An Open Architecture Framework for Safety and Security

Patrick Bikar
Solutions Architect, Cisco Public Safety & Security
Agenda

- Public Safety and Security: A Complex Discipline
- An Open Architecture Framework for Safety & Security
- Benefits of Adopting An Open Architecture Framework
- Next Steps
Agenda

- Public Safety and Security: A Complex Discipline
- An Open Architecture Framework for Safety & Security
- Benefits of Adopting An Open Architecture Framework
- Next Steps
Public Safety and Security
A Complex Discipline with Many Dimensions

Multiple Organizations
Police, Fire, Ambulance, National

Specific Requirements
Crisis management, Urban security, Border

Emerging Technologies
Sensors, artificial intelligence, video

Integrators and Providers
A variety of systems integrators and providers

In addition, each country/region/city does things its own way…
→ It is an enterprise architect’s worst nightmare!
What is an Architecture Framework?

Consistent, robust toolbox to:

- Capture complex requirements and constraints
- Facilitate communications with stakeholders—and consequently more easily obtain their endorsement
- Use well-defined functional building blocks to construct customized solutions

An Open Architecture Framework for Safety & Security must include:

- Architecture scope
- Architecture building blocks
- Architecture methodology
- Architecture principles

A Standardized Approach to Public Safety & Security is Required
Agenda

- Public Safety and Security: A Complex Discipline
- **An Open Architecture Framework for Safety & Security**
- Benefits of Adopting An Open Architecture Framework
- Next Steps
Six Architecture Building Blocks
Supporting the Architecture Framework for Safety and Security
Architecture Development Methodology: Overview

Stage 1: CIO

- <<Challenge>> is addressed by <<Challenge>> is addressed by... is addressed by

- <<Vision>> is supported by <<Business Goal>> is supported by <<Business Goal>> is supported by... is supported by

Stage 2: Solutions Architect

- <<Capability>> is addressed by <<Capability>> is addressed by... is addressed by

Stage 3: Systems Engineer

- ABB1, ABB2, ABB3, ..., ABB6

- <<Building-Block>> is addressed by <<Building-Block>> is addressed by... is addressed by

- <<Business Goal>> is supported by <<Capability>> is supported by <<Capability>> is supported by... is supported by
Example of Use Case Analysis: Blue Border Protection

Challenges:
- Drugs smuggling
- Criminal organizations abusing from immigrants
- Inability to predict refugee movement and profiling potential 'illegal immigrants'
- Strong influence of the public opinion about human rights
- Vastness of maritime border to control and protect
- Illegal fishing in out-of-bound territorial zones

Vision:
By leveraging new technologies, we will significantly reduce illegal immigration, drugs and weapons smuggling, and monitor movements of Persons of Interest (POI) and increase the efficiency of Border Control personnel.

Goals:
- Pervasive infrastructure
- Effectiveness of Deployed Units
- Effective chase, interception and conclusion through Inter-agency Collaboration
- Unification of Operations
- Environment & Pollution Monitoring

Stage 1: CIO
- By leveraging new technologies, we will significantly reduce illegal immigration, drugs and weapons smuggling, and monitor movements of Persons of Interest (POI) and increase the efficiency of Border Control personnel.

Stage 2: SA
- Command & Control Center Virtualization
- Unified situation awareness and control
- Consolidation and reporting
- Emergency Preparedness
- Mobility
- Data recording
- Multi-modal
- Layer 2 independency
- Interoperability
- Remote detection and identification of vehicle (marine, land, air)

Stage 3: SE
- ABB1: C4ISR Operations Center
- ABB2: Emergency-Grade Network
- ABB3: Emergency Collaboration
- ABB4: Sensing & Actuation
- ABB5: Empowered Mobile Workforce
- ABB6: Citizen-Authority Interaction

Note: Only the higher-level building-blocks are represented. The segmentation goes into further details in the blueprints.
Architecture Principles

- Openness and adherence to standards
- Focus on requirements and usability
- Secure and confidential operations
- Interoperability
- IP as the platform
- Service-orientation ➔ innovation
- Virtualization of services
- Generalized mobility
- Technology convergence
- Integration with legacy
- COTS equipment
- Low cost of operations
- Regulation compliance
Architecture Principles

- Openness and adherence to standards
- Focus on requirements and usability
- Secure and confidential operations
- Interoperability
- **IP as the platform**
- Service-orientation ➔ innovation
- Virtualization of services
- Generalized mobility
- Technology convergence
- Integration with legacy
- COTS equipment
- Low cost of operations.
- Regulation compliance
The Evolution of the Mission-Critical Network

IPv4

IPv6

Application Layer

Network Middleware

IPv4 Layer Protocol

IPv6 Layer Protocol

Application Layer

IP Infrastructure Services

Application Layer

IP Infrastructure Services

Middle layer of servers always needed because of broken E2E model

Patterned network Infrastructure including NAT

1970's era network protocol

Security Mobility NAT Traversal P2P Code

Smaller application code & Faster development leveraging Service Oriented Network Architecture

More powerful Flexible Next-gen Network Protocol

Small code footprint

Relies on Service Oriented Network Architecture to reduce software complexity & footprint size

