Substation Communications Design - Legacy to IEC 61850

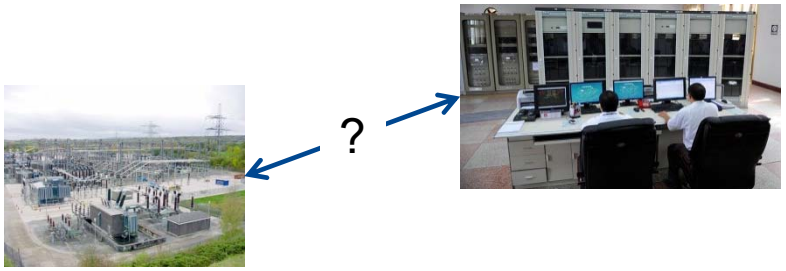
Part 3/3:
Reliability & Security

Tim Wallaert
Chris Jenkins

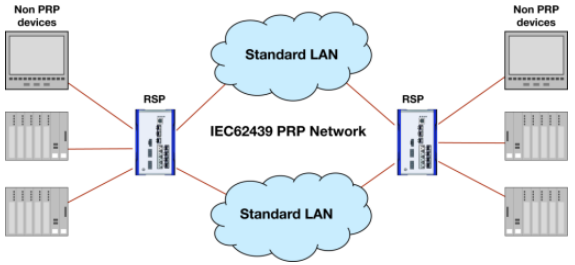
BELDEN
SENDING ALL THE RIGHT SIGNALS

Agenda

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

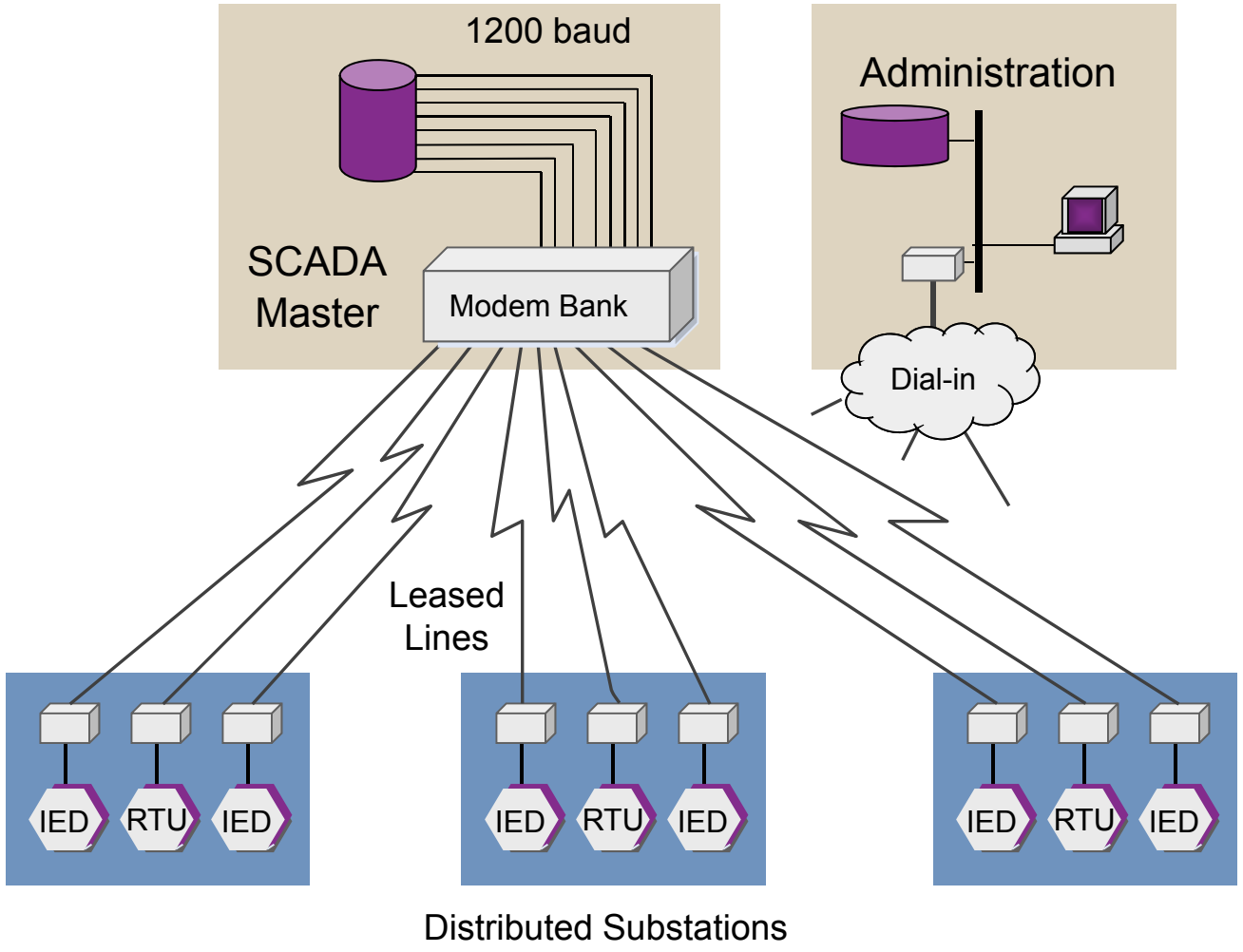


- How to Build a Redundant Network
  - RSTP
  - MRP
  - Routing
  - Router
  - Cellular
  - PRP/HSR

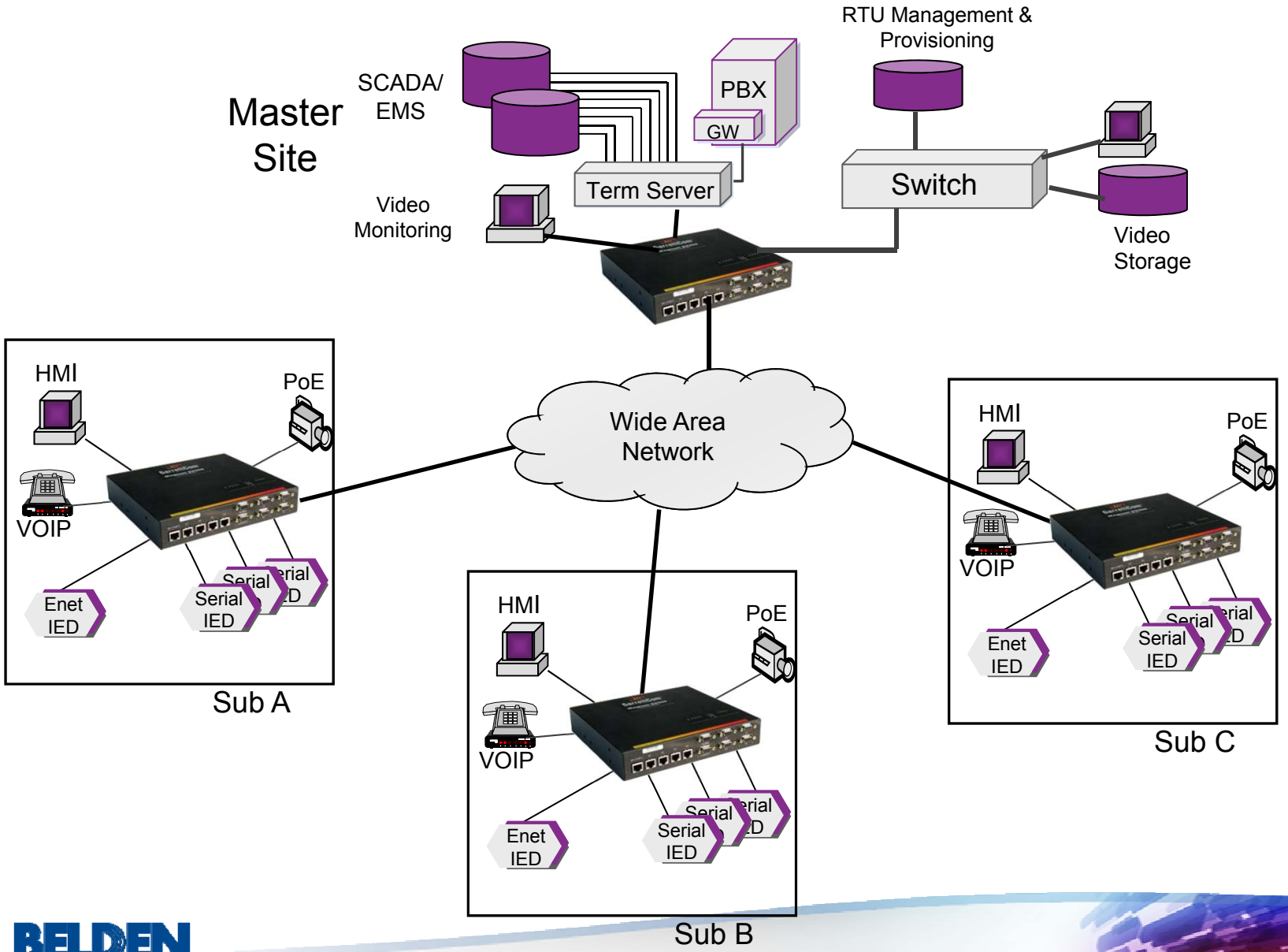


- How to Lock it Down
  - Firewalls
  - VPN
  - Port Security
  - Authentication

Legacy Utility Networks



Today's Digital Networks



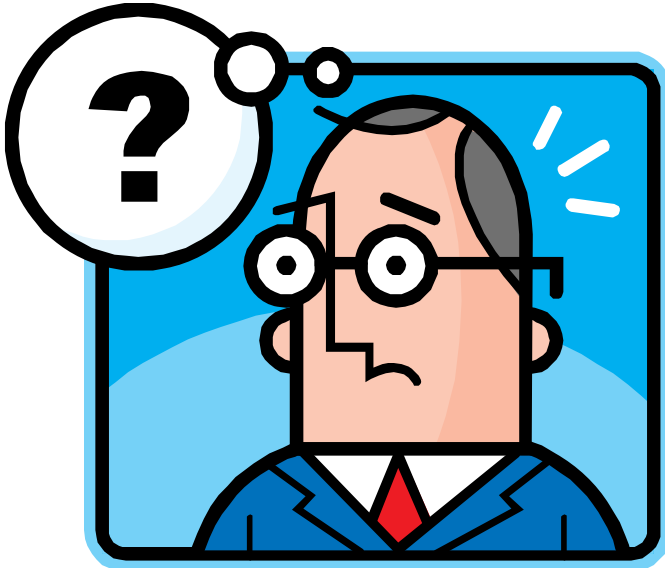
New networks have to be compliant…

- 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
SENDING ALL THE RIGHT SIGNALS

Belden delivers highly engineered signal transmission products for mission-critical applications in a diverse set of global markets

Product Platforms

- Networking
- Connectivity
- Cable

Applications

- Data
- Sound
- Video

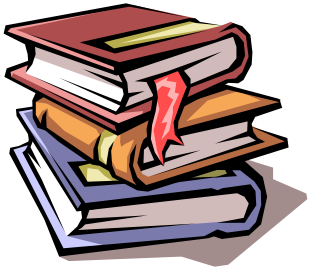
Vertical Markets

- Industrial
- Enterprise
- Broadcast
- Transportation
- Consumer Electronics

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

IEEE 1613

ESD	Contact	8kV
	Air	15kV
Radiated RF		35V/M
Fast Transient	I/O ports	4kV
	Power ports (HV and LV)	4kV
Oscillatory	I/O ports	2.5kV
	Power ports (HV and LV)	2.5kV
Dielectric Strength	HV power ports	3kV
	LV power ports	2kV
Operating Temperature		-40 to +85+ C

IEC 61850-3

ESD (61000-4-2)	Contact	8kV
	Air	15kV
Radiated RF (61000-4-3)		20V/M
Fast Transient (61000-4-4)	I/O ports	4kV
	Power ports (HV and LV)	4kV
Surge (61000-4-5)	I/O ports	4kV
	Power ports (HV and LV)	4kV
Conducted RF (61000-4-6)	I/O ports	10V
	Power ports (HV and LV)	10V
Magnetic Field (61000-4-8)		30A/m
Voltage Dips & Interrupts (61000-4-11)	HV power ports	Pass

Important Specs to Consider

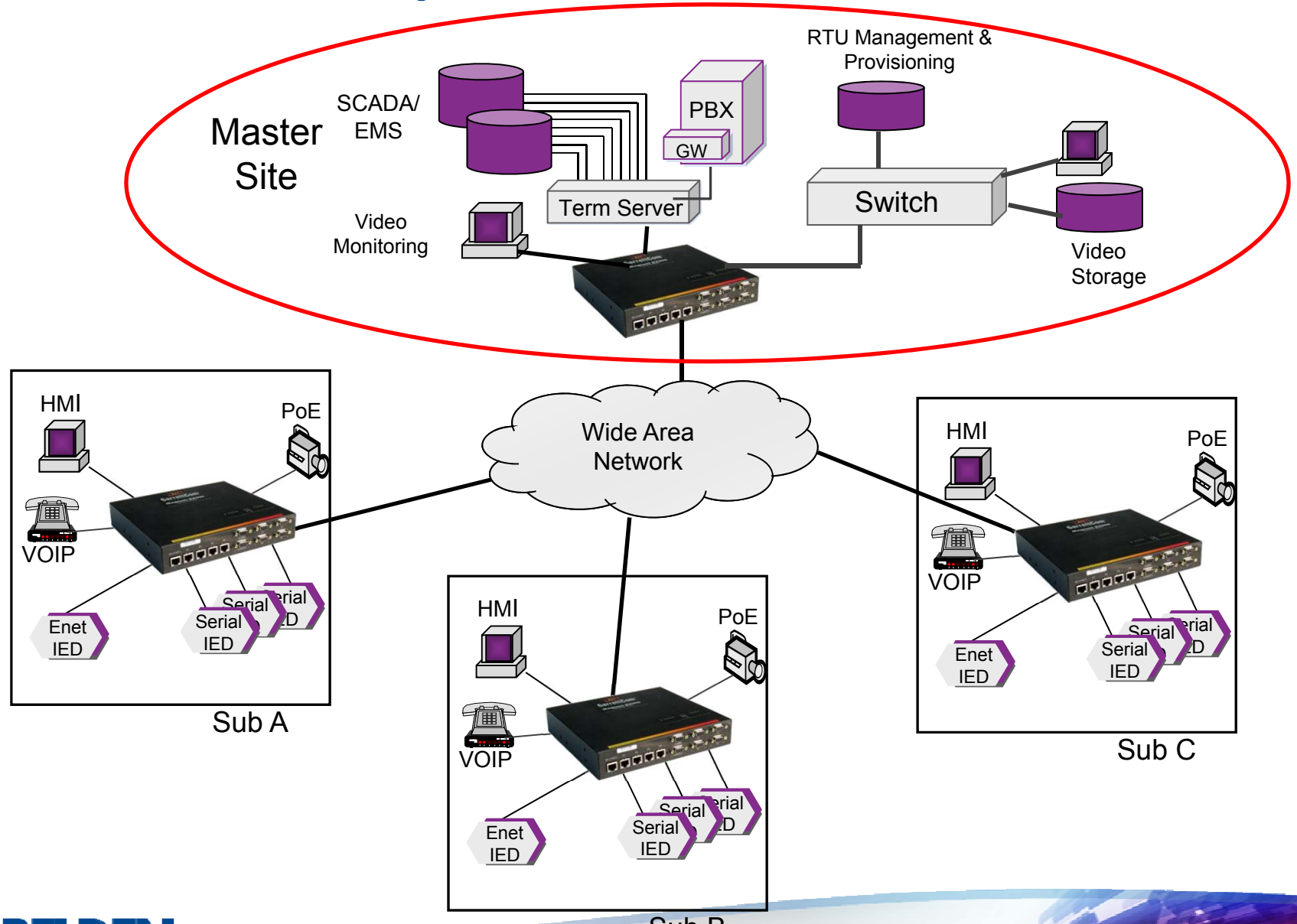
- Redundant Power options
  - Low and High voltage options
  - Dual power supply features
  - Hot Swappable

