Protecting Critical Infrastructure

IP Security Networks

Go Beyond the Enterprise

TJ Roe, RCDD - GarrettCom, Inc.

troe@garrettcom.com
Agenda

- Overview and Drivers
- Unique Considerations in Planning & Design for Industrial Applications
- Components - Why IP Now
- Benefits - Where Are the Opportunities
- Applications
- Trends
Opportunities for Industrial Security

• Increasing concerns lead to market growth
  – Asset protection
  – Public safety and employee safety
  – Regulatory compliance
  – Video integration with industrial operations
• More sophisticated, integrated solutions
• More challenging logistics
Criteria Driving IP Systems Outdoors

• Need to easily construct scalable systems
  – Grow to large numbers of cameras
  – System can be managed and upgraded
  – Integration with other network tools and applications

• Need easy access to information gathered
  – Easily stored and retrieved for event analysis
  – Many locations can share information
  – Timely delivery to people that need it
  – Real-time analysis and response
Installation Challenges

• How to construct and manage systems
• How to scale to hundreds of cameras
• Device specific challenges
  – Greater ambient temperature ranges
  – Integrated fiber ports
  – Form factors and alternative mounting options
  – Where to get dependable power for devices
Security Design Principles

Layering
• Deter
• Detect
• Delay

Respond/React

From Bicsi ESS Design Reference Manual
Integrated Security Networks

- Distributed, networked system with shared infrastructure
- Standards-based hardware/software components
- Integration with off-the-shelf and custom enterprise applications
Integrated Security Application

Analyze
- Motion Detection & Event Triggers
- Video Analytics
- Access Control
- Intrusion Detection

View / Decide
- Video Display
- Command Center Control
- Remote Display
- Map Display Geospatial Data

Manage
- Video Storage Retrieval
- Content Management & Database
- Alarms Reporting
- Computer Aided Dispatch

Digital Video
Sensors:
- Doors
- Card Keys
- Biometrics

GarettCom

BICSI
Public Safety

• Transportation systems
  – Airports
  – Seaports
  – Rapid Transit and Rail facilities

• Public Areas
  – Parks and recreational facilities
  – Sports facilities
  – Parking infrastructures
Transportation Rail Application

Typical SARL Station CCTV Network with Magnum PoE Switches Connecting Security Cameras

[Diagram showing a typical SARL station CCTV network with Magnum PoE switches connecting security cameras.]

- Platform Level
- East Bound
- West Bound
- Ground Level
- Concourse Level
- Station Controller
- Video Surveillance Workstation
- 19" LCD Wall Display
- Elevator
- Platform Head Wall Monitor
- Elevator

- Fixed IP Dome Camera 5-50 mm Lens
- IP Dome PTZ Camera
- Fixed IP Dome Camera 2.8 to 10 mm Lens
- GarrettCom Power over Ethernet (PoE) Switch
- Fixed IP Camera 2.8 to 12 mm Lens
- Outdoor Housing

- CAT5e Ethernet
- RG11 Coax cable
PoE for Installation Flexibility

Access Devices with Power-over-Ethernet (PoE):
Single cable for power and data (image)
Power over Ethernet - PoE

• PoE - a simplified means to power network edge devices
  – Cameras, VoIP phones, badge readers, sensors, WAPs, etc.
  – Power Sourcing Device = **PSE**, Powered Device = **PD**
  – PSE’s are PoE switches and Mid-span power insertion
• Currently used PoE standard is 802.3af
  – PoE supplies up to 15.4 watts to powered device lines
  – Due to transmission losses, only ~13 watts available to device
  – PoE protocol prevents power from being applied to non-PoE devices
• New Standard 802.3at, PoE+ (compatible with current standard)
  – Recently ratified by IEEE (Sept. 11, 2009)
  – New end devices currently under development, now unavailable
  – Provides roughly 2x power (28w) as compared to 802.3af
Parking Garage Call Station & Cameras

IP Mega-Pixel Camera

Call Station

IP Mega-Pixel Camera

IP Mega-Pixel Camera

IP Mega-Pixel Camera

IP Mega-Pixel Camera

IP Mega-Pixel Camera
Campus Call Station & Camera Example

IP Camera 360 Degree View

VolP Call Station

Future IP Call Tower & IP Camera Location

Industrialized / Hardend Ethernet Switch with Fiber Optic Connectivity, To Local IDF.
Parking Lot IP Camera Example: “What’s in the Junction Box?”

