

Peter Kreutzer, PSSAM/Automation Power World 2011 New Delhi, 2011-09-20

Secure and reliable Redundant communication network and cyber security

Content

- Reliable Substation communication networks
 - Introduction of IEC 62439 Redundancy
 - Comparison of different port redundancy methods
 - Experiences
- Cyber Security for Substation Automation
 - Key Cyber-Security initiatives
 - Cyber Security in the system lifecycle

IEC 61850

Redundancy Status

- In the current edition of IEC 61850 redundant communication is not defined
 - In the IEC 61850 committee it has been identified that the lack of redundancy definition in the standard is becoming a real concern in respect of interoperability
 - Preparation for defining redundancy in IEC 61850 is in the final stage
 - IEC 61850 Edition 2 covering redundancy will be ready in 2011
 - Redundancy will be added to station bus (IEC 61850-8-1) and to process bus (IEC 61850-9-2)
 - IEC 61850 will not invent the redundancy but refer to PRP/HSR of the IEC 62439 standard
-
- **PRP** (Parallel Redundancy Protocol)
 - **HSR** (High-availability Seamless Redundancy)

Comparing some characteristics

Redundancy protocols

Table 2 – Examples of redundancy protocols

Protocol	Solution	Frame Loss	Redundancy protocol	End node attachment	Network Topology	Recovery time for the considered failures	
IP	IP routing	Yes	Within the network	Single	Single meshed	> 30 s typical not deterministic	
STP	IEEE 802.1D	Yes	Within the network	Single	Single meshed	> 20 s typical not deterministic	
RSTP	IEEE 802.1D	Yes	Within the network	Single	Single meshed, ring	Can be deterministic following the rules of Clause 8	for SAS IEC 61850
CRP	IEC 62439-4	Yes	In the end nodes	Single and double	Doubly meshed, cross-connected	1 s worst case for 512 end nodes	
DRP	IEC 62439-6	Yes	Within the network	Single and double	Ring, double ring	100 ms worst case for 50 switches	
MRP	IEC 62439-2	Yes	Within the network	Single	Ring	500 ms, 200 ms, 30 ms or 10 ms worst case for 50 switches depending on the parameter set	
BRP	IEC 62439-5	Yes	In the end nodes	Double	Doubly meshed, connected	4,8 ms worst case for 500 end nodes	
PRP	IEC 62439-3	No	In the end nodes	Double	Doubly meshed, independent	0 s	for SAS IEC 61850
HSR	IEC 62439-3	No	In the end nodes	Double	Ring, meshed	0 s	

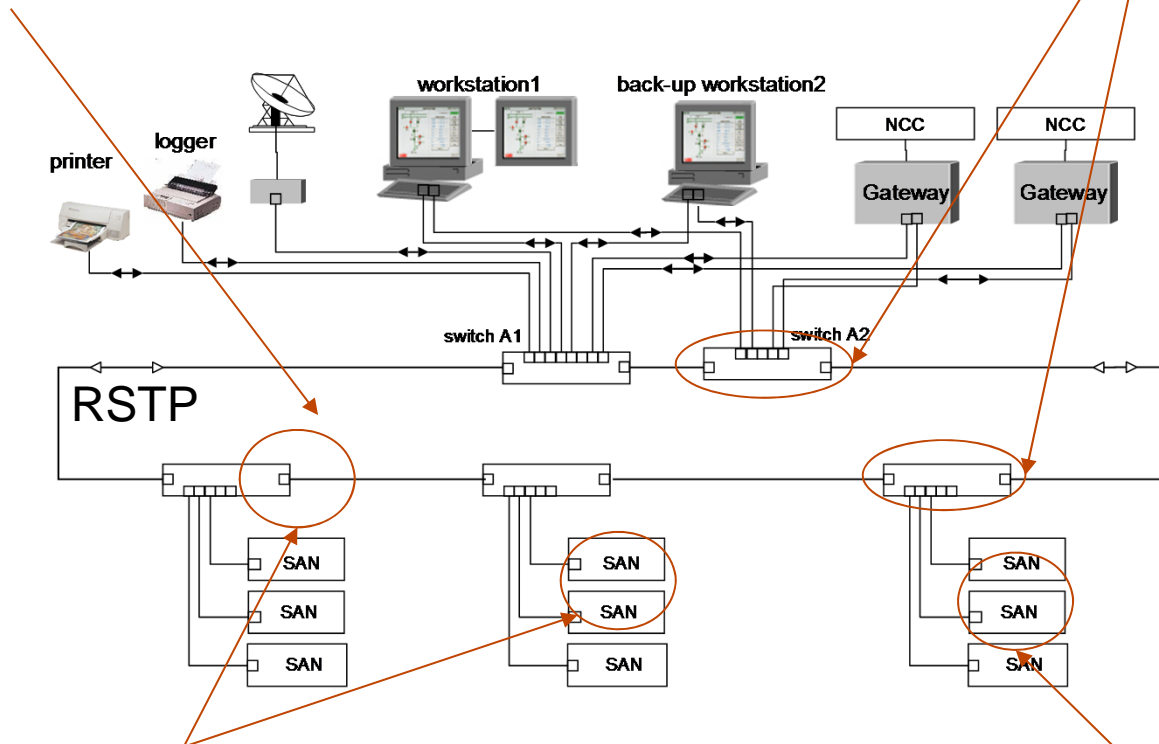
Reference: IEC 62439-1

Redundant network Single ring using external switches

Advantages and disadvantages

- Any topology supported: Tree, Star, Ring, meshed ☺
- Network is autonomous, independent of IEDs
- Standard Ethernet components, no special devices
- Flexible network speed (100MBit/s, 1GBit/s) and media
- Full bandwidth can be used, no double frames