Important Specs to Consider

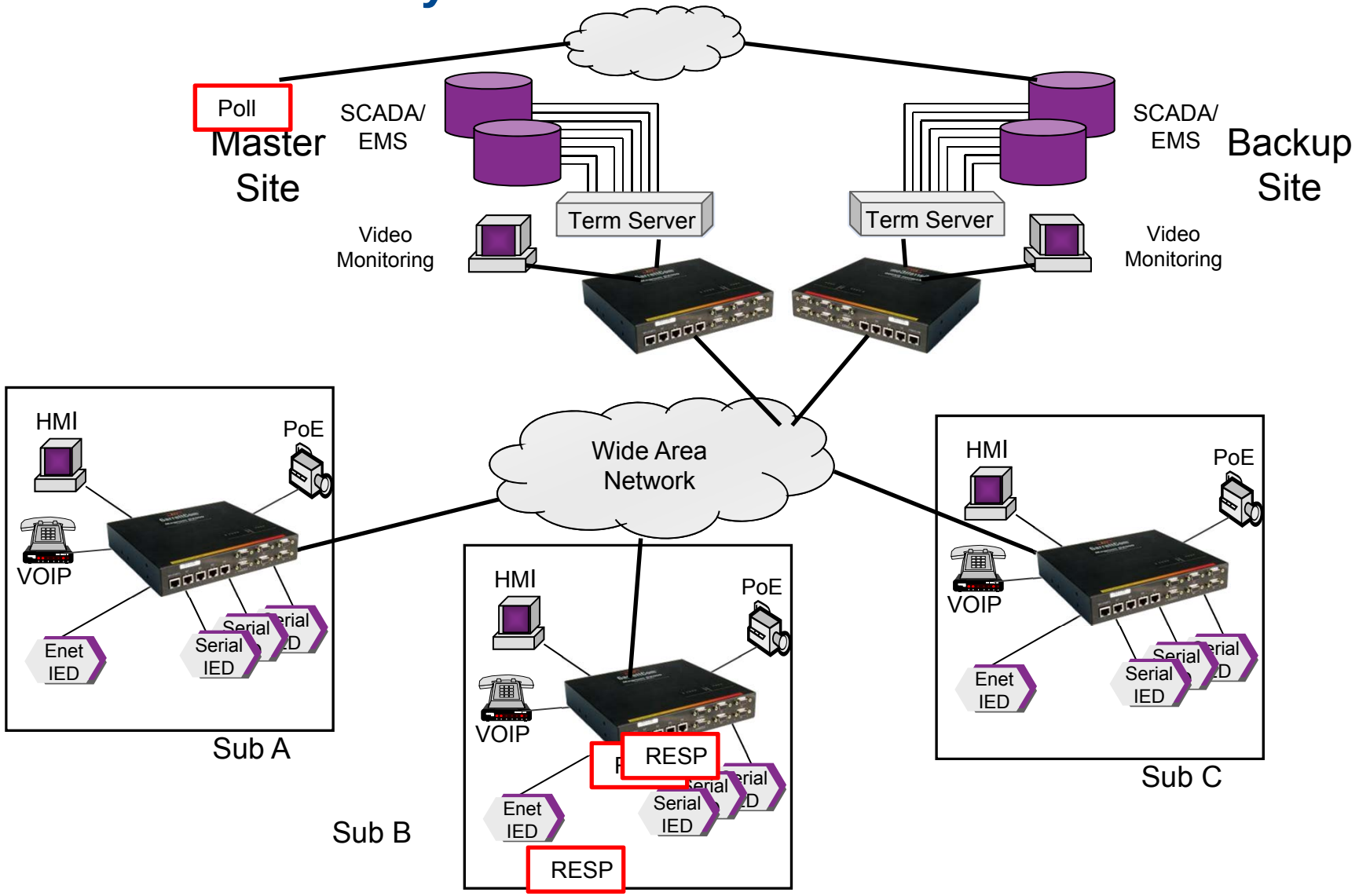
- Redundancy features
  - Serial Port
  - RSTP
  - MRP
  - RIP, OSPF, BGP
  - VRRP
  - Cellular redundancy
  - PRP/HSR
- Security
  - Encryption
  - Authentication
  - Firewalls
  - Detection

Redundancy Features

Serial Redundancy



Serial Redundancy



Ethernet Redundancy Protocols

Protocol	Current Standard	Typical Re-Config	Topology	Available since
Parallel Redundancy Protocol (PRP)	IEC 62439-3:2012-07	0mS	Any topology/mesh	2010
High-Availability Seamless Redundancy (HSR)	IEC 62439-3:2012-07	0mS	Pure Ring Only	2010
Rapid Spanning Tree Protocol (RSTP)	IEEE 802.1D-2004	5-20mS per switch	Any topology/mesh	2004
Media Redundancy Protocol (MRP)	IEC 62439-2:2010	200mS worst case, 50 switches max	Pure Ring Only	1998/2007
Routing Information Protocol (RIP & RIP 2)	RFC 1723	~30sec	small networks	1988/1994
Open Shortest Path First (OSPF)	RFC 2328	seamless	Any topology/mesh	1987/1998
Border Gateway Protocol (BGP)	RFC 4271	seamless	Any topology/mesh	1989/2006

