IT / OT Network Design

Best Practices

Mikkel Brodersen
Systems Engineer, Cisco Systems, Danmark
Oktober 2018
Industrial Network Convergence

Traditional

Converged Ethernet
Benefits of Industrial Ethernet in Factory Networks

**Increased Visibility**
- Connectivity to devices and controllers
- Manufacturing—enterprise integration

**Uptime and Performance**
- Security and reliability
- Network resiliency

**Increased Efficiency**
- Standard architecture—integration and support
- Scalable network platform—multiple applications

**Improved Event Response**
- Remote access
- Improved diagnostics and support
Connected Factory Solution

WHAT IS IT
Unified Converged Factory Network

CHALLENGE
Complex network silos creating downtime, data isolation and vulnerabilities. Inflexible and high TCO.

“Network issues took us hours and sometimes days to troubleshoot. The downtime associated with these issues was extremely costly.” - Dave Gutshall – Harley Davidson

CRITICAL NEEDS
- Converged Network for Flexible Automation
- Security Built-in
- Simple
- Rapid Fault Isolation
- Resiliency
- Quality of Service
- Ease of use (NAT)
- App / Data Integration
- Ruggedized

ARCHITECTURE

BUSINESS OUTCOMES
OEE Improvement  Reduced Downtime
Connected Factory
Designed for Digital Manufacturing
## Built on Industry Standards

### ISA95/Purdue Reference Model

<table>
<thead>
<tr>
<th>Level 5</th>
<th>Enterprise Network</th>
<th>Enterprise Security Zone</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>E-Mail, Intranet, etc.</td>
<td>Site Business Planning and Logistics Network</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Level 4</th>
<th>Industrial DMZ</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Gateway Services</td>
<td></td>
</tr>
<tr>
<td>Patch Management</td>
<td></td>
</tr>
<tr>
<td>AV Server</td>
<td></td>
</tr>
<tr>
<td>Application Mirror</td>
<td></td>
</tr>
<tr>
<td>Web Services Operations</td>
<td></td>
</tr>
<tr>
<td>Application Server</td>
<td></td>
</tr>
<tr>
<td>Firewall</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Level 3</th>
<th>Site Operations and Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>FactoryTalk Application Server</td>
<td></td>
</tr>
<tr>
<td>FactoryTalk Directory</td>
<td></td>
</tr>
<tr>
<td>Engineering Workstation</td>
<td></td>
</tr>
<tr>
<td>Remote Access Server</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Level 2</th>
<th>Industrial Zone</th>
</tr>
</thead>
<tbody>
<tr>
<td>FactoryTalk Client</td>
<td></td>
</tr>
<tr>
<td>Operator Interface</td>
<td></td>
</tr>
<tr>
<td>FactoryTalk Client</td>
<td></td>
</tr>
<tr>
<td>Engineering Workstation</td>
<td></td>
</tr>
<tr>
<td>Operator Interface</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Level 1</th>
<th>Cell/Area Zone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Batch Control</td>
<td></td>
</tr>
<tr>
<td>Discrete Control</td>
<td></td>
</tr>
<tr>
<td>Drive Control</td>
<td></td>
</tr>
<tr>
<td>Continuous Process Control</td>
<td></td>
</tr>
<tr>
<td>Safety Control</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Level 0</th>
<th>Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensors</td>
<td></td>
</tr>
<tr>
<td>Drives</td>
<td></td>
</tr>
<tr>
<td>Actuators</td>
<td></td>
</tr>
<tr>
<td>Robots</td>
<td></td>
</tr>
</tbody>
</table>
### Logical Architecture

**Built on Industry Standards**

<table>
<thead>
<tr>
<th>Zone</th>
<th>Component</th>
<th>Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise Zone</td>
<td>Enterprise Network</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>Site Business Planning and Logistics Network</td>
<td>4</td>
</tr>
<tr>
<td>DMZ</td>
<td>Demilitarized Zone—Shared Access</td>
<td></td>
</tr>
<tr>
<td>Manufacturing Zone</td>
<td>Site Manufacturing Operations and Control</td>
<td>3</td>
</tr>
<tr>
<td>Cell/Area Zone</td>
<td>Area Control</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Basic Control</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Process</td>
<td>0</td>
</tr>
</tbody>
</table>
Converged Plantwide Ethernet (CPwE)
Reference Architecture

Wide Area Network (WAN)
- Data Center - Virtualized Servers
  - ERP - Business Systems
  - Email, Web Services
  - Security Services - Active Directory (AD), Identity Services (AAA)
  - Network Services - DNS, DHCP
  - Call Manager

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

Enterprise
- Identity Services
- External DMZ/Firewall

Physical or Virtualized Servers
- FactoryTalk Application Servers
- Network & Security Services - DNS, AD, DHCP, Identity Services (AAA)
- Storage Array

Remote Access Server
- Patch Management
- AV Server
- Application Mirror
- Remote Desktop Gateway Server

Physical or Virtualized Servers
- ERP - Business Systems
- Identity Services
- Network Services - DNS, DHCP
- Call Manager