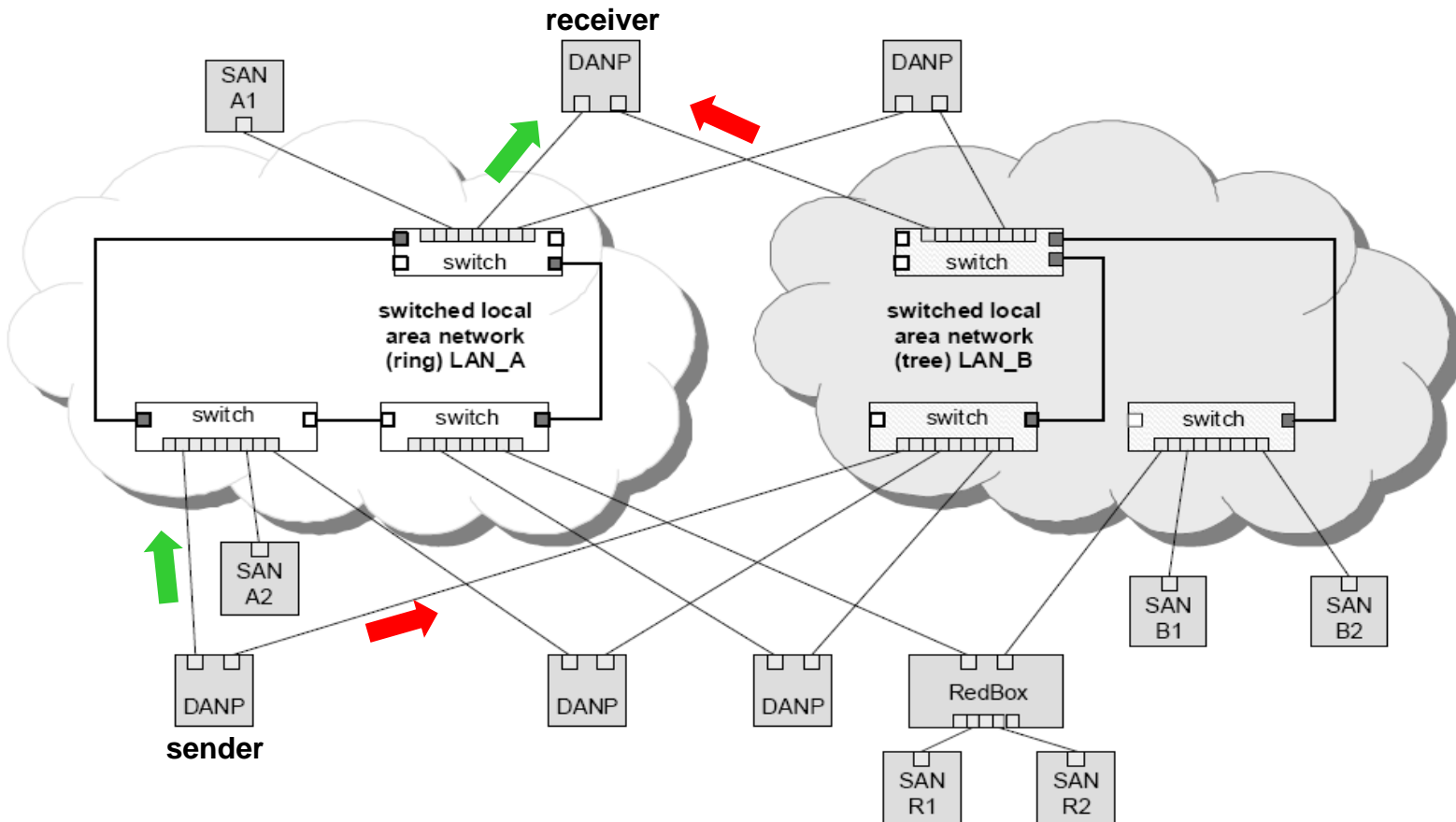
- ~5ms/switch failure recovery time ☹



- Failure or power-off of 2 or more IEDs has no impact to the network ☺
- Moderate costs for switches and network cabling ☹

- Fully Interoperability any IEC61850 3rd party IED can be connected to the network ☺

Redundant network with IEC 62439-3 PRP Parallel Redundancy Protocol



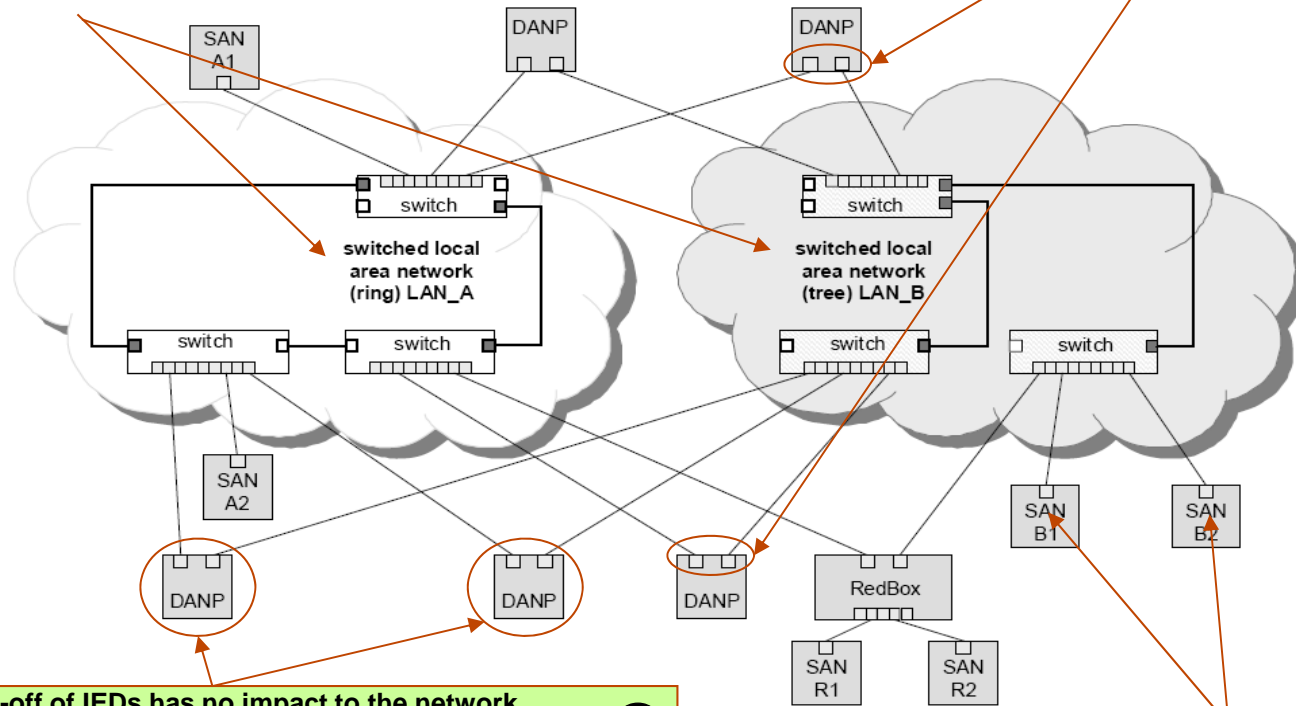
- Operation principle
 - DANP (Double Attached Node implementing PRP) are attached to 2 independent LANs
 - Source DANP sends same frame over both LANs
 - Destination DANP receives frame from both LANs, consumes 1st frame, discards the duplicated

Redundant network with IEC 62439-3 PRP

Advantages and disadvantages

- Any topology supported: Tree, Star, Ring, meshed ☺
- Network is autonomous, independent of IEDs
- Standard Ethernet components, no special devices
- Flexible network speed (100MBit/s, 1GBit/s) and media
- Full bandwidth can be used, frames run on separate LANs