RSTP Redundancy

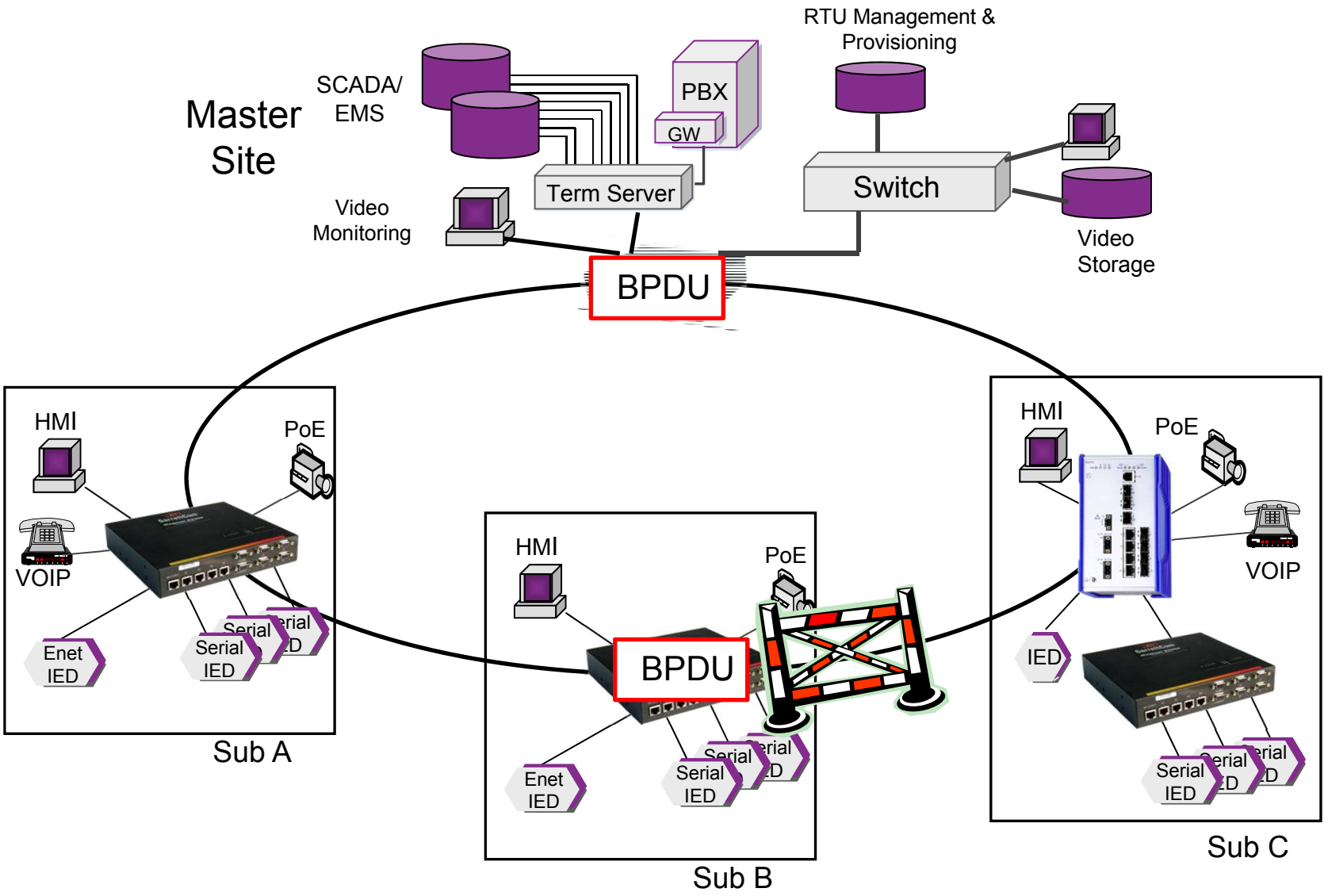
HIRSCHMANN

A BELDEN BRAND

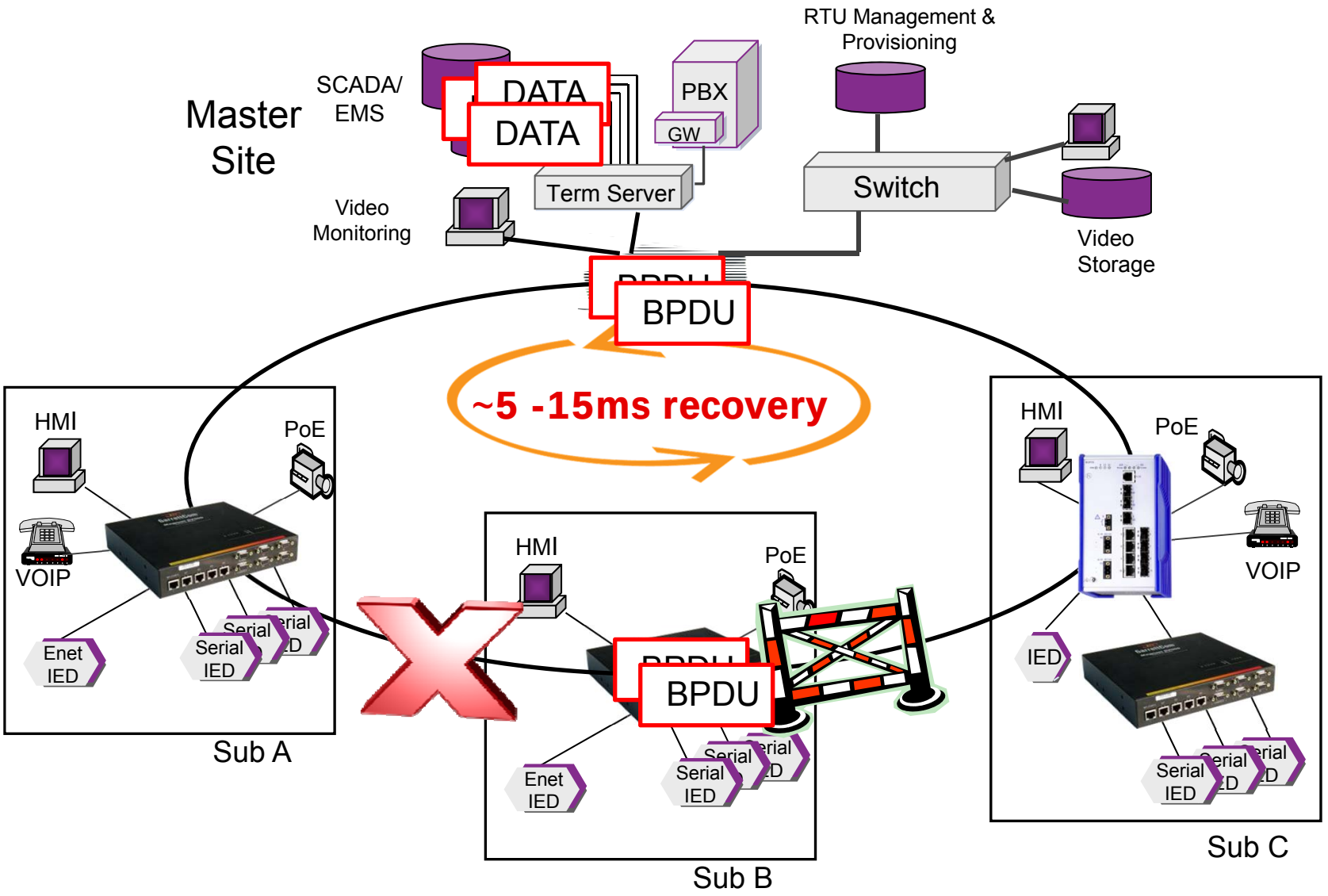
GarrettCom

A BELDEN BRAND

Rapid Spanning Tree Protocol (RSTP) Bridging

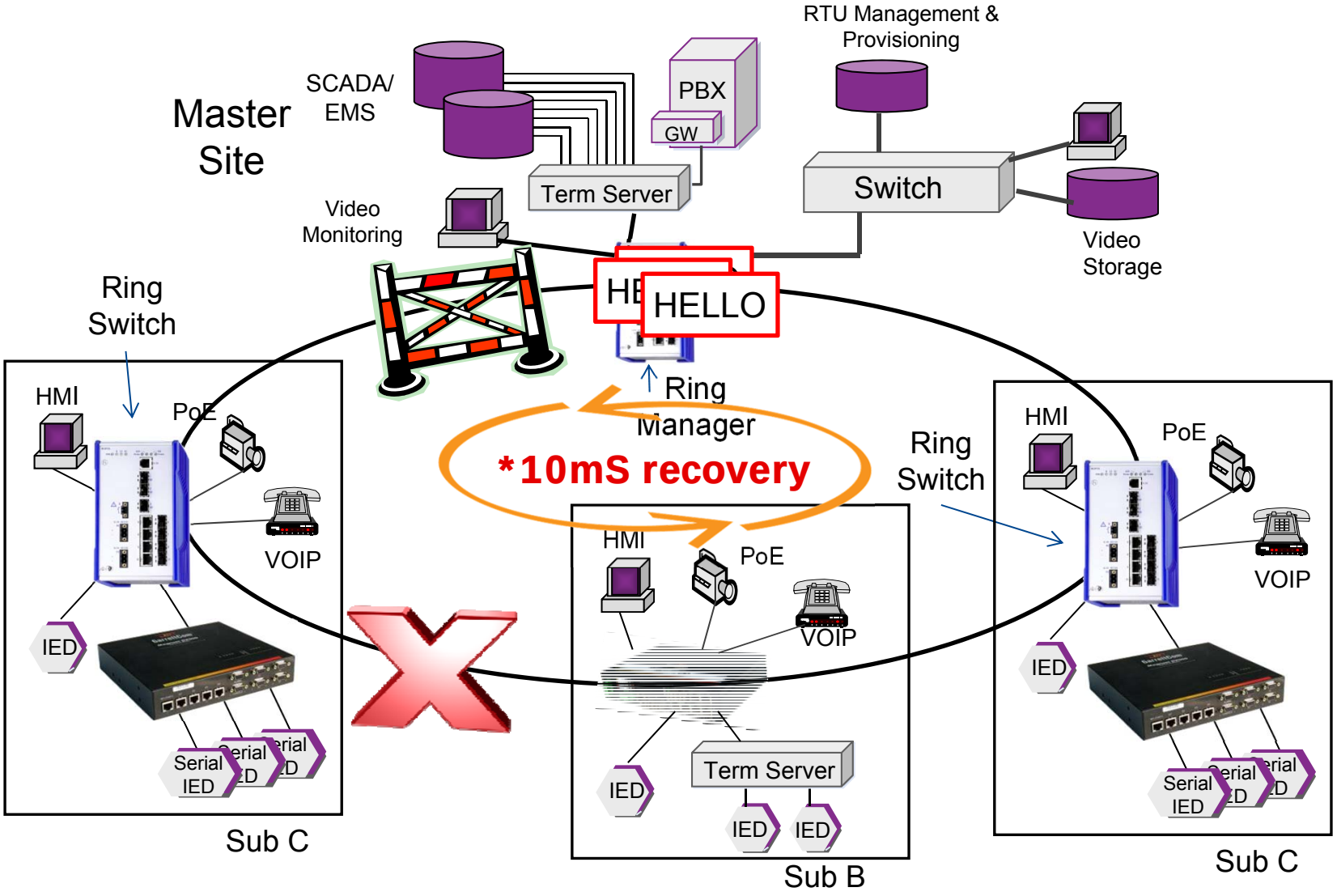


Rapid Spanning Tree Protocol (RSTP) Bridging



MRP Redundancy

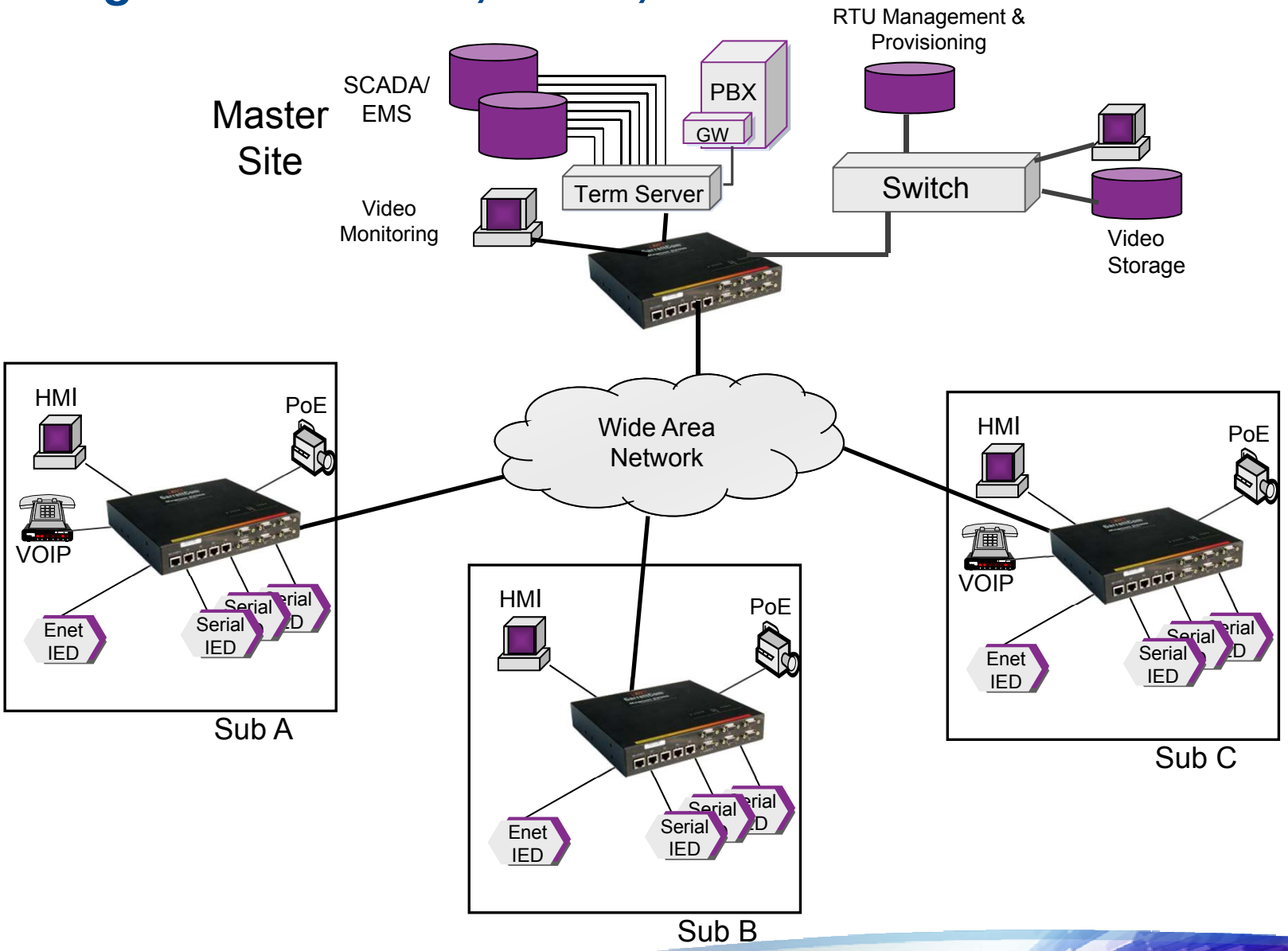
Media Redundancy Protocol (MRP)



