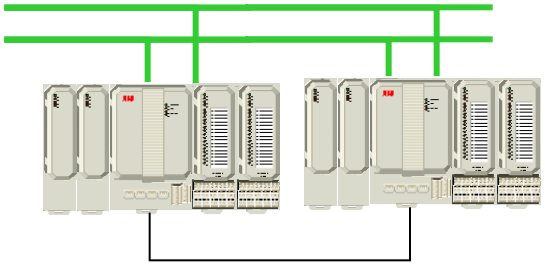
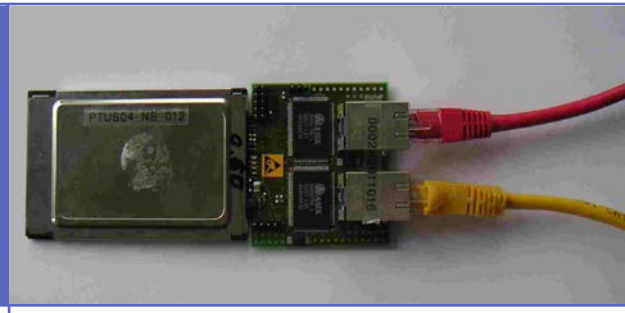
Standard Redundancy Methods for Highly Available Automation Networks

rationales behind the upcoming IEC 62439 standard

Hubert Kirrmann
ABB Switzerland Ltd,
Corporate Research





ETFA 2006

Scope

The good thing about “Industrial Ethernet” standards is that there are so many to choose from (IEC 61784) - you can even make your own.

It remains to be proved that the new networks are more reliable than the field busses that they are supposed to replace.

However, customers require the new technology to be “at least as dependable as the one it replaces”

But few “Industrial Ethernets” care about redundancy.

This talk shows what must be looked at when considering automation network redundancy and which solutions IEC 62439 proposes

1. Terms: availability and redundancy
2. Classification of requirements
3. Levels of device and network redundancy
4. Ethernet-based automation networks
5. Parallel (static) and serial (dynamic) redundancy
6. IEC 62439 solutions
7. Conclusion

Some terms

Availability applies to *repairable* systems

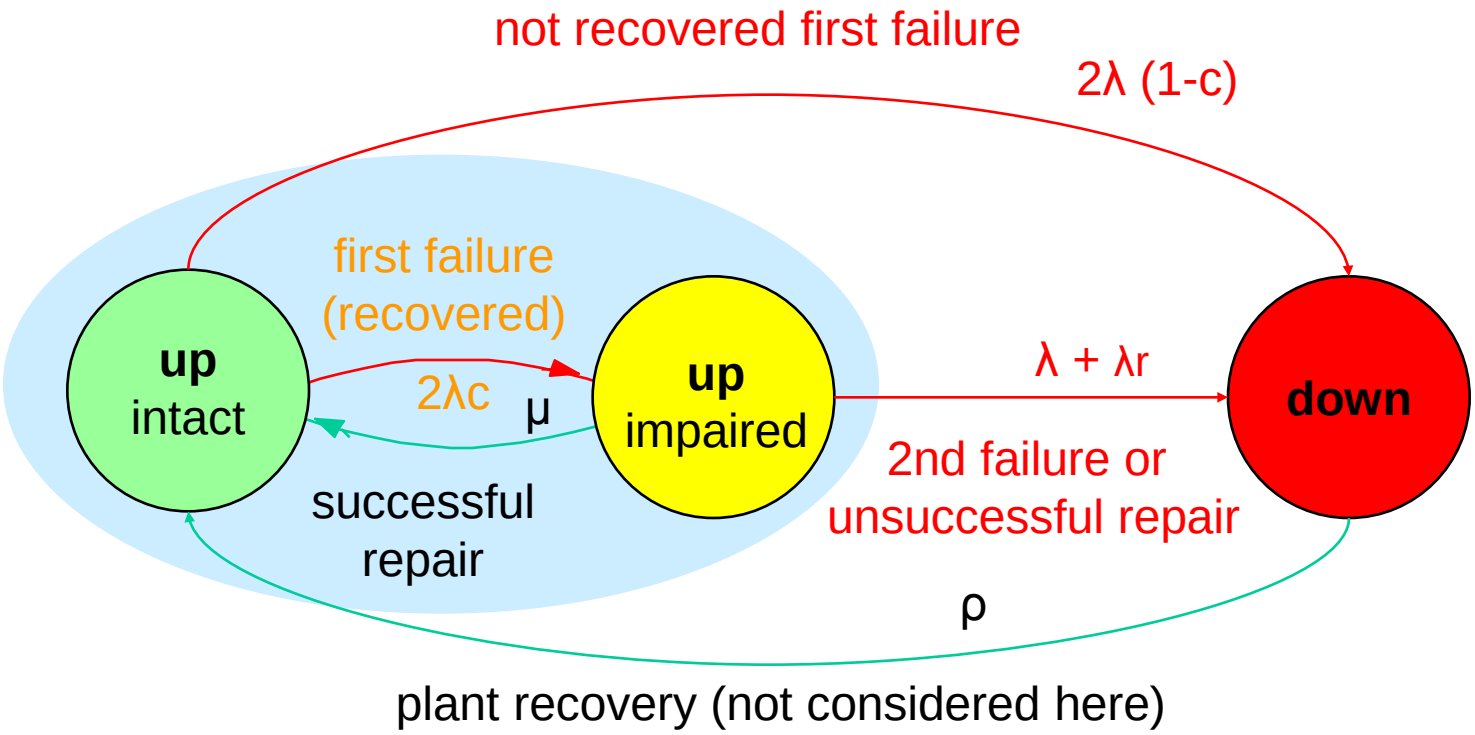
Availability is the fraction of time a system is in the “up” (capable of operation) state.

We consider systems in which availability is increased by introducing redundancy (availability could also be increased by better parts, maintenance)

Redundancy is any resource that would not be needed if there were no failures.

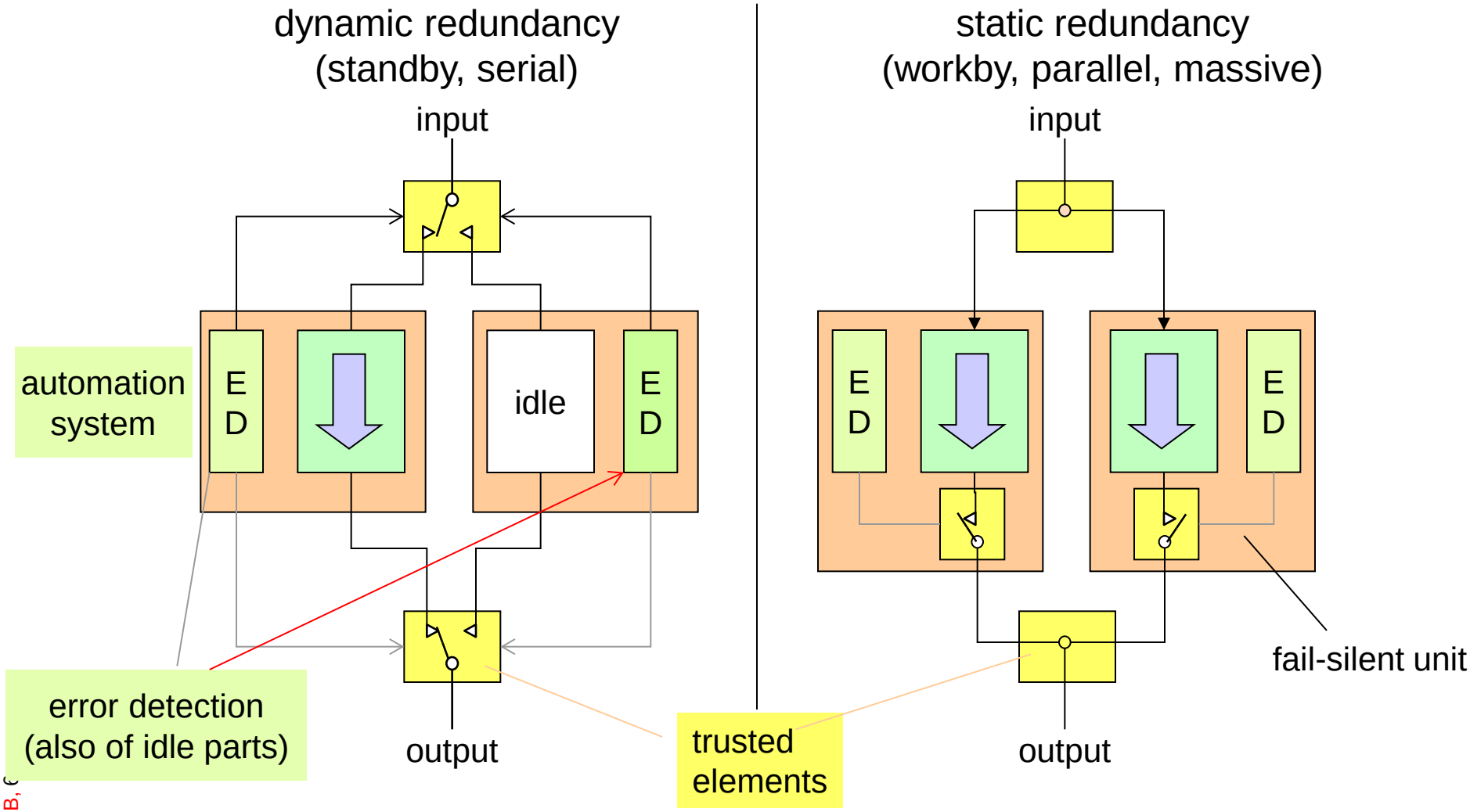
We consider automatic insertion of redundancy in case of failure (fault-tolerant systems) and automatic reinsertion after repair.