- 0ms failure recovery time ☺
- No frame loss

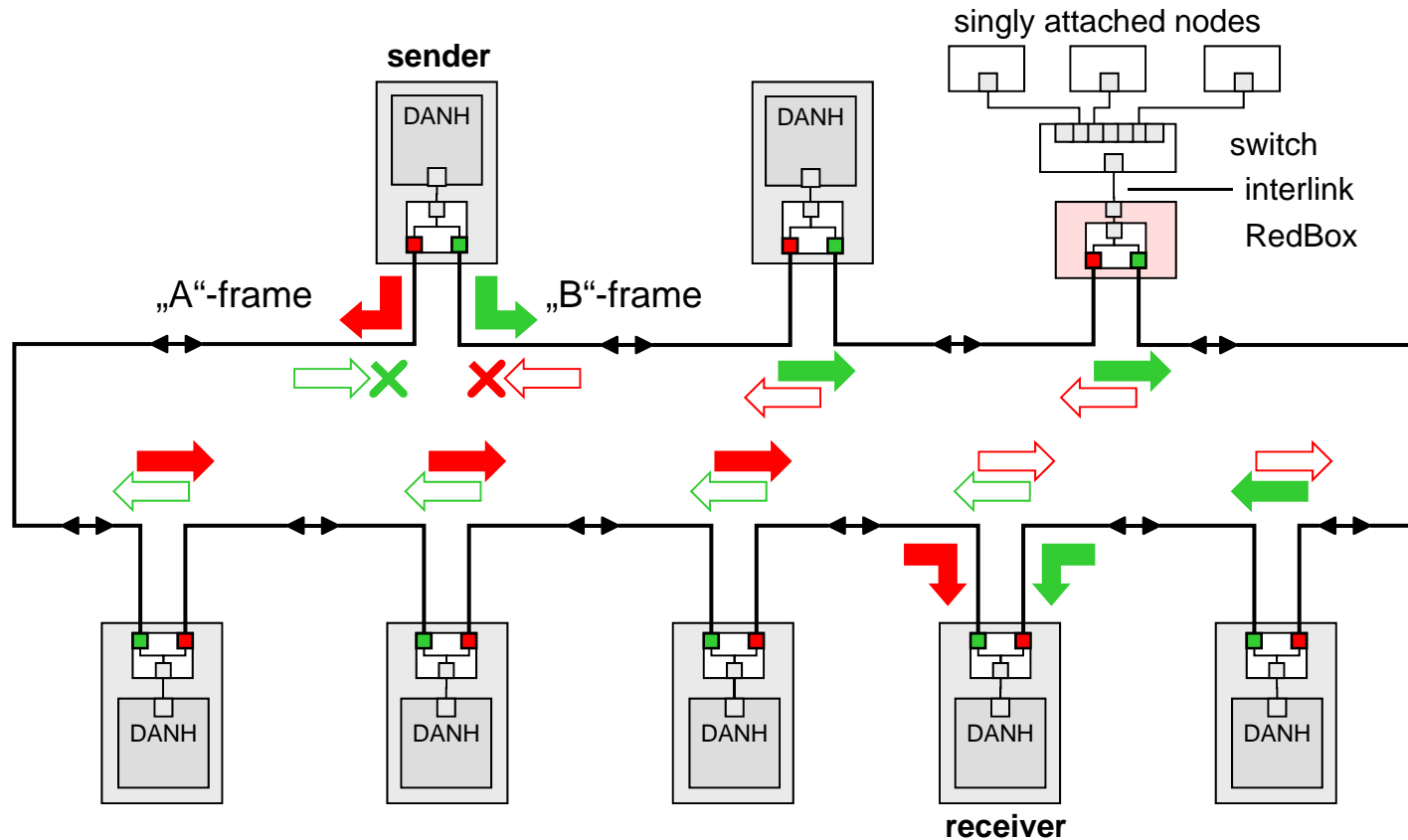


- Failure or power-off of IEDs has no impact to the network ☺

- High costs for switches and network cabling ☹

- Connecting single port IEDs directly to one network ☺
- Fully Interoperability with non redundant IEDs

Redundant network with IEC 62439-3 HSR High-availability Seamless Redundancy



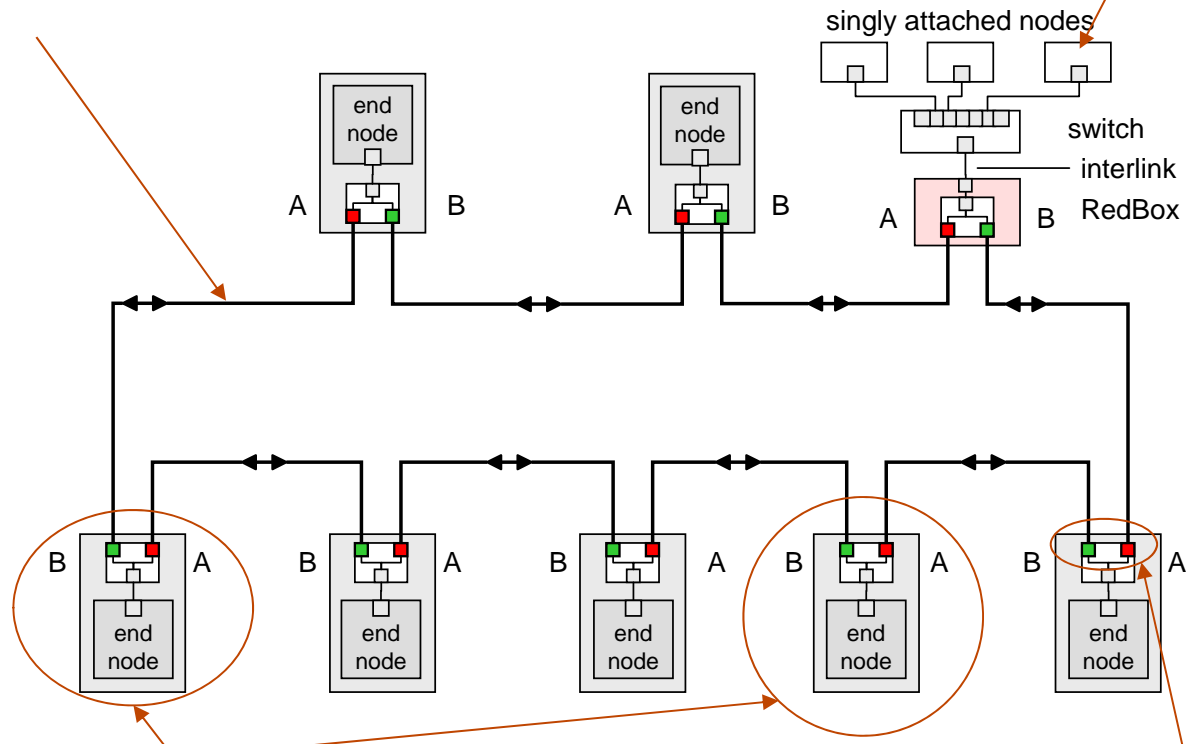
- Operation principle
 - DANH (Double Attached Node implementing HSR) has 2 ports operated in parallel
 - Source DANH sends a frame over each port ("A"-frame and "B"-frame)
 - Destination DANH receives frame from each port, consumes 1st frame, discards the duplicated
 - DANH support bridge functionality and forward frames from one port to the other (not frames that it injected)

Redundant network with IEC 62439-3 HSR

Advantages and disadvantages

- Only ring or ring of ring topologies ☹️
- IEDs are integral part of network
- Standard Ethernet components cannot be used
- Fix network speed (100MBit/s)
- Bandwidth is half (double messages over one network)

- No direct connection of single port IEDs possible (only via RedBox) ☹️
- Not interoperable with non redundant IEDs



- Failure or power-off of more than 2 IEDs has impact to the network ☹️

- Low cost (no switches and few network cables) 😊

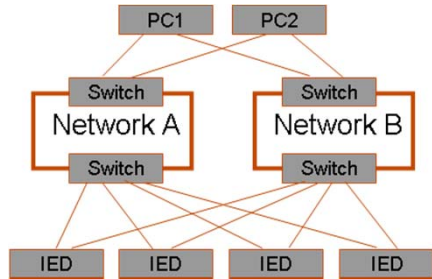
- 0ms failure recovery time 😊
- No frame loss



Redundant ports on IEDs

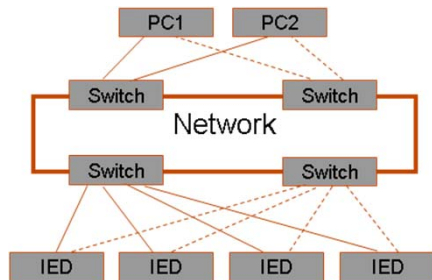
Summary of different redundancy methods

Redundant Network



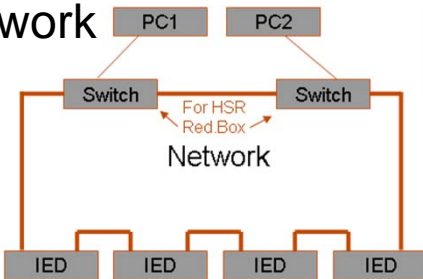
Method	IEC61850 8-1/9-2 Ed 2	Frame loss	Recovery time	Port redundancy	Network redundancy
PRP IEC 62439-3	yes	No	0 ms	yes	yes
Dual homing	No proprietary	No	0 ms	yes	yes

