Robustness Requirement in Industry and Energy

Thomas Müller

Zurich University of Applied Sciences
Institute of Embedded Systems
Technikumstrasse 9
CH-8401 Winterthur

Phone: +41 (58) 934 75 09
WWW: http://ines.zhaw.ch
E-Mail: muth@zhaw.ch

Thanks to the HSR Project Team for the slides

Prof. Dr. Hubert Kirrmann
ABB

Oliver Kleineberg
Hirschmann

Clemens Hoga
Siemens

Dr. Karl Weber
ZHAW

zhaw

HIRSCHMANN
A BELDEN BRAND

SIEMENS

Power and productivity for a better world™ ABB

Redundancy requirements in Energy

School of Engineering
InES Institute of Embedded Systems

- IEC TC57 WG10 (POWER SYSTEM IED COMMUNICATION AND ASSOCIATED DATA MODELS)
  studied how long the substation automation application can tolerate the loss of communication without causing a malfunction of the protection system (next slide).
- In substation automation, redundancy fulfilling the (n-1) criteria (no single point of failure) is crucial
- Substation automation systems require communication networks that fulfill the (n-1) criteria as well
- Most important criteria for redundancy is the recovery time:
  How long does it take to restore service after a failure

Recovery delay demands as shown in IEC 61850-5 ED2

School of Engineering
InES Institute of Embedded Systems

Communicating partners	Service	Application recovery tolerated delay	Required Communication Recovery Time
SCADA to IED, client-server	IEC 61850-8-1	800 ms	400 ms
IED to IED interlocking	IEC 61850-8-1	12 ms (with Tmin set to 4 ms)	4 ms
IED to IED, reverse blocking	IEC 61850-8-1	12 ms (with Tmin set to 4 ms)	4 ms
Protection trip excluding Bus Bar protection	IEC 61850-8-1	8 ms	4 ms
Bus Bar protection	IEC 61850-9-2 on station bus	< 1 ms	Bumpless
Sampled Values	IEC 61850-9-2 on process bus	Less then two consecutive samples	Bumpless

To fulfill these requirements, IEC 61850-8-1 and -9-2 uses redundancy solutions standardized for Industrial Ethernet by **IEC 62439-3.**

Standard IEC 62439:
High Availability Automation Networks

School of Engineering
InES Institute of Embedded Systems

- Ethernet based high availability networks
- Specifies relevant principles
- Independent of application protocol
- Can be used for any application
  - Industrial automation
  - Energy automation
  - Transportation
  - Medical
  - …

Redundancy solutions of IEC 62439

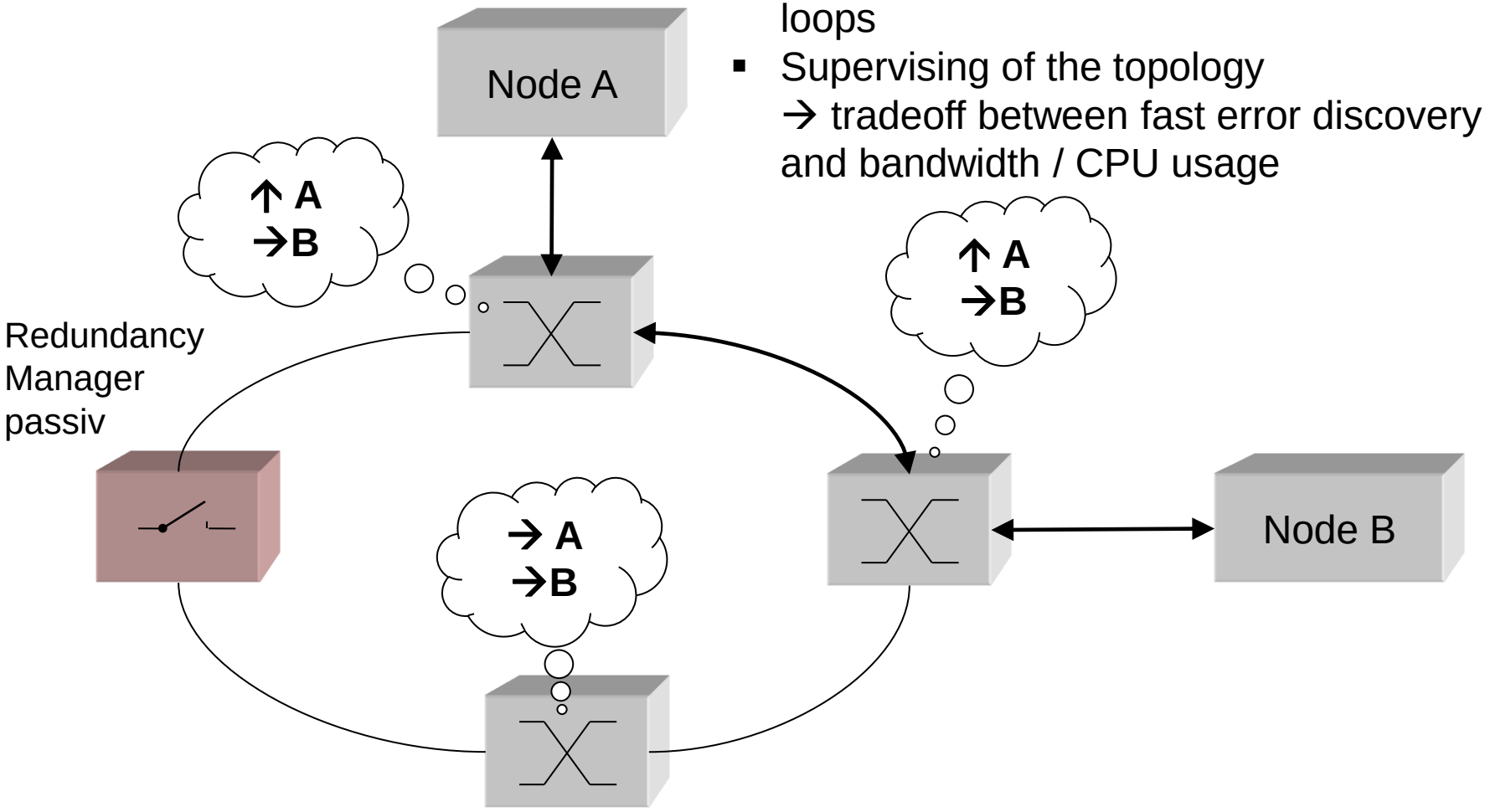
School of Engineering
InES Institute of Embedded Systems

- Protocols using Reconfiguration (with small recovery time)
  - RSTP (Rapid Spanning Tree Protocol)
    IEEE 802.1D-2004
    IEC 62439-1 Annex A (recovery time calculation methods)
  - MRP (Media Redundancy Protocol)
    IEC 62439-2
- Protocols with “zero” switchover time (seamless)
  - PRP (Parallel Redundancy Protocol)
    IEC 62439-3 Clause 4
  - HSR (High-availability Seamless Redundancy)
    IEC 62439-3 Clause 5