Availability states



we must consider all transitions, not just what happens after a failure

Classification of redundancy methods (1)



paradigm: spare tire

paradigm: double tires in trucks

Classification of redundancy methods (2)

Dynamic (standby, serial) redundancy	Static (parallel, workby) redundancy
Redundancy is not actively participating in the control. A switchover logic decides to insert redundancy and put it to work	Redundancy is participating in the control, the plant chooses the working unit it trusts.
This allows to:	This allows to:
+ share redundancy and load	+ provide bumpless switchover
+ implement partial redundancy	+ continuously exercise redundancy and increase fault detection coverage
+ reduce the failure rate of redundancy	+ provide fail-safe behavior
+ reduce common mode of errors	
-but switchover takes time	- but costs total duplication

1. Terms: availability and redundancy
2. Classification of requirements
3. Levels of device and network redundancy
4. Industrial Ethernet topologies
5. Industrial Ethernet stack and redundancy
6. IEC 62439 solutions
7. Conclusion

Requirements of fault-tolerant systems

degree of redundancy (full, partial duplication)
- “Hamming Distance”: minimum number of components that must fail to stop service

guaranteed behavior when failing
- fail-silent or not

switchover delay
- duration of loss of service in case of failure

reintegration delay
- duration of disruption to restore redundancy after repair (live insertion)

repair strategy
- 365/24 operation, scheduled maintenance, daily stops,…

supervision
- detection and report of intermittent failures (e.g. health counters).
- supervision of the redundancy (against lurking errors)

consequences of failure
- partial / total system loss, graceful degradation, fault isolation

economic costs of redundancy
- additional resources, mean time between repairs, mean time between system failure

factors depending on environment
- (failure rate, repair rate) are not considered here.

Switchover time and grace time

The switchover delay is the most constraining factor in fault-tolerant systems.

The switchover delay is dictated by the **grace time**, i.e. the time that the plant allows for recovery before taking emergency actions (e.g. emergency shut-down, fall-back mode).

E.g. Recovery time after a communication failure must be shorter than the grace time to pass unnoticed by the application.

The grace time classifies applications:

Uncritical	< 10 s	(not real time) Enterprise Resource Planning, Manufacturing Execution
Automation general:	< 1 s	(soft real-time) human interface, SCADA, building automation, thermal
Benign	< 100 ms	(real-time) process & manufacturing industry, power plants,
Critical:	< 10 ms	(hard real time) synchronized drives, robot control, substations, X-by-wire

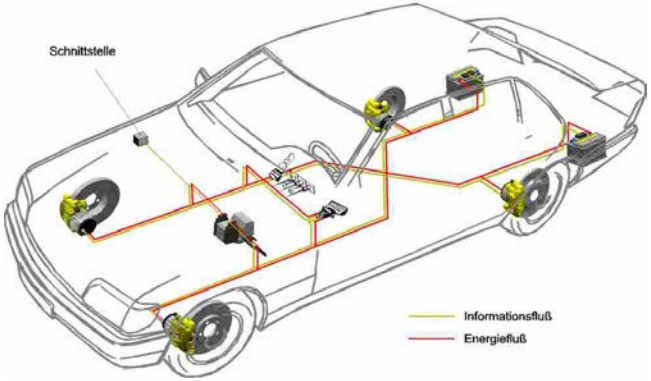
Grace time depends on the plant (typical figures)

cement: 10s

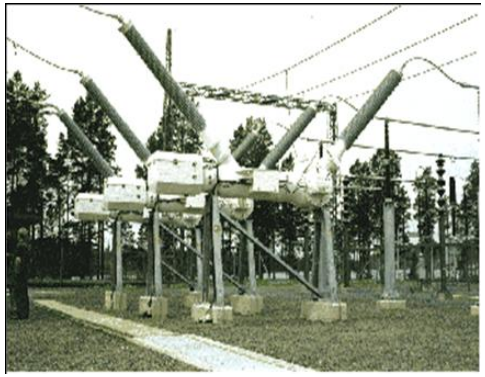
chemical: 1s

printing: 20 ms

tilting train: 100ms



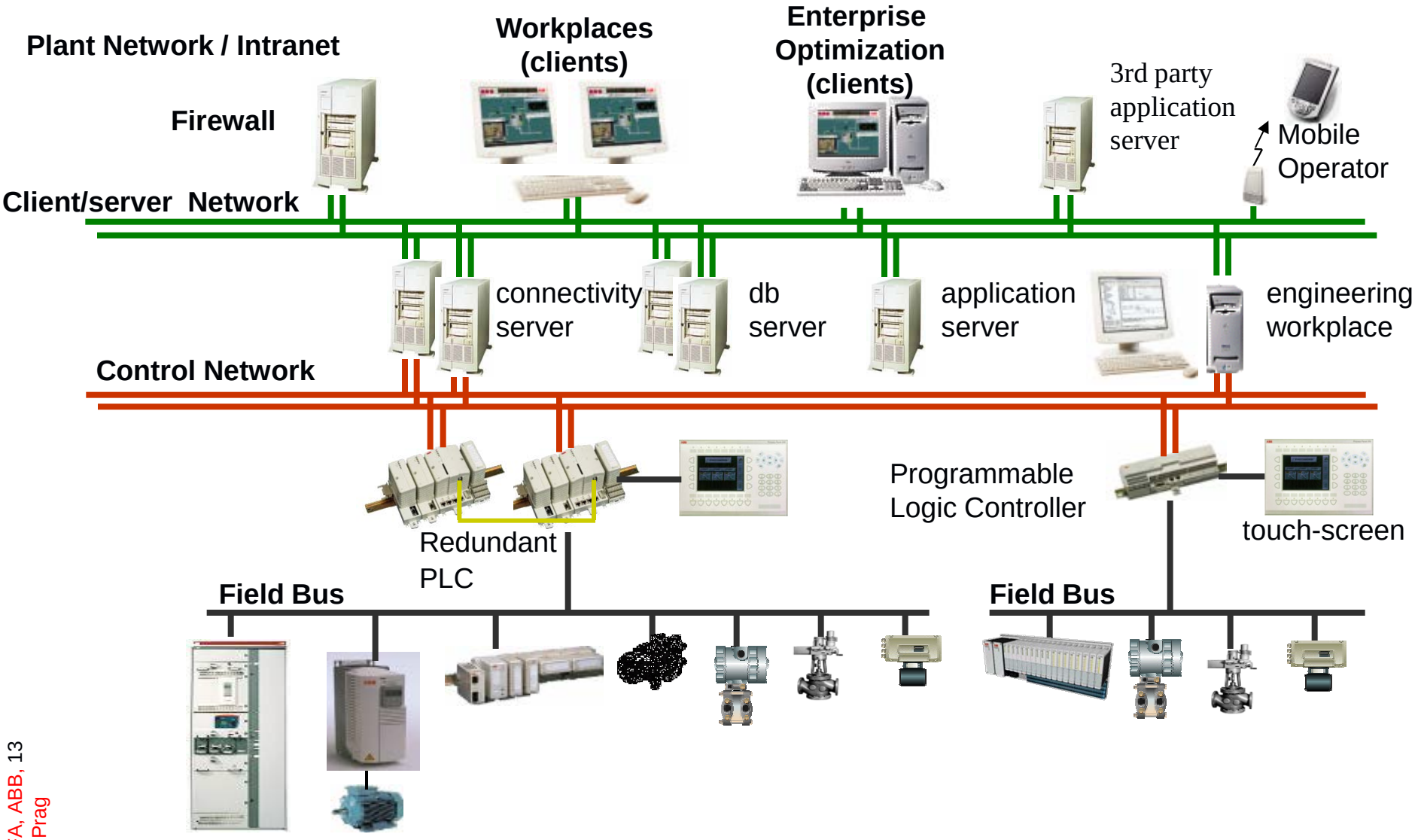
X-by wire: 10ms



substations: 5 ms

1. Terms: availability and redundancy
2. Classification of requirements
3. Levels of device and network redundancy
4. Industrial Ethernet topologies
5. Industrial Ethernet stack and redundancy
6. IEC 62439 solutions
7. Conclusion