Smaller form factors + integrated fiber ports allow design flexibility
Design – Aggregation switch

Integrated fiber and copper ports
Planning & Design

• Don’t forget documentation
• Planning and coordination with other trades
Critical Physical Security

- Power utilities
  - NERC/CIP
- Water systems
  - Biohazard
- Oil & gas, chemical
  - CFATS
- Other remote facilities
Federally mandated cyber security standards for power utilities:
NERC Critical Infrastructure Protection CIP-002---CIP-009

<table>
<thead>
<tr>
<th>CIP-002</th>
<th>Critical Cyber Asset Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIP-003</td>
<td>Security Management Controls</td>
</tr>
<tr>
<td>CIP-004</td>
<td>Personnel and Training</td>
</tr>
<tr>
<td>CIP-005</td>
<td>Electronic Security Perimeters</td>
</tr>
<tr>
<td>CIP-006</td>
<td>Physical Security of Critical Cyber Assets</td>
</tr>
<tr>
<td>CIP-007</td>
<td>Systems Security Management</td>
</tr>
<tr>
<td>CIP-008</td>
<td>Incident Reporting and Response Planning</td>
</tr>
<tr>
<td>CIP-009</td>
<td>Recovery Plans for Critical Cyber Assets</td>
</tr>
</tbody>
</table>
CFATS

- Chemical Facility Anti-Terrorism Standards
  - requires all chemical facilities to comply with regulatory requirements as detailed in 6CFR27
- Security vulnerability assessment (SVA)
- Develop a site security plan (SSP)
Special Challenges

- Installation
- Reliability
- Performance
- Security
Key Components of Reliability

• Reliable network components
  – Hardware made for harsh environments
  – High MTBFs
  – Device compatibility tested

• Resilient network design and topology
  – Devices, power, interconnects will eventually fail
  – A resilient network design can mask these failures
  – Modern software is designed for continuous uptime and network standards compliance for interoperability
Resilient Network Design

• Numerous protection protocols to enable resilient networks and maximize network uptime …

<table>
<thead>
<tr>
<th>Redundancy Feature</th>
<th>Line Cuts</th>
<th>Switch Failure</th>
<th>Power Failure (local)</th>
<th>Router Failure</th>
<th>Bandwidth Protection</th>
<th>Recovery Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet / Layer 2 Redundancy</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>15 mS + N*2ms</td>
</tr>
<tr>
<td>Rapid Spanning Tree Protocol (RSTP)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>15 mS + N*2ms</td>
</tr>
<tr>
<td>S-Ring</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>500ms + N*20ms</td>
</tr>
<tr>
<td>Dual Homing (Remote switch redundant path)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>300ms</td>
</tr>
<tr>
<td>LAN Aggregation Control Protocol</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>0 Seconds</td>
</tr>
<tr>
<td>IP / Layer 3 Redundancy</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>Variable</td>
</tr>
<tr>
<td>RIP / OSPF / BGP Alternate Routes</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>Variable</td>
</tr>
<tr>
<td>Redundant WAN (in conjunction with routing)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>Variable</td>
</tr>
<tr>
<td>Virtual Routing Redundancy Protocol (VRRP)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>Variable</td>
</tr>
</tbody>
</table>

• For Layer 2 Redundancy:
  – RSTP (IEEE 802.1-2004) recovers large rings or mesh networks rapidly
  – LACP allows LAN aggregation for increased bandwidth and redundancy
  – Avoid proprietary recovery protocols

• Redundant routes and VRRP provide fault tolerant networks at Layer 3
Redundancy Examples

- RSTP-2004 is Ideal for L2 networks needing:
  - Mission critical redundancy
  - Fastest / most predictable recovery times
St. Cloud Water Treatment

Redundant ring provides uptime for security
Resilient Layer 2 Network

- Ethernet RSTP network design can be tailored to fit the application
  - RSTP networks up to 100 nodes recover at speeds up to 2ms/node
Tampa Expressway

Redundant rings for traffic control, DMS, sensors and video surveillance

Multiple redundant rings for expanded system with high reliability
Special Challenges

• Installation
• Reliability
• Performance
• Security
Performance Issues

• Too many bits
  – Multiple dense video streams competing for finite network capacity