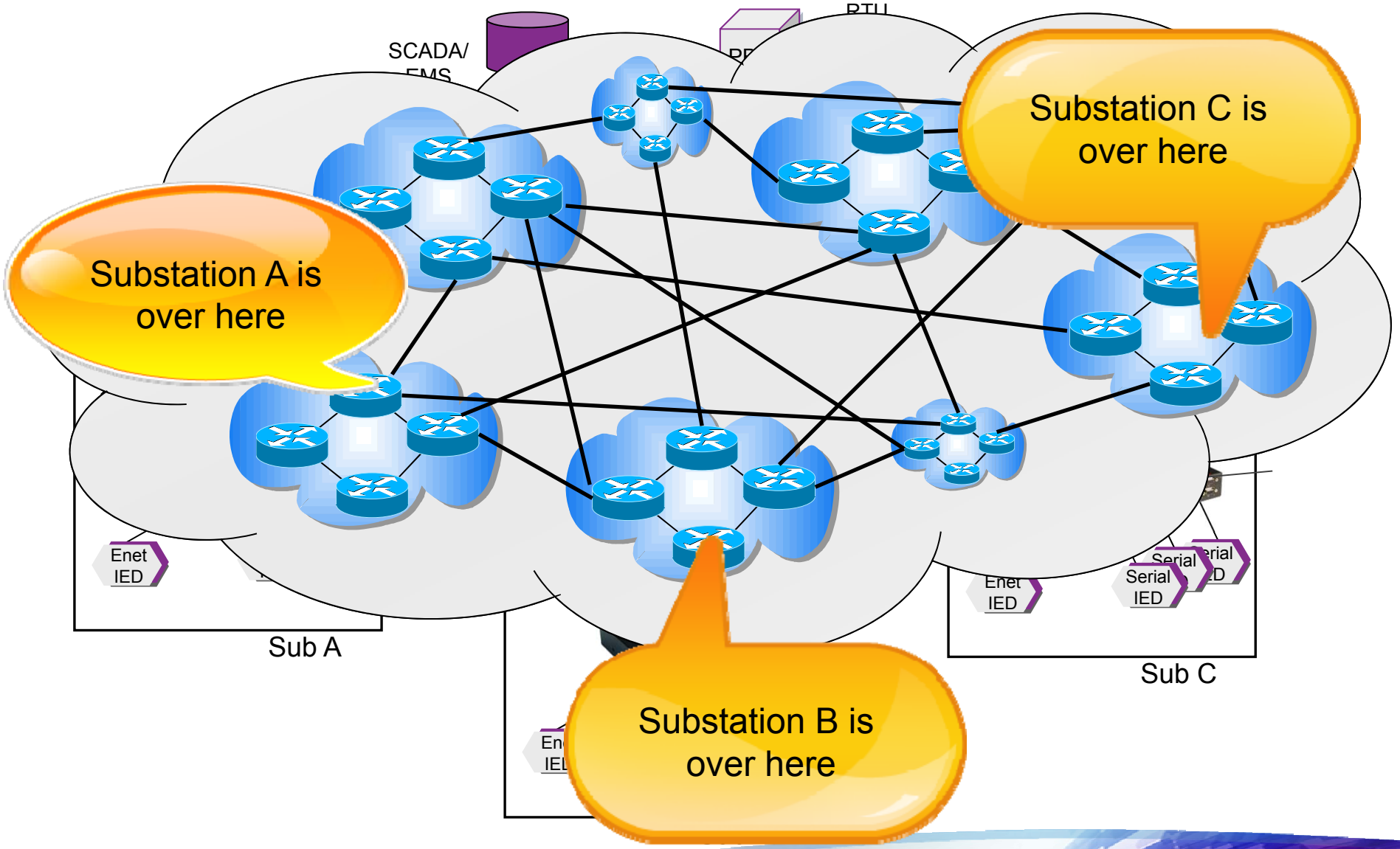
* 50 switches per ring max

Routing Protocol Redundancy

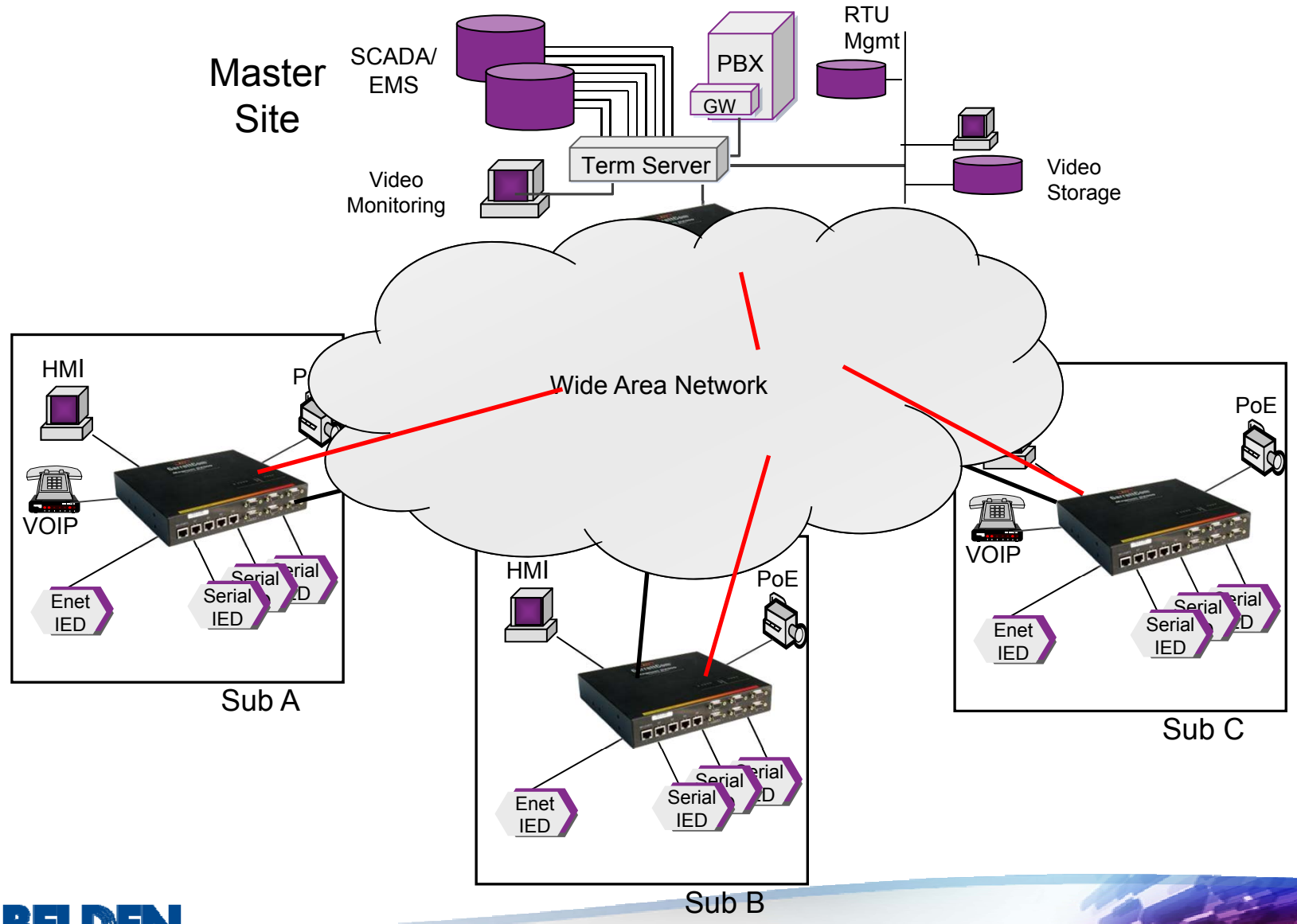
Routing Protocols RIP, OSPF, BGP



Routing Protocols RIP, OSPF, BGP

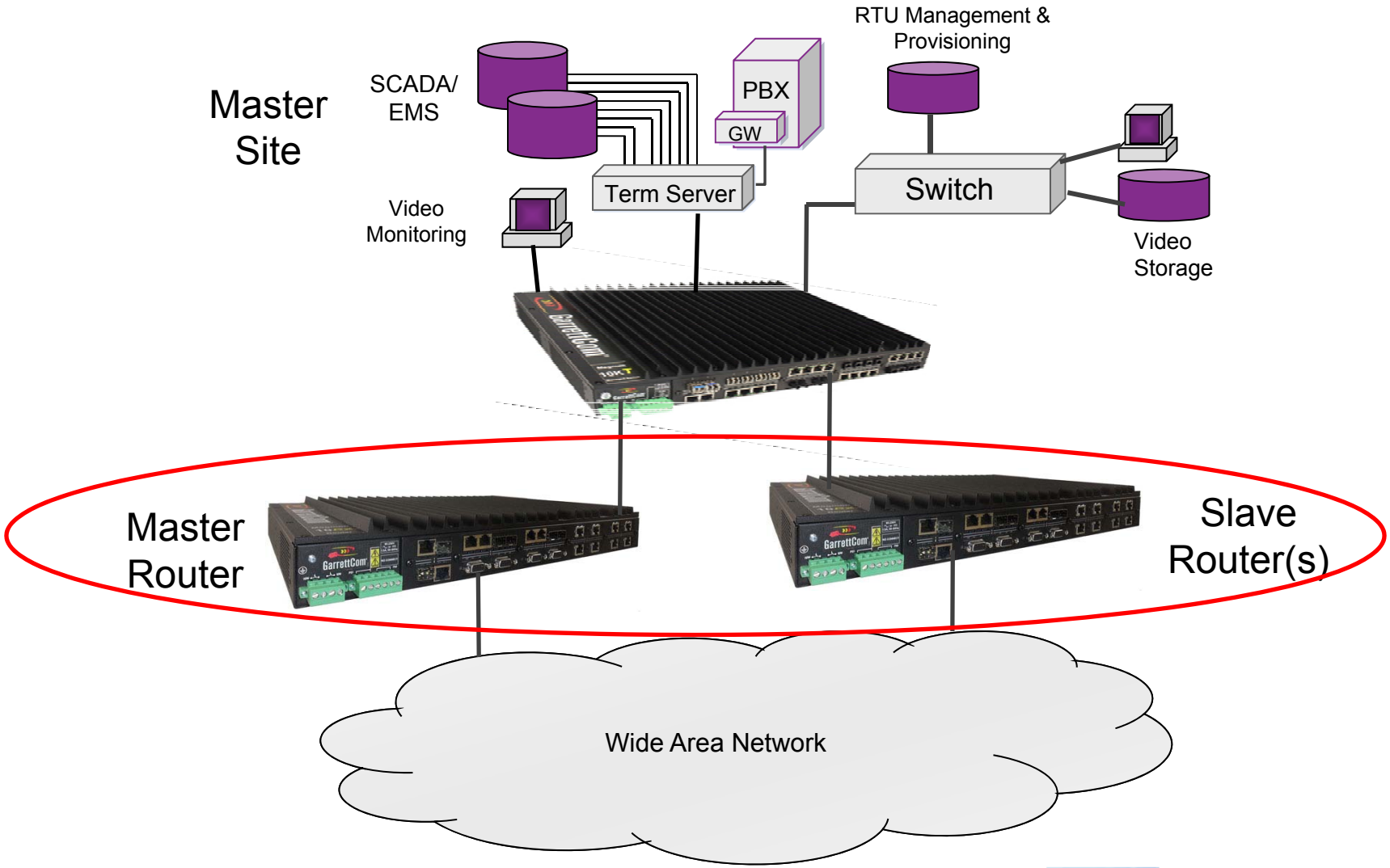


Routing Protocols RIP, OSPF, BGP

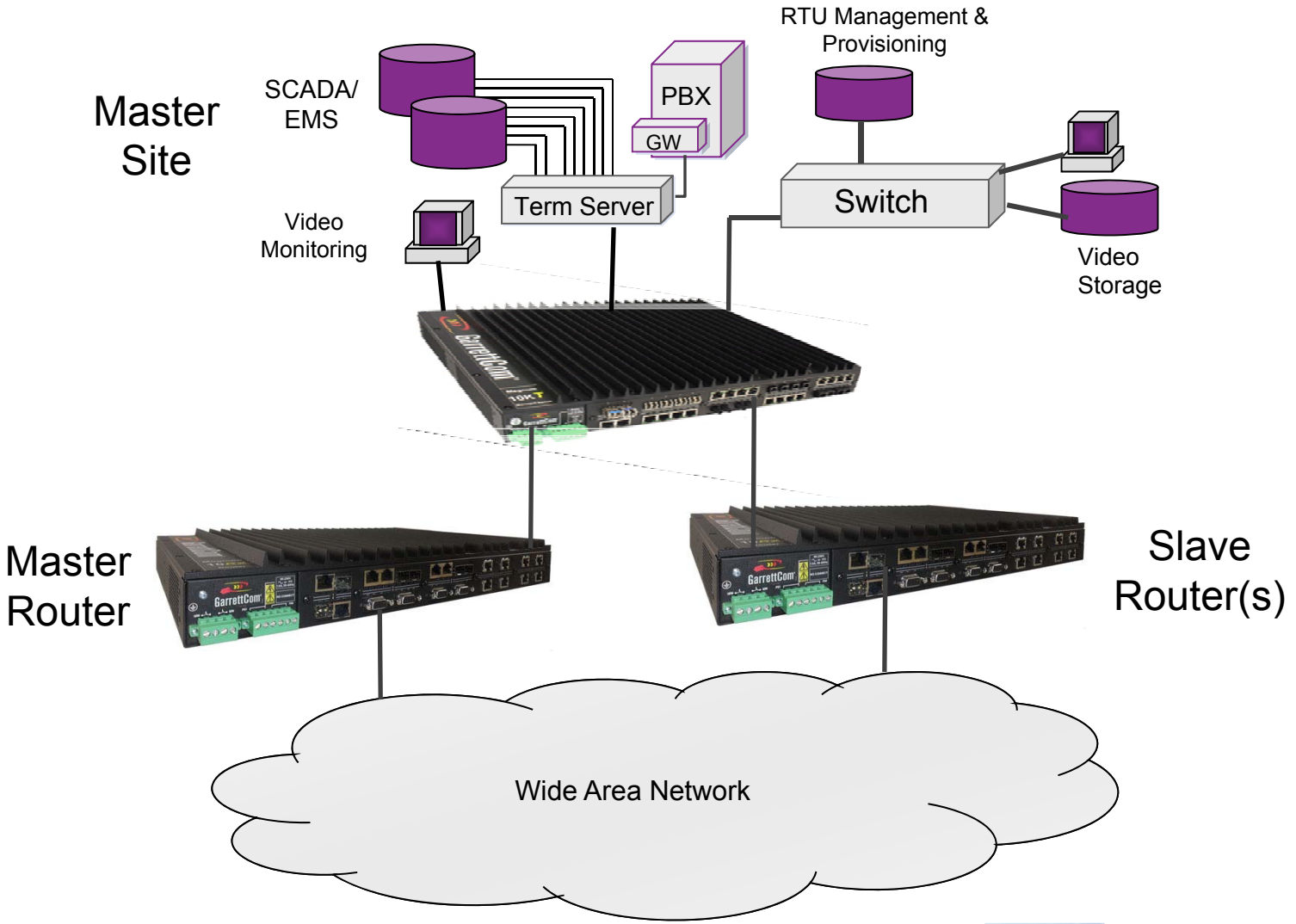


Router Redundancy

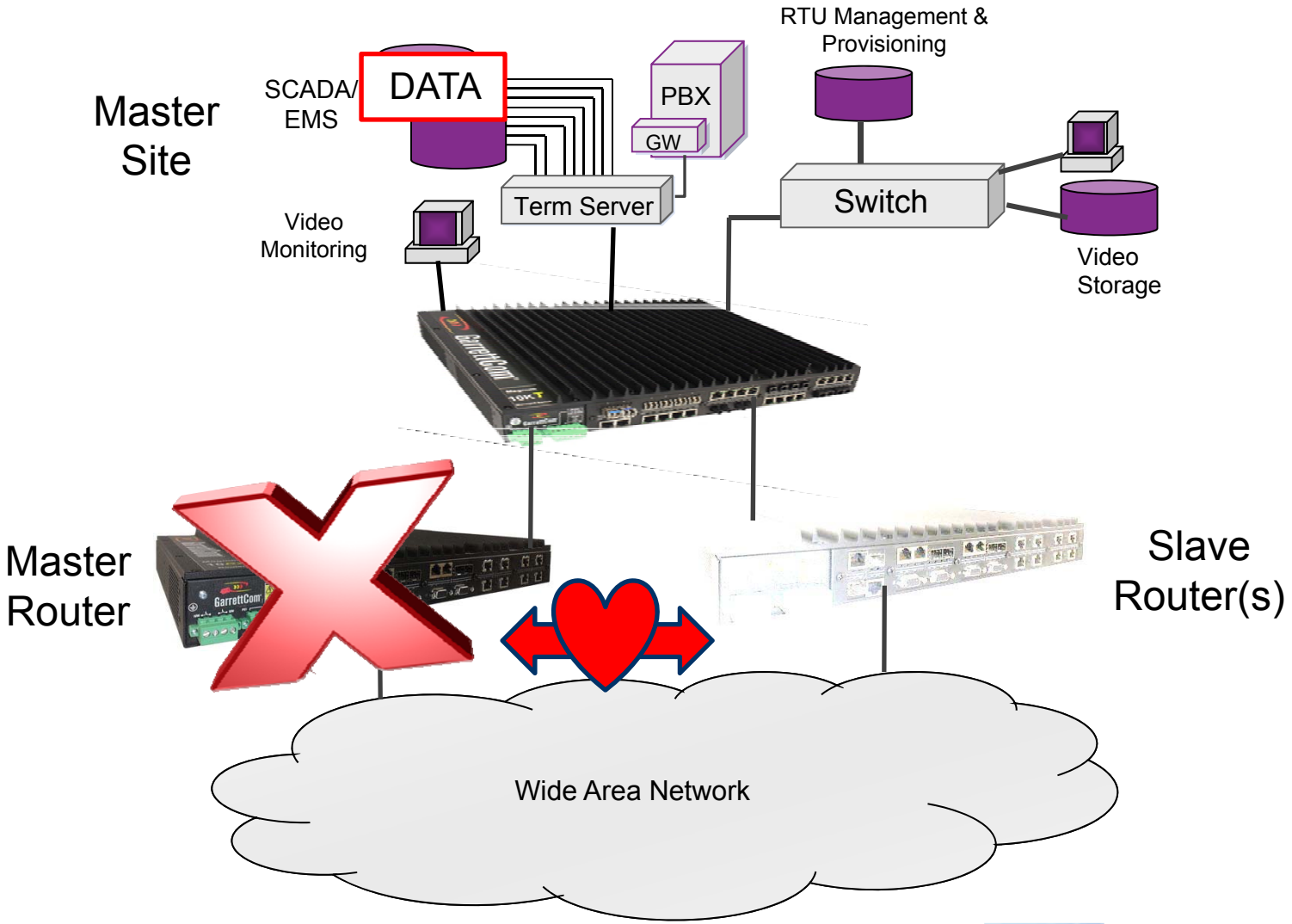
Virtual Router Redundancy Protocol (VRRP)