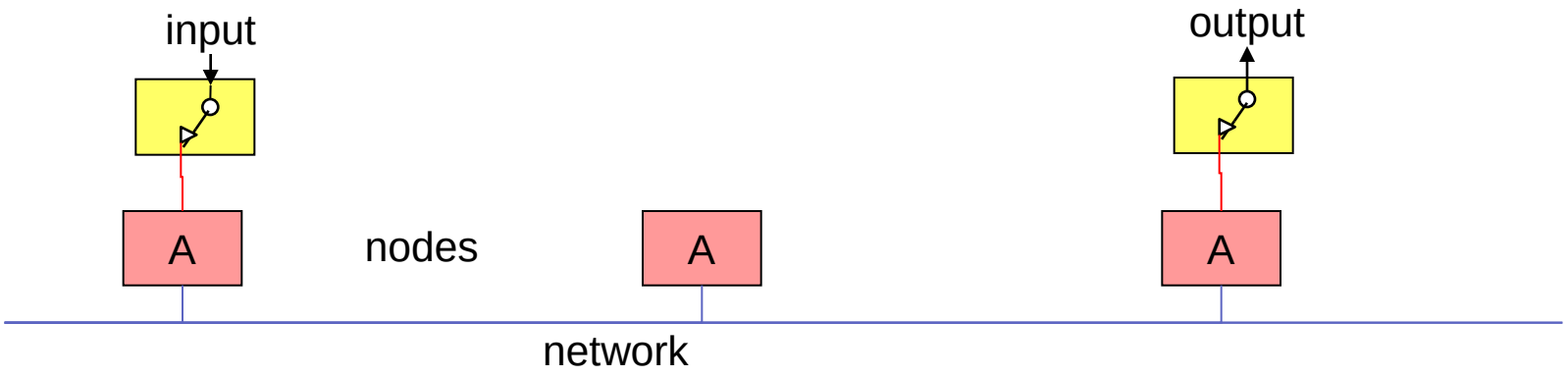
Automation Networks



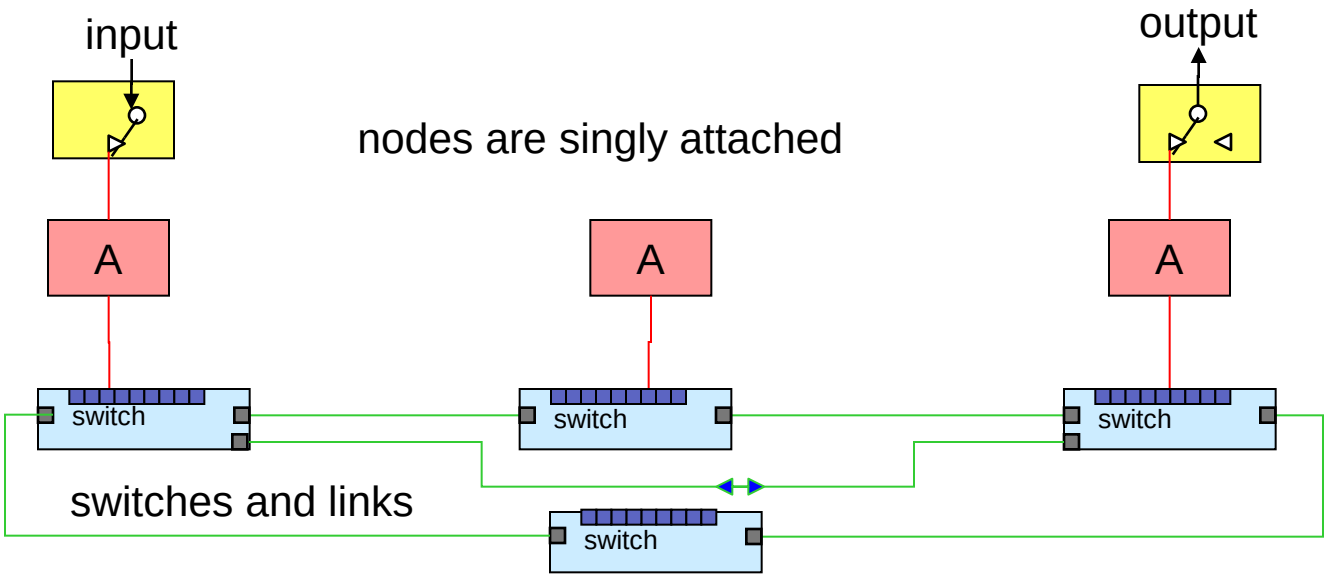
We consider networks for automation systems, consisting of nodes, switches and links.

Device and network redundancy (1)

1) No redundancy (except fail-silent logic)

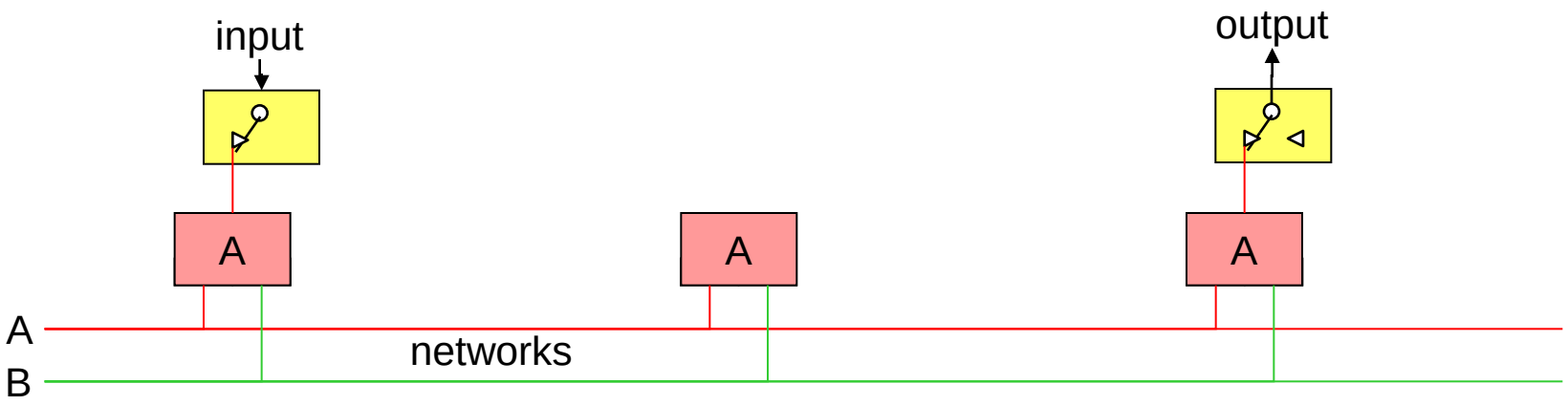


2) Redundancy in the network: protects against network component failures

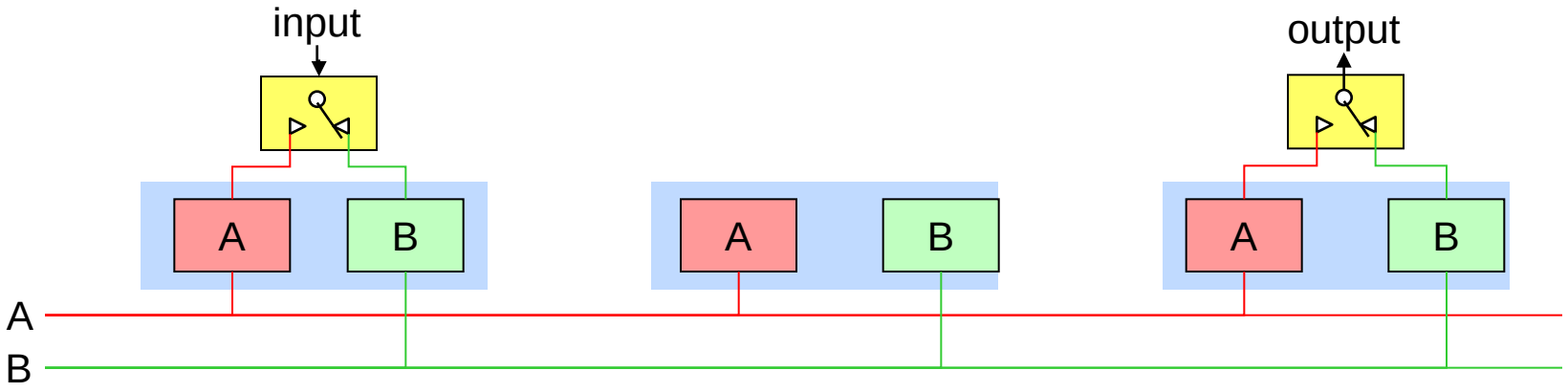


Device and network redundancy (2)

3) Doubly attached nodes protects in addition against network adapter failures

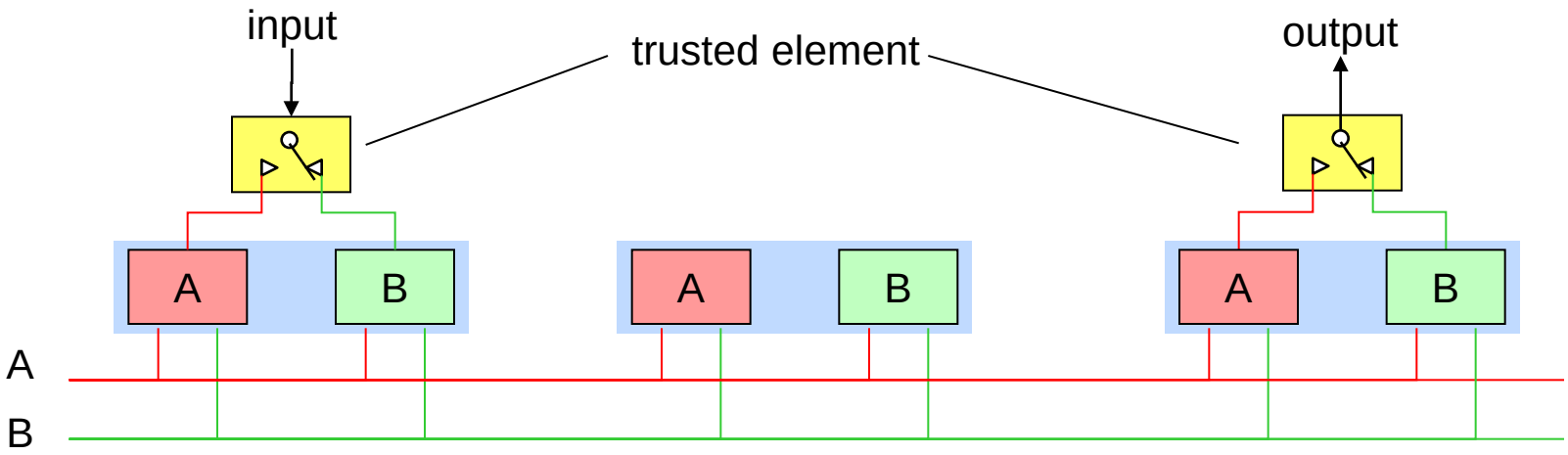


4) Redundant, singly attached nodes protect against node <u>or</u> network failures



Device and network redundancy (3)

5) Doubly attached nodes and network crossover protect against node <u>and</u> network failure