• Bits going everywhere
  – Many video streams are multicasting – potentially flooding networks

• Differing priorities among applications
  – Multiple different security functions on the same network compete with each other for priority
Performance Considerations

- Video is very bandwidth heavy
- Multiple cameras per node add up – even on G’bit rings!
- Multiple G’bit links should be considered for applications with:
  - High resolution cameras
  - High number of cameras
  - Possibility of significant future growth in nodes

<table>
<thead>
<tr>
<th>Resolution</th>
<th>Stream size (mbps)</th>
<th>50</th>
<th>100</th>
<th>150</th>
<th>200</th>
<th>250</th>
</tr>
</thead>
<tbody>
<tr>
<td>Poor</td>
<td>0.512</td>
<td>25.6</td>
<td>51.2</td>
<td>76.8</td>
<td>102.4</td>
<td>128</td>
</tr>
<tr>
<td>Low</td>
<td>1</td>
<td>50</td>
<td>100</td>
<td>150</td>
<td>200</td>
<td>250</td>
</tr>
<tr>
<td>Medium</td>
<td>3</td>
<td>150</td>
<td>300</td>
<td>450</td>
<td>600</td>
<td>750</td>
</tr>
<tr>
<td>High</td>
<td>6</td>
<td>300</td>
<td>600</td>
<td>900</td>
<td>1200</td>
<td>1500</td>
</tr>
</tbody>
</table>
Quality of Service (QoS) Technologies

- Different traffic types can be prioritized differently
  - DiffServ, or DSCP can be used at the IP layer
  - 802.1p can tag Ethernet frames for layer 2 priority
- Both functions allow traffic to be identified, marked and prioritized to achieve desired data transfer performance

<table>
<thead>
<tr>
<th>Priority Level</th>
<th>Traffic Type</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Best Effort</td>
<td>Web Access</td>
</tr>
<tr>
<td>1</td>
<td>Background</td>
<td>File Access</td>
</tr>
<tr>
<td>2</td>
<td>Standard</td>
<td>File Transfer</td>
</tr>
<tr>
<td>3</td>
<td>Business Applications</td>
<td>Business Critical Processing</td>
</tr>
<tr>
<td>4</td>
<td>Controlled Load</td>
<td>Streaming Multimedia</td>
</tr>
<tr>
<td>5</td>
<td>Interactive Voice and Video</td>
<td>IP Video</td>
</tr>
<tr>
<td>6</td>
<td>Layer 3 Network Control Traffic</td>
<td>Routing Protocols</td>
</tr>
<tr>
<td>7</td>
<td>Layer 2 Network Control Traffic</td>
<td>RSTP Protocols</td>
</tr>
</tbody>
</table>

- In a surveillance application, QoS can be used to ensure that network control traffic is not over-run by the bandwidth-heavy video streams
National Seaport Security Network

IP facilitates information sharing at dispersed locations – the right information to the right people at the right time!
Special Challenges

• Installation
• Reliability
• Performance
• Security
Network Security

- LAN Security
  - Port security
  - VLANs
  - Encryption
  - Who/what gets access to which ports?

- Perimeter Security
  - Firewall
  - WAN VPN
  - Keep the bad stuff out!

- Remote Access Security
  - Authenticate/authorize
  - Allow permitted remote operations

- Management Security
  - Secure mgmt. protocols
  - User authentication
  - Logging
Benefits

• Scalability
  – Add cameras, access points as network nodes
  – Add standard hardware for servers, storage, networks.
  – Leverage well known IT design practices.

• Multiple sites and remote decision makers.
  – Cameras, servers and command centers can be anywhere.

• New capabilities easily added later.
  – New software functions or hardware easily added.
  – Leverage advances in analytics and other applications.
Trends

• More integration “outside” of Enterprise
  - Added protection with Layering
  - Protects personnel on campus
• Analytics on all video feeds.
  – In cameras, and integrated with video platforms
• Standards for application integration
  – Web services XML APIs
• Information lifecycle management for video
  – Staged storage, secure repositories for clips
• Video, Voice, Data integration
  – Enterprise IT integration of Video, VoIP and Data
Questions/Comments/ Discussion

For more information, including

- application notes
- white papers
- resource docs

http://www.garrettcom.com/surveillance_security.htm

TJ Roe, RCDD - GarrettCom, Inc.

email: troe@garrettcom.com

Tel: (302)-235-0995