



Cisco Open Platform for Safety and Security: Understand the Sensing and Actuation 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 white paper, intended for organizations planning investments in security technology as well as solutions providers, focuses on the Sensing and Actuation building block:

- *Sensors* provide real-time information about people, objects, and environmental conditions.
- *Actuators* control network-connected devices such as fire sprinklers and building ventilation systems.
- *Analytics* software detects incidents by analyzing video and audio streams in real-time.
- *Sensor fusion and correlation* creates actionable intelligence by considering inputs from multiple types of sensors to minimize false positives and negatives.
- *Legacy integration* enables emergency organizations to increase the value of existing sensors and actuators by connecting them to the IP network.
- *A Common Operational Picture (COP)* provides a user-oriented, role-based view of the emergency situation by integrating information from multiple sources.

The Role of Sensing and Actuation in Safety and Security

Effective response to large-scale disasters requires that all participants can rapidly assess all available information. They also need the ability to take action without having to rely on deployed human forces.

To achieve these goals, emergency organizations use different types of sensors to collect information about people, objects, and the environment. Then they can respond automatically 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. You can use actuators to remotely lock doors, activate a building ventilation system, or sound an alarm, for example.

Effective sensing and actuation fulfills the following requirements:

- Consolidating information from different types of sensors and converting it to standard formats that different emergency organizations can interpret
- Analyzing and fusing information from multiple sources to create actionable intelligence, with a very low percentage of false positives or false negatives
- Automatically invoking actuators in response to sensor input. For example, you might define a policy to automatically activate the ventilation system when a sensor detects chemical levels exceeding a defined threshold.

By connecting sensors and actuators to the IP network, emergency organizations can accelerate detection, improve situational awareness, create a Common Operational Picture (COP), and accelerate response to events to improve outcomes.

The Sensing and Actuation building block provides these capabilities through the following components:

- Quantitative sensors
- Qualitative sensors
- Human identification (biometrics)
- Object identification
- Actuators
- Real-time analytics
- Sensor fusion, correlation, and baselining
- Legacy integration
- Common Operational Picture

The remainder of this white paper briefly describes the functions of each component. Emergency organizations and systems integrators can obtain individual building blocks from a technology provider that adheres to the Cisco Open Platform for Safety and Security architecture framework. For more information on how to integrate these components into customized solutions, please contact your local Cisco representative.

Quantitative Sensors

Quantitative sensors measure the physical and chemical properties of a system or its environment. Out-of-norm readings require investigation or action. The Cisco Open Platform for Safety and Security supports a wide variety of quantitative sensors, including:

- Proximity
- Temperature
- Light

- Pressure
- Humidity
- Flow
- Seismic/Acceleration
- Chemical, biological, radiological, nuclear, and explosive (CBRNE)



Technology Highlight: Arch Rock

Arch Rock, a pioneer in IP-based wireless sensor network technology, provides a complete solution to enable emergency organizations to rapidly develop and deploy wireless sensor networks—often in just one hour. Intelligent sensing points can be deployed anywhere, including on mobile items or hard-to-reach locations, without the constraints and costs of wiring. Arch Rock leverages IETF RFC4944, the standard for IPv6 communication over low-power IEEE 802.15.4 wireless radio.

Qualitative Sensors

While quantitative sensors report numerical data, qualitative sensors report the presence or absence of objects, activities, and patterns, using real-time analytics to produce actionable intelligence. The Cisco Open Platform for Safety and Security supports the following types of qualitative sensors:

- Video
- Audio
- Radar
- Sound Navigation and Ranging (SONAR)
- Terahertz imagery, which can be used to detect the presence of concealed weapons.

Technology Highlight: Cisco High-Definition Video Surveillance Cameras

Cisco Video Surveillance IP Cameras 4000 Series are true high-definition (HD) cameras designed to deliver outstanding image quality in a wide variety of conditions. They offer:

- True HD video and H.264 compression
- Progressive scan streaming up to 30 frames per second at 1080p (1920 x 1080) resolution
- Resolution of up to 60 frames per second at 720p (1280 x 720)
- Optional digital signal processor for edge-based analytics
- Dual streams
- Day and night operation
- Motion detection and event notification
- Embedded security with hardware encryption
- Flexible power options including Power over Ethernet (POE)



Human Identification (Biometrics)

Biometrics sensors can recognize individuals based on intrinsic physical or behavioral traits that have been previously collected. Today, biometrics sensors are used primarily to control access to buildings, secured areas, and networks. It is also possible to use biometrics to identify persons of interest in criminal activities. Table 1 shows examples of physiological and behavioral biometrics sensors.