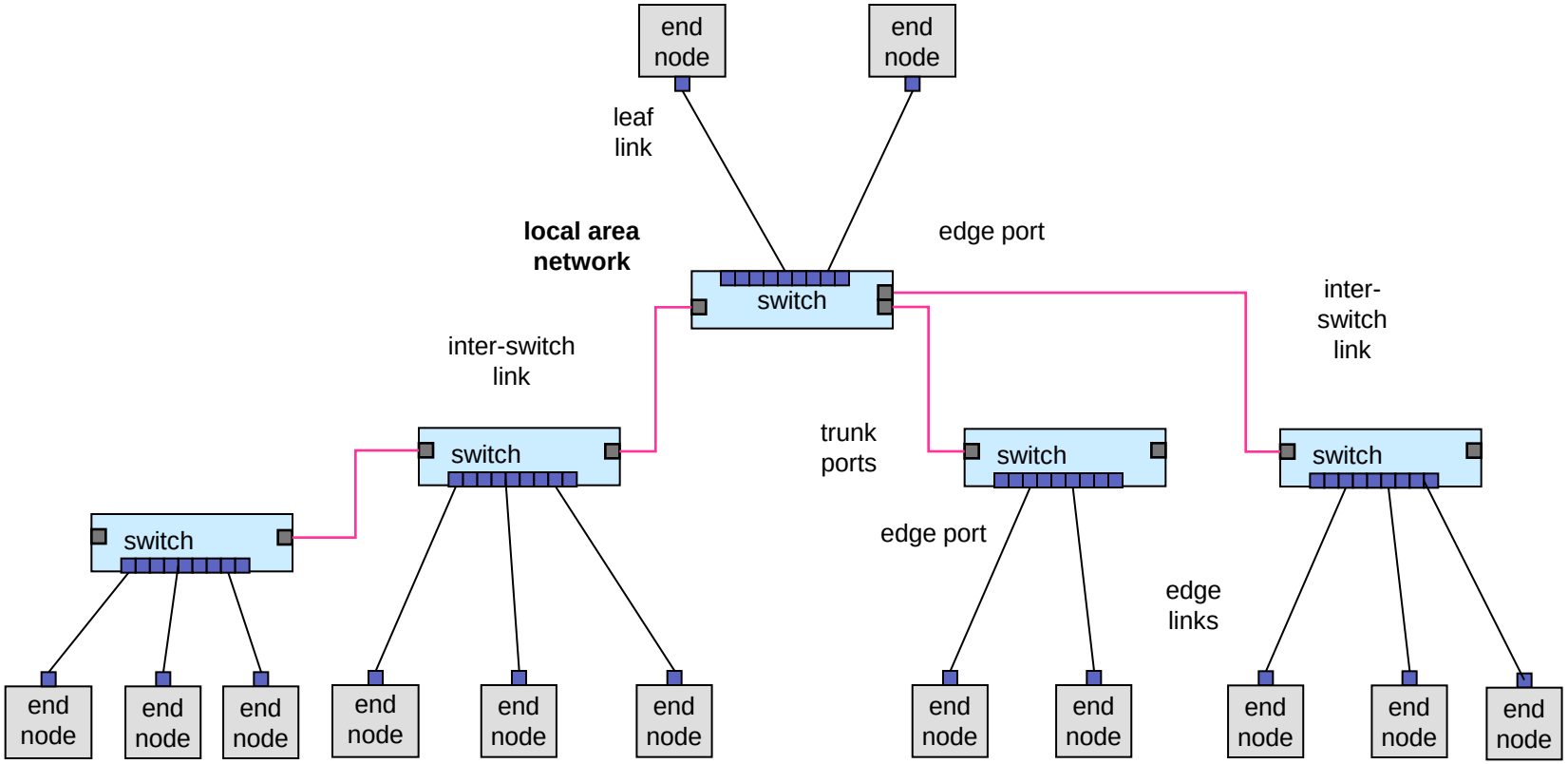
Crossover redundancy allows to overcome double failures (device and network).

However, use of crossover must be cautious, since crossover relies on elements that can represent single points of failure and should be very reliable to bring a benefit.

IEC SC65C addresses redundancy types 2 and 3 –
redundancy types 4 and 5 can be built out of the 2 and 3 solutions

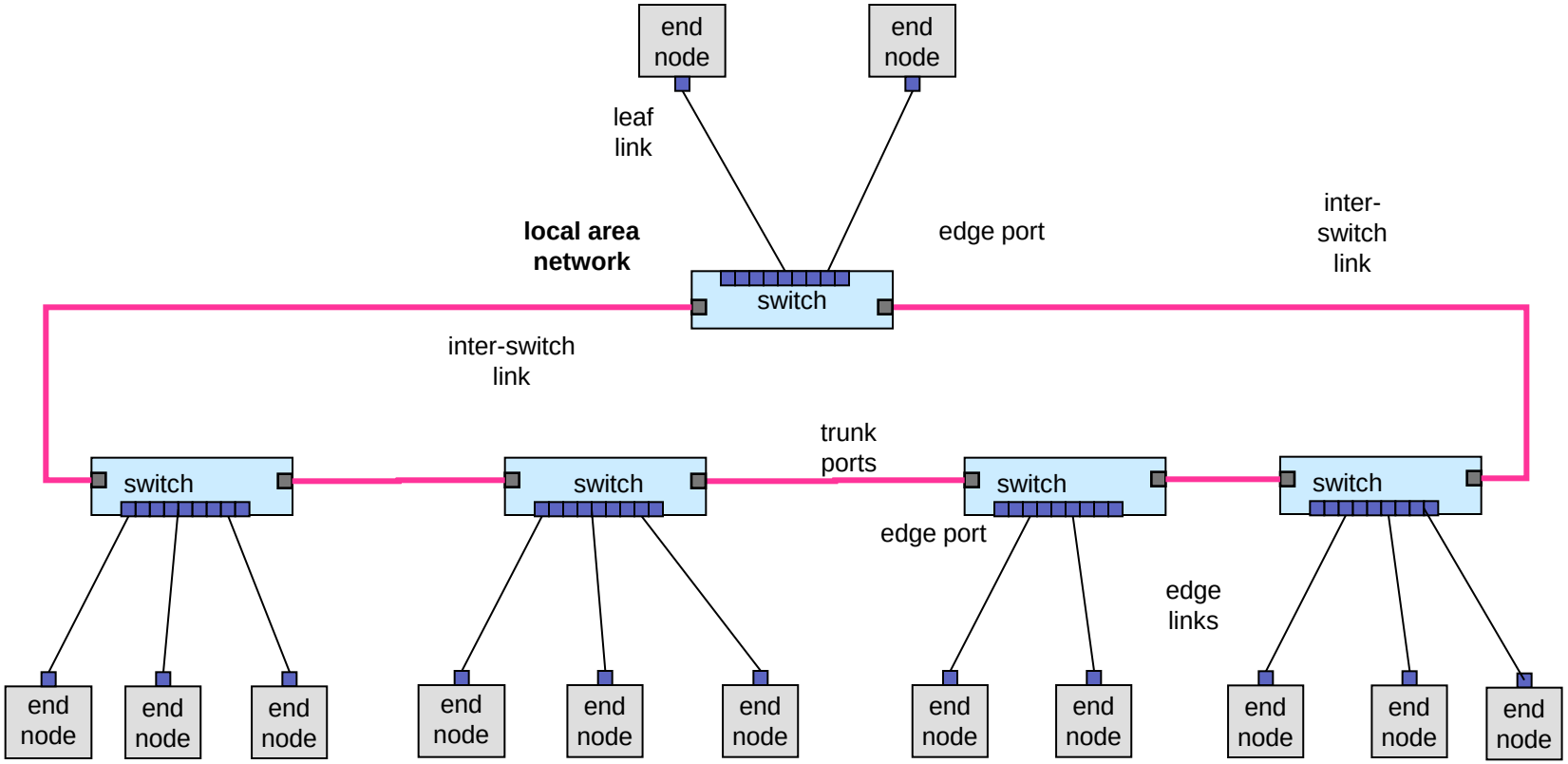
1. Terms: availability and redundancy
2. Classification of requirements
3. Levels of device and network redundancy
4. Industrial Ethernet topologies
5. Industrial Ethernet stack and redundancy
6. IEC 62439 solutions
7. Conclusion

Ethernet-based automation networks (tree topology)



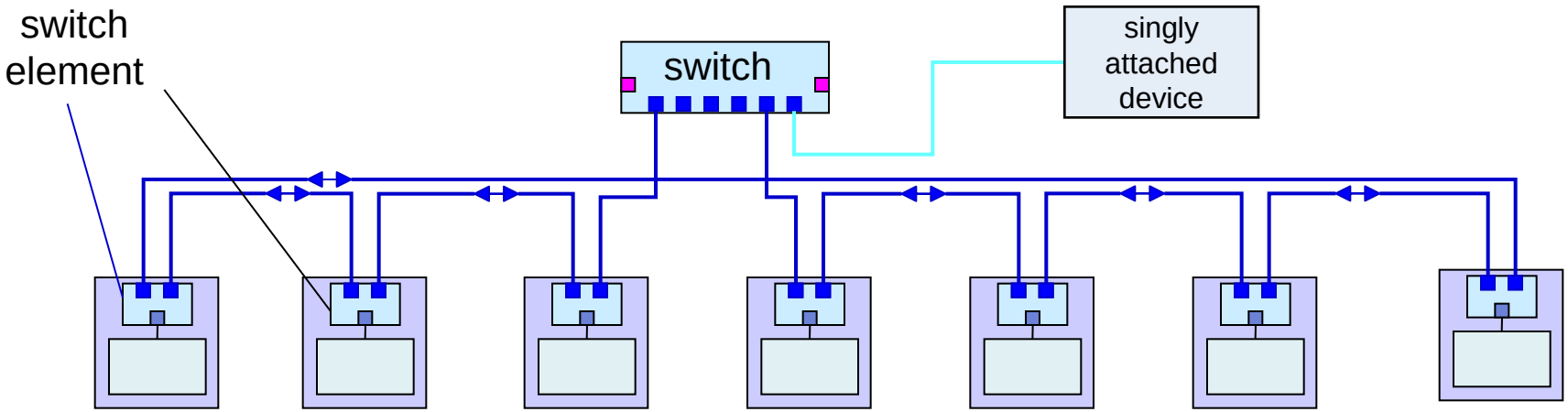
in principle no redundancy

Ethernet-based automation networks (ring topology)



longer delays, but already has some redundancy

Ethernet-based automation networks (ring of nodes)



