Substation Communications Design - Legacy to IEC 61850

Part 3/3: Reliability & Security

Tim Wallaert
Chris Jenkins
Agenda

• Substation to the Control Room Communications
  - Legacy networks
  - Networking today
  - CIP
  - Hardened equipment

• How to Build a Redundant Network
  - RSTP
  - MRP
  - Routing
  - Router
  - Cellular
  - PRP/HSR

• How to Lock it Down
  - Firewalls
  - VPN
  - Port Security
  - Authentication
Legacy Utility Networks

1200 baud
Modem Bank
SCADA Master

Leased Lines
Distributed Substations

Administration
Dial-in
Today’s Digital Networks

Master Site

Wide Area Network

SCADA/EMS

RTU Management & Provisioning

PBX

GW

Term Server

Switch

Video Monitoring

Video Storage

HMI

POE

VOIP

Enet IED

Serial IED

Sub A

Sub B

Sub C
New networks have to be compliant…

• What does “compliance” mean?
• FERC/NERC-CIP
  - Federal Energy Regulatory Commission
  - North American Electric Reliability Corporation
• http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx
• Critical Infrastructure Protection (CIP)
  • Version 1 enforced in 2008
  • Currently enforcing Version 3
  • Version 4 has been approved, April 2014 deadline
  • Still to be approved Version 5 is being pushed to replace Version 4
  • Version 5 has MANY changes including:
    • Encryption
    • Multi-Factor Authentication
Federal Regulation

• Critical Infrastructure Protection (CIP) is a group of standards enforced by NERC

• NERC does not certify equipment

• There is no such thing as a “CIP certified router”

• Belden provides equipment that enables customers to design and implement networks that are CIP compliant

• Constantly monitoring NERC for changes in standards and listening to feedback from our customers
“I need to upgrade my network and stay compliant, but how?”
Turn to a Trusted Leader

Belden delivers highly engineered signal transmission products for mission-critical applications in a diverse set of global markets.
Solutions Portfolio
Important Specs to Consider

• Experienced, Reliable Vendor

• Standards Based Equipment

• Environment
  ▪ Extended Temp ranges
  ▪ Noise Immunity
  ▪ IEEE1613
  ▪ IEEE61850-3
# Important Specs to Consider

<table>
<thead>
<tr>
<th>ESD</th>
<th><strong>IEEE 1613</strong></th>
<th><strong>IEC 61850-3</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact 8kV</td>
<td>8kV</td>
<td>Contact 8kV</td>
</tr>
<tr>
<td>Air 15kV</td>
<td></td>
<td>Air 15kV</td>
</tr>
<tr>
<td>Radiated RF</td>
<td>35V/M</td>
<td>Radiated RF</td>
</tr>
<tr>
<td>I/O ports 4kV</td>
<td>4kV</td>
<td>I/O ports 4kV</td>
</tr>
<tr>
<td>Power ports (HV and LV) 4kV</td>
<td>4kV</td>
<td>Power ports (HV and LV) 4kV</td>
</tr>
<tr>
<td>Oscillatory</td>
<td>2.5kV</td>
<td>Oscillatory</td>
</tr>
<tr>
<td>I/O ports 2.5kV</td>
<td></td>
<td>I/O ports 2.5kV</td>
</tr>
<tr>
<td>Power ports (HV and LV) 2.5kV</td>
<td>2.5kV</td>
<td>Power ports (HV and LV) 2.5kV</td>
</tr>
<tr>
<td>Dielectric Strength</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HV power ports 3kV</td>
<td></td>
<td>Conducted RF Pass</td>
</tr>
<tr>
<td>LV power ports 2kV</td>
<td></td>
<td>Power ports (HV and LV) 10V</td>
</tr>
<tr>
<td>Operating Temperature</td>
<td>-40 to +85°C</td>
<td>Magnetic Field Pass</td>
</tr>
<tr>
<td></td>
<td></td>
<td>30A/m</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Voltage Dips &amp; Interrupts Pass</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(HV power ports)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Pass)</td>
</tr>
</tbody>
</table>
Important Specs to Consider

- Redundant Power options
  - Low and High voltage options
  - Dual power supply features
  - Hot Swappable
Important Specs to Consider

• Redundancy features
  - Serial Port
  - RSTP
  - MRP
  - RIP, OSPF, BGP
  - VRRP
  - Cellular redundancy
  - PRP/HSR