Single Network



Channel Switching	No proprietary	Yes	typ. 10ms	yes	no
------------------------------	-------------------	-----	-----------	-----	----

IEDs active part of Network



HSR IEC 62439-3	yes	No	0 ms	yes	no
RSTP	no	Yes	typ. 100ms (ring with 20 nodes)	yes	no

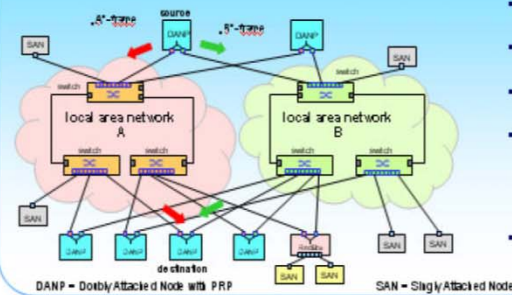
Experience CIGRE Session Paris 2010, PRP/HSR Demonstration

Highly Available Automation Networks for substations PRP (Parallel Redundancy) and HSR (Seamless Ring)

IEC 62439-3 specifies two protocols, PRP and HSR that operate on the same principle:

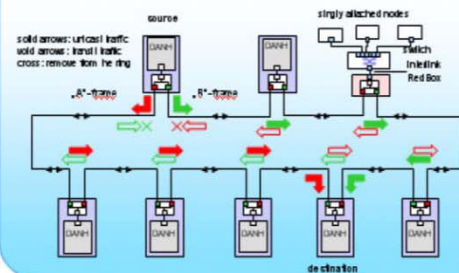
- Each node has two ports and sends two identical frames that include a sequence number.
- The two frames travel through two independent paths - one may get lost
- Each destination receives - when there is no fault - both frames and discard the duplicate

Parallel Redundancy Protocol (PRP) - IEC 62439-3 Clause 4



- end nodes (DANP) do not forward frames
- frame sequence number is hidden in trailer
- normal nodes (SAN) are attached to any LAN
- SAN attached to LAN A cannot communicate with SAN attached to LAN B except when attached to a RedBox
- PRP is easily implemented in software

High-availability Seamless Ring (HSR) - IEC 62439-3 Clause 5



- nodes (DANH) forward frames from port to port
- HSR-tagged frames are ignored by normal nodes (SAN) therefore:
- SAN need to be connected over RedBoxes
- Rings are connected over Quadboxes
- HSR requires hardware support to speed up forwarding

High-availability, (n-1) criteria fulfilled
Real-time traffic support
Zero recovery time upon failure
Application protocol independent
Apply to any Industrial Ethernet
Will be referenced in IEC 61850 Ed2

Integrates standard PCs (SAN)
Flexible topology
PRP and HSR are complementary
PRP and HSR can be coupled
Nodes can support both PRP & HSR
Open standard (IEC 62439-3)

Zero recovery time Ethernet redundancy for IEC 61850 HSR High-availability, Seamless Redundancy (IEC 62439-3 Cl. 5) Swiss KTI project: Evaluation and Interoperability

Motivation

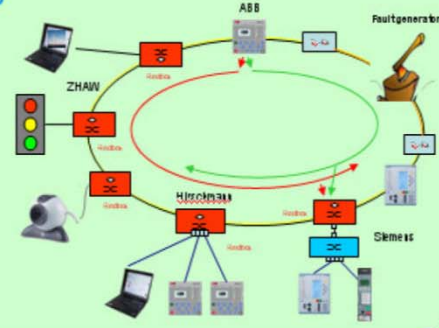
- IEC 61850 (Substation automation data communication) did not reference a network redundancy scheme
- IEC 61850 (Ed2) will specify the use of IEC 62439-3 (PRP & HSR) as protocol for seamless network redundancy
- HSR is a new protocol; interoperability test, evaluation and open components are crucial success factors

HSR benefits

- High-availability network (n-1 criteria)
- Zero recovery time upon failure
- Cost-effective hardware
- Flexible topology
- Complements PRP
- Open standard (IEC 62439-3 Cl. 5)
- Applicable to any Industrial Ethernet
- Referenced in IEC 61850

HSR principle and demo

- A source sends two frames simultaneously in both directions
- Each node forwards the transit traffic in both directions
- The destinations use the first frame and discard the duplicates
- Frames are tagged with a sequence number to recognize duplicates, enabling cut-through (immediate forwarding while receiving the frame)



Technology

- 100% Ethernet compatible
- Implementation: two-port device with an FPGA, duplicate discard in hardware
- Applications: electrical substations (IEC 61850) drives, streaming video, any Industrial Ethernet,

Team

ABB
hubert.kirmann@ch.abb.com
Hirschmann
oliver.kleineberg@belden.com
Siemens
clemens.hoga@siemens.com
Zurich University of Applied Sciences
hans.weibel@zhaw.ch



Experience with PRP

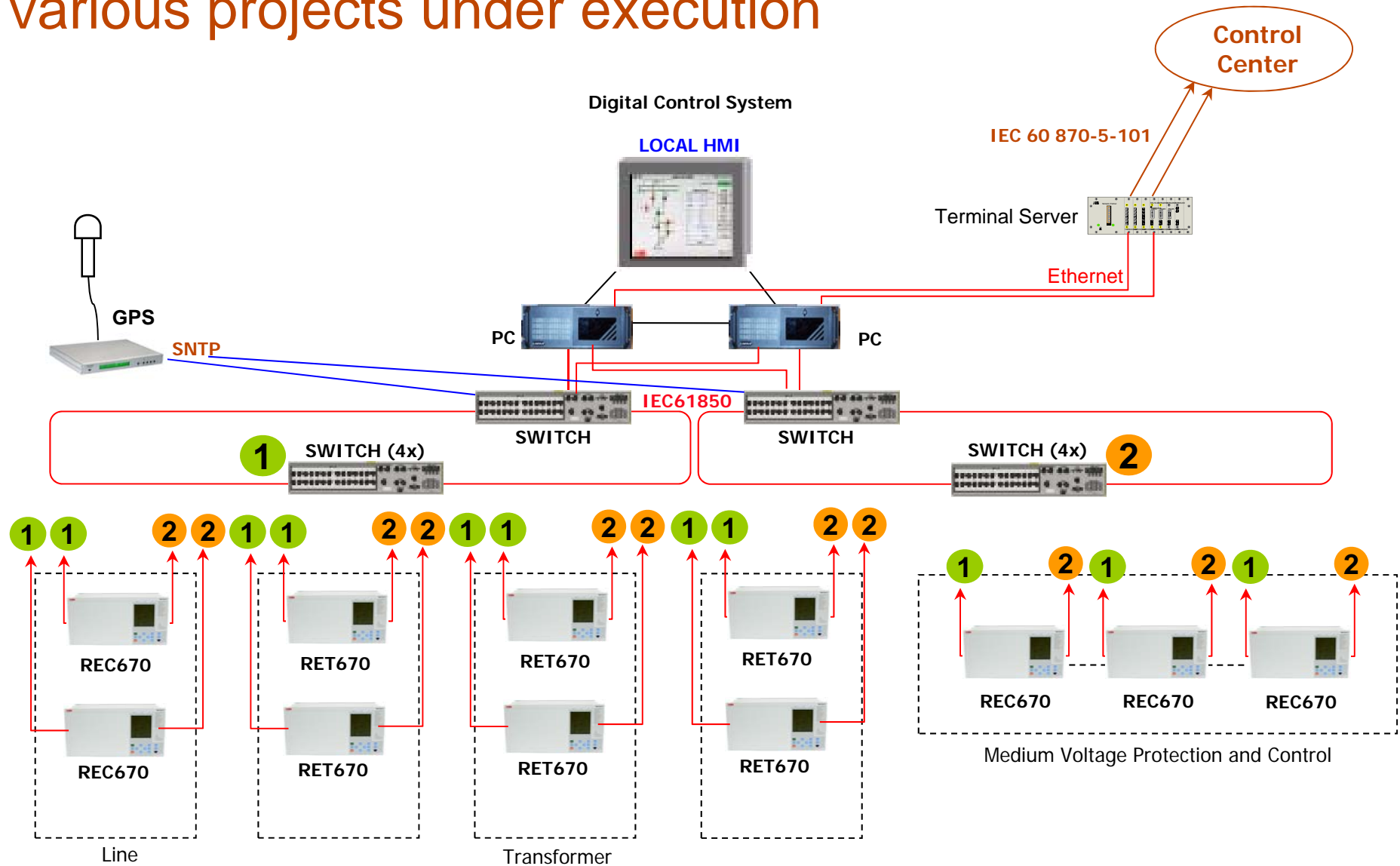
Successful long term in-house verification / pilot project