Example of using Reconfiguration: Media Redundancy Protocol

School of Engineering
InES Institute of Embedded Systems

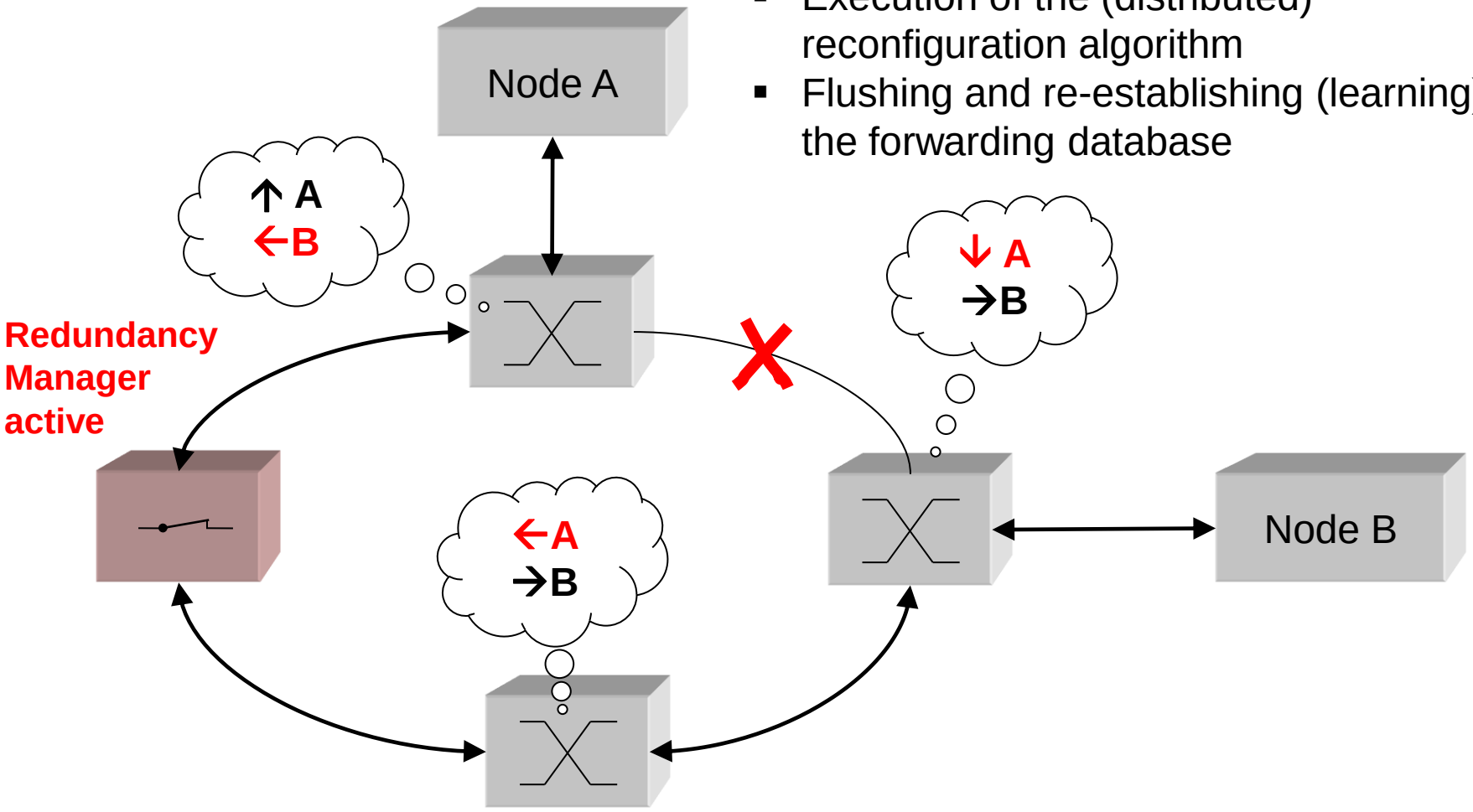
- Blocking redundant paths to prevent loops
- Supervising of the topology
  → tradeoff between fast error discovery and bandwidth / CPU usage



Example of using Reconfiguration: Media Redundancy Protocol

School of Engineering
InES Institute of Embedded Systems

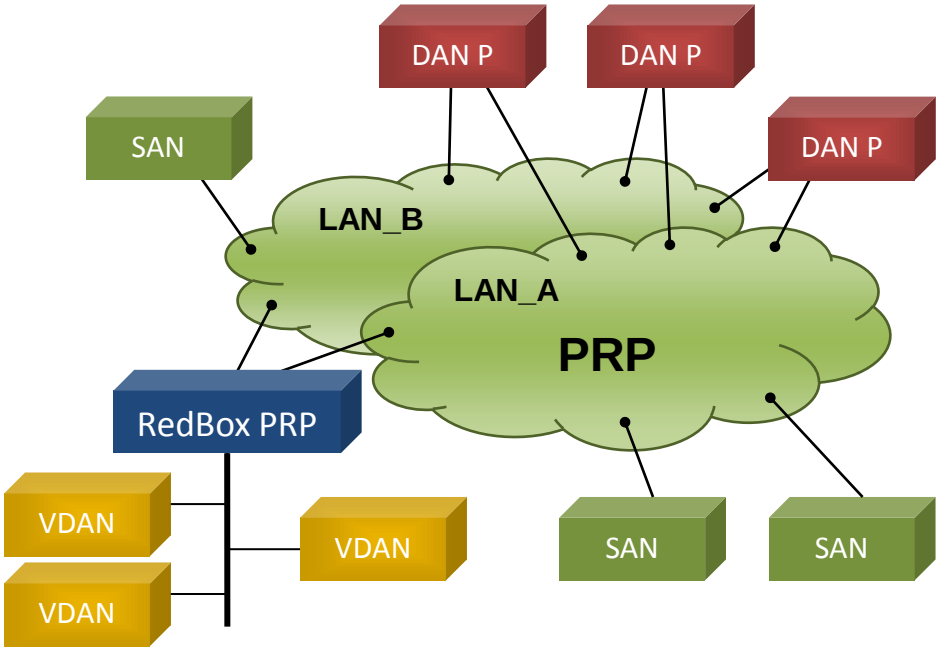
- Execution of the (distributed) reconfiguration algorithm
- Flushing and re-establishing (learning) the forwarding database



Parallel Redundancy (PRP)

School of Engineering
InES Institute of Embedded Systems

- PRP doubles network infrastructure
- Basic Redundancy Function requires Double Attached Nodes (DAN P): Same send/receive function on both ports
- No forwarding between the ports
- Standard Nodes directly attachable; but :
  - no redundancy support
  - no connectivity between LAN A /B
- Safe discard of duplicates by redundancy trailer added to frames (PRP 1: basically sender's frame sequence number)

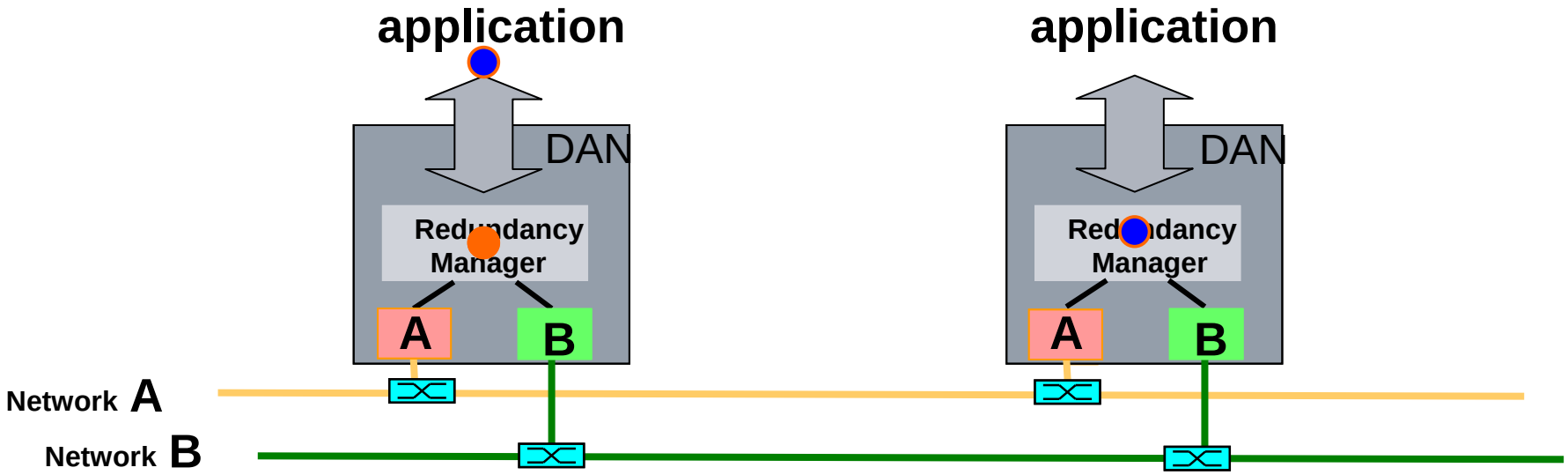


Redundancy Box (RedBox)

- Full connectivity for Virtual Dual Attached Nodes (VDAN)
- Acts as proxi node for VDAN

