CHAPTER 1

Overview

Executive Summary

In large and complex urban environments, it is critical for decision makers to reduce the time from detection of an incident to response by first responders. Additionally, it is very important that the information collected by the system supports the human operators in making key decisions and building confidence in those decisions. Finally, the system must allow for the dissemination of the right information (whether audio, video, pictures, and so on) to the right people at the right time. Cisco's use of the network to integrate various technologies and provide vital information in seconds to decision makers is key to the solution presented.

This solution shows how the integration of multiple sensors, video, computer command-and-control, and communications greatly aid in decision making and in reducing the time to send responders to the scene of a crisis. In addition to reducing time, this solution demonstrates how integrating these technologies across the network permits better situational awareness and command-and-control in a complex environment.

Solution Description

The Cisco Urban Security solution focuses on the products that are integrated into a solution and the services necessary to create a deployment for everyday operations that scale to support environments and their crisis situations. The scope of this solution's testing focuses on the functional interaction between the products tested and includes the actions and reactions necessary to properly monitor, interact, and respond to any situation. Specific use cases have been tested to show the capabilities of the products, components, and systems that have been included.

The focus areas of the solution include command-and control, sensing and actuation, and citizen-authority interaction. More information is available on these functions in Chapter 2, "Architecture Framework." Tying all of the products together to address these key elements of a large scale deployment is shown in Chapter 4, "Designing the Solution."

This is not a blueprint for how to deploy a large-scale safety and security implementation. Rather, this document shows the interaction between the components, explains how to accomplish the integration between components, and provides the direction that enables a successful deployment into an existing security environment.

Solution Benefits

If not properly planned, urban global growth patterns strain city services well beyond breaking point. As urban populations continue to grow at the expected rates, it is implausible to expect security services to scale commensurately without leveraging technological advances and innovations. This is especially true for Africa and Asia where the population growth rates are the highest. The specter of global terrorism exacerbates this problem because densely populated centers make ideal targets for exploitation, destruction, and disruption.

There is also a growing dependence on privately-owned (often government-regulated) infrastructures that are managed within, or are adjacent to, urban boundaries. Examples of this include petrochemical processing/distribution centers, seaports, harbors, and airports, as well as major stock exchanges and bourses. This interdependence stipulates that urban security designs should maintain an open architecture for assimilating outside data and sharing situational awareness among constituent groups.

The benefits of this approach include the following:

- More comprehensive awareness of emergency situations
- Faster retasking of critical resources and better coordination of inter-organizational response efforts
- Capability to easily link private and public security systems together, sharing response talk groups but also sharing important rich media such as videos, pictures, and maps
- Leveraging existing investments to provide a system that is more resilient, more adaptable, and better able to respond to the diverse threat environment
- Transforming Unified Communications to a mass notification system, supporting full response tracking for management of notification and awareness, covering response teams, stakeholders, and mass populace
- Interoperability with facility-based mass notification systems
- Interoperability with ubiquitous social networks and Web 2.0 capabilities
- Introducing personnel accountability capabilities, ensuring personnel are accounted for during emergency situations
- Interoperability with crowd-sourced (public-originated) events and public event sources
- Better capability for expansion and adaptability over time