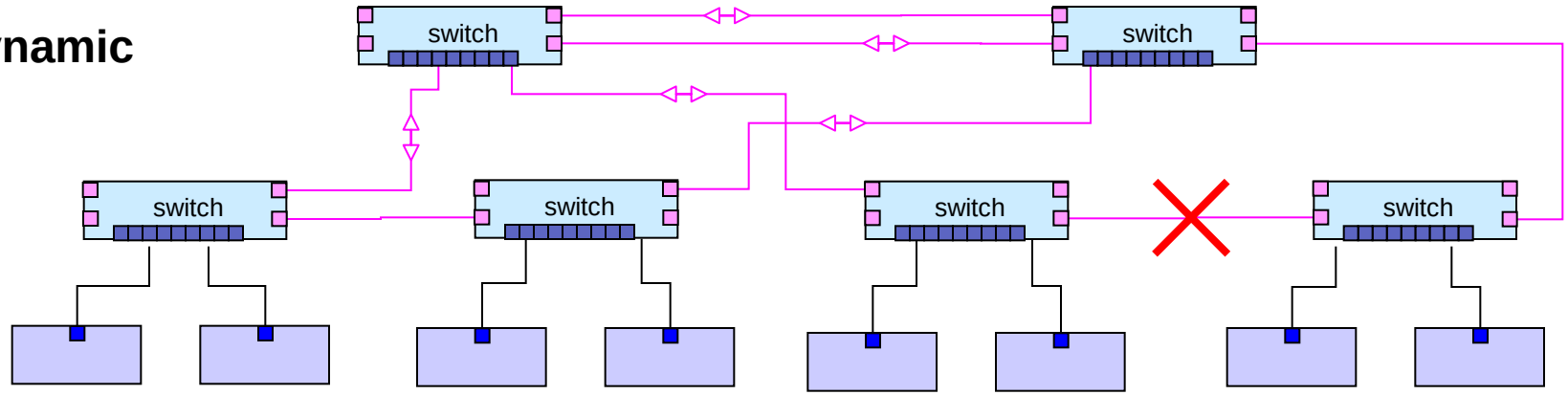
This topology is becoming popular since it suppresses the (costly) switches and allows a simple linear cabling scheme, while giving devices a redundant connection.

Operation is nevertheless serial redundancy, i.e. requires a certain time to change the routing.

Devices are doubly-attached, but do not operated in parallel.

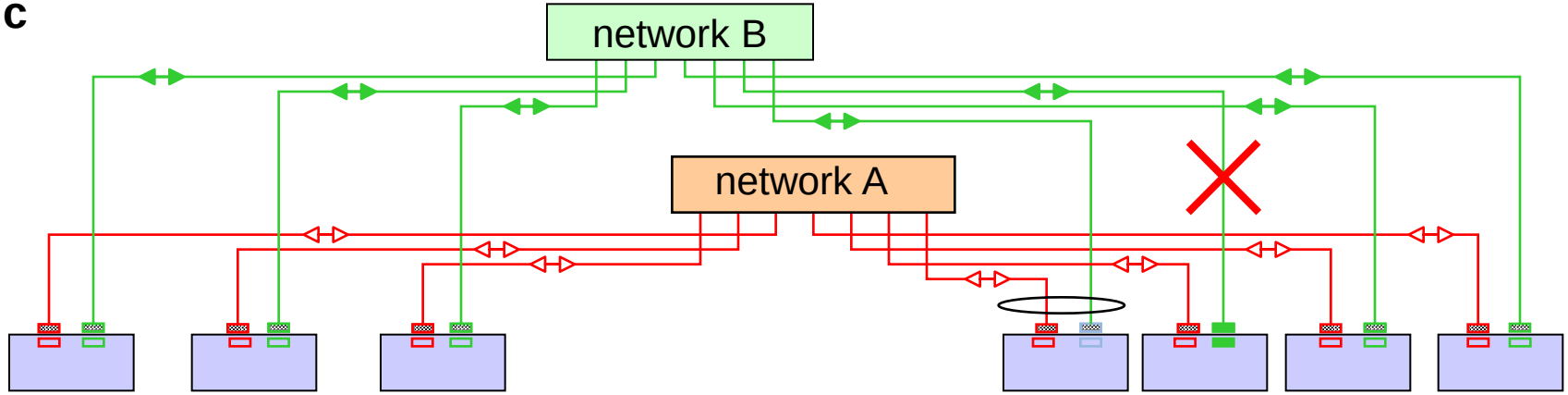
Dynamic and static redundancy in networks

Dynamic



in case of failure, switches route the traffic over an other port – devices are singly attached

Static

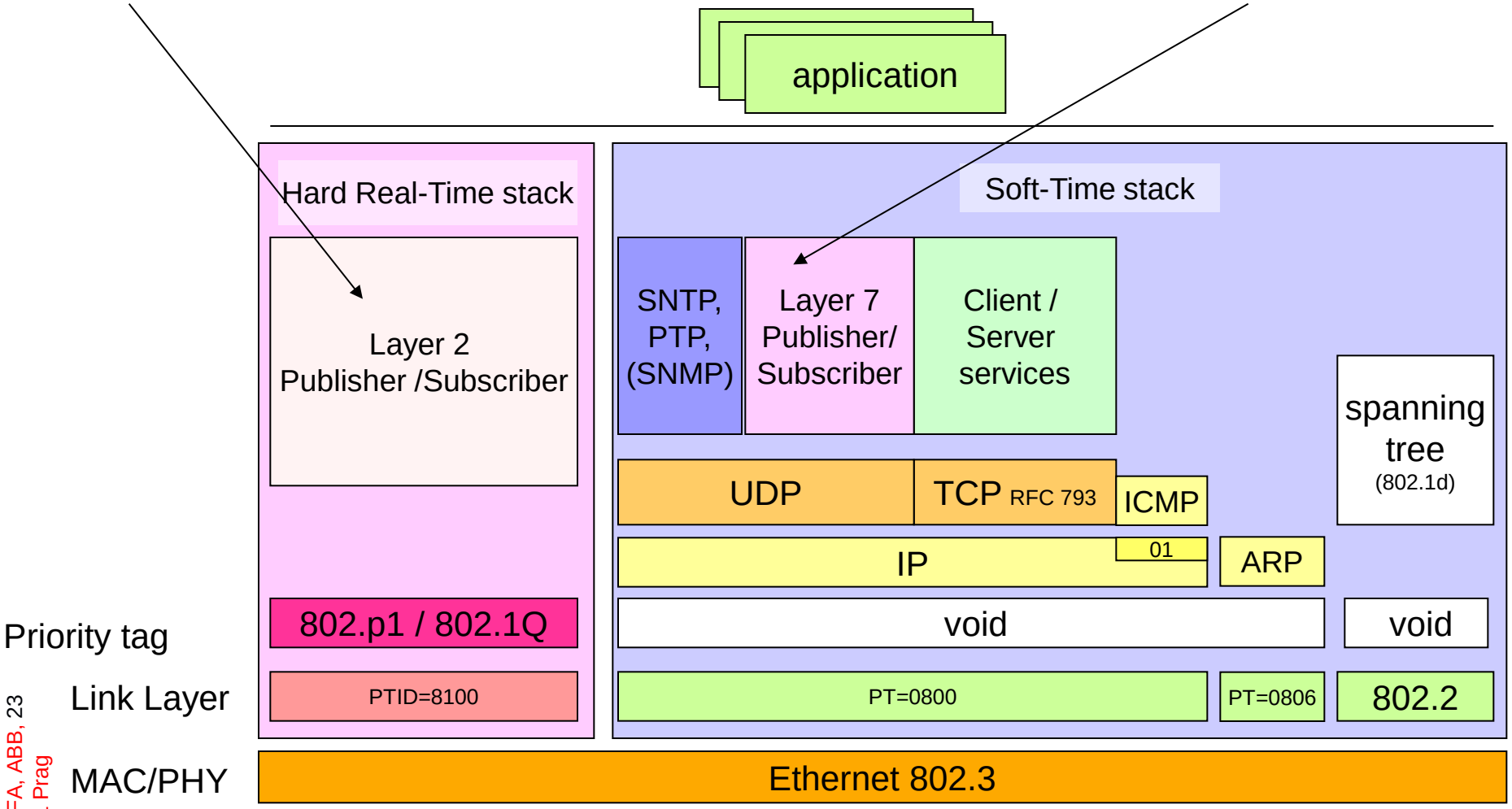


in case of failure the doubled attached nodes work with the remaining channel.
Well-known in the fieldbus workd

1. Terms: availability and redundancy
2. Classification of requirements
3. Levels of device and network redundancy
4. Industrial Ethernet topologies
5. Industrial Ethernet stack and redundancy
6. IEC 62439 solutions
7. Conclusion

What makes Industrial Ethernet special

Most “Industrial Ethernet” uses the classical TCP-UDP-IP stack and in addition **a layer 2 traffic** for real-time data (but some use UDP) and a **clock synchronization** (IEEE 1588)



Therefore, Industrial Ethernet redundancy must operate at level 2

Communication stack and redundancy

The redundant Ethernet solutions distinguish themselves by:

- the OSI level at which switchover or selection is performed.

