundancy:** A redundant and resilient network infrastructure is required to connect the disaster scene to the operations center.
- **Survivability:** If all existing infrastructure is down, emergency organizations need the ability to establish an ad hoc meshed network using all available nodes, which might include emergency vehicles or even the firefighters' personal equipment.
- **Mobility:** Personnel must be able to communicate even while on foot or in a moving vehicle.
- **Communications interoperability:** Personnel must be able to communicate using any device, including any type of radio as well as telephone, mobile phone, or PC.
- **Any network:** Emergency responders should be able to connect using the best available connection at the time, including WiFi, MPLS, satellite, and terrestrial trunked radio (TETRA).
- **Electric power:** A power outage can result in the loss of all systems on the emergency scene. Therefore, effective crisis management requires redundant circuits and networks and protection of electrical cables.
- **Emergency-grade network management:** During a crisis, operators might need to work from a different location, which means they should be able monitor and configure all network elements and services across local area networks, wide area networks and metropolitan area networks.

These capabilities are addressed by the **Mission-Critical Network** architecture building block in the Cisco Open Platform for Safety and Security.

Download a detailed white paper about the **Mission-Critical Network** architecture building block on: www.cisco.com/go/copss.

Goal 3: Seamless and Interoperable Collaboration

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. Required capabilities to meet this goal include:

- **Multimodal communications:** Responders need access to a variety of communications tools rather than having to rely exclusively on radio communications. Examples include voice, video, instant messaging, and Short Message Service (SMS).
- **The ability to establish spontaneous (rather than prescheduled) communications:** Emergency responders should be able to create ad hoc communications groups that link all people within a certain geographical area, regardless of their communication device or organization.
- **Communications interoperability:** The system should be able to connect different digital and analogue radios, and also allow people to join radio talk groups using traditional phones, IP phones, and laptops.

These capabilities are addressed by the **Incident Collaboration** architecture building block in the Cisco Open Platform for Safety and Security.

Download a detailed white paper about the **Incident Collaboration** architecture building block on: www.cisco.com/go/copss.

Case Study: San Diego County 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.

Goal 4: Environmental Monitoring and Control

To respond effectively, emergency personnel need to collect comprehensive information about people, objects, and the environment. Then also need the ability to respond to that information with actuators, which are mechanisms that act on devices—for example, to turn them on or off, adjust them, or move them. Required capabilities to achieve this goal include:

- **Risk-level monitoring:** Risk level should be continuously monitored and updated. As an example, trucks carrying inflammable material should carry RFID tags that are scanned when the truck enters and exits a tunnel, so that first responders know that these trucks are present.
- **Centralized control:** A centralized surveillance system should continuously monitor the tunnel environment and send an alert to the operations center if any abnormality is detected. During another tunnel disaster, for example, such a system would immediately identify faulty or disconnected sensors and actuators, including CCTV cameras, fire detection equipment, and mobile sensors on people and vehicles.
- **Resiliency:** The emergency sensing, acting, alerting, and communications systems must be redundant and designed to withstand extreme environmental conditions such as fire, dust, and humidity.
- **Sensors and actuators:** Sensors help to create a COP, and actuators take automatic action based on sensor input. For example, fire and smoke detection sensors automatically trigger the water sprinkler and activate barriers that keep additional vehicles from entering the tunnel.
- **Video anywhere:** All authorized personnel need the ability to directly access video cameras at the emergency scene, over the network. Real-time video enables more effective incident response and investigation.
- **Physical barriers:** The emergency operations center should be able to physically block the traffic approaching the crisis scene, such as a tunnel, with remotely controllable barriers. Road signs alone are not sufficient.
- **Reassessment:** Organizations involved in crisis response should periodically reassess technology. For example, a new generation of ventilation systems increases sanitary ventilation in standard conditions and can ensure the survival of people awaiting evacuation.
- **Ventilation:** New ventilation systems have continuous speed variators that can be remotely controlled from the operations center. These greatly enhance safety within tunnels and other enclosed areas.
- **Inside temperature:** Use a temperature sensor network to monitor temperature changes throughout the entire tunnel and in shelters and garages.
- **Firefighting system:** Operations center personnel can use actuator networks to control water valves and sprinklers.