Mobility Auto-configuration DNS

Security NAT Traversal Connections Multicast Distribution Transport

Bloated Code Footprint & Application complexity

NAT Traversal Directory service Client/server

DNS Routers DHCP Transport

Interoperable?
Agenda

- Public Safety and Security: A Complex Discipline
- An Open Architecture Framework for Safety & Security
- Benefits of Adopting An Open Architecture Framework
- Next Steps
Benefits of an Open Architecture Framework for Safety and Security

- Methodology to link business goals to functional building blocks
- Common reference → standard
- Service-orientation → unlocks innovation
## Public Safety references in Europe

<table>
<thead>
<tr>
<th>Country</th>
<th>User</th>
<th>Project</th>
<th>Architecture Building-block relevance</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPA</td>
<td>City of Rivas</td>
<td>• Reduces Costs and Decreases Energy Consumption, support green practices</td>
<td>• No1, No2, No3, No4, No5, No6</td>
</tr>
</tbody>
</table>
| IRL            | Dublin Airport                | • Video Surveillance  
                      • Storage                                                    | • No1, No4                           |
| UK             | North Wales Police            | • Voice services network to all 75 police stations with appr. 2.500 phones  | • No2, No3, No5                       |
| European country | Police                       | • Centralized Command&Control: Data Center, Mission Critical Network, UC in police stations | • No1, No2, No3, No6                  |
| SWI            | Police and City of Zurich     | • Wireless Video Surveillance for Euro2008  
                      • Mobile Access Router in cars                                | • No2, No4, No5                       |
| European country | MoJ                          | • Justice campus (switching, security, wireless )            | • No2                                 |
| European country | Highway operations            | • Fiber to the highway: UC, video surveillance, sensors, emergency poles on IP, 30% less salt | • No2, No3, No4                       |
| UK             | Derbyshire Fire Brigade       | • Unified Wireless Network to improve productivity, location services for asset control, | • No5                                |

**No1: Command & Control**  
**No4: Sensing & Actuation**  
**No2: Mission-Critical Network**  
**No5: Mobile Force**  
**No3: Incident Collaboration**  
**No6: Citizen-Authority Interaction**
Agenda

- Public Safety and Security: A Complex Discipline
- An Open Architecture Framework for Safety & Security
- Benefits of Adopting An Open Architecture Framework
- Next Steps
Next Steps

- Join the IPI workgroup: PSCEurope

- Read more on Cisco Open Platform for Safety and Security on: www.cisco.com/go/copss

THANK YOU FOR YOUR ATTENTION …
BACKUP SLIDES
Command and Control
Emergency Prevention, Preparation, Response, and Recovery

[C2] Description
- Provides up-to-date situational awareness, actionable intelligence, and decision support tools
- C2 contains:
  - Common operational picture (COP)
  - Unified process management
  - Identity, information, and intelligence management
  - Simulation and investigation
Today, first responders must rely on a variety of heterogeneous networks. MCN is required to optimize emergency operations through a unified, scalable, resilient, secure, and intelligent network platform.

MCN features:
- IP-layer abstraction
- Traffic optimization (QoS, resilience, multicast, traffic engineering, etc.)
- Self-defense (network access control, VPN, firewall, etc.)
- Mobility (wireless, geolocation, etc.)
- Data center technologies (high-performance computing, WAN optimization, etc.)
- Rapid deployment, etc.
Sensing and Actuation
Emergency Prevention, Preparation, Response, and Recovery

[S&A] Description

- S&A provides the Operations Center with a stream of local information and the means for swift, automated remote action.

- S&A contains:
  - Quantitative sensors
  - Qualitative sensors (including real-time analytics)
  - Human identification (biometrics)
  - Object identification (including RFID)
  - Sensor correlation and baselining
  - Actuators
  - Legacy integration
Citizen-Authority Interaction
Emergency Prevention, Preparation, Response, and Recovery

Cisco Open Platform for Safety and Security

[CAI] Description

Works in two directions:

- Citizen to authority: single point of contact for citizens to request emergency support
- Authority to citizen: sometimes referred to as “reverse-112”; allows authority to warn a specific group of individuals when an immediate danger is threatening (e.g., fire, bomb, bacteriological attack)
Mobile Force
Emergency Prevention, Preparation, Response, and Recovery

Cisco Open Platform for Safety and Security

- Deployed forces must be as effective in the field as they would be in the office, e.g.:
  - Security guard’s handheld device enabling remote access to video surveillance cameras
  - Police vehicle equipped with a mobile router providing secured access to central databases
  - Firefighter’s suit enhanced with an array of biosensors

- Rescue teams must be accurately briefed using the whole available information: location, type of accident, casualties, etc.

- Information must be role-based and presented through an intuitive GUI
Incident Collaboration
Emergency Prevention, Preparation, Response, and Recovery

[IC] Description

- Optimal collaboration of the first responders between themselves and with the operations center
- Independent on the specific technology used (IP, analog or digital radio, etc.) or on the medium (voice, video, IM, SMS)
- Ad hoc communication groups, linking all persons within a certain geographical area, independently of their communication device or their organization