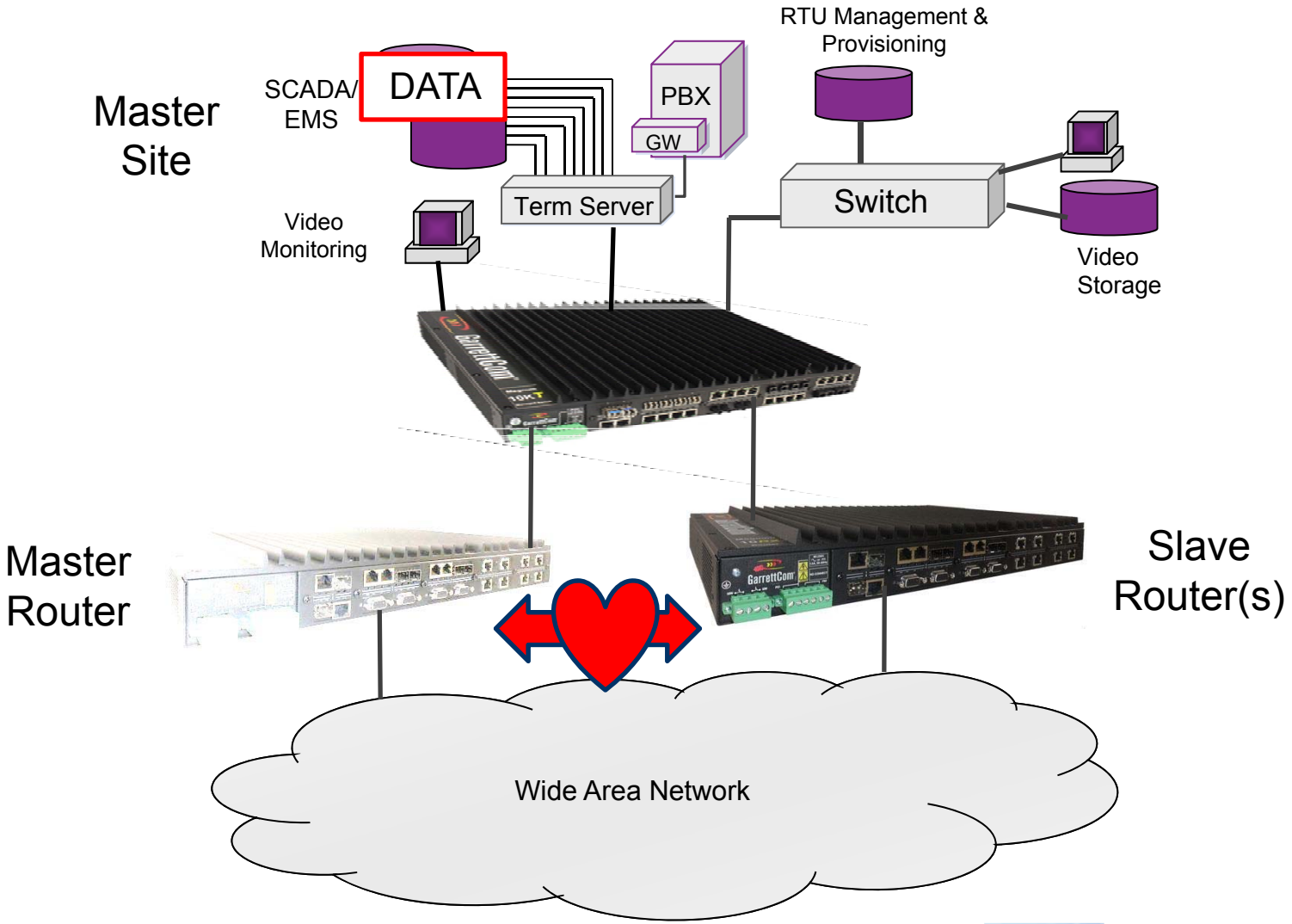
Virtual Router Redundancy Protocol (VRRP)



Virtual Router Redundancy Protocol (VRRP)



Virtual Router Redundancy Protocol (VRRP)