- whether they operate with dynamic or static redundancy

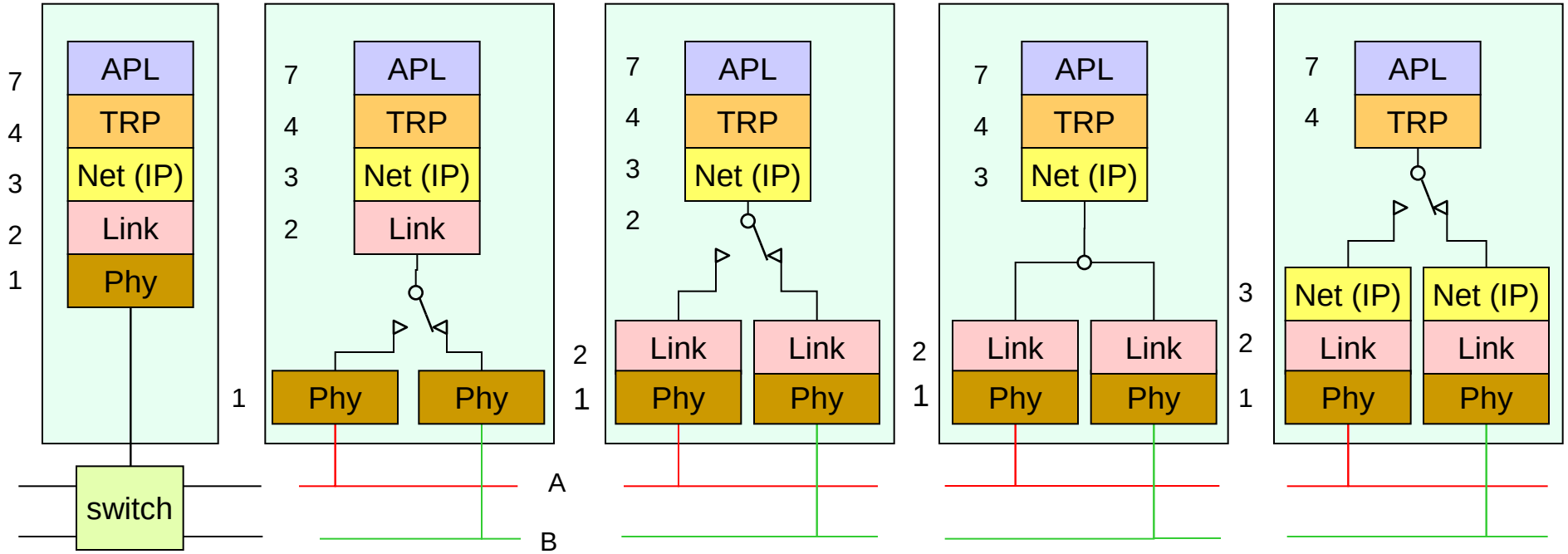
Industrial protocols operate both at network layer (IP) and at link layer (e.g. Real Time traffic, clock synchronization traffic),

Redundancy only at network level is not sufficient, it must be implemented at layer two to account for industrial Ethernets that use these layers.

Since standard methods handle effectively redundancy at the network layer (TCP / IP), network level redundancy is separated from the device-level redundancy.

Commercial solutions to redundancy in the nodes

(no duplication of nodes)



only redundancy within the network	physical layer (drivers)	link layer (drivers and controller)	link layer (drivers and controller)	network layer (drivers, controller and network routing)
1N	1 Ethernet controller	2 MAC Addresses	1 MAC Addresses	2 IP Addresses

the level of redundancy can be identified by the addresses used

Methods for dynamic redundancy in networks

-IP protocol	Layer 3 (network)	10s or more – unsuited for Industrial Ethernet
-RSTP (IEEE 802.1D)	Layer 2 (switches):	1 s typical, less in fixed topography
-HyperRing	Layer 3 (ring)	200 ms

-The switchover time of dynamic redundancy is limited by the detection time of the failure.

(or rather, by the interval at which the non-failure is checked, since failures can't be relied upon to announce themselves).

1. Terms: availability and redundancy
2. Classification of requirements
3. Levels of device and network redundancy
4. Industrial Ethernet topologies
5. Industrial Ethernet stack and redundancy
6. IEC 62439 solutions
7. Conclusion

Rules of order of MT9

1) the standard redundancy solution is independent of the higher protocols used

2) the standard shall be compatible with existing equipment, especially commercial PCs and switches, where no redundancy is used

3) the standard shall define the layout rules and especially the integration of different levels of redundancy

4) the standard shall define means to supervise the redundancy, e.g. using SNMP

5) the standard shall define scenarios for life insertion and reintegration of repaired components

6) the standard shall define measurable performance goals, such as switchover times and reintegration time

7) if several solutions emerge, the standard shall specify their (distinct) application domains and recommendation for their use

MT9 shall not consider safety or security issues – for this there are other standards.

IEC 62439 solutions

MT9 decided to address requirements separately

A) general automation systems
the standard recommends to use **RSTP**
(base: IEEE standards, RSTP) – no need for a new standard < 500 ms

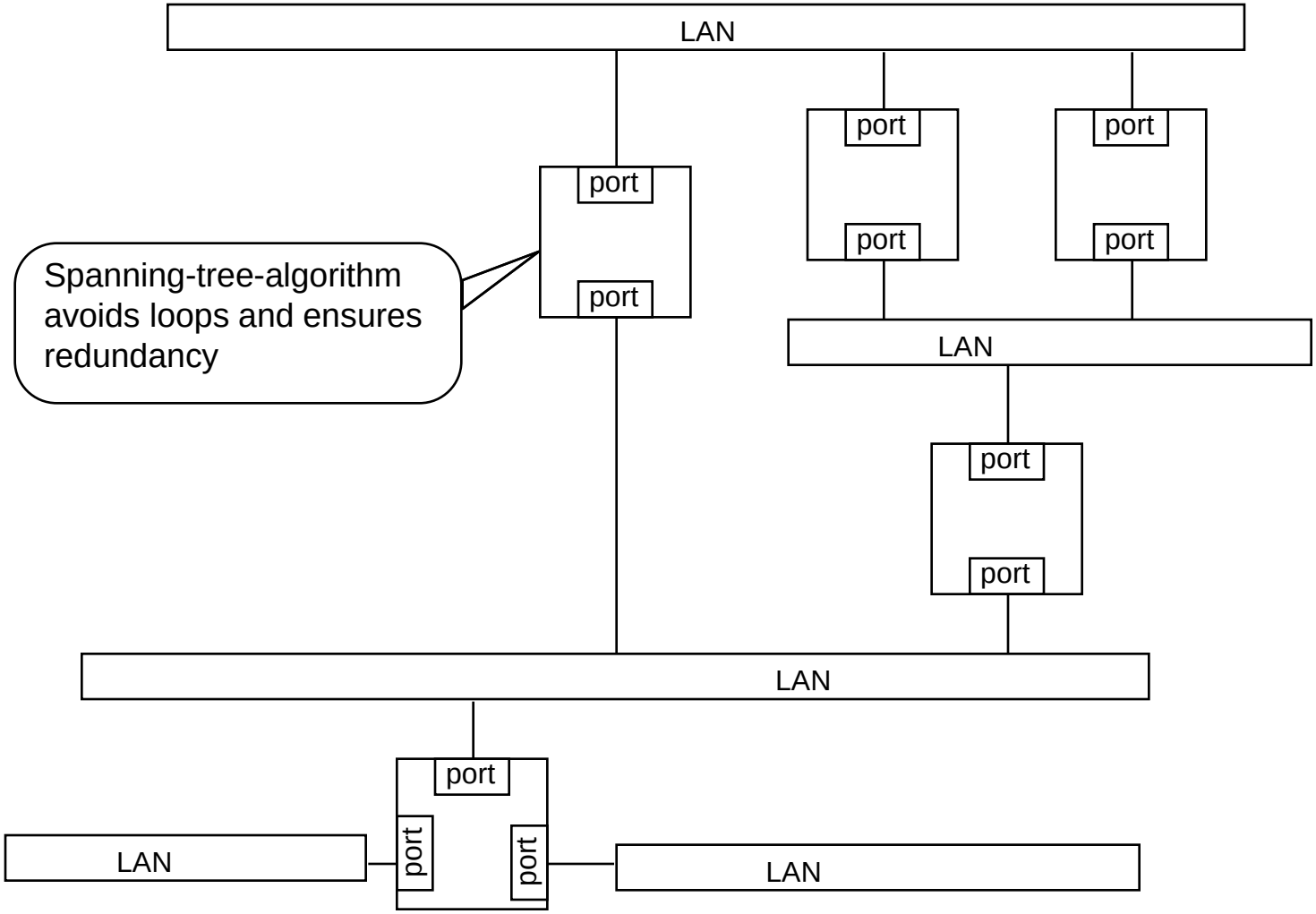
B) benign real-time systems that are cost-sensitive, grace time < 200 ms
the standard shall define an adequate switch redundancy scheme and redundant devices attachment.
(base: RSTP and further developments – solution: **MRP**

C) critical real-time systems that require higher coverage, grace time < 2 ms
the standard shall define a parallel network solutions and redundant device attachment.
(base: ARINC AFDX and similar – solution **PRP**

D) legacy solution based on Fieldbus Foundation

The Rapid Spanning Tree Protocol

Standardized by IEEE 802.1D (replaces the obsolete STP)