- Continues long term in-house test at the ABB system verification center
- Successfully working since more than a year.
- All stability and stress tests passed
- PRP is well proven, uses minimal configuration effort and is interoperable with single attached devices

Experience with PRP

Various projects under execution



Conclusion

- Recommendation if redundant links on IEDs is required
 - **PRP for ...**
 - High demanding applications (High-voltage transmission substations, Complex industrial applications, ...)
 - Large systems
 - GOOSE is used for time critical applications
 - **HSR for ...**
 - Small systems (Distribution applications)
 - GOOSE is used for time critical applications

Cyber Security for Substation Automation

Cyber Security for Substation Automation

Why is Cyber Security an issue?

- Cyber security has become an issue **by introducing Ethernet (TCP/IP) based communication protocols** to industrial automation and control systems. e.g. IEC60870-5-104, DNP 3.0 via TCP/IP or IEC61850
- **Connections to and from external networks** (e.g. office intranet) to industrial automation and control systems have opened systems and can be misused for cyber attacks.
- **Cyber attacks on industrial automation and control systems are real and increasing**, leading to large financial losses
- **Utilities need to avoid liability** due to non-compliance with regulatory directives or industry best practices;

Cyber Security for Substation Automation Drivers and attackers

Main Benefit

Reduce risk of damage by cyber attacks

Current drivers

Currently many initiatives and activities driven by technology, solutions and FUD

Cyber security approaches should be based on an understanding of risk

Who are the attackers?

- Accidents / Mistakes
- Rogue insider
- Malware
- Thieves / Extortionists
- Enemies / Terrorists



Bottom line is

likelihood is unknown
consequences are potentially huge

Cyber Security for Substation Automation

Key Cyber-Security initiatives

Standard	Main Focus	Status
NIST SGIP-CSWG	Smart Grid Interoperability Panel – Cyber Security Working Group	On-going *
NERC CIP	NERC CIP Cyber Security regulation for North American power utilities	Released, On-going *
IEC 62351	Data and Communications Security	Partly released, On-going *
IEEE PSRC/H13 & SUB/C10	Cyber Security Requirements for Substation Automation, Protection and Control Systems	On-going*
IEEE 1686	IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities	Finalized
ISA S99	Industrial Automation and Control System Security	Partly released, On-going *

* On-going: major changes will affect the final solution

IEC 62351 – Status Overview

Ongoing changes will affect the final version

IEC 62351	Power systems management and associated information exchange - Data and communications security	Official Status	Actual Status
Part 1	Communication network and system security – Introduction to security issues	TS	TS
Part 2	Glossary of terms	TS	TS
Part 3	Security for profiles including TCP/IP	TS	New Version Planned (depending on Part 9)
Part 4	Profiles including MMS	TS	New Version Planned (depending on Part 9)
Part 5	Security for IEC 60870-5 and derivatives	TS	New Version Planned (depending on ext. to IEC104)
Part 6	Security for IEC 61850	TS	Changes in progress
Part 7	Network and system management (NSM) data object models	TS	TS
Part 8	Role-Based Access Control	ACDV	ACDV
Part 9	Key Management (Certificate Handling)	NWP	NWP
Part 10	Security Architecture	NWP	NWP

NWP — New Work Item Proposal
 ANW — Approved New Work
 ACDV — Draft approved for Committee Draft with Vote
 CDTS — Circulated Draft Technical Specification
 TS — Technical Specification

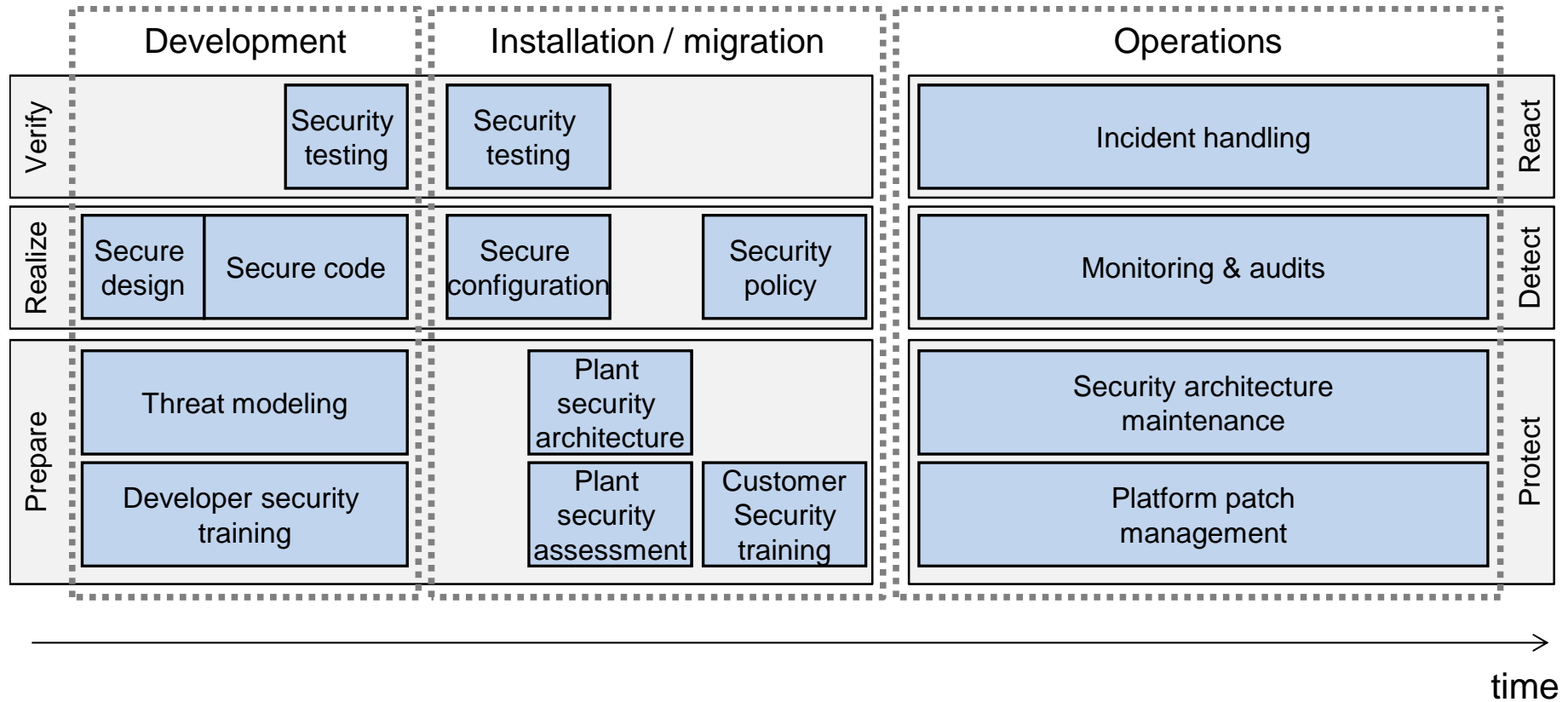
Cyber Security for Substation Automation

