IT and OT Convergence - Recommendations for Building an Industrial IoT-Ready Manufacturing Network

Arun Siddeswaran, Cisco Systems, Inc.
Gregory Wilcox, Rockwell Automation, Inc.

February 22, 2017
Agenda

• Secure Connectivity between Manufacturing and Business Systems
  – Business Outcomes
  – Bridging OT-IT
  – Key Requirements / Key Tenets

• Key Takeaways

• Recommended Resources
Industrial IoT - Business Outcomes
Industrial IoT - Business Outcomes

- **Reduced Downtime**: 48%
  - Unplanned downtime down from 11% to 5.8%

- **Reduction in Defects**: 49%
  - Defect rate down from 4.9% to 2.5%

- **New Product Introduction**: 23%
  - New product introduction cycle time reduced from 15 to 11 months

- **OEE Improvement**: 16%
  - Average OEE improved from 74% to 86%

- **Improved Inventory**: 35%
  - Inventory turns increased from 14 to 19

- **Reduction in Energy Use**: 18%
  - Annual energy cost down from $8.4M to $6.9M

Industrial IoT - Business Outcomes

• Smart Devices, Smart Machines, Smart Manufacturing
• Customer choice of best-in-class products through Industrial IoT device coexistence and interoperability
• Standard Network Services; Standard Network Tools
• Pervasive Asset Optimization and Utilization
  – Common infrastructure devices and tools
  – Human assets: knowledge, experience, training
• Better Analytics
  – Device/Machine, System/Plant, Enterprise
• Enables Innovative Technologies
  – Mobility – Personnel and Equipment
  – Cloud – On Premise and Off Premise
Industrial OT vs Enterprise IT Networks
# Industrial OT vs. Enterprise IT Networks

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Industrial OT Network</th>
<th>Enterprise IT Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Technology</td>
<td>Standard IEEE 802.3 Ethernet and proprietary (non-standard) versions</td>
<td>Standard IEEE 802.3 Ethernet</td>
</tr>
<tr>
<td></td>
<td>Standard IETF Internet Protocol (IPv4) and proprietary (non-standard) alternatives</td>
<td>Standard IETF Internet Protocol (IPv4 and IPv6)</td>
</tr>
<tr>
<td>Network Availability</td>
<td>Switch-Level and Device-Level Topologies</td>
<td>Switch-Level topologies</td>
</tr>
<tr>
<td></td>
<td>Ring Topology is predominant for both, Redundant Star for switch topologies is emerging</td>
<td>Redundant Star Topology is predominant</td>
</tr>
<tr>
<td></td>
<td>Standard IEEE, IEC and vendor specific Layer 2 resiliency protocols</td>
<td>Standard IEEE, IETF, and vendor specific Layer 2 and Layer 3 resiliency protocols</td>
</tr>
<tr>
<td>Service Level Agreement (SLA)</td>
<td>Mean time to recovery (MTTR) - Minutes, Hours</td>
<td>Mean time to recovery (MTTR) - Hours, Days</td>
</tr>
<tr>
<td>IP Addressing</td>
<td>Mostly Static</td>
<td>Mostly Dynamic</td>
</tr>
</tbody>
</table>
## Industrial OT vs. Enterprise IT Networks

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Industrial OT Network</th>
<th>Enterprise IT Network</th>
</tr>
</thead>
</table>
| Traffic Type | Primarily local – traffic between local assets  
Information, control, safety, motion, time synchronization, energy management  
Smaller frames for control traffic  
Industrial application layer protocols: CIP, PROFINET, IEC 61850, Modbus TCP, etc. | Primarily non-local – traffic to remote assets  
Voice, Video, Data  
Larger packets and frames  
Standard application layer protocols: HTTP, SNMP, DNS, RTP, SSH, etc. |
| Performance  | Low Latency, Low Jitter  
Data Prioritization – QoS – Layer 2 & 3                                                   | Low Latency, Low Jitter  
Data Prioritization – QoS – Layer 3                                                   |
| Security     | Open by default, must close by configuration and architecture  
Industrial security standards – e.g. IEC, NIST  
Inconsistent deployment of security policies  
No line-of-sight to the Enterprise or to the Internet | Pervasive  
Enterprise security standards  
Strong security policies  
Line-of-sight across the Enterprise and to the Internet |
What are best practices
Structured and Hardened Architectures