RSTP performance

+: IEEE standard, field proven, large market, cheap

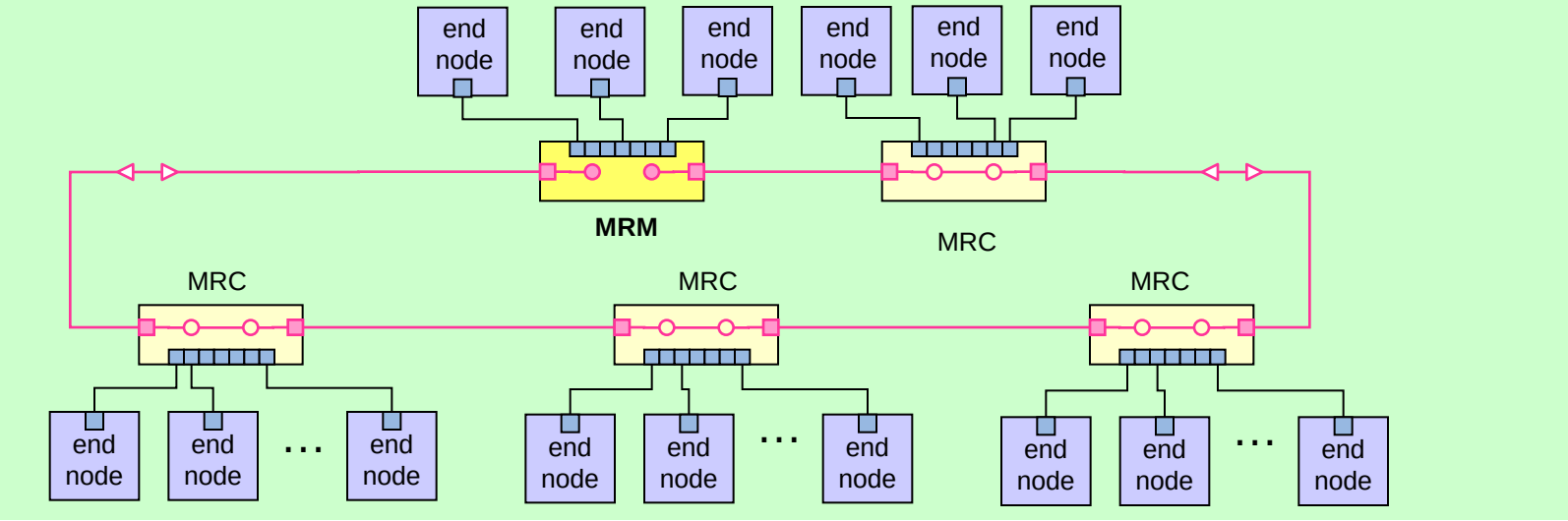
+: no impact on the end nodes (all end nodes are singly attached)

+: can be implemented in the nodes if the nodes contain a switch element

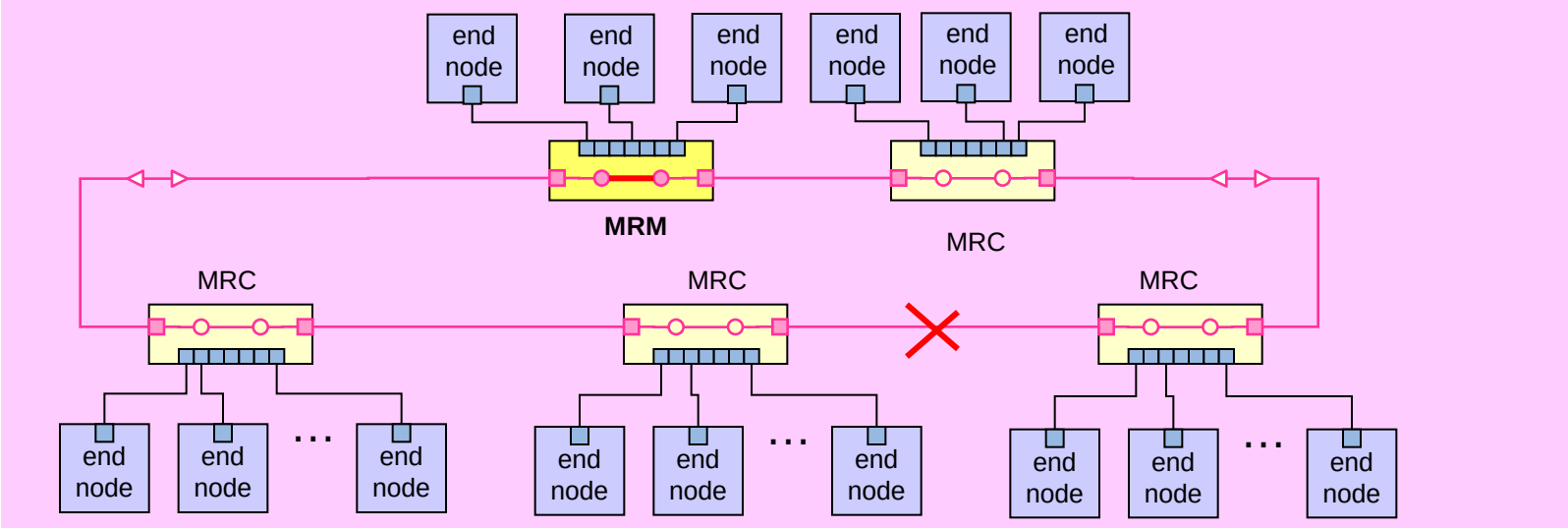
-: RSTP is in fame of being rather slow (some seconds switchover time). However, if the topology is fixed, RSTP switches can learn the topography and calculate alternate paths in case one should fail. Some manufacturers claim recovery delays <100 ms for selected configurations

MRP (based on Siemens-Hirschmann hyperring)

intact ring



broken ring



the Medium Redundancy Master (MRM) controls the ring
the Medium Redundancy Clients (MRC) close the ring

MRP

The MRM checks the integrity of the ring by sending in both direction test frames.

These test frames are forwarded by all intact switches and inter-switch links.

If the MRM does not receive its own frames over its other interface, it closes the ring at its location, reestablishing traffic.

Supervision frames allows to locate the source of the trouble.

+: fast switchover (< 200ms worst case)

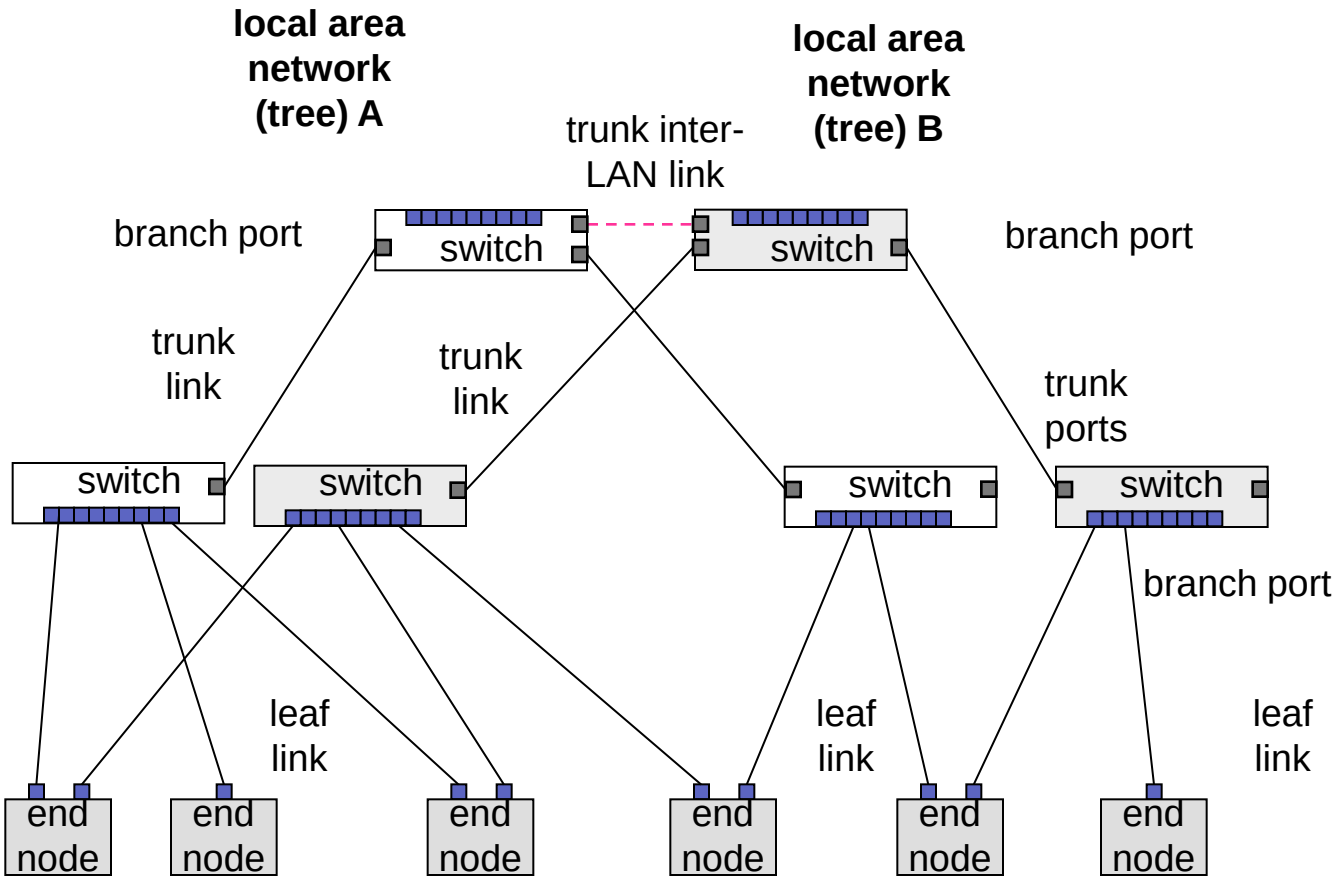
+: no impact on the nodes

+: no increase in network infrastructure.

-: MRP switches are not compatible with RSTP switches, limited market

-: limited to ring topology

Fieldbus Redundancy Protocol



FRP

The Fieldbus Redundancy Protocol is derived from the Fieldbus Foundation H3 network.

It uses two separate networks, to which devices are attached through two network adapters.

The networks are used alternatively rather than in parallel.