• Security
  - Encryption
  - Authentication
  - Firewalls
  - Detection
Redundancy Features
Serial Redundancy

Master Site

SCADA/EMS
Video Monitoring
Term Server
PBX
GW
Switch
Video Storage

RTU Management & Provisioning

Wide Area Network

Sub A

HMI
VOIP
Enet IED
Serial IED
PoE

Sub B

HMI
VOIP
Enet IED
Serial IED
PoE

Sub C

HMI
VOIP
Enet IED
Serial IED
PoE
Serial Redundancy

Master Site

Backup Site

Sub A

Sub B

Sub C

Poll

SCADA/EMS

Video Monitoring

Term Server

Term Server

Video Monitoring

Wide Area Network

HMI

VOIP

PoE

Enet IED

Serial IED

HMI

VOIP

PoE

Enet IED

Serial IED

HMI

VOIP

PoE

Enet IED

Serial IED

RESP

RESP

Backup Site

SCADA/EMS

Video Monitoring

Mast Site

Term Server

Video Monitoring

Term Server

Video Monitoring

Wide Area Network

HMI

VOIP

PoE

Enet IED

Serial IED

HMI

VOIP

PoE

Enet IED

Serial IED

HMI

VOIP

PoE

Enet IED

Serial IED

Term Server

Video Monitoring

Term Server

Video Monitoring

Wide Area Network

HMI

VOIP

PoE

Enet IED

Serial IED

HMI

VOIP

PoE

Enet IED

Serial IED

HMI

VOIP

PoE

Enet IED

Serial IED

Term Server

Video Monitoring

Term Server

Video Monitoring

Wide Area Network

HMI

VOIP

PoE

Enet IED

Serial IED

HMI

VOIP

PoE

Enet IED

Serial IED

HMI

VOIP

PoE

Enet IED

Serial IED
# Ethernet Redundancy Protocols

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Current Standard</th>
<th>Typical Re-Config</th>
<th>Topology</th>
<th>Available since</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parallel Redundancy Protocol (PRP)</td>
<td>IEC 62439-3:2012-07</td>
<td>0mS</td>
<td>Any topology/mesh</td>
<td>2010</td>
</tr>
<tr>
<td>High-Availability Seamless Redundancy (HSR)</td>
<td>IEC 62439-3:2012-07</td>
<td>0mS</td>
<td>Pure Ring Only</td>
<td>2010</td>
</tr>
<tr>
<td>Rapid Spanning Tree Protocol (RSTP)</td>
<td>IEEE 802.1D-2004</td>
<td>5-20mS per switch</td>
<td>Any topology/mesh</td>
<td>2004</td>
</tr>
<tr>
<td>Open Shortest Path First (OSPF)</td>
<td>RFC 2328</td>
<td>seamless</td>
<td>Any topology/mesh</td>
<td>1987/1998</td>
</tr>
</tbody>
</table>
RSTP Redundancy
Rapid Spanning Tree Protocol (RSTP) Bridging

Master Site
- SCADA/EMS
- Video Monitoring
- Term Server
- Switch
- Video Storage
- BPDU

Sub A
- HMI
- VOIP
- PoE
- Enet IED
- Serial IED

Sub B
- HMI
- PoE
- Enet IED
- Serial IED

Sub C
- HMI
- PoE
- VOIP
- IED
- Serial IED
- Serial IED
- Serial IED
- Serial IED

RTU Management & Provisioning
- PBX
- GW
Rapid Spanning Tree Protocol (RSTP) Bridging

Master Site

SCADA/EMS
Video Monitoring

DATA

DATA

PBX

GW

Switch

Video Storage

RTU Management & Provisioning

Sub A

HMI

POE

Enet IED

Serial IED

Sub B

HMI

POE

Enet IED

Serial IED

Sub C

HMI

POE

Enet IED

Serial IED

~5 - 15ms recovery
MRP Redundancy
Media Redundancy Protocol (MRP)