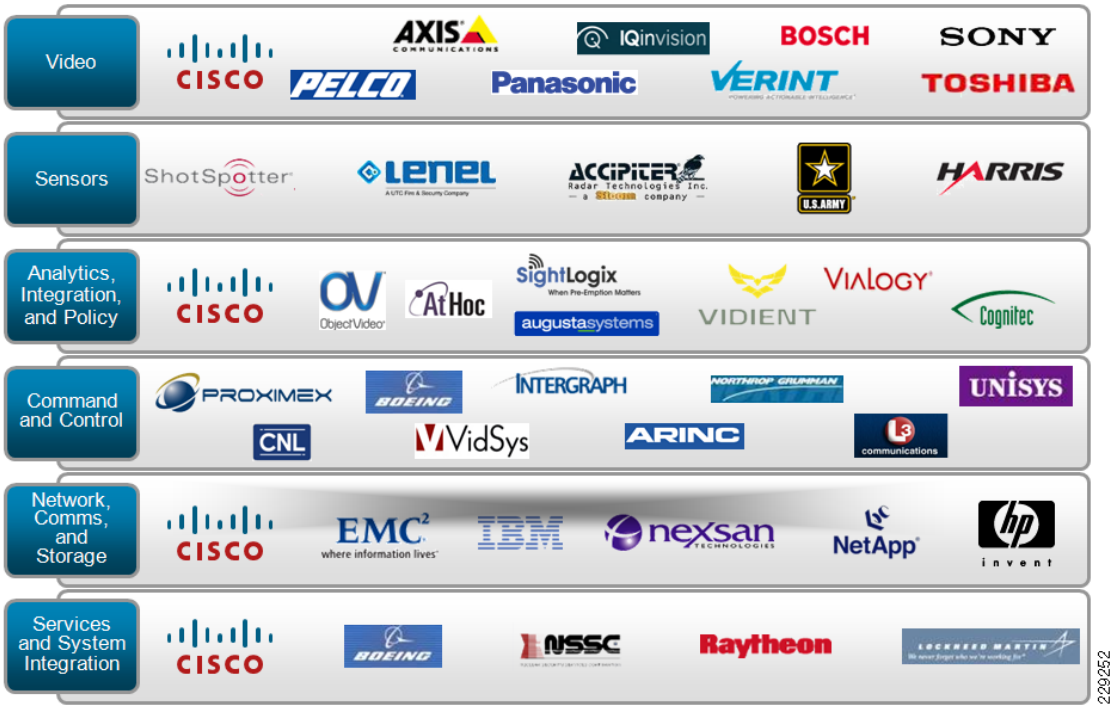
Scope of the Solution

Chapter 4, “Designing the Solution.”highlights the thought process used to determine which components to use and the best way to go about integrating them. Typically, there are multiple ways to integrate the various components.

The focus of this design guide is to help the reader understand the capabilities of the components. There are many ways to integrate different products, and the design guide shows just one way on how the integration testing was accomplished.

Additionally, there are multiple partners that provide the same capabilities in various spaces. As shown in Figure 1-1, there are many different partners that provide similar capabilities.

Figure 1-1 Physical Security Partner Eco-System



Every customer situation is different, and each customer is likely to have a different set of requirements and existing partner components. Understanding how the functions interact versus which partner provided which component is the more important lesson to learn.

Chapter 5, "Integrating the Applications" provides the details of how the components were integrated for testing purposes, showing enough detail so that the reader can understand and integrate this or similar components in their own environment.

This design guide is intended to show how the components used in this solution can be integrated to solve particular business problems. Where HA and scalability documentation exists for a particular component, it is referenced. However, it is best to refer to the product documentation wherever possible for those specific design details.

Use Cases

The following use cases were selected to assist in identifying the products and integration necessary to address these challenges. This is merely a subset of a much greater list of functionality that one would expect to see in designing an Urban Security solution. However, this subset does allow for the identification of specific design criteria and should provide real-life examples of how these components would/could be used in the real world.

Fire Alarm/Smoke Alarm

Multiple scenarios can be used to simulate fire and smoke alarms. These include smoke detectors, fire alarms, infrared cameras, and citizen-reported incidents. While there are strict regulations on the deployment of fire alarm systems, the incident can be handled using a consolidated interface to quickly resolve the incident.

Scenario 1

1. A fire/smoke detector is triggered (simulated in the lab).
2. Cameras in close proximity to the sensor that initiated the alarm are trained on the location.
3. Central Operations is notified of the situation:
   a. Audio alarm
   b. Text notification via phone system
   c. Video notification via digital media
4. Central Operations assesses the situation and takes appropriate actions:
   a. Notification of first responders with location, video feed
   b. Citizen notification via loud speaker, digital media
   c. Initiation of a perimeter monitoring situation, with tripwire crossing notifications when unauthorized personnel pass into the area
5. Central Operations continues to monitor situation via video feeds and provides coordination between first responders
   a. Creates a private communications channel between fire, police, and authorized persons for the duration of the incident
   b. Streams video to the personnel on-site
6. Central Operations sends an accountability notification to facility personnel, and tracks responses to ensure all affected personnel is accounted for.