Cellular Redundancy

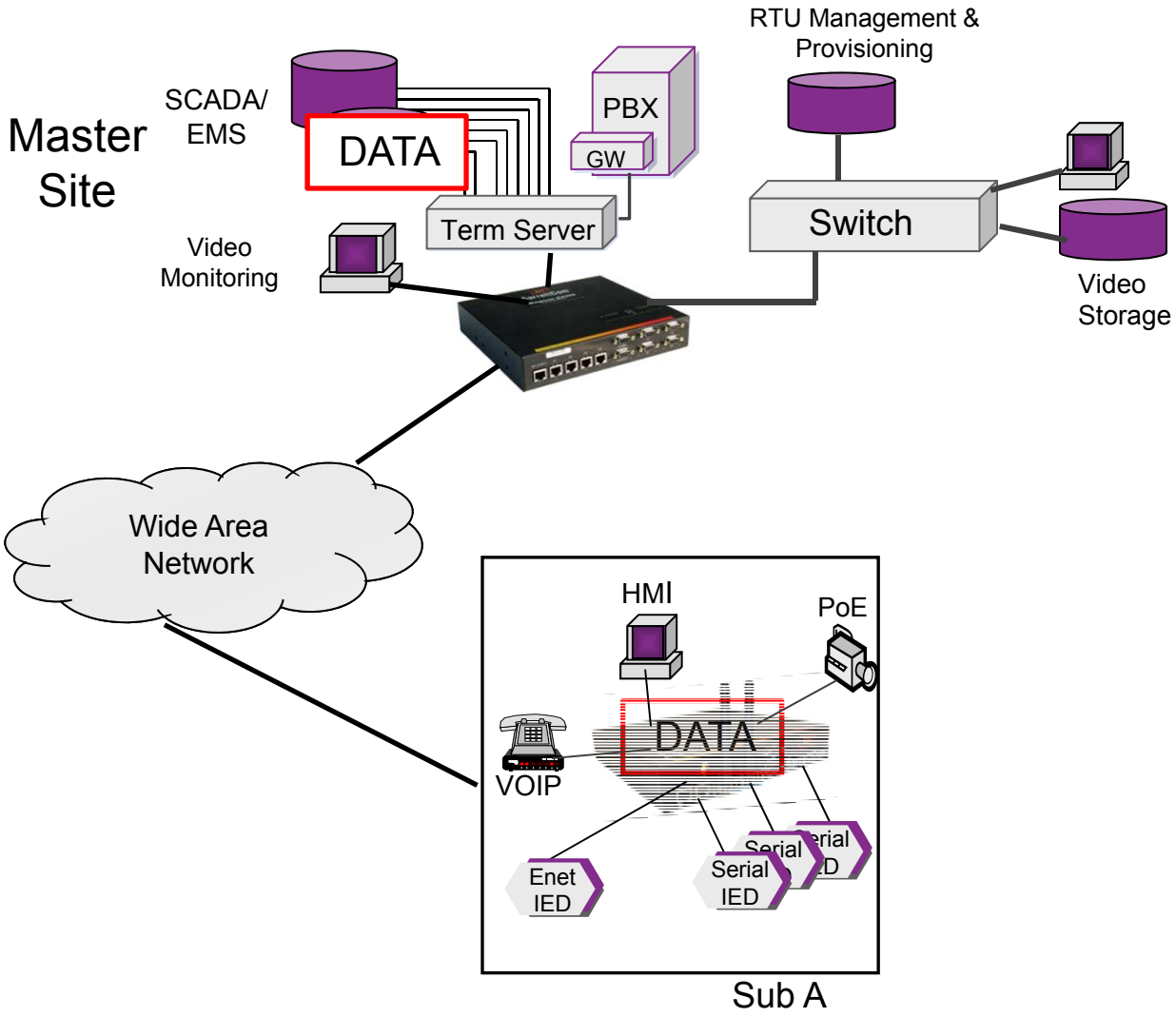
HIRSCHMANN

A BELDEN BRAND

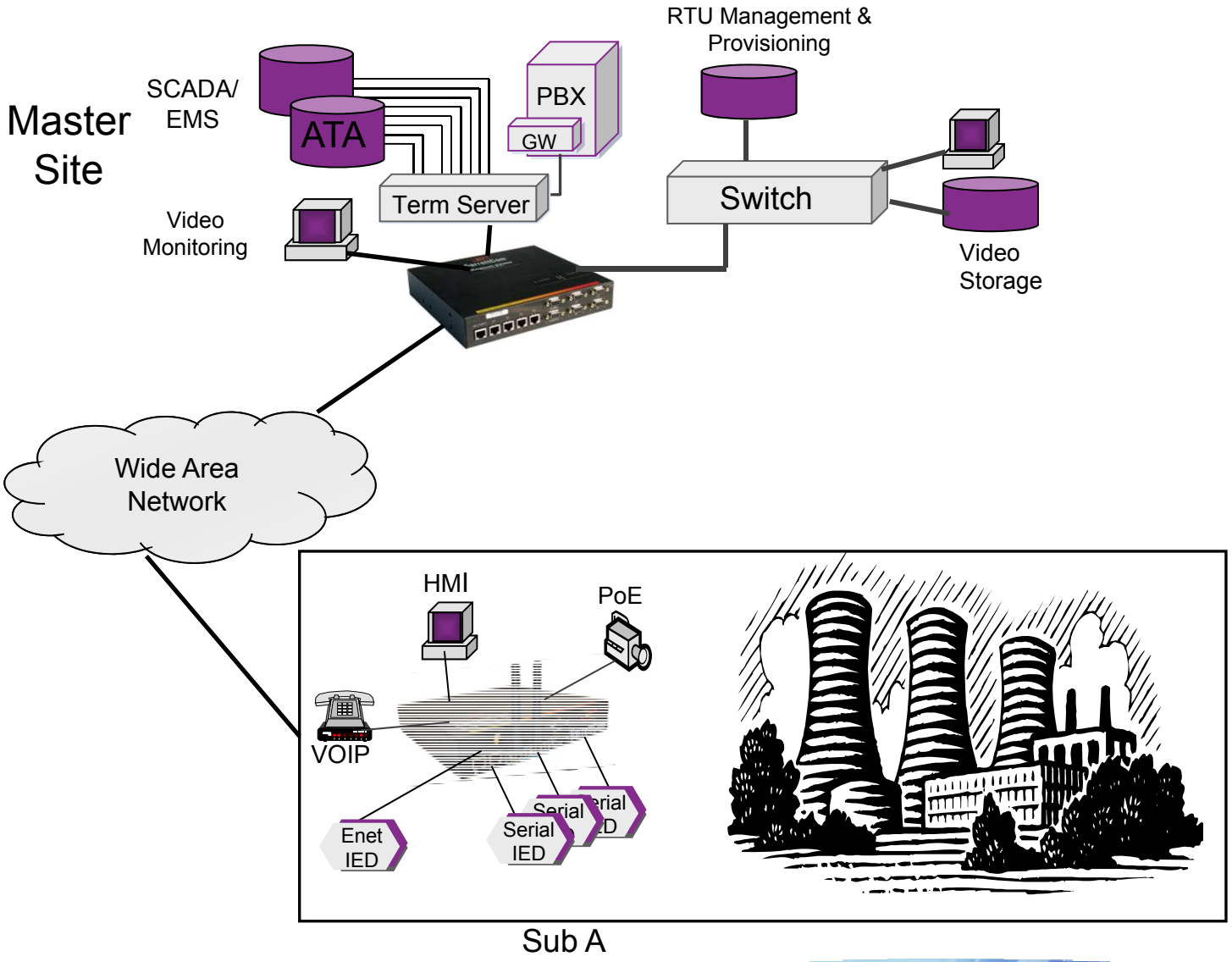
GarrettCom

A BELDEN BRAND

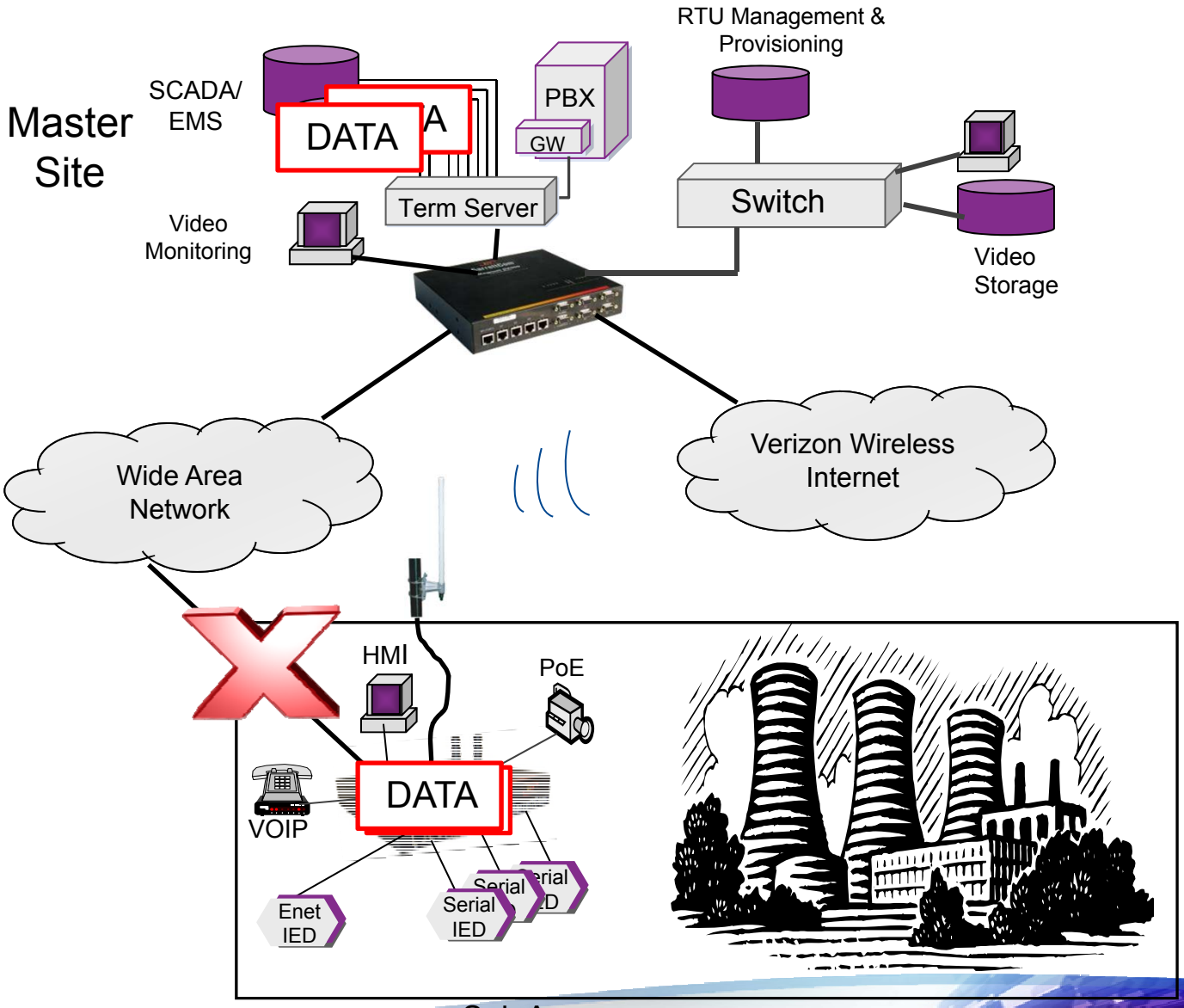
Before Cellular



Before Cellular



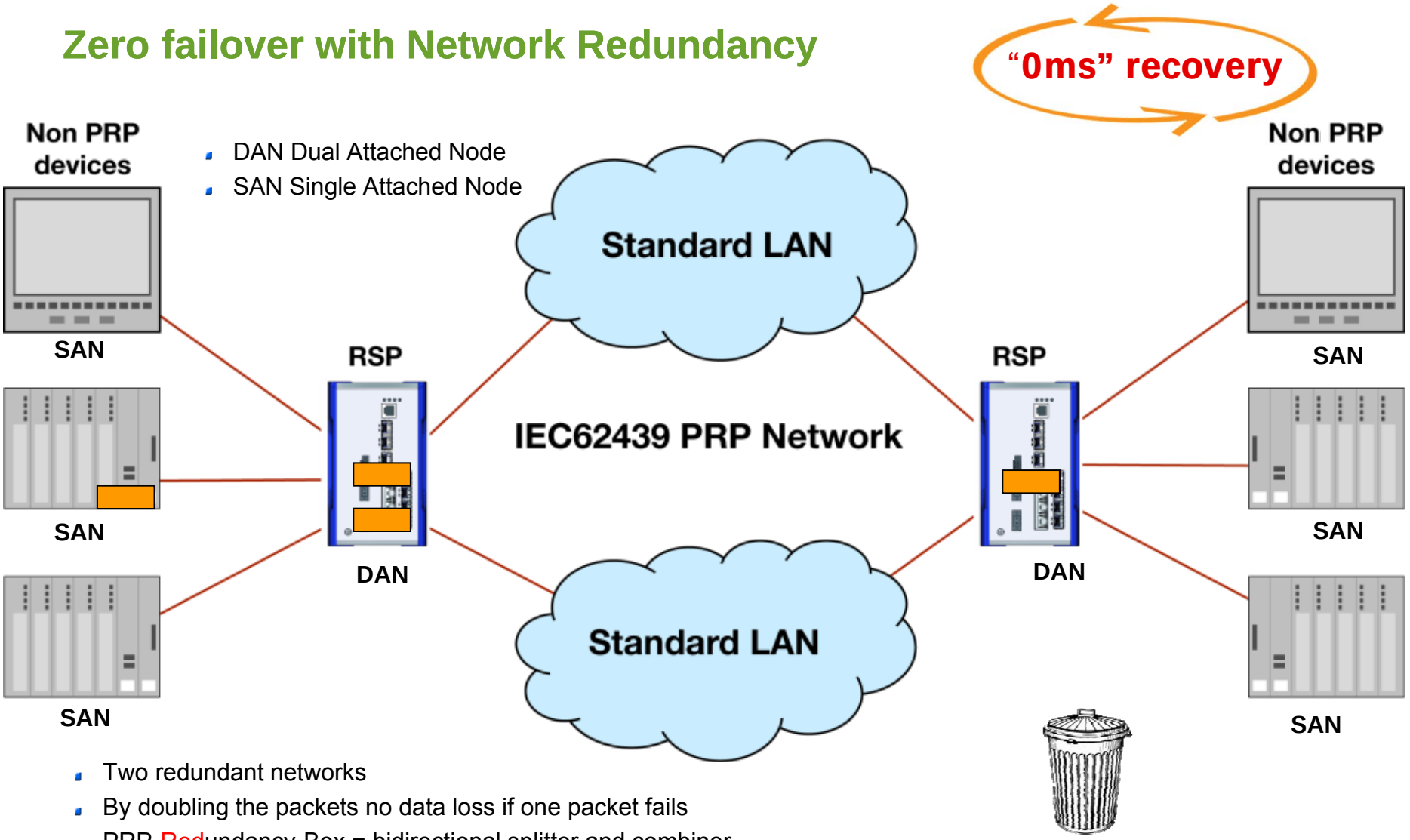
Cellular Backup



PRP/HSR Redundancy

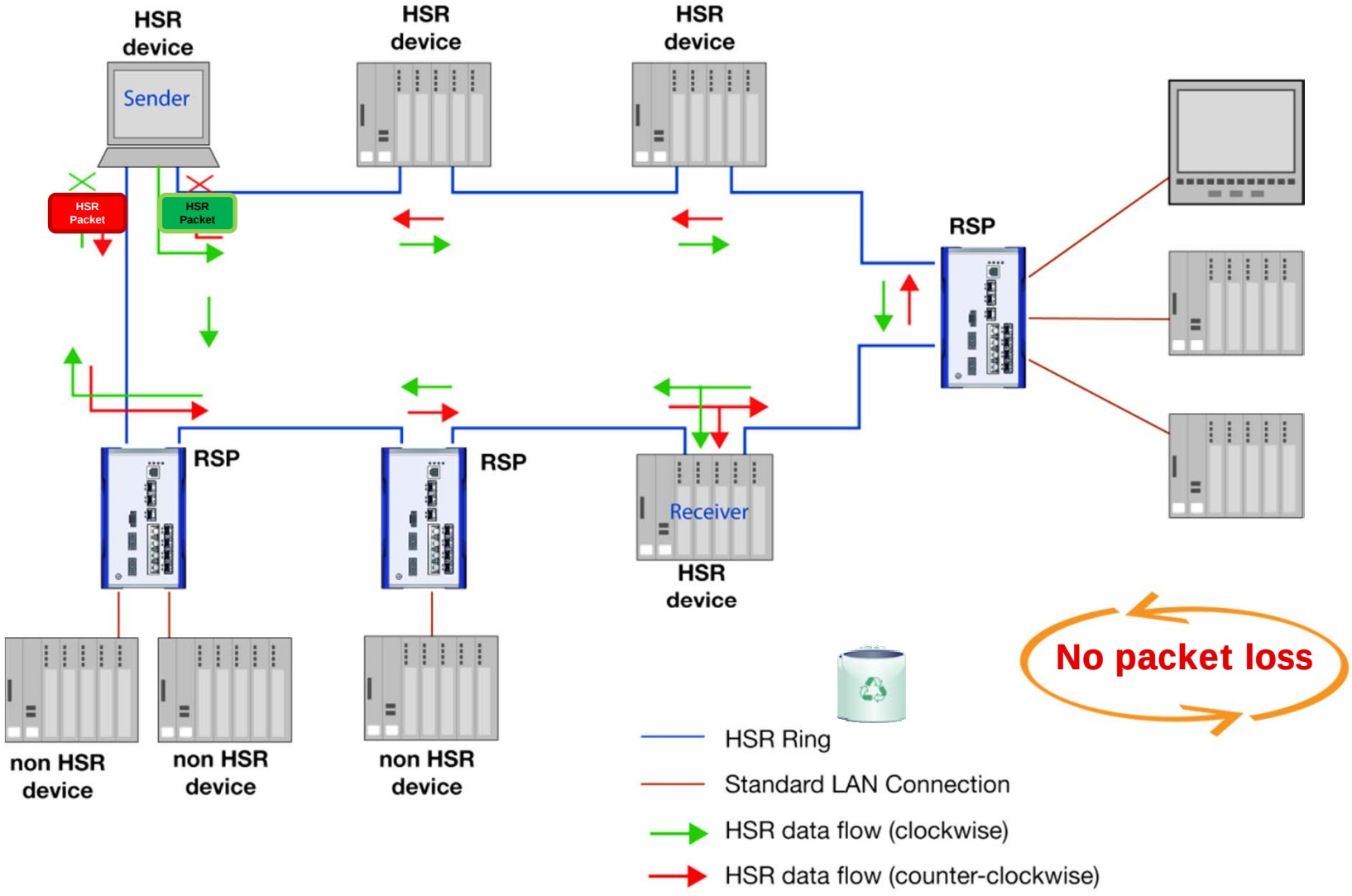
Parallel Redundancy Protocol (PRP)

Zero failover with Network Redundancy



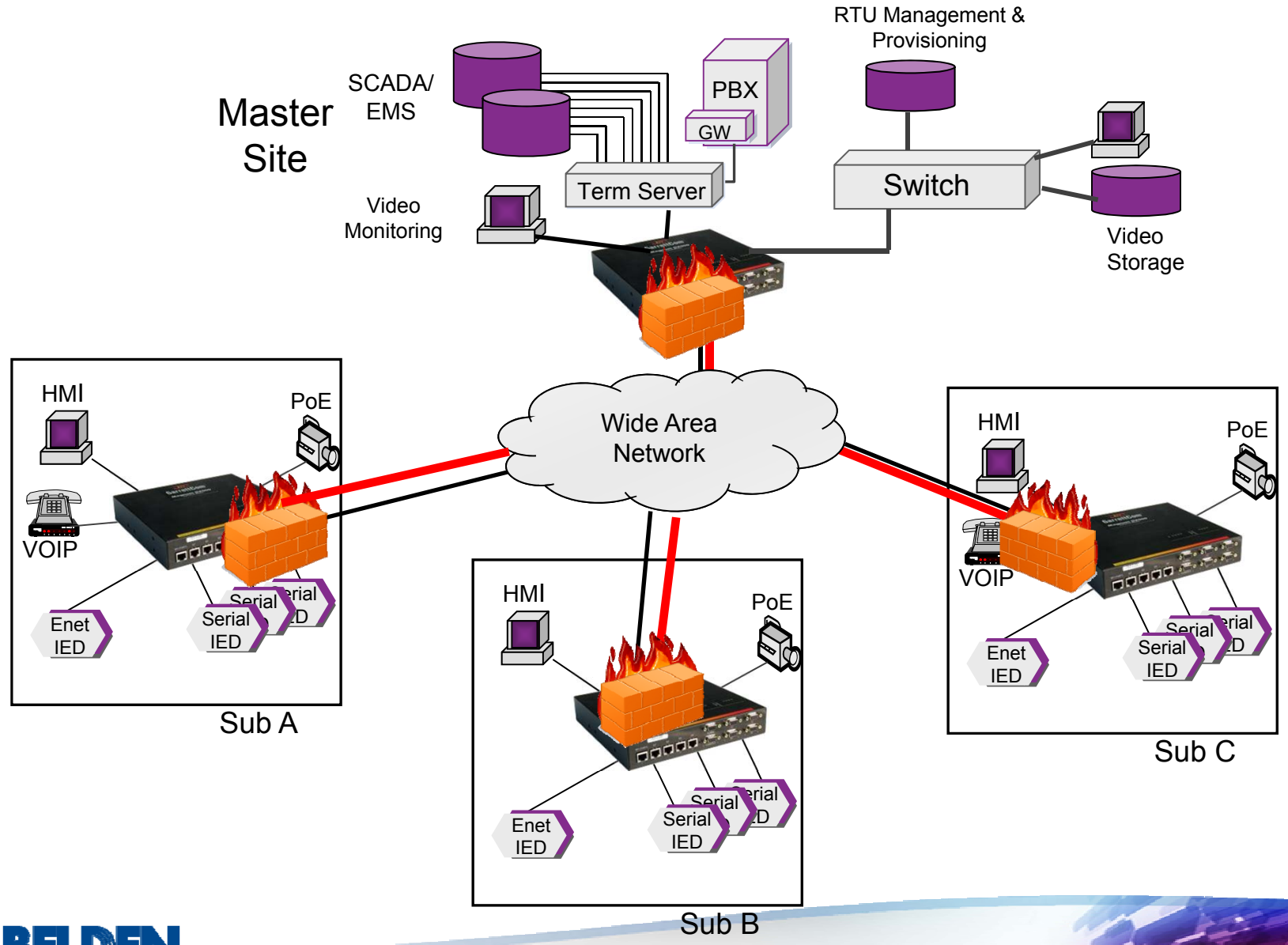
- Two redundant networks
- By doubling the packets no data loss if one packet fails
- PRP-Redundancy-Box = bidirectional splitter and combiner

High-Available Seamless Redundancy (HSR)