Distribution Switch Stack
- Active/Standby
- Inter-zone traffic segmentation
- ACLs, IPS and IDS
- VPN Services
- Portal and Remote Desktop Services proxy

Cell/Area Zone - Levels 0–2
Redundant Star Topology - Flex Links Resiliency
Unified Wireless LAN (Lines, Machines, Skids, Equipment)

Cell/Area Zone - Levels 0–2
Ring Topology - Resilient Ethernet Protocol (REP)
Unified Wireless LAN (Lines, Machines, Skids, Equipment)

Cell/Area Zone - Levels 0–2
Linear/Bus/Star Topology
Autonomous Wireless LAN (Lines, Machines, Skids, Equipment)

Level 3 - Site Operations
(Control Room)
Converged Plantwide Ethernet (CPwE) Reference Architecture

Enterprise/IT Integration
- Collaboration
- Wireless
- Application Optimization

Enterprise Zone (Levels 4-5)
- Physical or Virtualized Servers
- FactoryTalk Application Servers and Services Platform
- Network & Security Services – DNS, DHCP, Identity Services (AAA)
- Storage Array
- Remote Desktop Gateway Server

Industrial Demilitarized Zone (IDMZ)

Wide Area Network (WAN)
- Data Center - Virtualized Servers
  - ERP - Business Systems
  - Email, Web Services
  - Security Services - Active Directory (AD), Identity Services (AAA)
  - Network Services – DNS, DHCP
  - Call Manager

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

Remote Access Server

Patch Management
- AV Server
- Application Mirror
- Remote Desktop Gateway Server

IPhone

Active/Standby

IPS and IDS

Portal and Remote Desktop Services proxy

Camera

Controller

WGB

Level 3 - Site Operations
( Control Room)

Enterprise/IT Integration

Collaboration

Wireless

Application Optimization

Application and Data Share

Access Control

Threat Protection

Site Operations and Control

Multi-Service Networks

Network and Security Management

Routing

EtherNet/IP

PROFINET (Industrial Protocols)

Real-Time Control

Fast Convergence

Traffic Segmentation and Management

Ease of Use

Cell/Area Zone - Levels 0–2

Redundant Star Topology - Flex Links Resiliency

Unified Wireless LAN (Lines, Machines, Skids, Equipment)

Cell/Area Zone - Levels 0–2

Ring Topology - Resilient Ethernet Protocol (REP)

Unified Wireless LAN (Lines, Machines, Skids, Equipment)

Cell/Area Zone - Levels 0–2

Autonomous Wireless LAN (Lines, Machines, Skids, Equipment)
Connected Factory Reference Architectures

Converged Plantwide Ethernet (CPwE)

- Tested, validated and documented reference architectures
  - Developed from use cases - customer and application
  - Tested for performance, availability, repeatability, scalability and security
  - Comprised of Cisco® and Rockwell Automation® Validated Designs

- Built on technology and industry standards
- “Future-ready” network design
- Content relevant to both OT and IT Engineers

- Deliverables
  - Recommendations, best practices, design and implementation guidance, documented test results and configuration settings
  - Simplified design, quicker deployment, reduced risk in deploying new technology
Networking Best Practices – Cell/Area Zone

Best Practices For Reducing Latency and Jitter, and to Increase Data Availability, Integrity and Security

• IP Multicast Control
  • IGMP Management

• Segmentation
  • Virtual LANs (VLANs)

• Prioritization
  • Quality of Service (QoS)

• Apply Resiliency Protocols and multi-path topologies
  • Use Fiber-media uplinks for fast convergence

• Defense-in-Depth Security
Cell/Area Zone Overview

Cell/Area Zone - Functional Area of a Production Facility. Considerations Include:

- Environmental constraints
- Range of device intelligence
- Time-sensitive applications
Typical Cell/Area Zone Traffic Flows

CIP Implicit - 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 - Informational control and administration
- Intra- and inter-cell/area zone traffic flow
- Non-critical administrative or data traffic using TCP
  - ~1500 Bytes, infrequent
  - Above 500 ms
Resiliency for Industrial Applications
Supporting Multiple Topologies

- Ring Convergence
  - Resilient Ethernet Protocol (REP)
  - Achieves ~50 ms convergence in large, complex networks
- Redundant Star Convergence
  - Multiple protocol options
  - Convergence times of <100ms for Flexlinks and Etherchannel
- Tested with Rockwell applications and multicast traffic
- Fast convergence avoids application reset and improves uptime
- Critical for industrial applications

![Diagram showing network topologies with convergence examples]
Schneider EcoStructure Building Network
Industrial Network Topologies

