



Open Platform for  
Safety and Security:  
Reduce Investment  
Risk and Increase  
Rewards for Innovation

## Contents

What You Will Learn	2
Challenge: Safety and Security Technologies Evolve Constantly	2
Cisco Open Platform for Safety and Security	3
Types of Safety and Security Incidents the Framework Addresses	3
Solution Building Blocks	4
Benefits for Emergency Organizations and Solutions Providers	5
How the Ecosystem Partners Developed the Framework	6
Conclusion	7
For More Information	7

### What You Will Learn

The Cisco Open Platform for Safety and Security is an architecture framework for designing and selecting solutions to prevent, prepare for, respond to, and recover from incidents. The framework defines the functionalities required for a range of safety and security domains, including crisis management, urban security, border control, critical infrastructure protection, asset protection, mass venues and events, transportation, and prisons and probation.

This white paper is intended for people who invest in safety and security technology as well as vendors planning their solutions development strategy. It explains the rationale for the Cisco Open Platform for Safety and Security:

- Reducing risk by ensuring that investments align with long-term vision and goals
- Providing a common reference for solution providers and the organizations that are evaluating solutions
- Encouraging innovation by increasing the returns from development efforts

### Challenge: Safety and Security Technologies Evolve Constantly

Emergency organizations need to meet increasingly stringent operational requirements with constantly changing technology. The environment is highly complex:

- Multiple organizations using different communications technologies need to collaborate (Figure 1).
- Each country, region, or city has specific requirements and particular ways to address them.
- Vendors continually introduce new technologies that can enhance the effectiveness of public safety organizations, such as artificial intelligence, video analytics, IPv6, mobility, sensors, and biometrics.
- Public safety organizations want to extend the life of existing investments, such as analog video surveillance cameras and sensors, while also deploying new technology that can help to save lives and property.

**Figure 1 Public Safety and Security Is a Complex Discipline with Many Stakeholders**



### Cisco Open Platform for Safety and Security

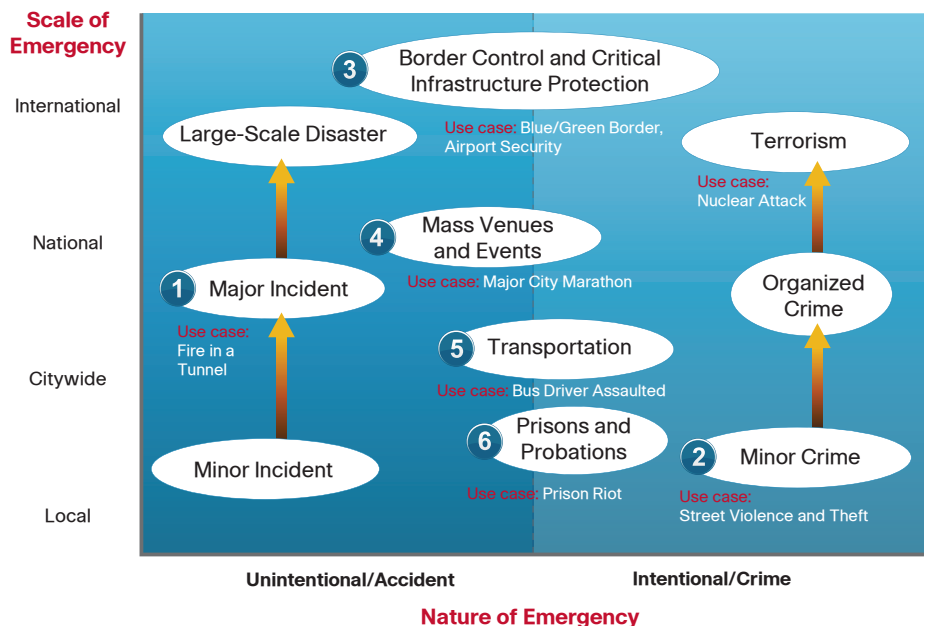
Cisco and its ecosystem partners developed the Cisco Open Platform for Safety and Security to help emergency organizations and solutions vendors optimize their investments in this complex environment. The partners collaborated with customers and industry consortia to develop the following principles for the framework:

- Openness and adherence to standards
- Usability for emergency personnel
- Secure and confidential operations
- Service-oriented building blocks that customers and systems integrators can combine to take advantage of previous development efforts
- IP as the platform
- Scalability
- Virtualized services, enabling a distributed environment
- Generalized mobility
- Technology convergence
- Interoperability
- Integration with existing solutions
- Commercial off-the-shelf (COTS) components
- Low cost of operations
- Compliance with national and international regulations

### Types of Safety and Security Incidents the Framework Addresses

Cisco Open Platform for Safety and Security defines the functional requirements for different types of safety and security incidents, called domains. The partners identified six categories of incidents, based on their scale and nature (unintentional or intentional), as shown in Figure 2. Table 1 lists examples of incidents in each category.

**Figure 2 Safety and Security Events Can Be Categorized Based on Scale and Nature**

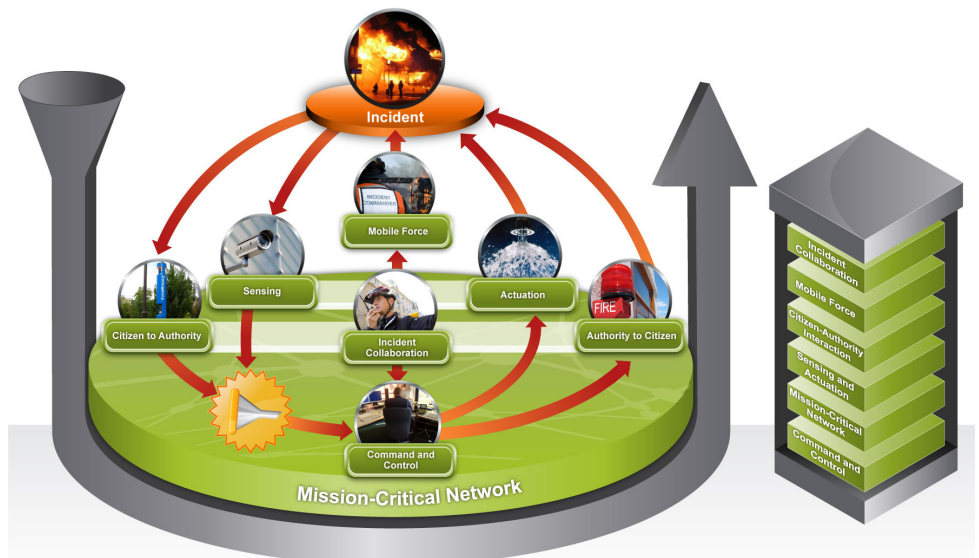


### Solution Building Blocks

The Cisco Open Platform for Safety and Security is built upon six high-level architecture building blocks. Emergency organizations and systems integrators can combine the building blocks to fulfill the functional requirements of each safety and security domain shown in Table 1. The framework defines the building blocks in terms of their function instead of specifying a particular product. This gives emergency organizations the flexibility to select different solutions based on their country and individual requirements. It also makes it easier to identify any missing capabilities in a specific solution.

Each of the six building blocks defines a set of functionalities and components (Figure 3):

**Figure 3 Safety and Security Architecture Building Blocks**



- Command and Control:** This provides the emergency management team with up-to-date situational awareness, actionable intelligence, and decision support tools.
- Mission-Critical Network:** Public safety and security organizations typically use multiple networks, including Terrestrial Trunk Radio, WiMax, WiFi, 3G, and satellite communications technologies. Consolidating these networks into a unified Mission-Critical Network platform optimizes emergency operations. The Mission-Critical Network must be scalable, resilient, secure, and intelligent.
- Incident Collaboration:** The effectiveness of communications between first responders and the command and control center can have life-or-death consequences. The Incident Collaboration building block helps to ensure that teams can communicate using any available technology, including IP and analog or digital radio, as well as any media, including voice, video, instant message (IM) or short message service (SMS), and data.