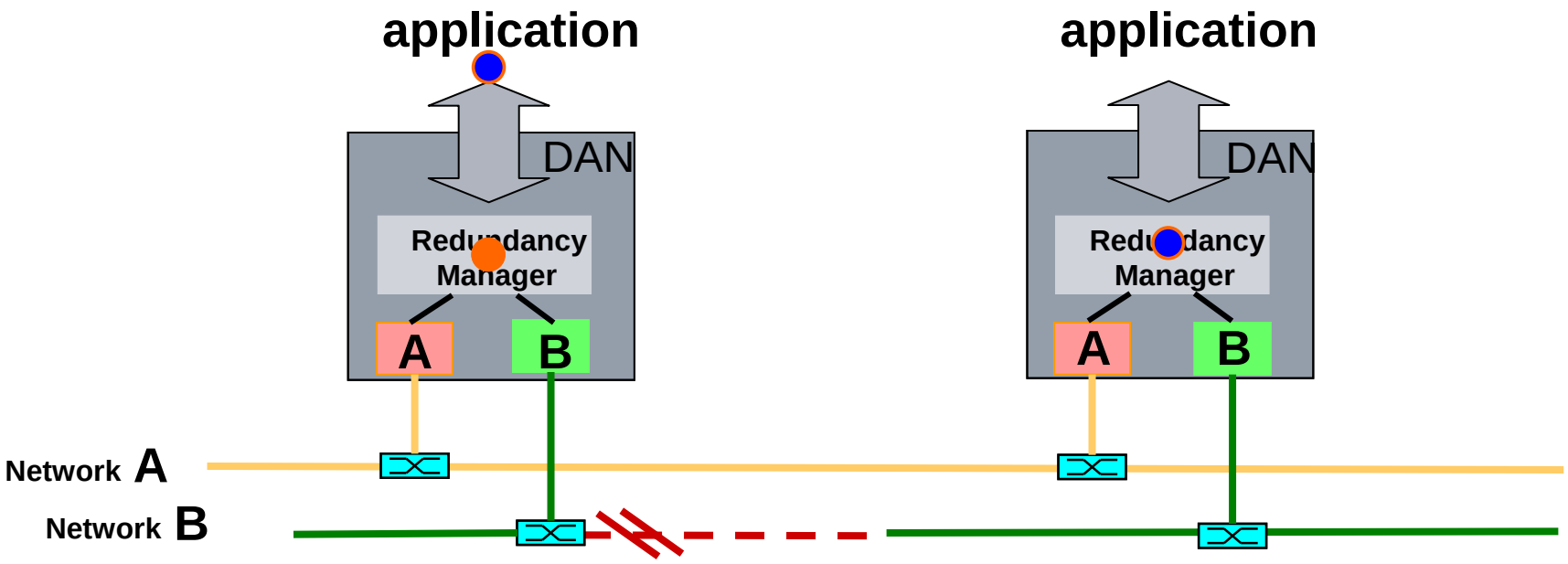
PRP normal operation

School of Engineering
InES Institute of Embedded Systems



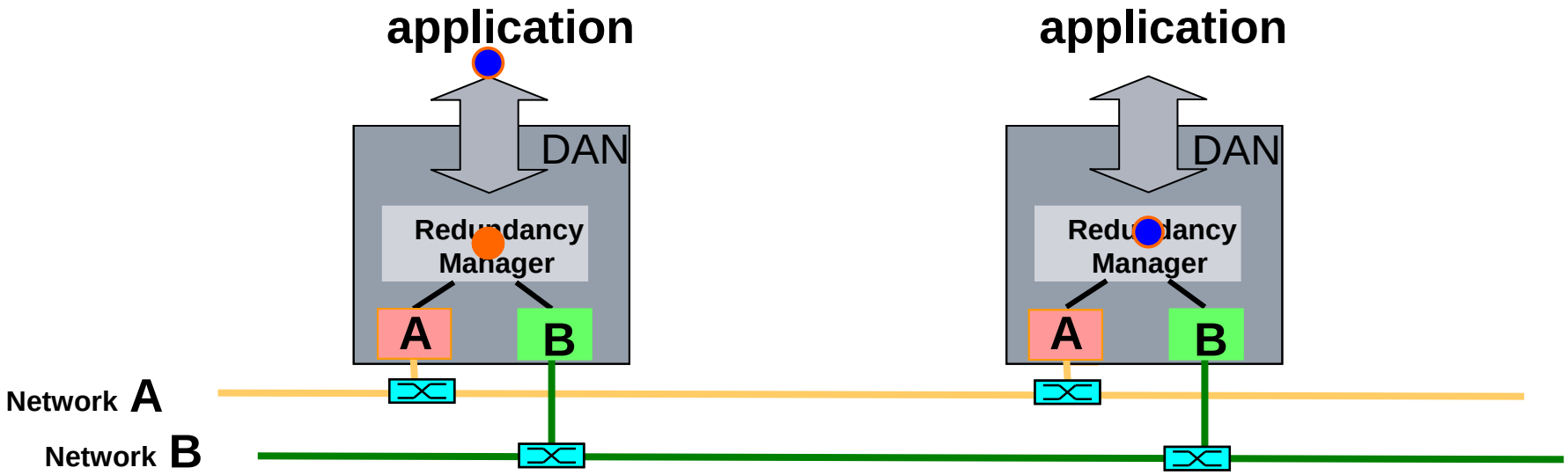
PRP operation with fault

School of Engineering
InES Institute of Embedded Systems



PRP normal operation (with long delay on Network B)

School of Engineering
InES Institute of Embedded Systems



- «Memory» for previously received frames required (duplicate discard buffer)
- Buffer size depends on maximal difference of network delay
- In case of a «forgotten» frame the duplicate is not discarded → but (most likely) it will be eliminated by upper layers

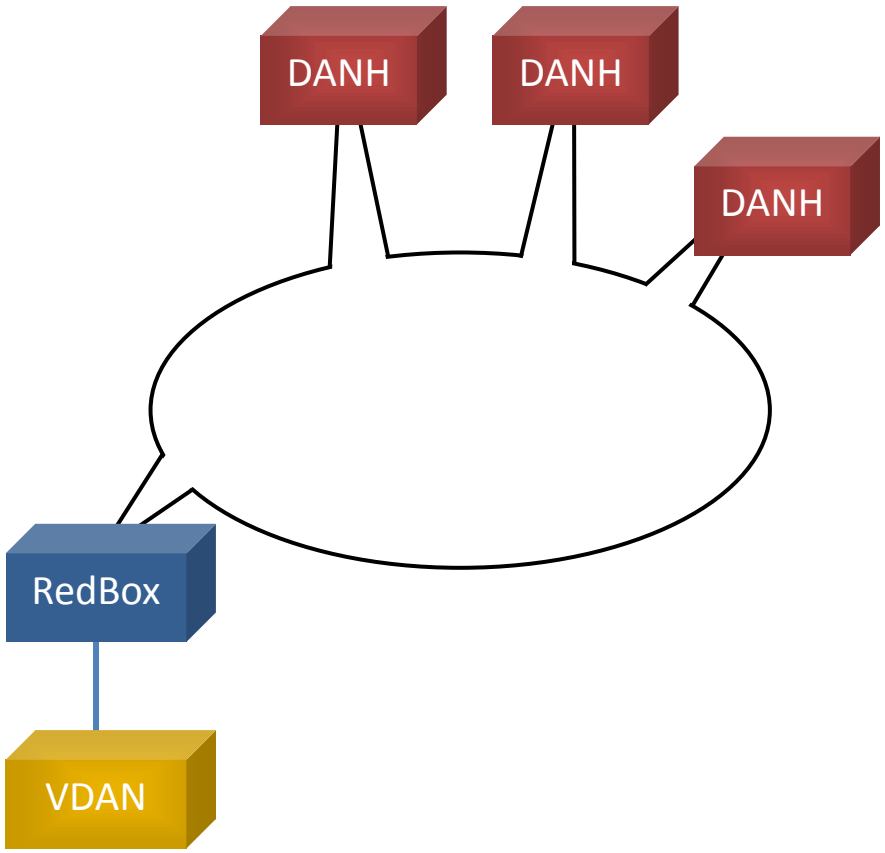
PRP Parallel Redundancy Protocol (IEC 62439-3 Clause 4)

School of Engineering
InES Institute of Embedded Systems

- PRP provides (n-1) redundancy (no single point of failure) and availability increase is high.
- PRP requires the full duplication of the network, but only of those parts that require seamless redundancy.
- The two networks must be completely independent (power, topology changes etc.) to avoid common mode errors
- PRP allows to attach standard Ethernet devices to one of the LANs. Therefore, networks with redundant and non-redundant parts can be built.
- PRP can be easily implemented in software by a dedicated driver that manages two standard Ethernet ports.