Table 1 Use Biometrics Sensors to Recognize People

Physiological	Behavioral
Fingerprint Palm print Hand geometry Hand veins Facial recognition Facial thermograph Iris Retinal scans Ear canal Odor DNA	Signature Voice recognition Gait Keystroke entry, including speed and pressure

Technology Highlight: Cognitec

[Cognitec Systems](#) provides face recognition solutions that are used to prevent identity fraud, secure borders, and support physical access control. The solutions provide best-in-class biometric recognition accuracy, response times, scalability, and reliability. An open system architecture simplifies integration with other systems.



Object Identification

Emergency organizations need the ability to identify objects and their locations, as well as the contents of containers. For example, first responders at a disaster scene can use object identification technologies to determine the location of supplies and communications equipment. Object identification usually involves collecting information from multiple sensors and then analyzing it, either manually or with analytics software.

Functional components of object identification include:

- **RFID:** RFID tags can be affixed to objects such as a supply kit or communications device. Active RFID tags (transponders) contain a battery or other power source that periodically emits a signal that can be picked up by a wireless network. This lets you identify the object's location. To read a passive tag, which does not contain a power source, you simply aim a reader at it.
- **Bar codes:** Also affixed to the object, bar codes represent data about the object as variable-width lines, or as patterns of squares, dots, hexagons, and other geometric patterns.
- **Optical Character Recognition:** This involves using a handheld scanner to capture handwritten or printed text and convert it to electronic text stored in a file.



Technology Highlight: AeroScout

[AeroScout](#) products use standard WiFi wireless networks to accurately locate and track 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.

Actuators

An actuator is a mechanism that can turn a device on or off, adjust it, or move it. Use network-connected actuators to remotely lock and unlock doors, turn on fire sprinklers, activate video surveillance cameras, capture a chemical sample, and more. Actuators can be manually invoked through a computer interface. They can also be automatically invoked in response to sensor input, based on organizational policy. An example of a policy is to begin streaming video if a motion sensor is activated.

Following are the functional building blocks for actuation:

- **Physical access controls:** Activate barriers and magnetic door locks.
- **Fire sprinkler:** Typically, temperature sensors automatically invoke fire sprinklers.
- **Heating, ventilation, and air conditioning (HVAC):** Control the temperature, noxious gas level, and humidity within a building. For example, a ventilation actuator lets you vent a closed area in response to the release of chemical agents.
- **Lighting:** Centrally control all lights in a building—for example, by turning them on if an intruder is detected.



Technology Highlight: Cisco Physical Access Control

The [Cisco Physical Access Control](#) solution lets you control from one to several thousand doors. Lock and unlock doors according to a predefined schedule, when someone swipes an access card, or using a web interface. Integrate Cisco Physical Access Control with Cisco Video Surveillance Manager to view live or recorded video of people entering or leaving secured areas.

Real-Time Analytics

Analytics software processes inputs from sensors (video, radar, terahertz imaging, and so on) to detect events of interest. These events can include intruders, someone tailgating into a building after an authorized person swipes an access card, or suspicious objects. Sophisticated analytics software can also recognize faces and voices, identify suspicious behavior, perform license plate recognition, and recognize the signage on vehicles carrying dangerous goods.



Technology Highlight: ObjectVideo

[ObjectVideo](#) software analyzes video to detect, classify, and track objects of interest according to user-defined rules. Use it to monitor any type of facility, including dams, seaports, energy plants, government buildings, and military infrastructure. You can identify events and activities such as perimeter breaches, loitering, unauthorized entry or exit, and theft. When user-defined rules are violated, ObjectVideo immediately invokes the rules by generating an alert or triggering another action, such as recording video with Cisco Video Surveillance Manager.

Sensor Fusion, Correlation, and Baselineing

Traditionally, emergency organizations monitor input from each type of sensor on a separate interface, in isolation from input from other types of sensors. Combining inputs can give a more complete picture of the event. For example, in oil and gas production facilities, fusing input from pressure, heat, and infrared sensors enables earlier and more accurate detection of incipient leaks. When sensor readings are only slightly out of range—but for all three sensors—the likelihood of an incipient leak is quite high. The associated policy might be to notify the plant or rig supervisor, shut valves, and shut down processing operations. If only one reading is out of range, the policy might be simply to notify the appropriate personnel.