Back to the basics

- Accept responsibility
- Security is about processes
- Ignore compliance - at least at first
- There is no such thing as 100% security
- Security does not come for free

Cyber Security for Substation Automation

Cyber Security in the system lifecycle



Cyber Security for Substation Automation

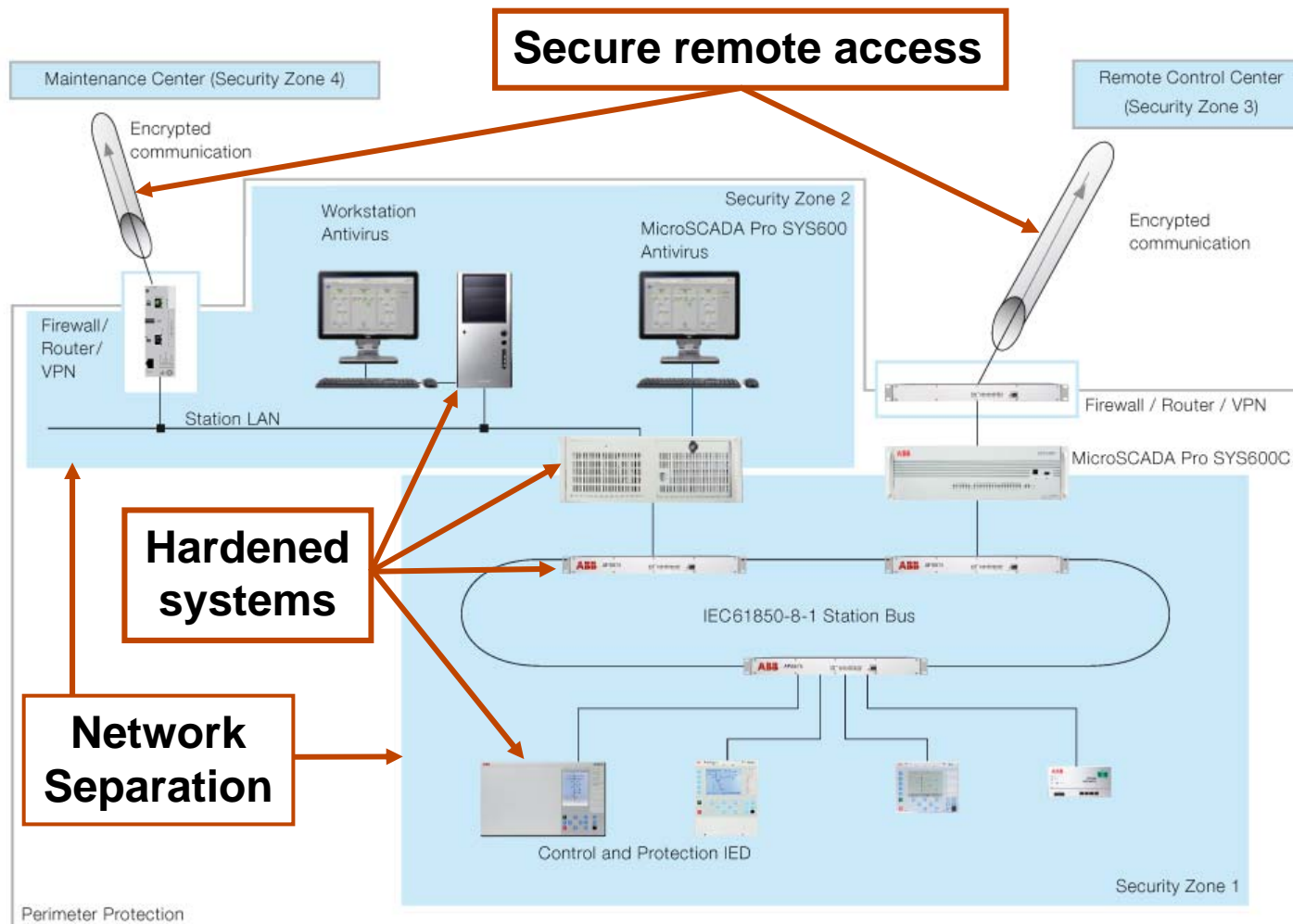
A pragmatic approach

- Defense in depth
- Least-privileges
- Network separation
- System Hardening
- Protected communications
- Secure remote access








All while keeping an eye on reliability, interoperability and performance.

Cyber Security for Substation Automation

Typical substation automation system architecture



Cyber Security for Substation Automation Trends

	Today	Trend
Regulation & Government initiatives	NERC CIP regulation for securing Bulk Electric System 	Additional security regulations expected for Smart Grid and will cover all voltage level  Government organizations increase attention to securing critical infrastructure 
Application Focus	Focus on Network Management and DCS 	Focus on end-to-end security 
Business aspects	Smart Grid stimulus funding tied to sound security approach  Avoiding fines associated with non-compliance (end-users)	Reduction of risks associated with cyber security 