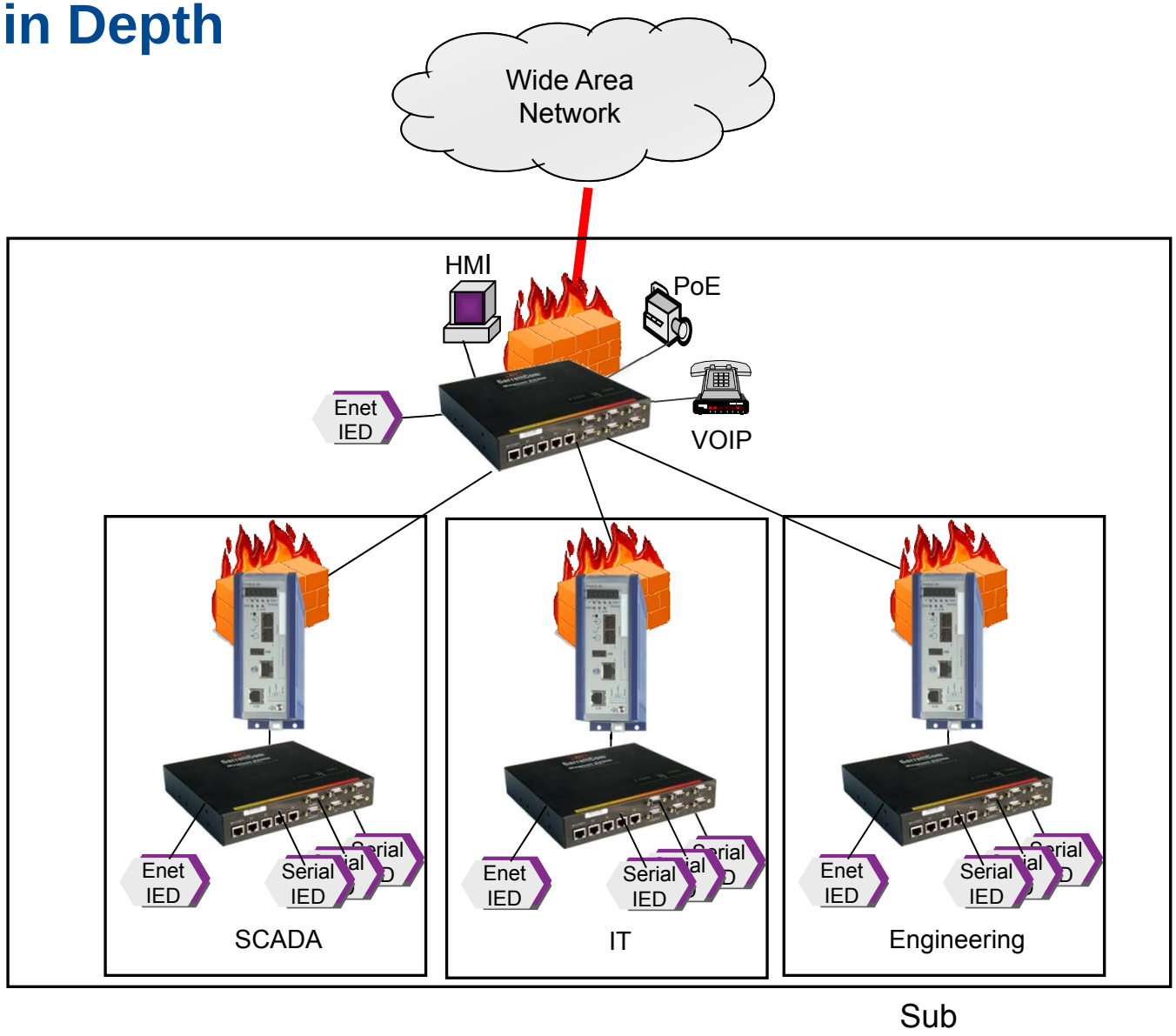


Security

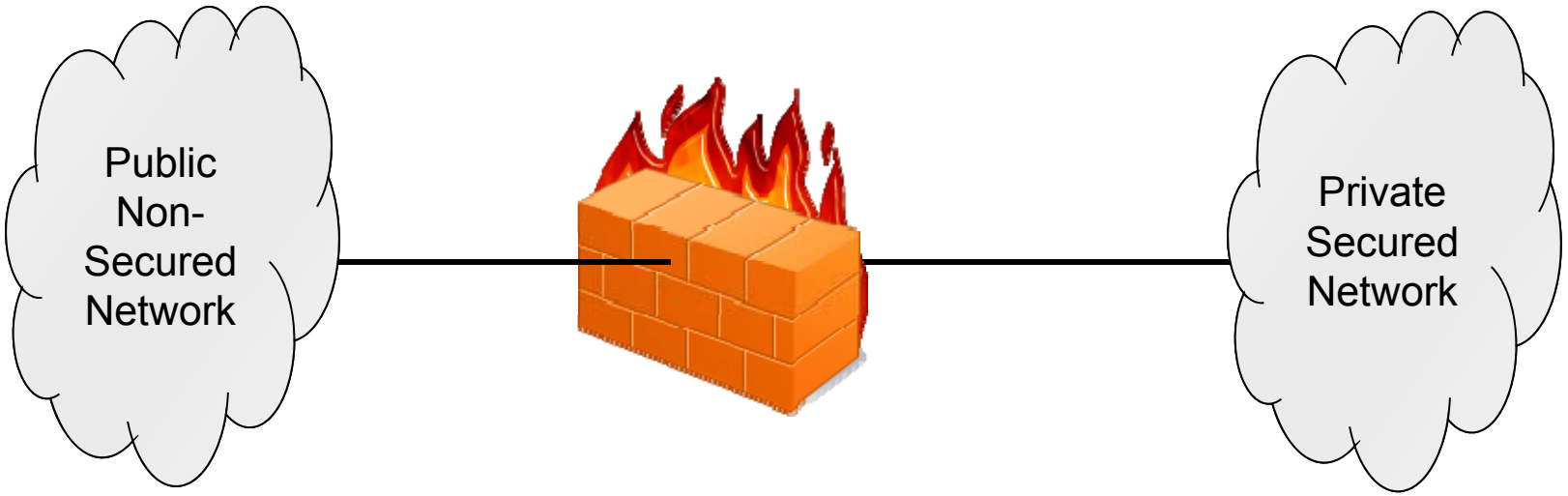
Today's Networks



Defense in Depth



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

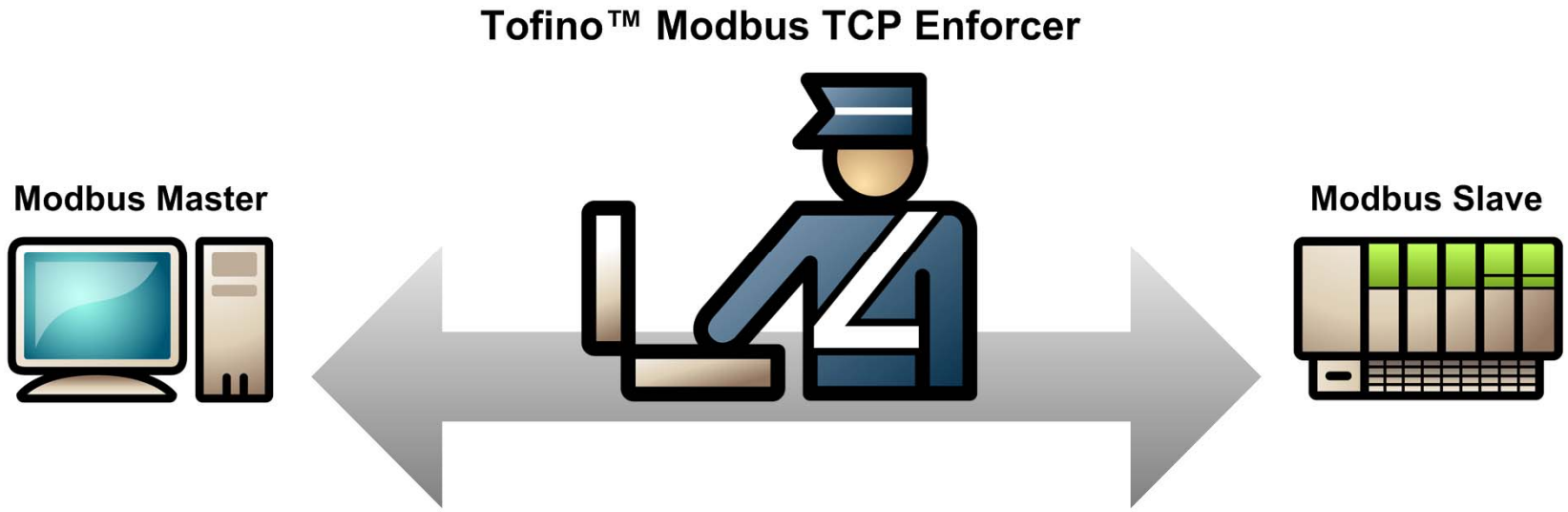
DX

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

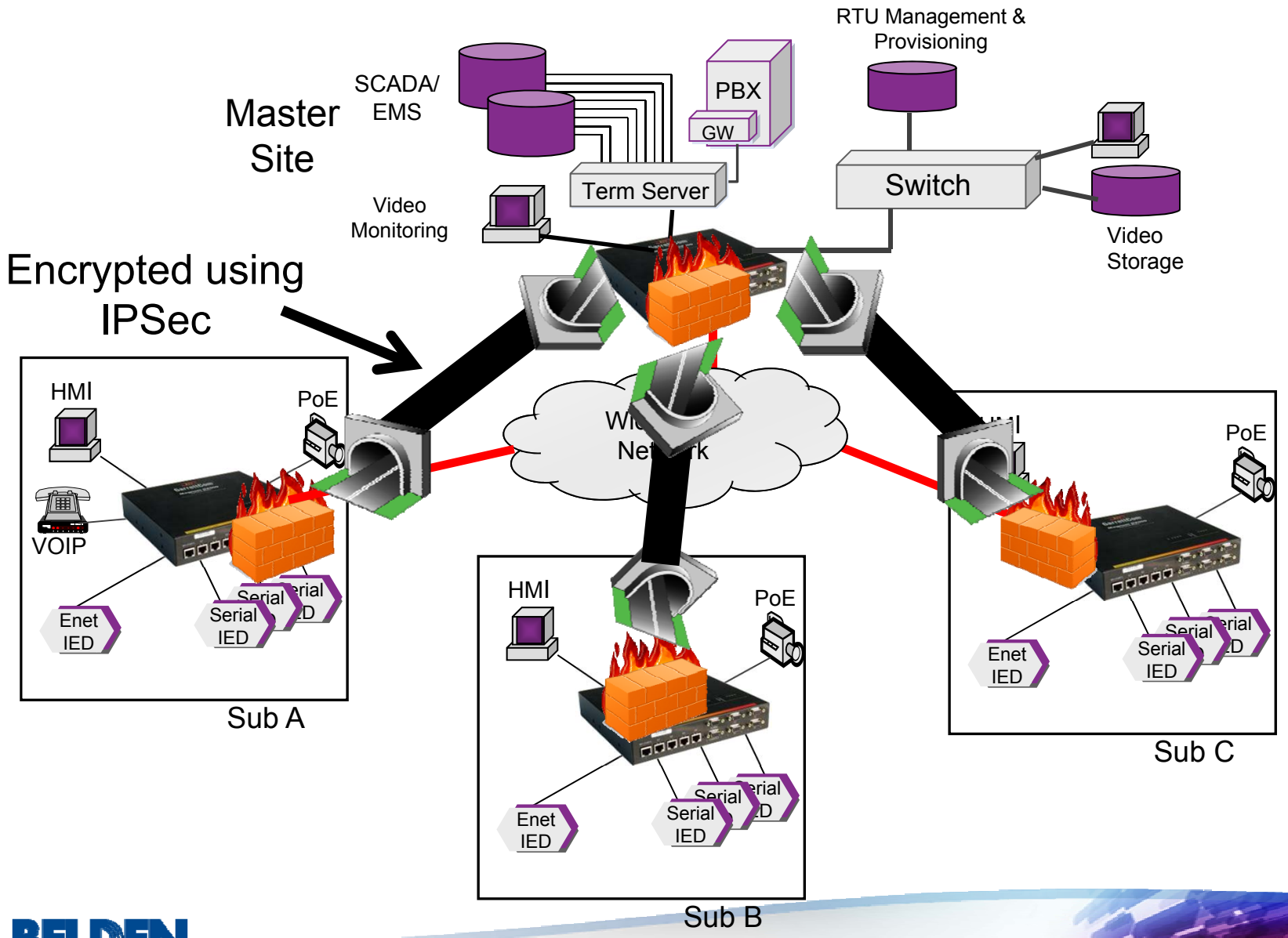


VPN

HIRSCHMANN
A BELDEN BRAND

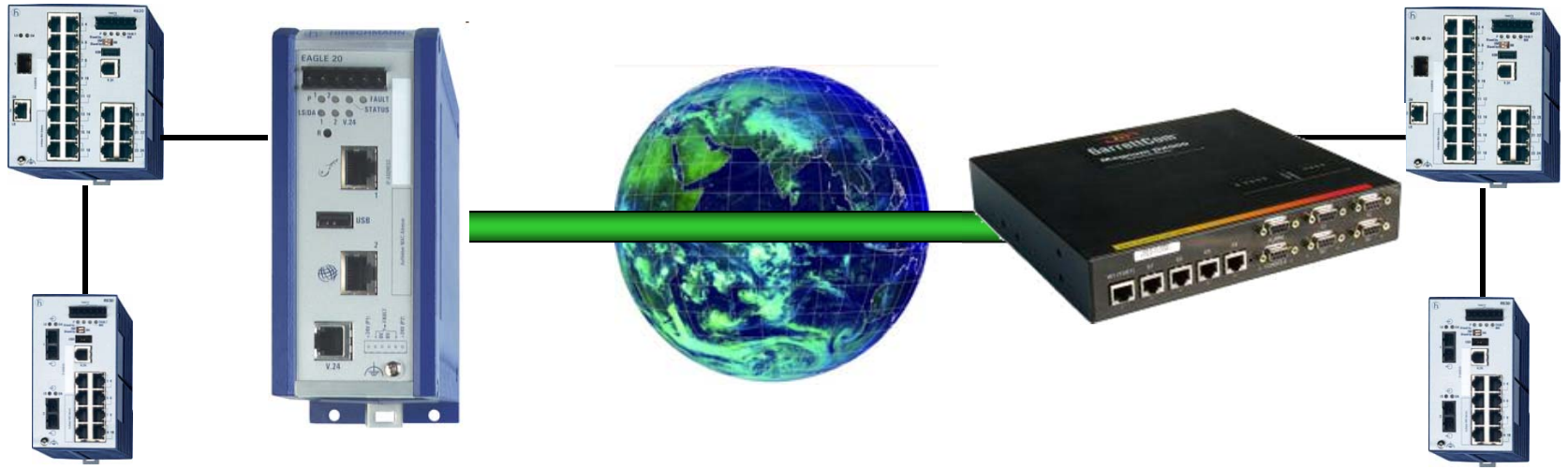
GarrettCom
A BELDEN BRAND

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

HIRSCHMANN

A BELDEN BRAND

GarrettCom®

A BELDEN BRAND

Port Security

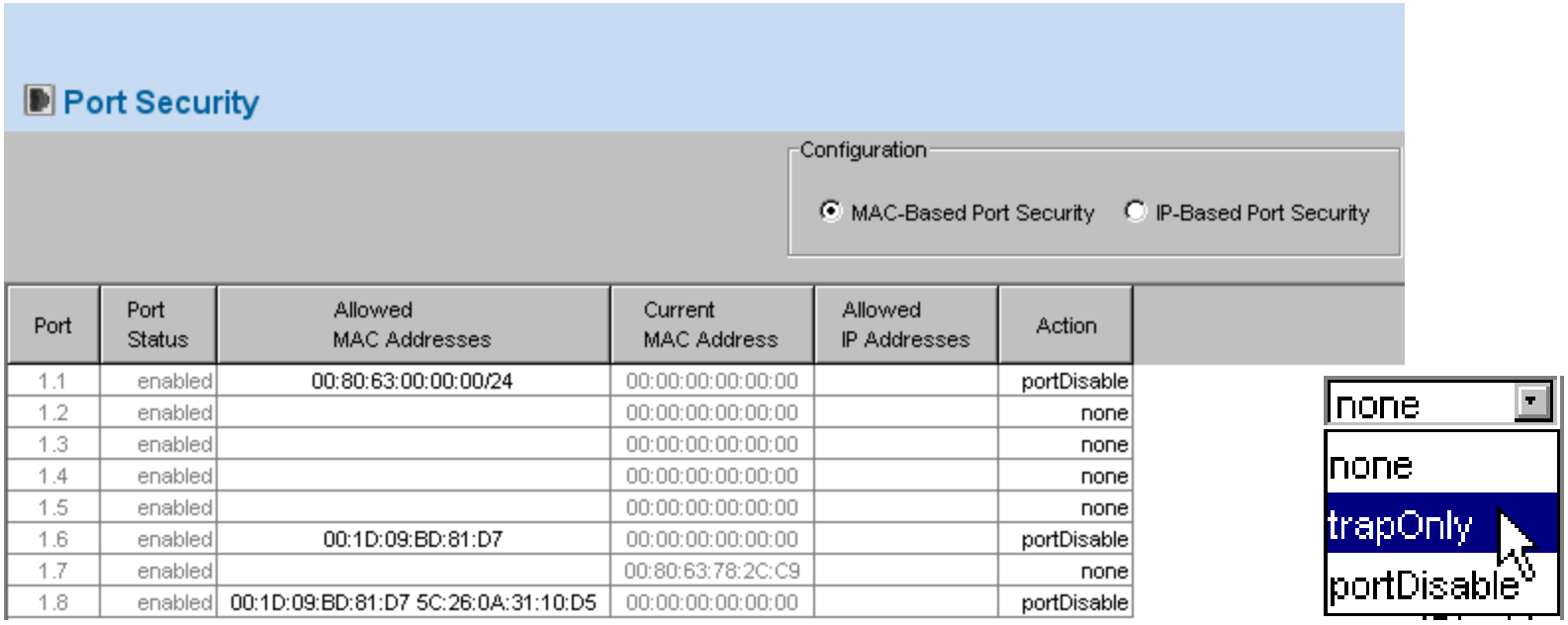
- Default with all ports “administratively set to DOWN”
- Some devices support “no tail ending”. Port is locked after being unplugged. Must be enabled by administrator
- Physical port security devices

- Unusual port connectors provide a small level of security

Figure	Pin	Function	
	1	TD+	Transmit Data +
	2	RD+	Receive Data +
	3	TD-	Transmit Data -