HSR basics

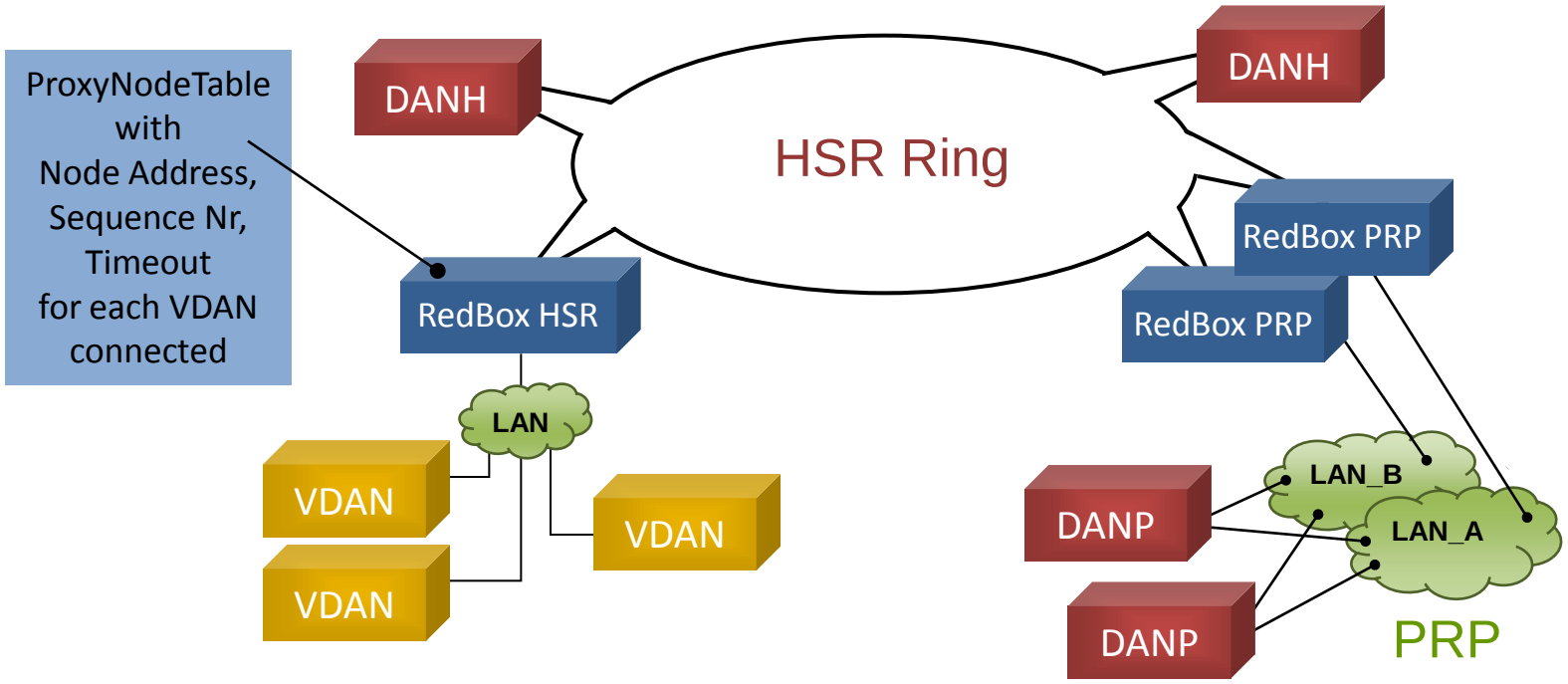
School of Engineering
InES Institute of Embedded Systems



- HSR and PRP share same semantics (both in standard IEC 62439-3)
- Send/receive function same as PRP
- Forwarding between the ports
- Basic forwarding rule is broadcast-like:
  - Frames are forwarded on all ports
  - A frame is sent only once per port
- Cut through switching applied to minimize forwarding delay → redundancy header (instead of trailer)
- Loop suppression mechanism:
  - Receiver removes frame (unicast)
  - Sender removes sent frame
  - Frames found in duplicate discard buffer are removed (for extended topologies)

HSR RedBox in an open Environment

School of Engineering
InES Institute of Embedded Systems



Standard Nodes Operation

- Redundancy Box (RedBox HSR) with 3 Ports (2 HSR, 1 Interlink)
- acts as proxy for VDAN (Virtualy Dual Attached Nodes)

PRP Coupling

- Redundancy Box (RedBox PRP)
- Conversion of Frame Format (Tag)
- Suppression of back feeding between LAN_A and LAN_B

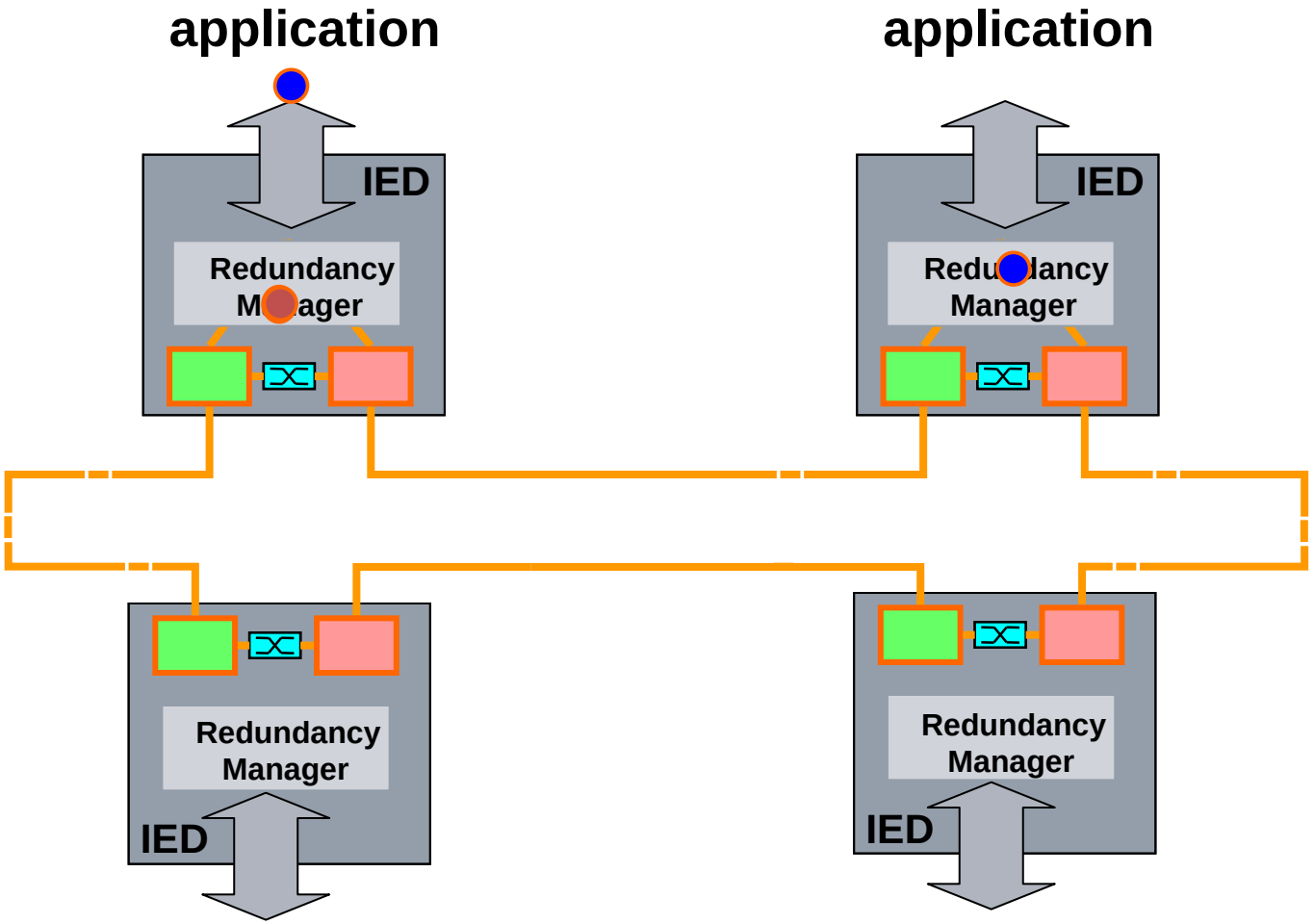
HSR High-availability seamless redundancy IEC 62439-3 Clause 5

School of Engineering
InES Institute of Embedded Systems

- Provides (n-1) redundancy for all network components (no single point of failure)
- Provides seamless redundancy for station bus and process bus
- Allows to build rings without using switches
- Cost-effective solution
- Requires dedicated hardware to keep the forwarding delay low.