Master Site

SCADA/EMS

Term Server

PBX

GW

Switch

Video Monitoring

Video Storage

Ring Switch

HELLO

*10mS recovery

Sub B

RTU Management & Provisioning

Sub C

Ring Switch

Ring Manager

* 50 switches per ring max

Sub C

HMI

VOIP

PoE

SERIAL IED

IED

Sub C

HMI

VOIP

PoE

SERIAL IED

IED

* 50 switches per ring max
Routing Protocol
Redundancy
Routing Protocols RIP, OSPF, BGP
Routing Protocols RIP, OSPF, BGP

Substation A is over here

Substation B is over here

Substation C is over here
Routing Protocols RIP, OSPF, BGP

Master Site

SCADA/EMS

Term Server

PBX

GW

Video Storage

Video Monitoring

Sub A

HMI

VOIP

Enet IED

Serial IED

Sub B

HMI

Enet IED

Serial IED

Sub C

HMI

Enet IED

Serial IED

Wide Area Network

Routing Protocols RIP, OSPF, BGP
Router Redundancy
Virtual Router Redundancy Protocol (VRRP)
Virtual Router Redundancy Protocol (VRRP)
Virtual Router Redundancy Protocol (VRRP)
Virtual Router Redundancy Protocol (VRRP)

Master Site
- SCADA/EMS
- Term Server
- Video Monitoring
- RTU Management & Provisioning

Slave Router(s)
- Master Router
- Switch
- Video Storage
- Wide Area Network

DATA
Cellular Redundancy
Before Cellular

Master Site

SCADA/EMS

Video Monitoring

Term Server

PBX

GW

RTU Management & Provisioning

Switch

Video Storage

Wide Area Network

Sub A

DATA

HMI

PoE

VOIP

Enet

Serial

Serial

IED

IED

IED
Before Cellular

Master Site

SCADA/EMS

ATA

PBX

GW

Term Server

Switch

Video Monitoring

Video Storage

RTU Management & Provisioning

Wide Area Network

HMI

PoE

VOIP

Enet IED

Serial IED

Sub A

© 2014 Belden Inc. | belden.com | @BeldenInc
Cellular Backup

Master Site

SCADA/EMS

Video Monitoring

Term Server

PBX

GW

Switch

Video Storage

Wide Area Network

Verizon Wireless Internet

Sub A

HMI

POE

Enet IED

Serial IED

Serial IED

DATA

SciDAC

VoIP

DATA

© 2014 Belden Inc. | belden.com | @BeldenInc
PRP/HSR Redundancy
Parallel Redundancy Protocol (PRP)

Zero failover with Network Redundancy

- Two redundant networks
- By doubling the packets no data loss if one packet fails
- PRP-Redundancy-Box = bidirectional splitter and combiner

IEC62439 PRP Network

- DAN Dual Attached Node
- SAN Single Attached Node

“0ms” recovery

Non PRP devices

By doubling the packets no data loss if one packet fails

PRP-Redundancy-Box = bidirectional splitter and combiner
High-Available Seamless Redundancy (HSR)

No packet loss
Security
Today’s Networks
Defense in Depth

Wide Area Network

HMI

PoE

VOIP

Enet IED

Serial IED

SCADA

IT

Engineering

Enet IED

Serial IED

Serial IED

Sub
Firewalls

- Integrated or standalone device that can be configured to allow or block specific traffic and users
- DX/10Series Routers offer integrated Firewall features
- Eagles are standalone devices
Firewalls

- Firewall with Stateful Packet Inspection (SPI)
  - Both IP and MAC address filtering supported
- Network Address Translation (NAT)
- VPN support

Eagle

10XTS, 10ETS, 10RX

DX
Eagle 20 Tofino – Firewall + DPI

- Firewall with Stateful Packet Inspection (SPI)
- Layer 2 Bridge with No IP Address
  - No disruption to existing network design
  - VERY secure
- Content Inspection filters traffic at the protocol level (Deep Packet Inspection)
  - Modbus/TCP
  - others to follow
- Simple deployment, configuration and management
Tofino™ Modbus TCP Enforcer LSM: Content Inspector for Modbus

- Protocol ‘Sanity Check’ blocks any traffic not conforming to the Modbus standard
- Control engineer defines list of allowed Modbus commands, registers and coils
- Automatically blocks and reports any Modbus traffic that does not match your rules
VPN
Virtual Private Networks

Master Site

Encrypted using IPSec

Sub A

Sub B

Sub C

Virtual Private Networks
Security - VPN

- Hardware and software encryption
- Multiple tunnel support
- Pre-Shared Key (PSK) or X.509 Certificates
- IPSec
- DX/10Series Routers offer integrated VPN features
- Eagles are standalone devices
Port Security
Port Security