Cell/Area Zone Topology Options

<table>
<thead>
<tr>
<th></th>
<th>Linear</th>
<th>Ring</th>
<th>Redundant Star</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cabling Requirements</td>
<td>⬜</td>
<td>⬜</td>
<td>⬜</td>
</tr>
<tr>
<td>Ease of Configuration</td>
<td>⬜</td>
<td>⬜</td>
<td>⬜</td>
</tr>
<tr>
<td>Implementation Costs</td>
<td>⬜</td>
<td>⬜</td>
<td>⬜</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>⬜</td>
<td>⬜</td>
<td>⬜</td>
</tr>
<tr>
<td>Redundancy and Convergence</td>
<td>⬜</td>
<td>⬜</td>
<td>⬜</td>
</tr>
<tr>
<td>Disruption During Network Upgrade</td>
<td>⬜</td>
<td>⬜</td>
<td>⬜</td>
</tr>
<tr>
<td>Readiness for Network Convergence</td>
<td>⬜</td>
<td>⬜</td>
<td>⬜</td>
</tr>
<tr>
<td>Overall in Network TCO and Performance</td>
<td>Worst</td>
<td>OK</td>
<td>Best</td>
</tr>
</tbody>
</table>
# Network Resiliency Protocols

Selection is Application Driven

<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>

* Not part of CPwE

- Process and Information
- Time Critical
- Loss Critical
Security - an enabler of IoT and ISA 99

- Increased resiliency
- Integrated OT/IT security
- Industrial threat protection
- Simplified compliance
- Secure connectivity
- Unmanaged switch replacement

**Securely Connect**  
**Increase Resilience**  
**Simplify Operations**
Security Architecture for IoT

- Device hardening with 802.1AR and ACT2 security chip
- Network hardening tools
- Certificate-based identities, user names & passwords
- Role based Access Control
- 802.1x-based access control for meters, routers, grid devices
- Link-layer encryption in RF Mesh
- Group-based key generation and management (mesh)
- Network-layer encryption for WAN Backhaul (IPSec)

Secure Device Identity via Digital Certificates
Strong user identities with Role-Based Access

Time-stamped logs, correlation at SIEM
Separation of AMI vs. non-AMI traffic, segmentation

Secure storage for encryption keys
Secure encryption keys
Network-layer encryption (IPSec)
Link-layer encryption (AES-128)
Network Segmentation

- Default Auth policy on ISE for switchport is configured as “open access” – i.e. no NAC blocking
- PxGrid attribute “Cell-1” matches a Profiling policy on ISE and triggers corresponding Authorization policy
- ISE Authorization policy can be used to dynamically apply dACL, SGT or VLAN to switchports to segment the assets
- OT user and IT user are working with asset identities rather than IP addresses
Enabling IT-OT partnership to secure the OT network

Operational Environment
- Modbus
- CIP
- PROFINET
- BACNet

Industrial Network Director

IT / Security
- ISE
- pxGrid
- REST API

SGACL Segmentation
- IE Switching
- SGT dACL
- SXP
- pxGrid

IT / Security
- NGFW
- SGT Firewall Rules

Context based Host Groups
- Stealthwatch
How do we secure all this things?

Manufacturer Usage Description
IoT Device Business Challenges

**Device Visibility**
- Do you know devices well enough to differentiate service?

**Intent-based Policy**
- Does customer know the behavior of devices to build their policy?

**Standard based**
- Is there any industry standard way of connecting IoT devices to enterprise network?
MUD Ecosystem Architecture

**Phase 1: Visibility**
- Device emits a URL using DHCP, LLDP, or through 802.1x
- ISE receives MUD URI, Groups device and sends MUD URI to IOT Controller
- IOT Controller talks to MUD File server, downloads MUD File and applies policy on ISE
- ISE pushes DACL/SGACL (policies) to network devices
- Network devices implement and enforce desired policies

**Phase 2: Policy**

**Phase 3: Trusted Introduction**

- Manufacturer
- MUD File Server
- IOT Controller
- ISE
- Switches
- Critical IoT Asset
DevNet site commissioned to support developers

Manuafacturer Usage Description

MUD is an authoritative identifier of IoT devices on the network, as it allows manufacturers to expose the identity and intended use of their devices using an IETF approved standard. This bridges the gap between the manufacturer and the user, and facilitates a level of trust and security that network and security administrators truly value. Device manufacturers can thus enhance the security of their devices, and Integrators can leverage this to segment a network with “Things.”

Let's play in the MUD to make it stick
Benefits

Customer
- **Reduces threat surface** of exploding number of devices
- Almost no additional CAPEX
- Standard approach to determining manufacturer intent
- Eases and scales access management decisions

Manufacturer
- Reduces manufacturer product risk at almost no cost
- Will increase customer satisfaction and reduce support costs
- **Avoids the front page**
- **Standards-based approach**
Cisco Validated Design (CVD)

Converged Plantwide Ethernet (CPwE) Design and Implementation Guide

Updated: September 9, 2011

EcoStruxure Building Ethernet Network Design for MP Series Controllers

How to combine Cisco Industrial Ethernet Switches with the EcoStruxure Building system to create a secure and resilient BMS architecture

Cisco Connected Factory—PROFINET Wireless Design and Implementation Guide

First Published: October 2017

Network Solution Guide

Document Version 1.2.1 September 22, 2018