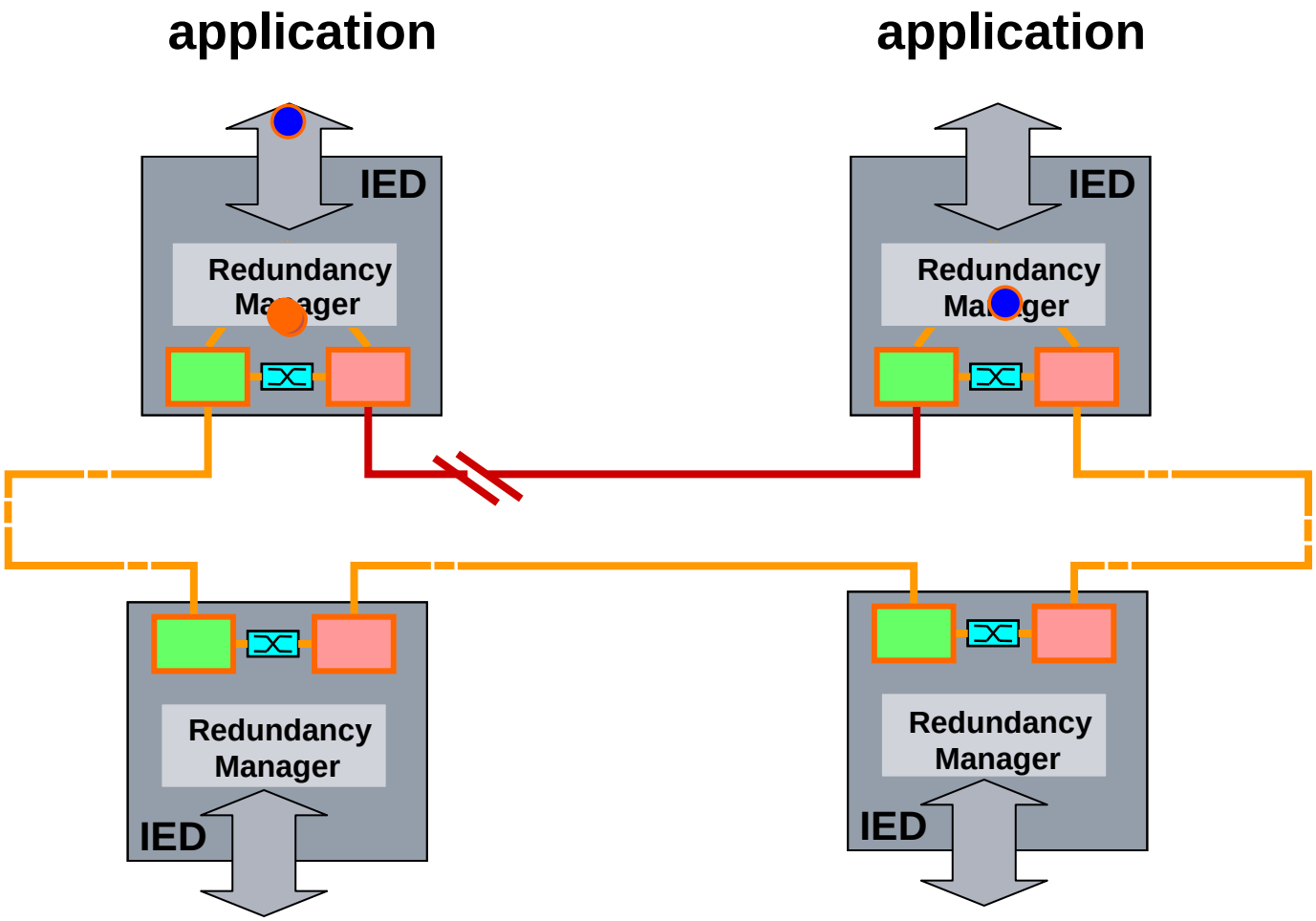
HSR normal operation (unicast)

School of Engineering
InES Institute of Embedded Systems



HSR operation with fault

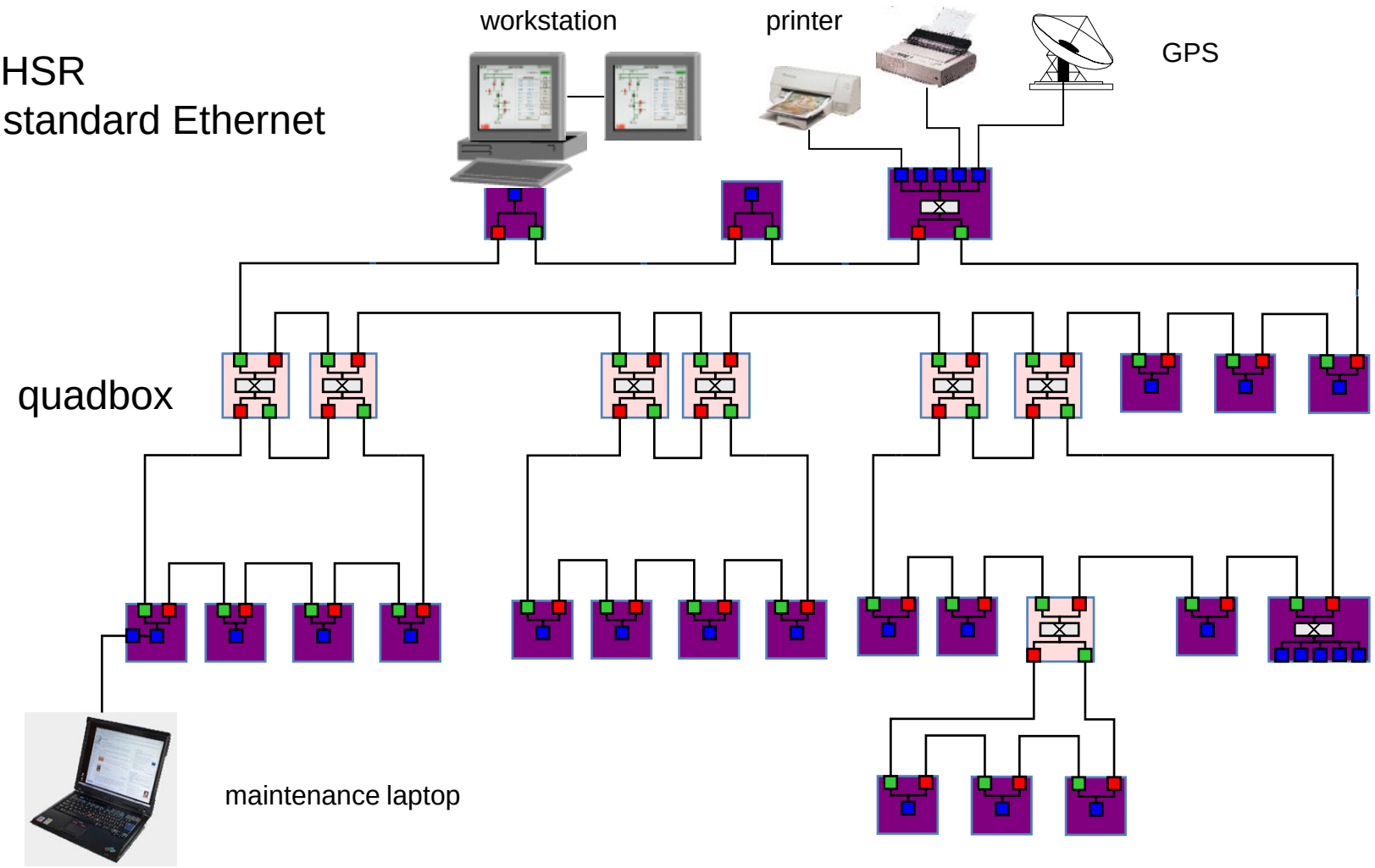
School of Engineering
InES Institute of Embedded Systems



HSR: rings of rings: three levels

School of Engineering
InES Institute of Embedded Systems

- HSR
- standard Ethernet



- no RSTP protocol any more (but can be used)
- note that level 3 is singly attached (only one quadbox)