+: provides cross-redundancy (double fault network and node)

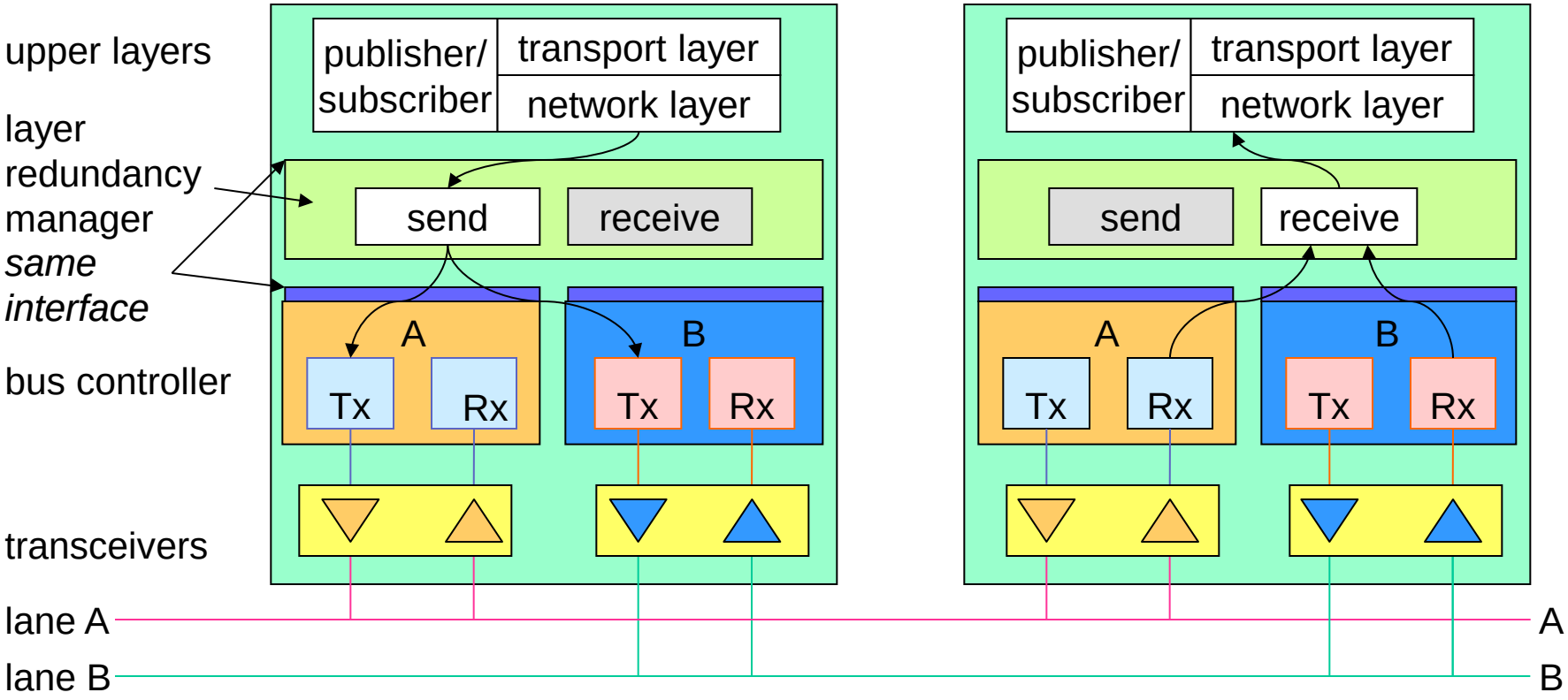
+: provides protection against adapter failures

-more than double network costs with respect to non-redundant networks

-large effort for building doubly-attached nodes.

-switchover time not specified

Parallel Redundancy Protocol

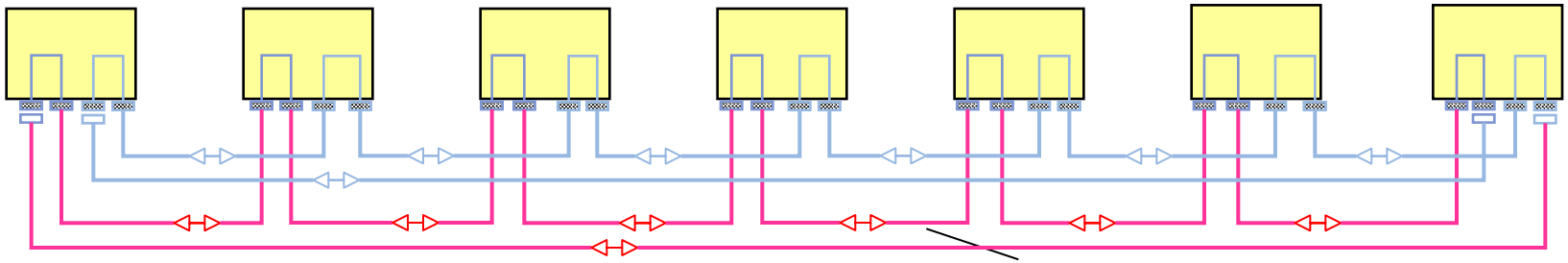


send on both lines: each frame is send on both A and B lines, frames over A and B have different transmission delays (or may not arrive at all)

receive on both lines: the stack receives both frames from both lines treated as equal, a "merge layer" between the link and the network layer suppresses duplicates.

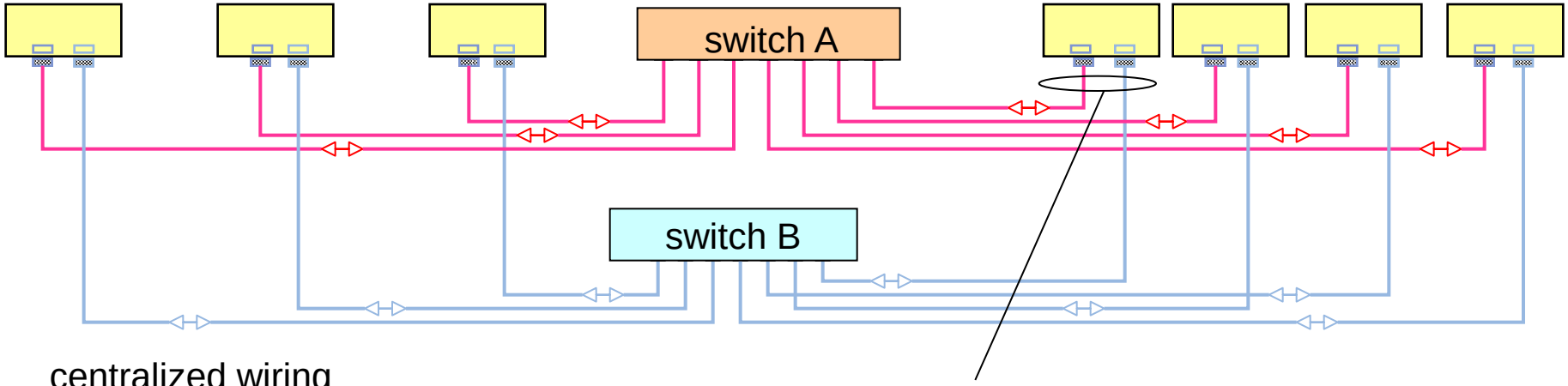
PRP layout examples

Party-Line topology



Star topology

switches separately powered



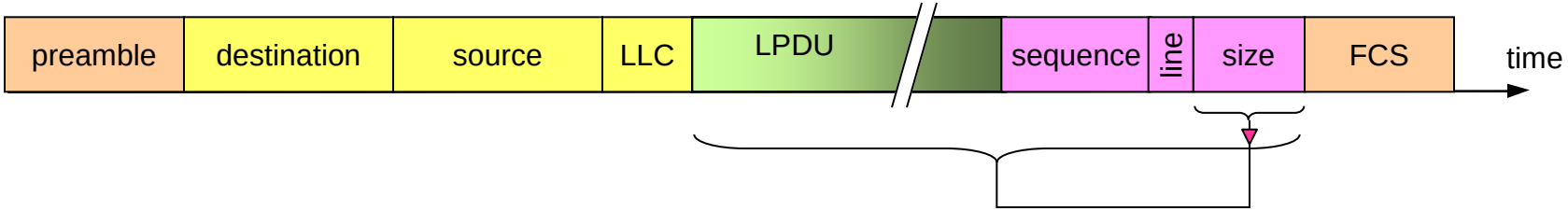
centralized wiring

common mode failures cannot be excluded since wiring comes close together at each device

PRP suppressing duplicates

To ease duplicate rejection, PRP nodes append a sequence number to the frames along with a size field that allows to determine that the frame belongs to the PRP protocol. This trailer is invisible to the higher layers (considered as padding)

Receivers discard duplicates using a sliding drop window protocol



PRP

+ PRP allows bumpless switchover, no frames are lost

+ During normal operation, PRP reduces the loss rate

+ PRP checks the presence of nodes by periodical supervision frames that also indicate which nodes participate in the protocol and which not

-: double network costs

-: doubly attached devices are costly to build

-: frame size must be limited to prevent frames from becoming longer than the IEEE 802.3 -maximum size (but most switches and Ethernet controllers accept frames up to 1536 octets)

1. Terms: availability and redundancy
2. Classification of requirements
3. Levels of device and network redundancy
4. Industrial Ethernet topologies
5. Industrial Ethernet stack and redundancy
6. IEC 62439 solutions
7. Conclusion

Conclusion

IEC 62439 satisfies the needs of the Industrial Ethernets belonging to the IEC 61784 suite with three (four) solutions:

-RSTP is sufficient for many applications–with improvements for fixed configuration

-MRP: a ring-based protocol for demanding automation networks and singly attached nodes

-PRP: a parallel network protocol for critical applications requiring doubly attached nodes.

-FRP, especially in conjunction with Fieldbus Foundation, requiring doubly attached nodes.

ETFA 2006

Consider redundancy failure