	4	RD-	Receive Data -
	Housing: shield		

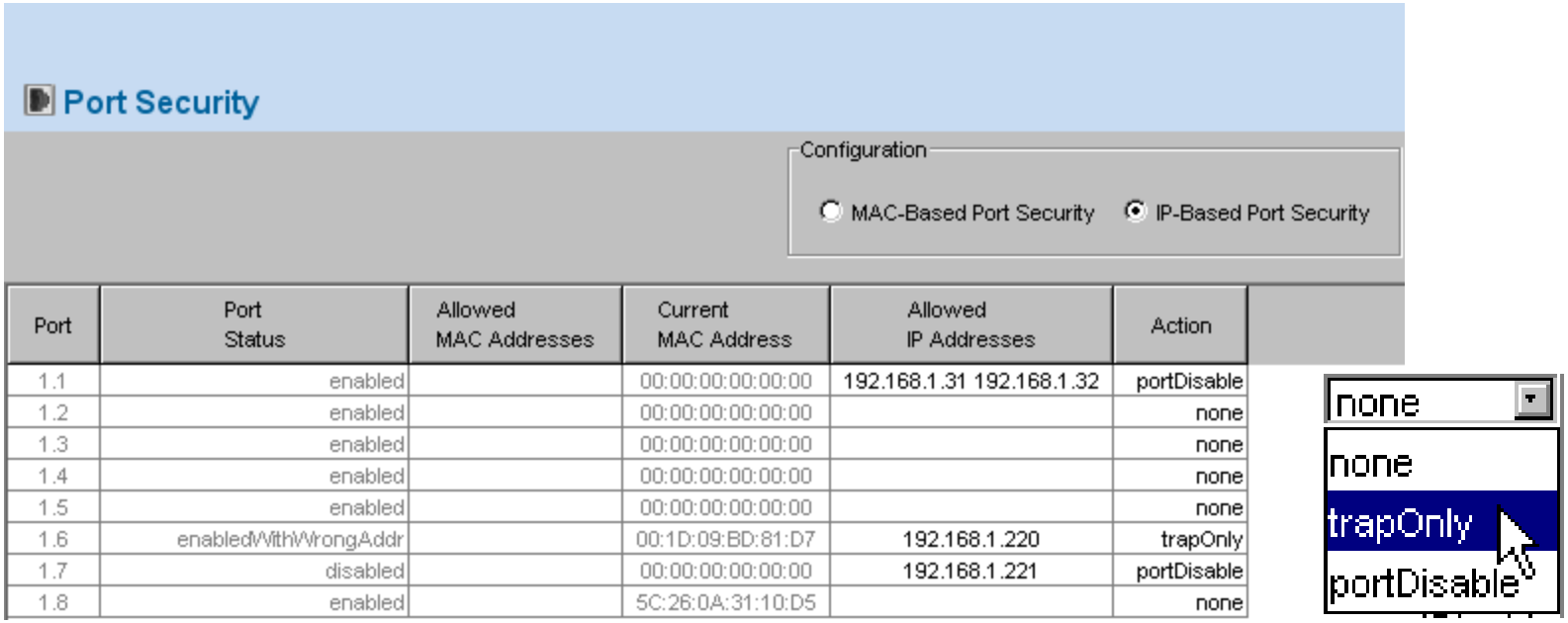
MAC Based Port Security

- 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.



IP Based Port Security

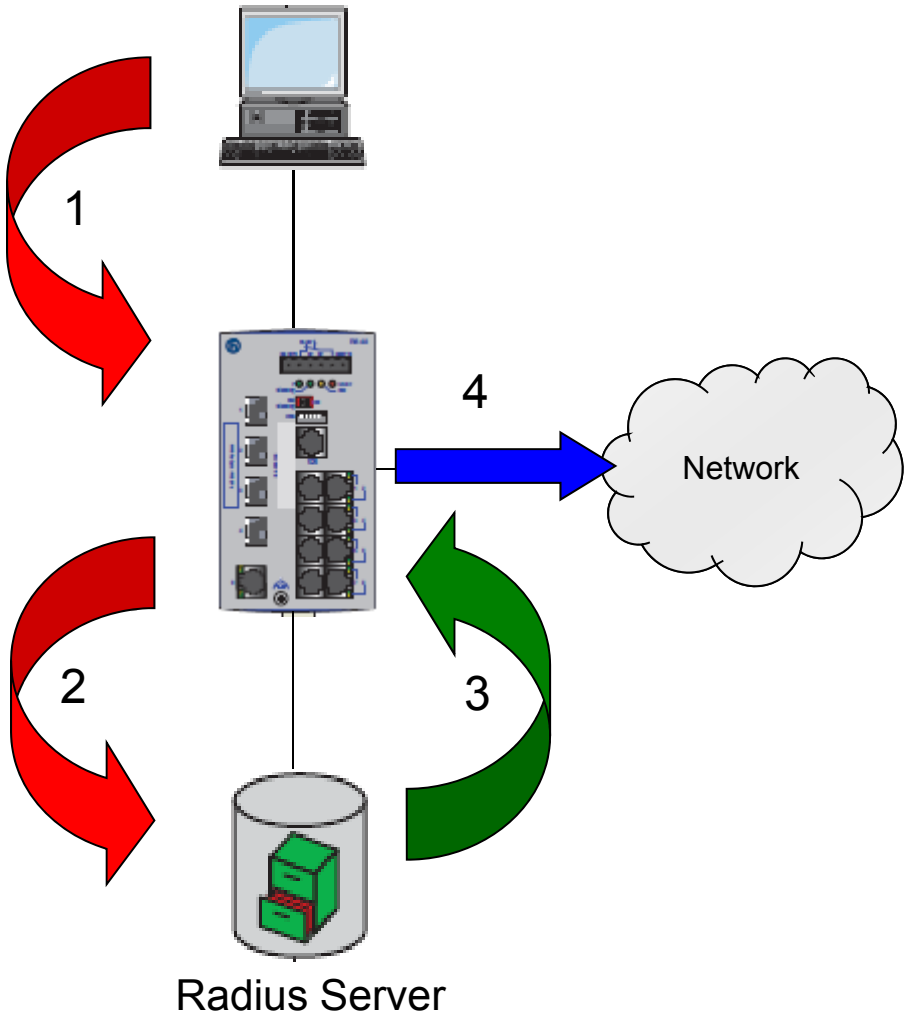
- Secures physical ports by applying a IP based filter on a per port basis which allows only the authorized IP address to forward traffic from the given port.



Authentication

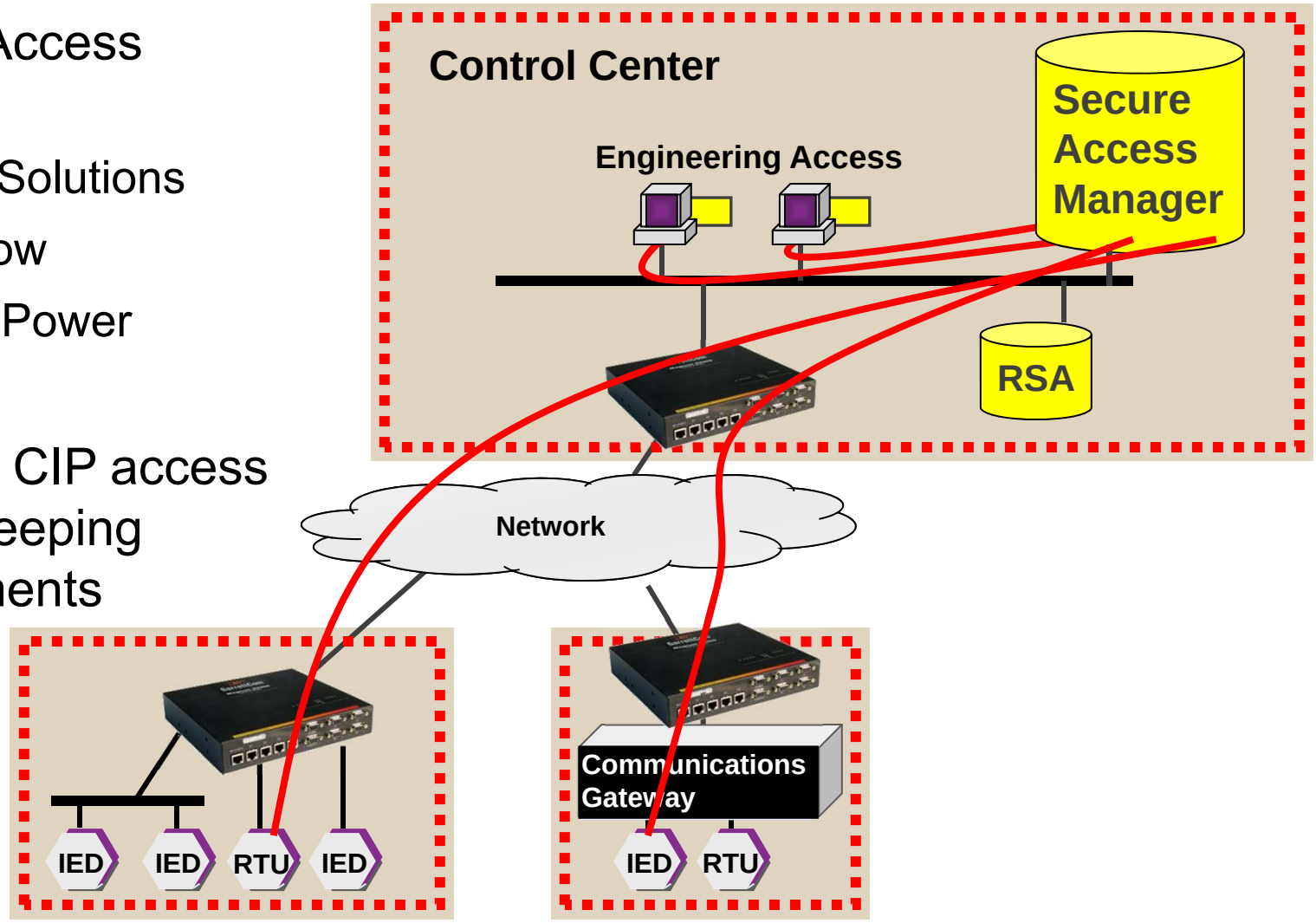
Authentication

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



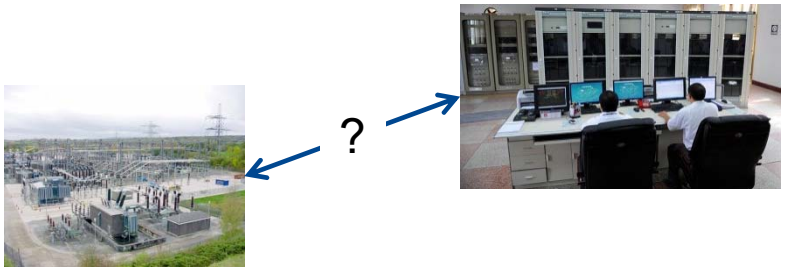
Authentication

- Secure Access Servers
  - Subnet Solutions
  - CrossBow
  - Cooper Power
- Satisfies CIP access record keeping requirements

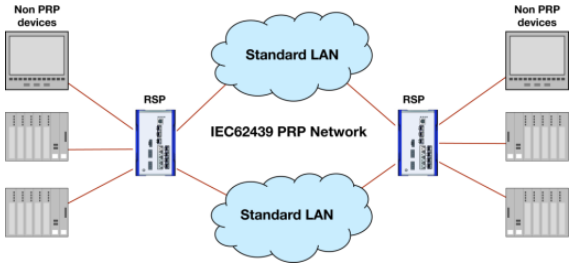


Summary

- 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/
   - 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/

Thank you for your interest in this presentation!

Belden.com | @BeldenInc