ABB's Cyber Security Activities Summary

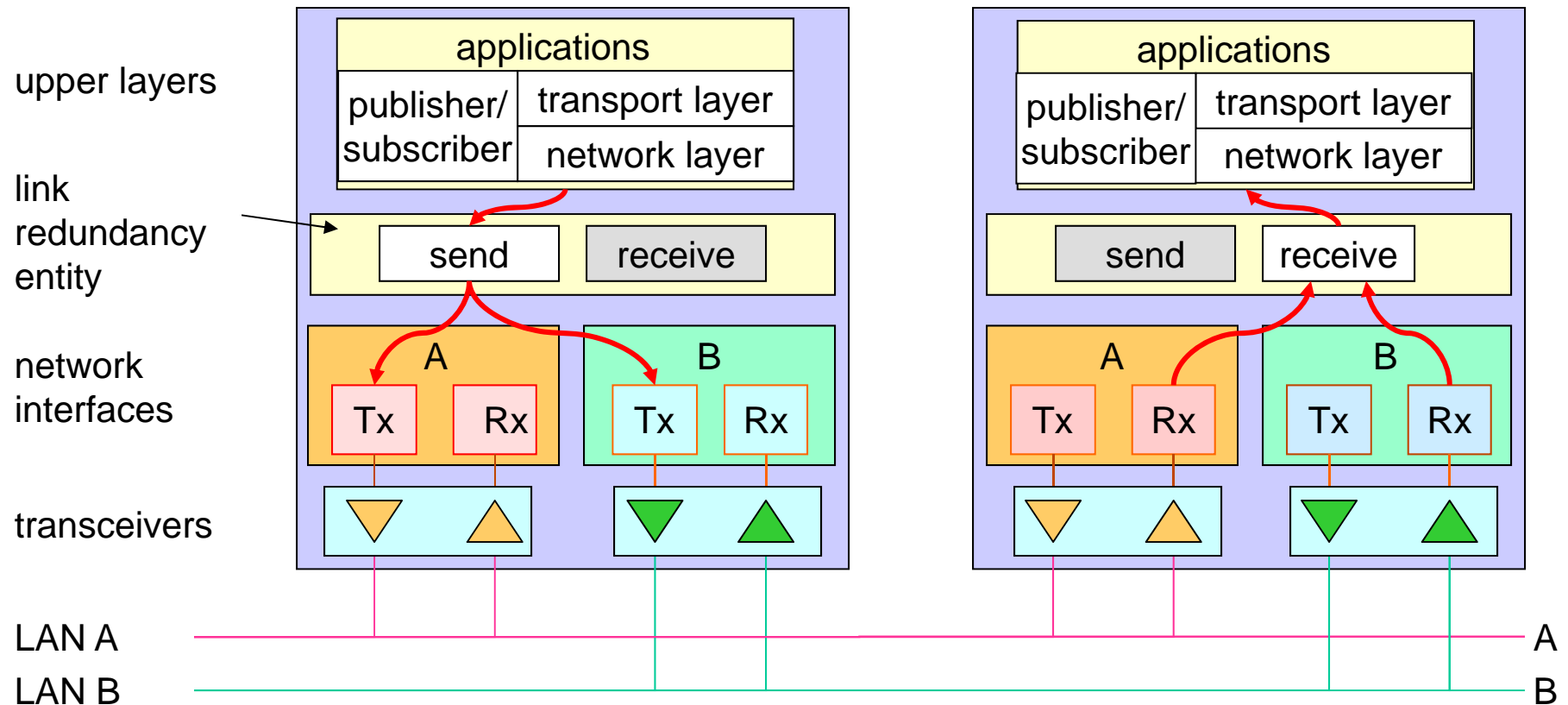


- Security is well established within ABB
- Today we can deliver products and systems that meet most customer security requirements to a high degree
- We will continue to adapt our products and system to meet additional requirements from customers and standards

Power and productivity
for a better world™



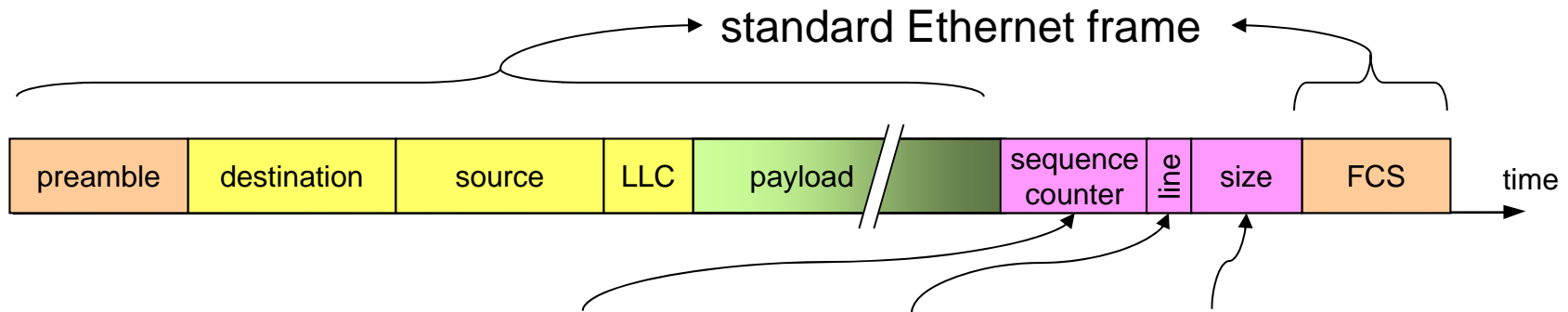
Redundant network with IEC 62439-3 PRP Parallel Redundancy Protocol



- **Send on both LANs:** the stack sends each frame simultaneously on LAN A and LAN B. Frames over LAN A and B have different transmission delays (or may not arrive at all)
- **Receive from both LANs:** the stack receives both frames, the entity between the link and the network layer handles the frames and can filter duplicates. Both lines are treated equal.
- Each node in PRP has the same MAC address and the same IP address on both network interfaces.

Redundant network with IEC 62439-3 PRP

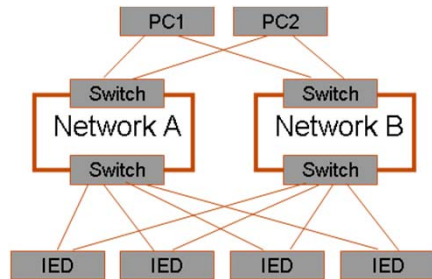
Discarding duplicates: Sequence counter



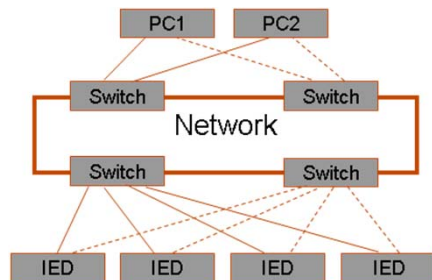
- each frame carries a **sequence counter**, a **line indicator** and a **size field**, inserted after the payload to remain transparent to normal network traffic.
- the send inserts the same sequence counter in both frames of a pair, and increments it by one for each sending from this node to that other node.
- the receiver keeps track of the sequence counter for each frame for each source MAC address it receives frames from. Frames with the same source and counter value coming from different lines are ignored.
- to this purpose, each node keeps a table of all other nodes in the network, based on observation of the network. This allows to detect nodes absence and bus errors at the same time.

Redundant ports on IEDs

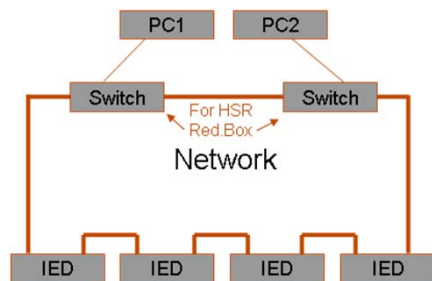
Overview of different redundancy methods



- Redundant Network
 - PRP (IEC 62439-3)
 - Dual homing (proprietary)