The value of the Sensor Fusion, Correlation, and Baselineing component includes:

- Detecting anomalous conditions, such as a gas or chemical leak, by analyzing data and correlating it with information from other sensors.
- Reducing false positives and false negatives, for more actionable intelligence, by using diverse sensing technologies.
- Monitoring system health so that you know when a sensor has failed. If a gas sensor is out of calibration and not detecting the correct level of a gas, a technician might be exposed to toxic levels and placed in harm's way.
- Establishing automated notification of appropriate personnel based on inputs from diverse sensors, devices, and system.



Technology Highlight: CACI

CACI provides customized Cisco Integrated Services Routers (ISRs) for emergency response, telemedicine, mining, infrastructure protection, border security and surveillance, enterprise safety and security, and remote automated branch. 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. The solutions are compact, modular, and designed for rapid deployment.



Technology Highlight: ViaLogy

ViaLogy SPM™ Sensor Policy Manager™ combines inputs from multiple networked sensors to provide a complete, real-time operational picture and reduce false positives and negatives. Unlike sensor-management solutions that work only with limited numbers and types of sensors, ViaLogy SPM software fuses and normalizes the inputs from any network-integrated sensor, from any manufacturer, and makes the information available in a distributed manner, from any web browser. Adding a new sensor takes just a few mouse clicks, and you can quickly add support for a new type of sensor. You can use a web browser interface to associate sensor inputs with real-time actions, such as notifying emergency personnel or activating other sensors.

Legacy Integration

Your organization might already have hundreds or thousands of sensors and actuators. Many might be connected to proprietary networks, or not connected at all. You can increase the value of these assets by connecting them to your IP network.



Technology Highlight: Augusta Systems

EdgeFrontier™ from [Augusta Systems](#) enables you 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. You build a converged security platform that can intelligently process data from electronic, physical, and IT security assets. Using your existing network for remote monitoring and data sharing reduces the total cost of ownership and increases return on investment from the network and edge assets.

Common Operational Picture

The COP building block is also part of the Command and Control architecture building block of the Cisco Open Platform for Safety and Security.

A COP is an important part of interagency collaboration. Commanders in all organizations participating in the response can view an identical two- or three-dimensional map of the incident scene, including real-time locations of hostile and friendly participants. The COP might also show other relevant information, such as the location and direction of a fire or chemical plume.

The functional components for the COP building block include:

- **Integration services:** Fuse input from multiple sensors that use different communications protocols.
- **Geospatial engine:** Represent events of interest on two- or three-dimensional maps.
- **Role-based information:** Determine the information that different participants need to do their jobs, to avoid overwhelming them with too much information.
- **Routing engine:** Disseminate information to the correct people.
- **Rules engine:** Define and apply rules for responding to sensor input.
- **Dispatch engine:** Support manual dispatch operations, using radio, paging, or phone calls to any communications device.



Technology Highlight: Swan Island

[Swan Island Networks](#) provides a managed service called TIES®, which fuses open-source and proprietary information from thousands of sources. These can include local, national, and global incident maps; 911 feeds; weather data; flood maps; health advisories and alerts; and traffic information. The service filters data for relevance and presents it as a COP for authorized personnel in multiple organizations. TIES creates an online virtual watch center and disseminates alerts and notifications of potentially disruptive events to web-based and mobile clients.



Technology Highlight: VidSys

[VidSys](#) Situation Management and Video Management applications provide a COP that synthesizes all alarms and events. This increases situational awareness and reducing the number of false alarms. Action plans decrease response times by automating the control of devices and systems. Command center staff can lock doors, control cameras, send warning messages, contact first responders, and send video to field personnel on handheld computers and smartphones. The applications track and log all situations from initial alarm to resolution, enforcing the use of standard operating procedure and supporting compliance. Data logs provide forensic information for analysis and evaluation of systems and response teams.

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 Sensing and Actuation building block provides the capabilities to:

- Rapidly detect suspicious conditions using a variety of sensors
- Fuse sensor inputs to create actionable intelligence
- Respond according to policy by gathering more input or invoking action
- Create a COP to enable interagency collaboration

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.

 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)