Unattended Object/Loitering

There are many locations and situations where detecting an unattended object is considered safe practice. In the more obvious situations, detecting a package or piece of luggage left unattended in a train station or airport can be cause for concern. A less obvious situation is the presence of a vehicle in a forbidden location or an area where it has been left unattended for a period of time. In addition, there is typically a lot of background movement of people or vehicles, making it harder to pick out specific objects. There are situations where either of these may not be cause for concern, so including the ability to evaluate the situation is imperative.

Scenario 2

1. Normal video surveillance of a typical environment that includes foot or vehicle traffic is in operation.
2. A person walks into the frame and sets down a package.
   a. Small package
   b. Large package
3. The individual walks away and leaves the package behind.
4. Video surveillance should identify the package left unattended via video analytics.
5. The policy engine re-trains other cameras in the area on the package.
6. Notification is made to Central Operations:
   a. Appropriate audio/video alarms are initiated
   b. Video surveillance from all cameras available

7. Central Operations assesses the situation and takes appropriate actions:
   a. Personnel notification via radio, wireless phone, desk phone
   b. Citizen notification via loud-speaker, digital media displays

Scenario 3

1. Normal video surveillance of a typical environment that includes foot or vehicle traffic is in operation.
2. A vehicle pulls into a no-parking location and stops.
3. After a set period of time, it is determined that this situation needs to be investigated.
4. Notification is made to Central Operations:
   a. Appropriate audio/video alarms are initiated
   b. Video surveillance from all cameras available
5. Central Operations assesses the situation and takes appropriate actions:
   a. Personnel notification via radio, wireless phone, desk phone
   b. Citizen notification via loud-speaker, digital media displays

Video Tripwire Crossing

Tripwire crossing can have various meanings based on the location and type of sensors. In a large area such as an airport or oil refinery, sensors can be monitoring the fence line, watching for suspicious movement. In a border situation, it can be monitoring a state or country line, or a river for illegal crossings. In a train station, it can be watching for track crossings, but having the need to differentiate between a track crossing and a worker on a catwalk. From a harbor port perspective, it can be the detection of a ship crossing into local waters, either in a port area or up to 10 miles off-shore.

Scenario 4

1. Normal video surveillance of an area identified as off-limits is in operation.
2. A person walks into the frame.
   a. Audio alarm initiated requesting person to leave area
   b. Central Operations notification occurs, providing video feed
3. The individual leaves and no further action is required.
4. Normal video surveillance of an area identified off-limits resumes.

Scenario 5

1. A person walks into the frame.
   a. Audio alarm initiated requesting person to leave area
   b. Central Operations notification occurs, providing video feed
2. The individual continues into the unauthorized area.
3. Central Operations assesses the situation and takes appropriate actions:
   a. Personnel notification via radio, wireless phone, desk phone
   b. Additional audio alarms initiated via loudspeaker

Unauthorized Building Access/Forced Entry

Controlling physical access to a location is as much about keeping unauthorized persons out of an area as it is about allowing authorized persons into the same area. To make this a bit more difficult, this profile can change based on situational conditions or time of day.

For example, consider a lab environment. During normal conditions, there are lab workers that are allowed into the area to perform their job. If, however, a situation arises where a spill occurs in the lab, there should be an alarm to evacuate the area, and that area should now be off-limits to normal workers but still allow first responders into the area. So, dynamically changing the security profile based on situational or operational awareness is a requirement.

This example can be expanded to include access for shift workers, allowed access only during their particular shift, or allowing only maintenance personnel access after hours.

Scenario 6

1. Forced entry is detected on a door location.
2. Central Operations is notified of the situation:
   a. Text notification
   b. Audio alarm in Central Operations and door location
   c. Video surveillance of the door is available
3. Central Operations assesses the situation and takes appropriate actions:
   a. Personnel notification via radio, wireless phone
4. Central Operations continues to monitor the situation.

Scenario 7

1. Door access is set up to allow workers into the area.
2. A situation occurs within the location; that is, a fire or chemical sensor alarm occurs in the area.
3. Central Operations is notified of the situation:
   a. Text notification and desktop notification
   b. Audio alarm in Central Operations and alarm location
   c. Video surveillance of the entire area
4. Central Operations assesses the situation and takes appropriate actions:
   a. Personnel are notified via loud speaker to evacuate the location and report to muster station
   b. Door access profile is changed to allow all workers egress, but only first responders ingress to the location
   c. Personnel are provided further instructions via digital media at the muster station
5. Central Operations continues to monitor the situation.