- **Sensing and Actuation:** This building block streams information from sensors at the incident scene to the operations center. It also provides the means for swift and automated remote action in response to sensor input. For example, if a sensor detects a fire in a tunnel, it can automatically activate lighting actuators to indicate the safest exit.
- **Mobile Force:** First responders perform most effectively when they have access to voice, video, and data in the field. The Mobile Force building block delivers services to the field over wireless networks. It enables police officers in their vehicles to securely access central databases. And fire commanders can monitor conditions at the scene through the biosensors on firefighters' suits.
- **Citizen-Authority Interaction:** The Citizen-Authority Interaction building block provides two-way communications capabilities. Citizens can use a single phone number (such as 112, 911, or 999) or website to request emergency support. Conversely, authorities can alert a specific group of individuals about immediate danger, such as a fire, bomb, or biological attack. This capability is sometimes called Reverse 911.

### Benefits for Emergency Organizations and Solutions Providers

Major benefits of the Cisco Open Platform for Safety and Security include:

- **Reducing investment risk by ensuring that investments align with long-term vision and goals:** Operational requirements and solutions change over time, making it difficult for emergency organizations to decide where to invest limited funds. The Cisco Open Platform for Safety and Security enables emergency organizations to link their business goals to functional building blocks, ensuring that investments will provide long-term value.
- **Providing a common reference for solution providers to describe their offerings:** A common reference helps public safety organizations accurately compare different vendors' products.
- **Encouraging innovation:** Systems integrators can cost-effectively build customized solutions from building blocks that are offered as services. Solutions providers that develop a building block can include it in multiple solutions, which speeds time to market and significantly increases the return on investment from the development effort.

### How the Ecosystem Partners Developed the Framework

Cisco and its partners followed a three-step process to develop the architecture for each of the six domains:

- **Step 1: Identify one or more real-life use cases for each domain.**

**Table 1 Examples of Incidents in Each of the Six Safety and Security Domains**

Safety and Security Domain	Examples
Crisis Management	Tunnel disaster
Urban Security	Street violence Theft
Border Control and Critical Infrastructure Protection	Illegal immigration Nuclear plant surveillance and protection
Mass Venues and Events	Crowd violence at sporting events
Transportation	Assault of bus drivers
Prison and Probation	Prison riots

Examples include the Mont Blanc Tunnel Disaster of 1999 for Crisis Management, and illegal immigration across the Mediterranean Sea serves for Border Control. For each use case, the team analyzed:

- Challenges: What are the pain points?
- Vision: What transformation will address these challenges?
- Goals: What specific goals support the vision?

- **Step 2: Map each goal to the required capabilities.** If the goal is unified operations, for example, the capabilities required to support might be:
  - Command and Control Center virtualization
  - Unified situational awareness and control
  - Consolidated reporting
  - Emergency preparedness

The team tried to define capabilities that support multiple goals. For example, a capability for Command and Control Center virtualization can be used for Crisis Management as well as other domains.

- **Step 3: Map each capability to one or more functional building blocks of the architecture framework.**

No single company can provide all pieces of the puzzles. Therefore, nearly all solutions combine components from Cisco and its ecosystem partners.

## Conclusion

Public safety and security is a complex and rapidly changing 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. Emergency organizations benefit from a well-defined roadmap, a standard for comparing vendor offerings, and the flexibility to integrate solutions from multiple vendors. Solution providers, in turn, benefit from well-understood requirements and the opportunity to reuse their building blocks in multiple solutions, increasing return on investment.

## For More Information

To read more about the Cisco Open Platform for Safety and Security, including partner profiles, visit: <http://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](http://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.