Summary

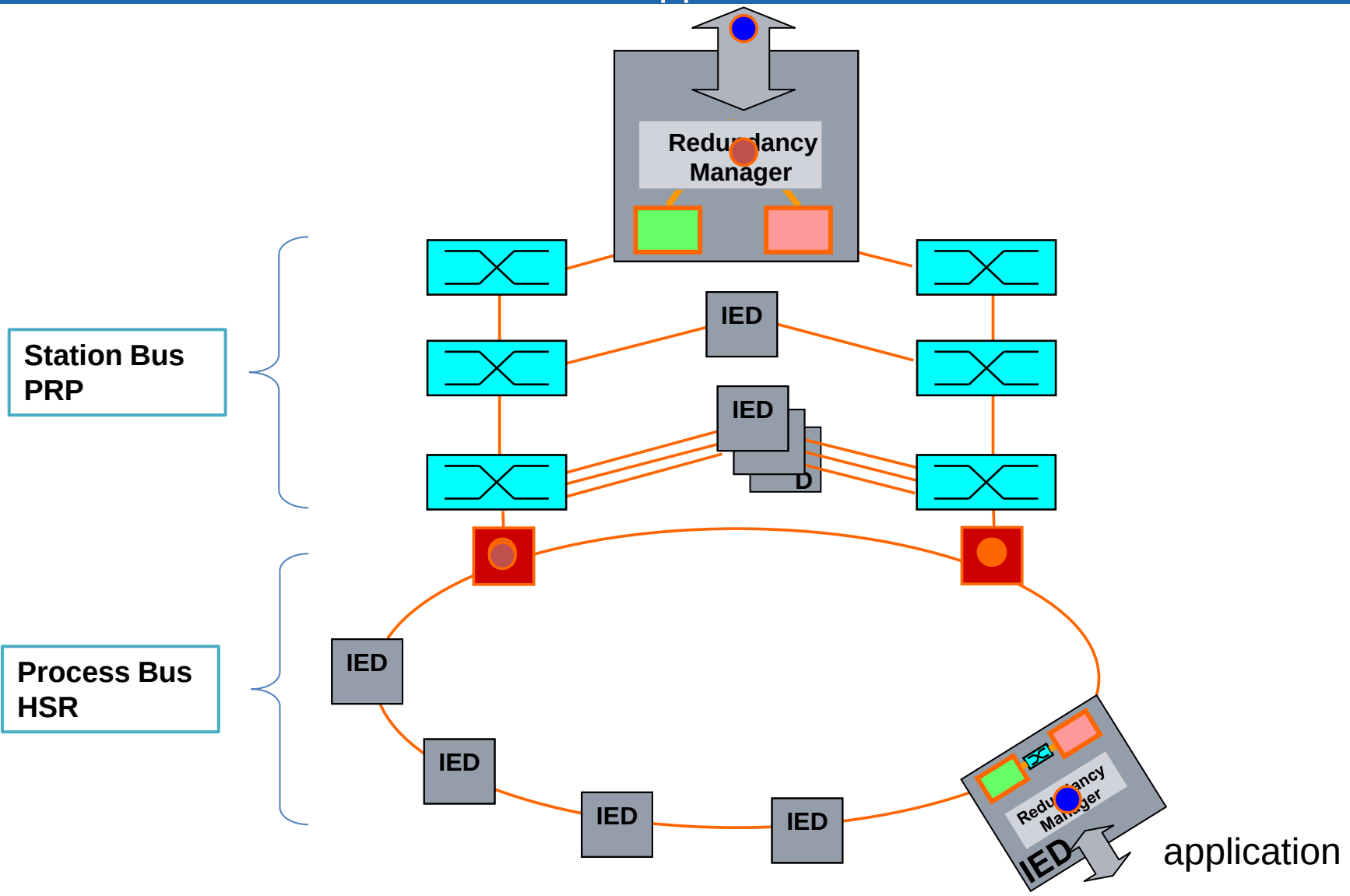
IEC 61850 specifies several redundancy methods

PRP seamless, for high-end substations, combines topologies redundant and not redundant, easily to implement in software
SW-Drivers available from at least two suppliers (ZHAW, NetModule);
RedBox IP (VHDL and Code) for FPGA-Implementation from ZHAW.

HSR seamless, for voltage levels and process bus, rings and rings of rings
Requires nodes with dedicated hardware, but after this initial investment, provides a cost-effective redundancy.
Allows ring and parallel topologies, but not mixing redundant and non-redundant devices on the same network (RedBox is required).
Several companies are developing components with the support of the KTI project of ZHAW.

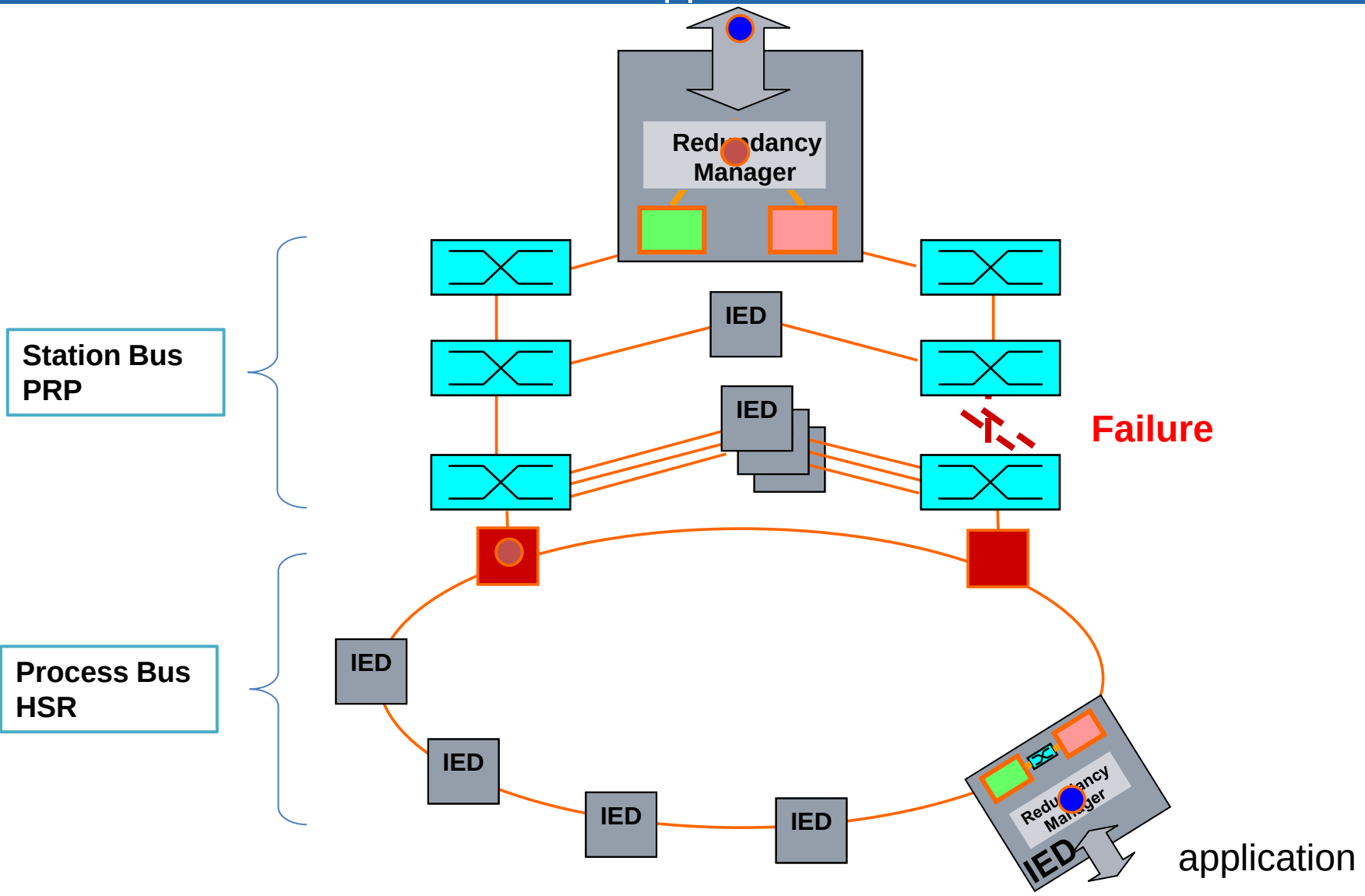
PRP/HSR in Parallel and Ring Redundancy

School of Engineering
InES Institute of Embedded Systems



PRP/HSR in Parallel and Ring Redundancy

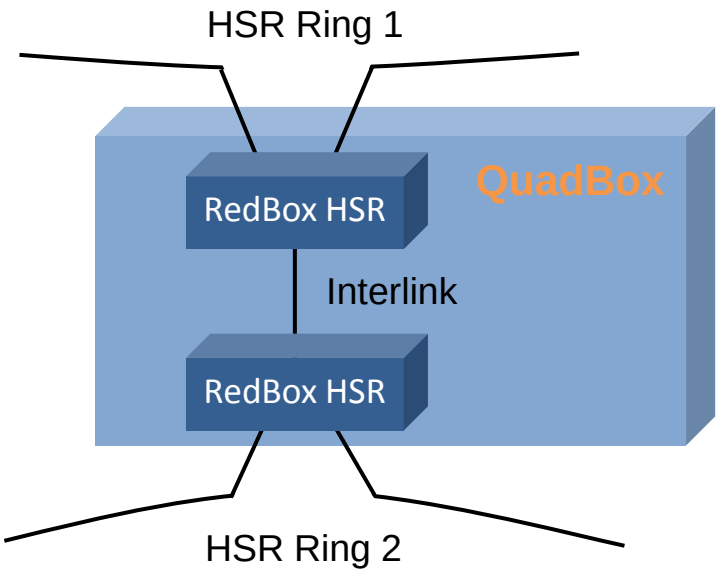
School of Engineering
InES Institute of Embedded Systems