These capabilities are addressed by the **Sensing and Actuation** architecture building block in the Cisco Open Platform for Safety and Security.

Download a detailed white paper about the **Sensing and Actuation** architecture building block on: www.cisco.com/go/copss.

Goal 5: Effectiveness of Deployed Units

To protect lives and property, emergency responders in the field need access to critical information and services from any place, any time, and in the right format. During hurricane Katrina, for example, organizations involved in rescue and recovery efforts needed to establish remote worksites at the edge of the heavily flooded Gulf Coast. The objective is to empower deployed forces to be as effective in the field as they would be in the office. Required capabilities to meet this goal include:

- **Mobile information:** Rescue teams need an intuitive interface that they can use on the way to a disaster scene to obtain the most up-to-date information about the incident, even if it is incomplete.
- **Personal sensors:** Personal area sensors affixed to first responders' clothing or bodies measure heartbeat, air composition, temperature, and more. The operations center can use this information to monitor the environment and protect personnel.
- **Localized information:** Emergency responders don't need all information about the unfolding crisis, but rather the subset of information that's relevant to their role and location. Stress seriously limits the amount of information a human is able to process.

These capabilities are addressed by the **Mobile Force** architecture building block in the Cisco Open Platform for Safety and Security.

Download a detailed white paper about the **Mobile Force** architecture building block on: www.cisco.com/go/copss.

Case Study: City of Austin, Texas

The City of Austin integrated a rapidly deployable communications system into its mobile command vehicle, ensuring that first responders have network access even in the event of a power outage or a massive disruption to the public communications infrastructure. The equipment in the vehicle automatically connects using whatever method is available: wired, wireless mesh, or satellite. Once connected, the system provides wired and wireless connectivity in and around the vehicle so that public safety personnel can use laptops, handhelds, and other devices to access maps, database information, streaming video, and more. The system also enables the city to support the more than a dozen different radio systems used by its various agencies, including push-to-talk radios and regular phones, as well as to communicate with the emergency medical service dispatch team within the city's Combined Transportation Emergency and Communications Center. Having all the different types of radio and other voice technologies available in one system enables incident commanders to make informed decisions and relay those decisions to the field as quickly as possible.

Goal 6: Enhanced Communication to and from the Victims

Authorities and citizens need to be able to communicate during an emergency. For example, citizens should be able to report information to authorities using phones, videophones, SMS, and Multimedia Message Service (MMS). And authorities need ways to alert and instruct targeted groups of citizens using automated phone calls, broadcasts to all mobile phones in a geographic area, digital signage, and other methods. Required capabilities to meet this goal include:

- **Location-specific signage:** The emergency operations center should distribute timely, accurate, and location-specific messages about the incident to the motorists, personnel, and first responders. For example, electronic signs at the tunnel entrance of the tunnel should immediately (and automatically) indicate: "Fire in the Tunnel—Do Not Enter."

- **Emergency calls:** Citizens should be able to communicate with the emergency operations center through a variety of means, such as an alert switch, voice call, video call, instant message, SMS, and intercom.
- **Multimodal signage and communication:** People might not be able to see electronic signs in certain emergency conditions. Loudspeakers might also be required to disseminate instructions such as “Get out of your vehicle and seek shelter.”
- **Emergency calling devices:** Infrastructure should be equipped with devices that people can use to communicate. Examples include intercoms in ventilation conduits and audio-video links in shelters.

These capabilities are addressed by the **Citizen-Authority Interaction** architecture building block in the Cisco Open Platform for Safety and Security.

Download a detailed white paper about the **Citizen-Authority Interaction** architecture building block on: www.cisco.com/go/copss.

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 Crisis Management domain to ensure they have the needed capabilities. Goals include:

- Unified operations
- Resilient and ubiquitous infrastructure
- Interoperable collaboration
- Environmental monitoring and control
- Effective deployed units
- Enhanced communication with the victims

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.

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. (0907R)