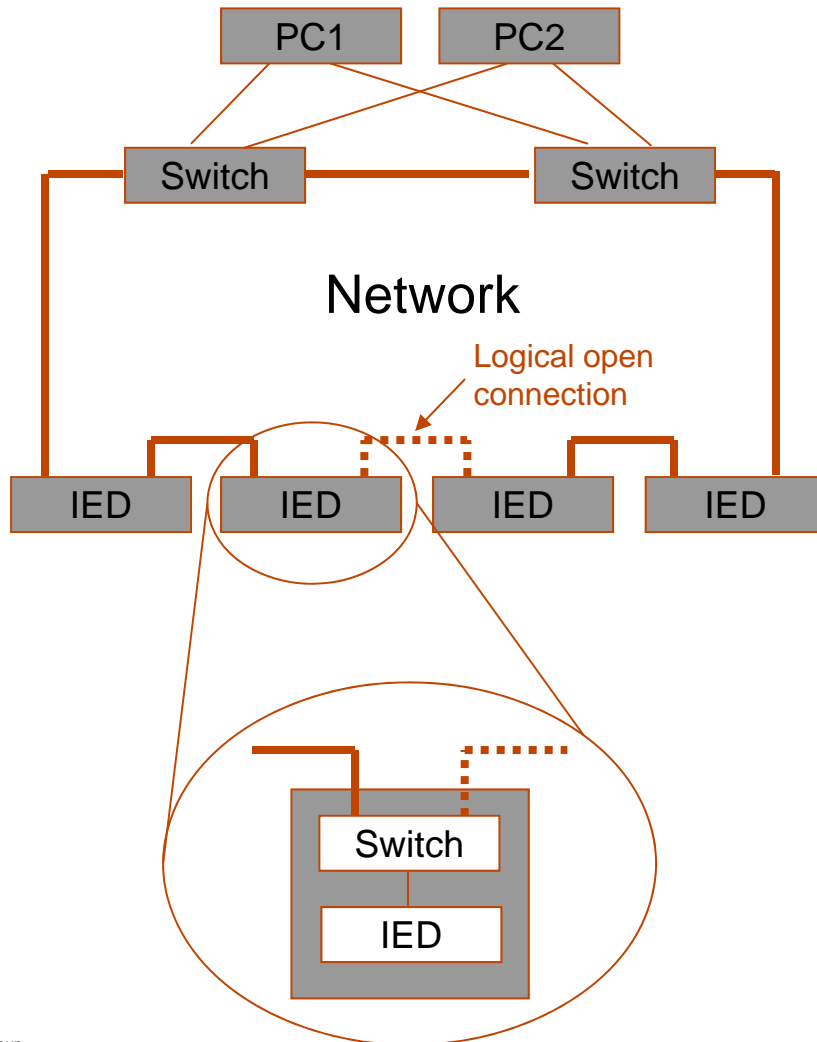


- Single Network
 - Channel switching (proprietary)



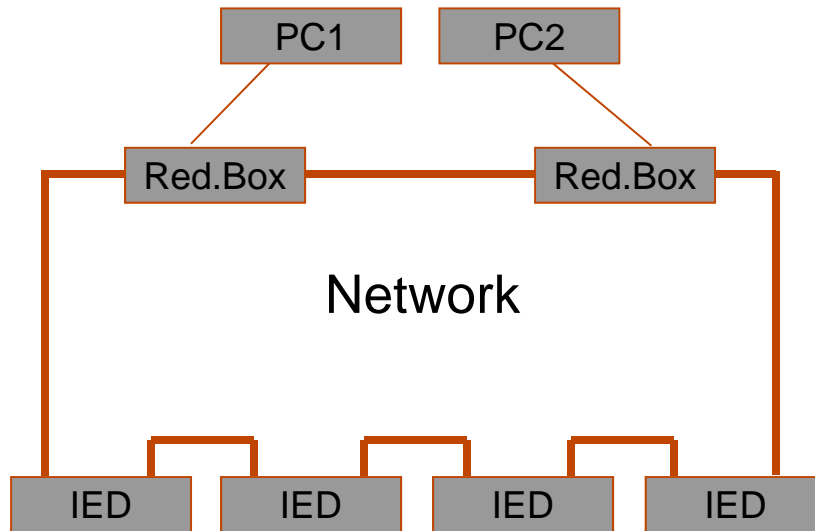
- Single Network, IEDs active part of Network
 - HSR (IEC 62439-3)
 - RSTP

Integrated Ethernet Switch with RSTP Principle



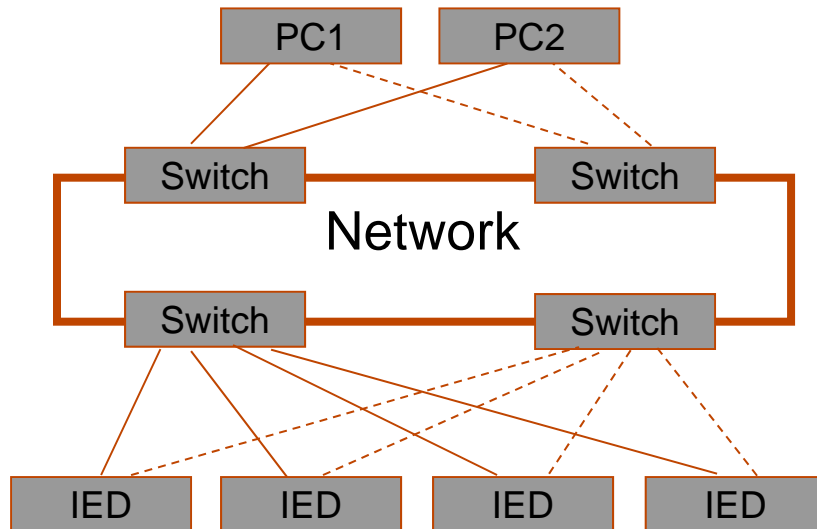
- Operation Mode
 - 2 ports active
 - RSTP protocol for ring redundancy
 - Recovery time typically 100ms (depends on the number of nodes and type of failure)
- Advantage
 - Low-cost
- Disadvantage
 - Slow recovery performance
 - Use GOOSE only for not time critical applications
 - Messages can be lost during recovering phase
 - No network redundancy
 - IEDs are active part of the network
 - Disconnecting, power-off IEDs disturbs or interrupts the network
 - Transmission delay by each “hop” (each IED)
 - Not interoperable with e.g. HSR

Integrated Ethernet Switch with HSR Principle



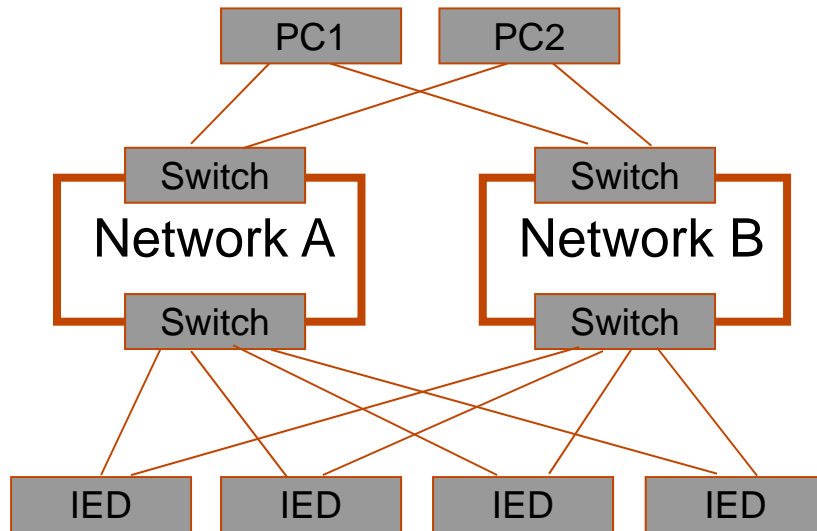
- Operation Mode
 - 2 ports active
 - HSR protocol for ring redundancy
 - Switch over time 0ms
- Advantage
 - Low-cost
 - No recovery time
 - No messages are lost
 - Standard according IEC 61850-8-1/9-2 Edition 2
- Disadvantage
 - No network redundancy
 - IEDs are active part of the network
 - Disconnecting, power-off IEDs disturbs or interrupts the network
 - Transmission delay by each “hop” (each IED)

Channel Switching Method Principle



- Operation Mode
 - 1 Port active
 - 1 Port monitored passive (only link to switch is monitored)
 - Switch over time approx. 10ms
- Advantage
 - IEDs are not active part of the network
- Disadvantage
 - Slow switch-over performance
 - Use GOOSE only for not time critical applications
 - Messages can be lost during switch-over
 - No network redundancy, IEDs have to be on the same network
 - Not according IEC 61850-8-1
 - Not interoperable with e.g. PRP

Parallel Redundancy Protocol (PRP) Principle



- Operation Mode
 - 2 Ports active
 - Messages are sent / received simultaneously on both ports
 - Switch over time 0ms
- Advantages
 - No recovery time
 - No messages are lost
 - Network redundancy (Network A and B)
 - IEDs are not active part of the network
 - Standard according IEC 61850-8-1/9-2 Edition 2
- Disadvantages
 - Higher cost