Key Requirements
- Scalable
- Reliable
- Safe
- Secure
- Future-ready

Key Tenets
- Smart Endpoints
- Segmentation (Zoning)
- Managed Infrastructure
- Resiliency
- Time-critical Data
- Wireless - Mobility
- Holistic Defense-in-Depth Security
- Convergence-ready
Zoning Through Segmentation

Level 5
Level 4
E-Mail, Intranet, etc.
Site Business Planning and Logistics Network
Remote Desktop Gateway Services
Patch Management
AV Server
Application Mirror
Web Services Operations
Application Server
Firewall
Web/Email/ZIP
Industrial DMZ
Level 3.5
Enterprise Security Zone
Levels 4-5

Level 3
FactoryTalk Application Server
FactoryTalk Directory
Engineering Workstation
Remote Access Server
Site Operations and Control

Level 2
FactoryTalk Client
Operator Interface
Operator Interface

Level 1
Batch Control
Discrete Control
Drive Control
Continuous Process Control
Safety Control

Level 0
Sensors
Drives
Actuators
Robots

Enterprise Security Zone(s)
Levels 0-3
Industrial Security Zone(s)
Levels 0-3

Cell/Area Zone(s)
Levels 0-2

Area Supervisory Control
Basic Control

Site Operations and Control

Process

Technical Track
© 2017 ODVA, Inc.
2017 Industry Conference & 18th Annual Meeting
All rights reserved.
Plant-wide Zoning

- Functional / Security Areas
- Smaller Connected LANs
  - Smaller Broadcast Domains
  - Smaller Fault Domains
  - Smaller Domains of Trust
- Industrial IoT Technology
- Building Block Approach for Scalability
Zoning Through Segmentation

Key Tenets

- Smart Endpoints
- Segmentation (Zoning)
- Managed Infrastructure
- Resiliency
- Time-critical Data
- Wireless - Mobility
- Holistic Defense-in-Depth Security
- Convergence-ready
Wired Access Overview
**Typical Zone Traffic Flows**

**CIP Implicit Traffic- Producers & Consumer**

- >80% local
- Cyclical I/O traffic, UDP unicast and multicast
- <500 Bytes, Frequent 0.5 to 10’s of ms, typically 20 ms

**CIP Explicit Traffic - Informational control and administration**

- Intra- and inter-cell/area zone traffic flow
- Non-critical administrative or data traffic using TCP
- ~1500 Bytes, infrequent
Industrial Network Topologies

Switch-level Topologies

Device-level Topologies
<table>
<thead>
<tr>
<th>Function</th>
<th>Process Automation</th>
<th>Discrete Automation</th>
<th>Loss Critical</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Information Integration, Slower Process Automation</td>
<td>Time-critical Discrete Automation</td>
<td>Multi-axis Motion Control</td>
</tr>
<tr>
<td>Comm. Technology</td>
<td>.Net, DCOM, TCP/IP</td>
<td>Industrial Protocols, CIP, Profinet</td>
<td>Hardware and Software solutions, e.g. CIP Motion, PTP</td>
</tr>
<tr>
<td>Period</td>
<td>1 second or longer</td>
<td>1 ms to 100 ms</td>
<td>100 µs to 10 ms</td>
</tr>
<tr>
<td>Industries</td>
<td>Oil &amp; Gas, chemicals, energy, water</td>
<td>Auto, food and beverage, electrical assembly, semiconductor, metals, pharmaceutical</td>
<td>Utilities Subset of Discrete automation</td>
</tr>
<tr>
<td>Applications</td>
<td>Pumps, compressors, mixers; monitoring of temperature, pressure, flow</td>
<td>Material handling, filling, labeling, palletizing, packaging; welding, stamping, cutting, metal forming, soldering, sorting</td>
<td>Life/equipment safety, Synchronization of multiple axes: printing presses, wire drawing, web making, picking and placing</td>
</tr>
</tbody>
</table>