- Default with all ports “administratively set to DOWN”
- Some devices support “no tail ending”. Port is locked after being unplugged. Must be enabled by administrator
- Physical port security devices

- Unusual port connectors provide a small level of security

<table>
<thead>
<tr>
<th>Figure</th>
<th>Pin</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>1</td>
<td>TD+ Transmit Data +</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>RD+ Receive Data +</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>TD- Transmit Data -</td>
</tr>
<tr>
<td>1</td>
<td>4</td>
<td>RD- Receive Data -</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Housing: shield</td>
</tr>
</tbody>
</table>
MAC Based Port Security

- Secures physical ports by applying a MAC based filter on a per port basis which allows only the authorized MAC address to forward traffic from the given port.

<table>
<thead>
<tr>
<th>Port</th>
<th>Port Status</th>
<th>Allowed MAC Addresses</th>
<th>Current MAC Address</th>
<th>Allowed IP Addresses</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>enabled</td>
<td>00:80:63:00:00:00/24</td>
<td>00:00:00:00:00:00</td>
<td>none</td>
<td>portDisable</td>
</tr>
<tr>
<td>1.2</td>
<td>enabled</td>
<td>00:00:00:00:00:00</td>
<td>00:00:00:00:00:00</td>
<td>none</td>
<td>none</td>
</tr>
<tr>
<td>1.3</td>
<td>enabled</td>
<td>00:00:00:00:00:00</td>
<td>00:00:00:00:00:00</td>
<td>none</td>
<td>none</td>
</tr>
<tr>
<td>1.4</td>
<td>enabled</td>
<td>00:00:00:00:00:00</td>
<td>00:00:00:00:00:00</td>
<td>none</td>
<td>none</td>
</tr>
<tr>
<td>1.5</td>
<td>enabled</td>
<td>00:00:00:00:00:00</td>
<td>00:00:00:00:00:00</td>
<td>none</td>
<td>none</td>
</tr>
<tr>
<td>1.6</td>
<td>enabled</td>
<td>00:1D:09:BD:81:D7</td>
<td>00:00:00:00:00:00</td>
<td>none</td>
<td>portDisable</td>
</tr>
<tr>
<td>1.7</td>
<td>enabled</td>
<td>00:80:63:78:2C:C9</td>
<td>00:00:00:00:00:00</td>
<td>none</td>
<td>none</td>
</tr>
<tr>
<td>1.8</td>
<td>enabled</td>
<td>00:1D:09:BD:81:D7 5C:26:0A:31:12:D5</td>
<td>00:00:00:00:00:00</td>
<td>none</td>
<td>portDisable</td>
</tr>
</tbody>
</table>
IP Based Port Security

- Secures physical ports by applying an IP based filter on a per port basis which allows only the authorized IP address to forward traffic from the given port.
Authentication
Authentication

• Switches and Routers support RADIUS Authentication
  - Protects access to the console ports
  - Authenticates users to the network
  - Helps satisfy CIP authentication requirements
Authentication

- Secure Access Servers
  - Subnet Solutions
  - CrossBow
  - Cooper Power

- Satisfies CIP access record keeping requirements
Summary

• Substation to the Control Room Communications
  - Legacy networks
  - Networking today
  - CIP
  - Hardened equipment

• How to Build a Redundant Network
  - RSTP
  - MRP
  - Routing
  - Router
  - Cellular
  - PRP/HSR

• How to Lock it Down
  - Firewalls
  - VPN
  - Port Security
  - Authentication
Top Three Takeaways

• Multiple Redundant protection schemes to pick from when designing/upgrading a network

• Security Features that support CIP compliant networking requirements

• Belden - Industry Leading Product Depth and Experience
Additional Resources & Assistance

1. Obtain further Substation Communication resources from our website:
   - [www.belden.com/power-td/](http://www.belden.com/power-td/)
   - This webpage includes substation communication diagrams and other useful tools

2. Contact a Belden representative for assistance:
   - Call 510-438-9071 if you are in the U.S. or Canada
   - Or complete the form at [www.belden.com/contact/](http://www.belden.com/contact/)

Thank you for your interest in this presentation!