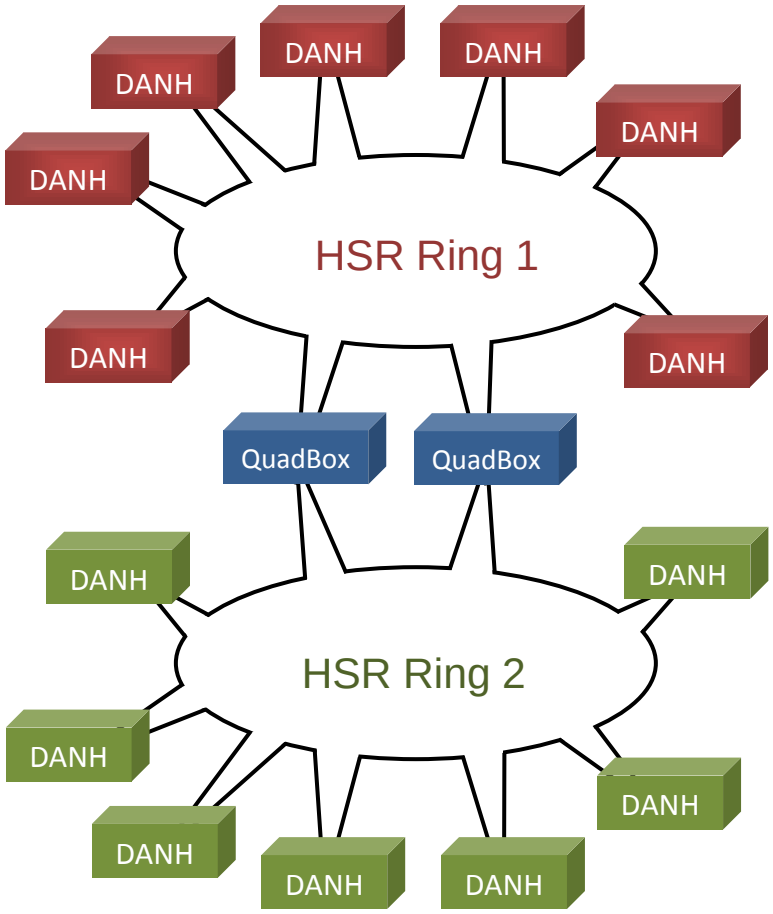


HSR Ring Coupling

School of Engineering
InES Institute of Embedded Systems

- Ring Coupling connects networks – not a single node
- Basic QuadBox can be implemented using 2 standard RedBoxes HSR





- This basic two ring topology does no traffic partitioning because all frames are forwarded to both rings

HSR Enhanced Ring Coupling (future)

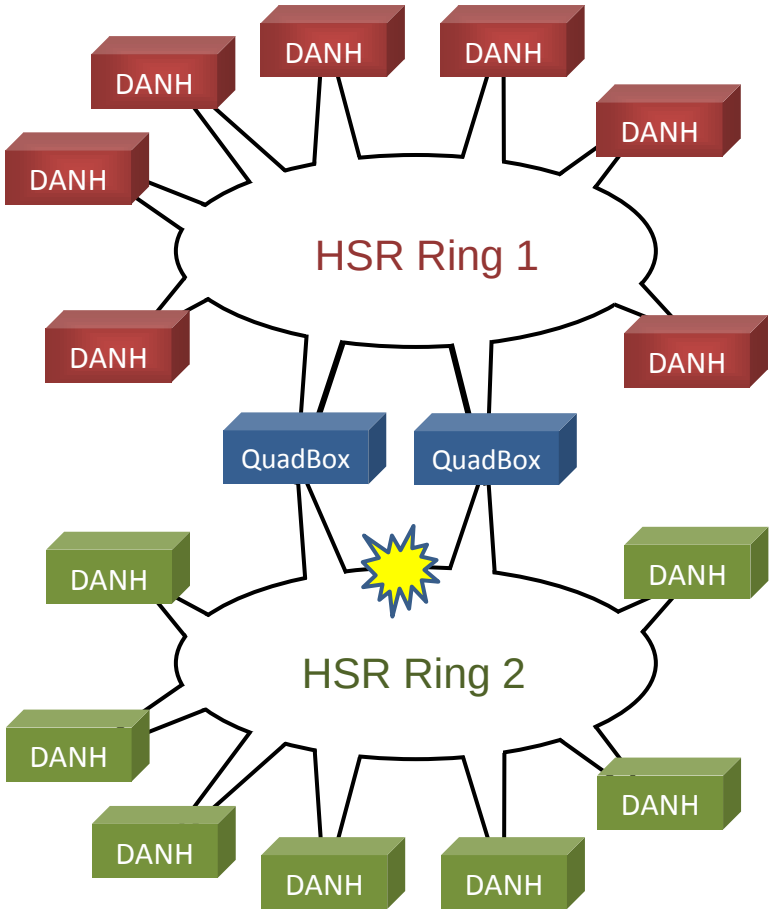
School of Engineering
InES Institute of Embedded Systems

- Use of any possible path is NOT a good idea:
  - In presence of high network load
  - Different wire speed

→ Enhance HSR RedBoxes with duplicate Filtering and Forwarding Rules

- Shall ring 1 (2) be used as bypass for link errors?

→ Overload can cause duplicate detection to fail: Problem of circulating frames



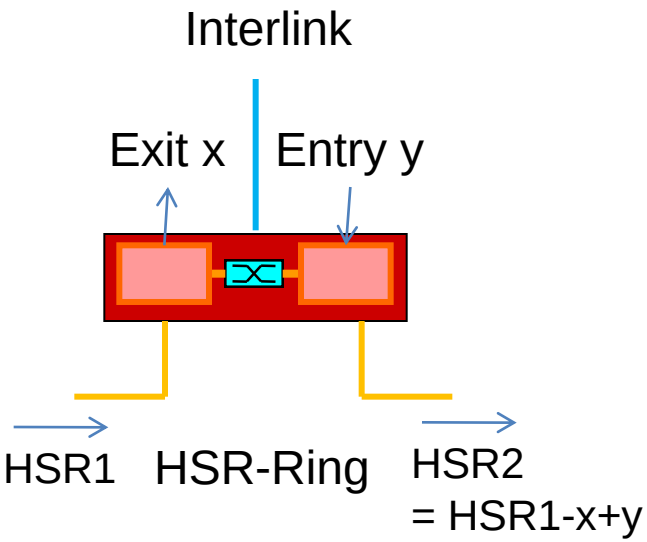
Effects of Overload

Critical load situation occur

- with increased number of nodes
- with sporadic traffic pattern
- In presence of network errors
- in emergency situations