Source: ARC Advisory Group
## Network Resiliency Protocols

<table>
<thead>
<tr>
<th>Resiliency Protocol</th>
<th>Mixed Vendor</th>
<th>Ring</th>
<th>Redundant Star</th>
<th>Net Conv &gt;250 ms</th>
<th>Net Conv 50-100 ms</th>
<th>Net Conv &lt; 0~10 ms</th>
<th>Layer 3</th>
<th>Layer 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>STP (802.1D)</td>
<td></td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td></td>
<td>☐</td>
</tr>
<tr>
<td>RSTP (802.1w)</td>
<td></td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td></td>
<td>☐</td>
</tr>
<tr>
<td>MSTP (802.1s)</td>
<td></td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td></td>
<td>☐</td>
</tr>
<tr>
<td>PVST+</td>
<td></td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td></td>
<td>☐</td>
</tr>
<tr>
<td>REP</td>
<td></td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td></td>
<td>☐</td>
</tr>
<tr>
<td>EtherChannel (LACP 802.3ad)</td>
<td></td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td></td>
<td>☐</td>
</tr>
<tr>
<td>MRP (IEC 62439-2)*</td>
<td></td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td></td>
<td>☐</td>
</tr>
<tr>
<td>Flex Links</td>
<td></td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td></td>
<td>☐</td>
</tr>
<tr>
<td>PRP/HSR (IEC 62439)*</td>
<td></td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td></td>
<td>☐</td>
</tr>
<tr>
<td>DLR (IEC &amp; ODVA)</td>
<td></td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td></td>
<td>☐</td>
</tr>
<tr>
<td>StackWise</td>
<td></td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td></td>
<td>☐</td>
</tr>
<tr>
<td>HSRP</td>
<td></td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td></td>
<td>☐</td>
</tr>
<tr>
<td>VRRP (IETF RFC 3768)</td>
<td></td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td></td>
<td>☐</td>
</tr>
</tbody>
</table>

**Legend**
- Process and Information
- Time Critical
- Loss Critical
Convergence-Ready
Challenge - Ethernet Growing Pains

- Ethernet networks continue to grow:
  - Each skid/machine adds another 5 - 50 EtherNet/IP enabled devices
  - Every line adds another 250 - 1,000 EtherNet/IP enabled devices

How do I connect all these skids/machines into a plant network to gain the advantages?
Layer 2 Network Address Translation (NAT)

Outside Subnet
(ex. 10.0.0.x)

Many Outside IP addresses
(One per device wishing to be accessible from the Outside Subnet)

NAT Enabled Device

Many Inside IP addresses
(One per connected device)

Inside Subnet
(ex. 192.168.1.x)
Layer 2 NAT Design Scenario #1
Single-Cell, Single VLAN per Switch

<table>
<thead>
<tr>
<th>Inside to Outside NAT Table</th>
<th>Inside</th>
<th>Outside</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.10</td>
<td>10.10.10.10</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Outside to inside NAT Table</th>
<th>Outside</th>
<th>Inside</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.10.30</td>
<td>192.168.1.30</td>
<td></td>
</tr>
</tbody>
</table>

Machine
Inside Address
192.168.1.10

Outside
Inside
10.10.10.30
192.168.1.30

Inside to Outside
NAT Table
Outside to inside
NAT Table
Wireless Access Overview
Wireless Technology Overview - Benefits of Industrial WLAN

- Lower installation and operational costs
  - Cabling and hardware reduction
  - Minimizing cable failures
- Connection to hard-to-reach and restricted areas
- Equipment mobility
  - New and more efficient applications
- Workforce mobility
  - Higher productivity and less downtime
  - Operators, engineering and maintenance, Industrial IT
- Asset Tracking
  - Track assets of people to optimize cost and for safety
Challenges of wireless communication

- **Half-duplex shared medium:**
  - Only one radio can transmit on a particular wireless channel
  - A radio cannot transmit and receive at the same time on the same channel

- **Higher latency, jitter and packet loss** compared to wired Ethernet
  - Media contention, collisions and interference
  - Can be minimized but not eliminated

- **Signal quality may change** over time

---

**Wireless advantages > challenges when**

- **WLAN is designed and maintained properly**
- **Used for appropriate applications**
Autonomous WLAN Architecture
Unified WLAN Architecture
Holistic Defense-in-Depth Security
Industrial Network Security Framework

Enterprise Zone: Levels 4-5

- Physical or Virtualized Servers
  - Patch Management
  - AV Server
  - Application Mirror
  - Remote Desktop Gateway Server

Industrial Demilitarized Zone (IDMZ)

- Plant Firewalls
- Active/Standby
- Inter-zone traffic segmentation
- ACLs, IPS and IDS
- VPN Services
- Portal and Remote Desktop Services proxy

Industrial Zone: Levels 0-3

- Plant-wide Firewall Management
- Network Security
- Application Security
- Remote Access Server (RAS)

Level 3 – Site Operations

- Computer Hardening
- Application Hardening

Level 2 – Area Supervisory Control

- FactoryTalk Client
- Wireless LAN (WLC)
- Active
- Standby

Level 1 - Controller

- Controller
- Industrial Firewall
- I/O Soft Starter
- MCC
- Drive

Level 0 - Process

- Controller
- I/O

IT Security Architects in Collaboration with Control Systems Engineers

Control System Engineers in Collaboration with IT Network Engineers (Industrial IT)

Control System Engineers (OT)

IEC 62443
- Zones & Conduits
- Confidentiality, Integrity, Availability
NIST 800-82
- Cybersecurity Framework
ICS-CERT
- Recommended Practices

ODVA 2017
Industry Conference and 18th Annual Meeting
Secure Remote Connectivity

Enterprise Zone: Levels 4-5

Industrial Demilitarized Zone (IDMZ)

Industrial Zone Levels 0-3
(Plant-wide Network)

Cell/Area Zones - Levels 0-2
(Lines, Machines, Skids, Equipment)
Key Takeaways

• **Plant-wide reference architectures** - Simplified design, quicker deployment, reduced risk in deploying new technology

• **Wired access** topology and protocols based on plant layout, convergence and application requirements

• **Layer 2 NAT** helps end users to easily *integrate skids/machines* into their larger plant network without extensive coordination with OEMs

• **Wireless access offers multiple advantages**, enables secure personnel access, equipment to equipment communication and asset tracking

• **Defense-in-depth security** offers multiple layers of threat detection and prevention
Recommended Resources

• ODVA
  – The Common Industrial Protocol (CIP) and the Family of CIP Networks
  – Network Infrastructure for EtherNet/IP: Introduction and Considerations
  – Media Planning and Installation Manual
  – Guidelines for Using Device Level Ring (DLR) with EtherNet/IP
  – Securing EtherNet/IP Networks

• Converged Plantwide Ethernet (CPwE) Architectures
  – Cisco
  – Rockwell Automation

• Education / Awareness
  – Industrial IP Advantage (IIPA) eLearning industrial-ip.org

• Training / Certification
  – Industrial Networking Specialist
    • IMINS Training, 200-401 Exam
  – CCNA Industrial
    • IMINS2 Training, 200-601 Exam
Thank You