Effects

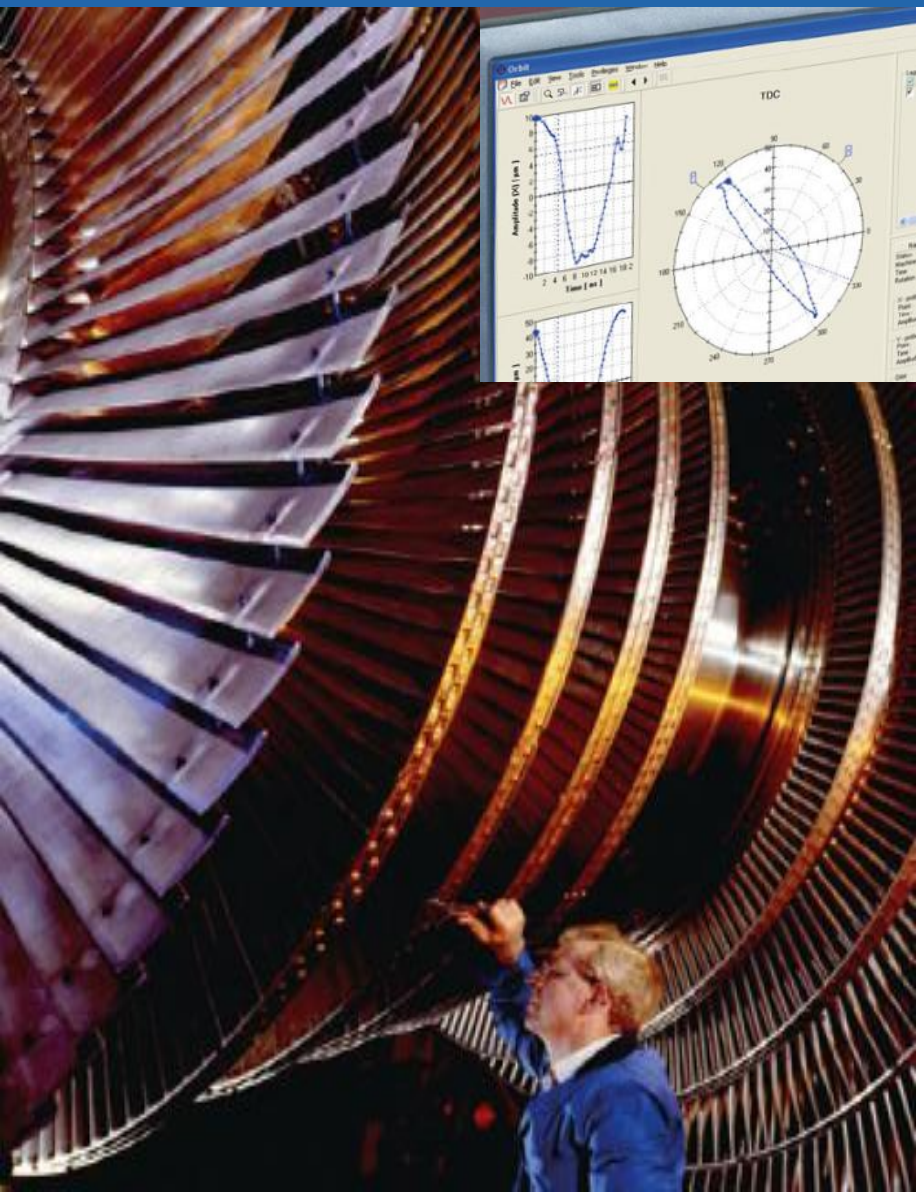
- Queuing of frames in ring
- Additional resources needed
- Increased latencies
- Frame losses or duplication
- Thread (for availability)



Load grows if x < y

Application example: Meetering and Functional Safety

School of Engineering
InES Institute of Embedded Systems



Requirements/characteristics:

- Robust synchronization
- Guarantied Transmission of Taco-Signal
- High peek bandwidth in case of error- or diagnoses operation
- Safety-critical alarms
- High availability

Solution:

- Synchronization using PTP (IEEE 1588)
- Reserved time slot for time- and safety-critical frames
- HSR as redundancy protocol

Audio / Video

School of Engineering
InES Institute of Embedded Systems

Goal:
Replacement of
cross-point switchers

- by the network in
- Broadcasting Centers
- Theaters, opera houses
- Live events (concerts)

Requirements:

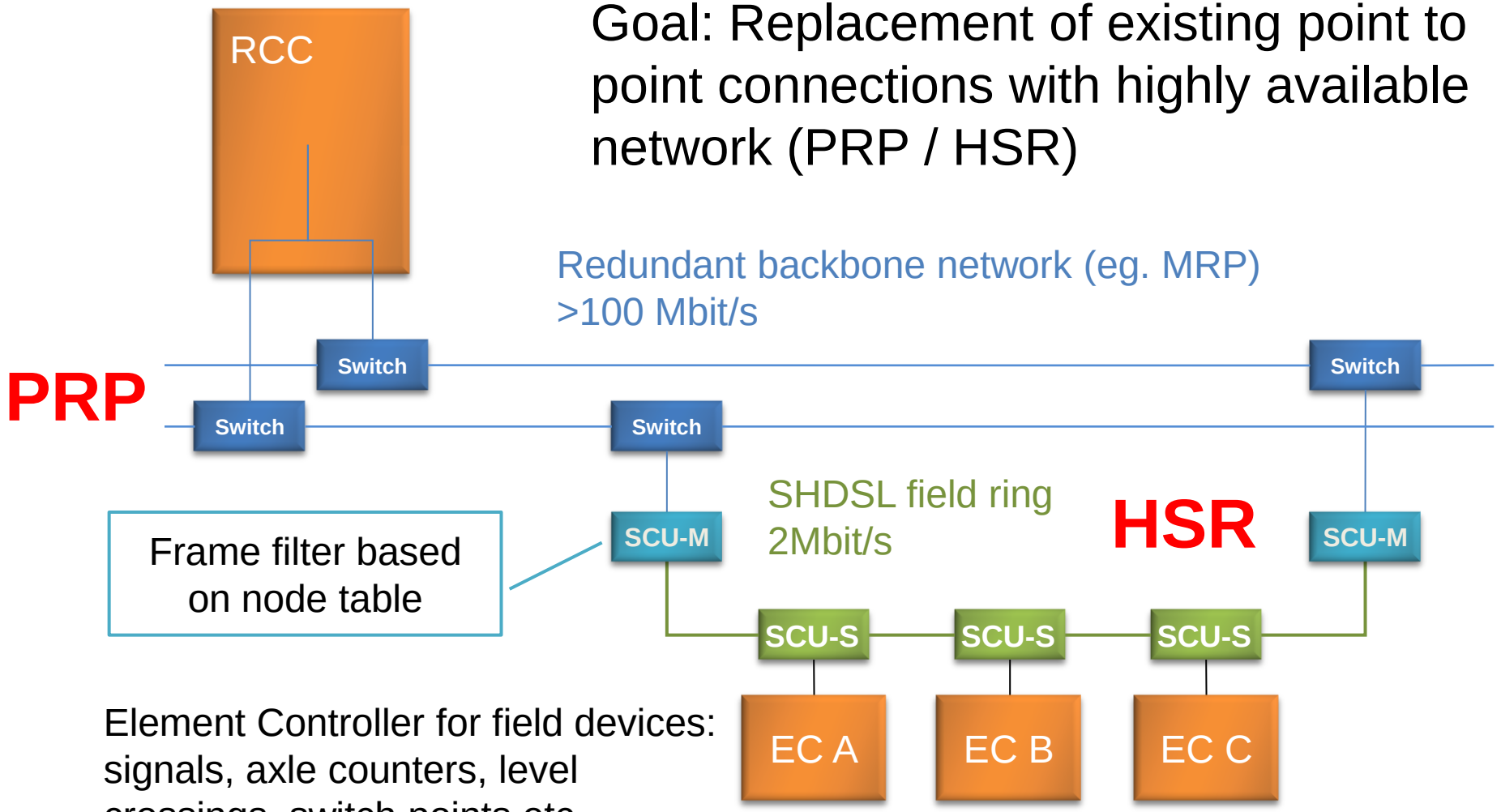
- Highly scalable design (from one up to thousands of channels)
- Phase locked word clocks with short synchronization time
- Streaming with low latency
- Seamless redundancy

Solution: again PTP and HSR like redundancy (merging in play out buffer)

Application example: Interlocking Network

School of Engineering
InES Institute of Embedded Systems

Railway Control Center



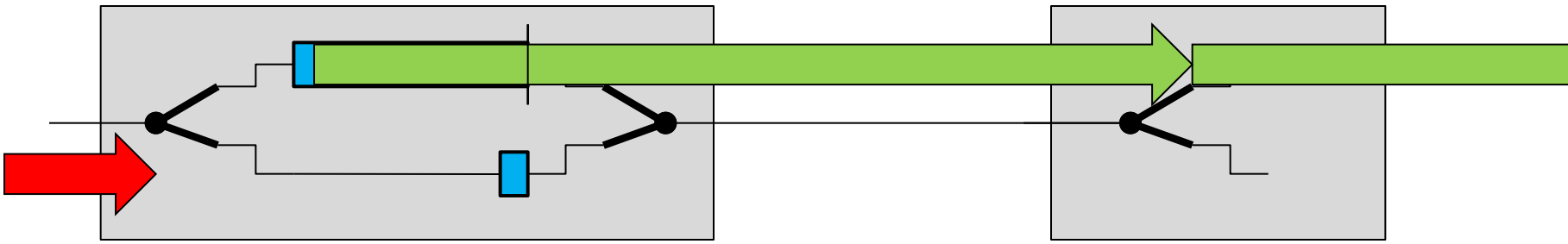
Application example: Interlocking Network (II)

School of Engineering
InES Institute of Embedded Systems

- Problem:
  - Security protocol allows only minimal delay of acknowlege

  → Avoid delay of RT-Frames by long Non-RT-Frames
- Solution:
  - Suspend (not abort) transmission of Non-RT-Frames

  → Layer 1 signaling is required (implemented in SHDSL-MAC)



Application example:
Interlocking Network Demonstrator

School of Engineering
InES Institute of Embedded Systems