Considerações sobre a interdependência de sistemas redundantes e impactos na confiabilidade, segurança e simplicidade de subestações digitais

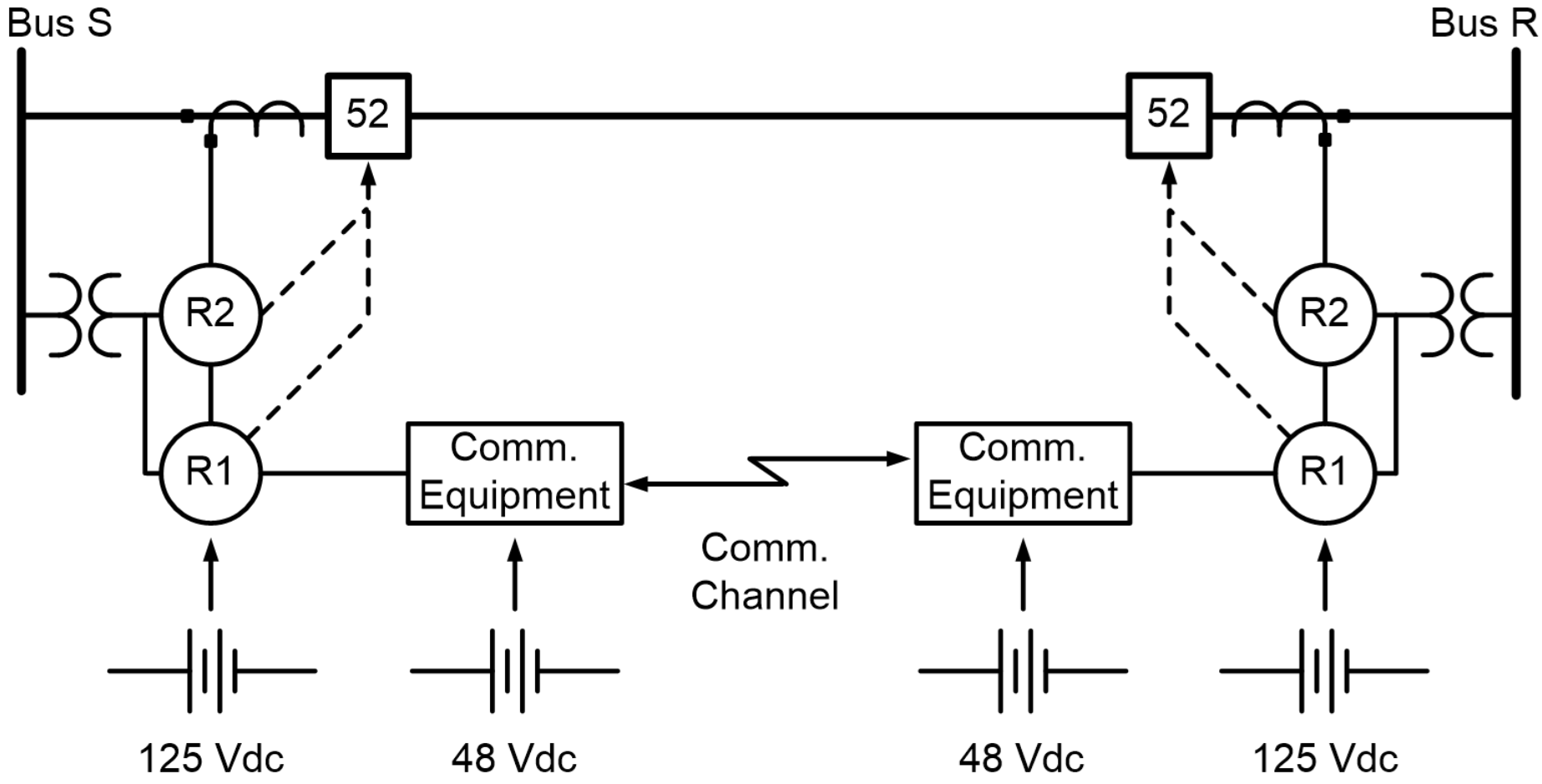
Ricardo Abboud

Protection Schemes Redundancy

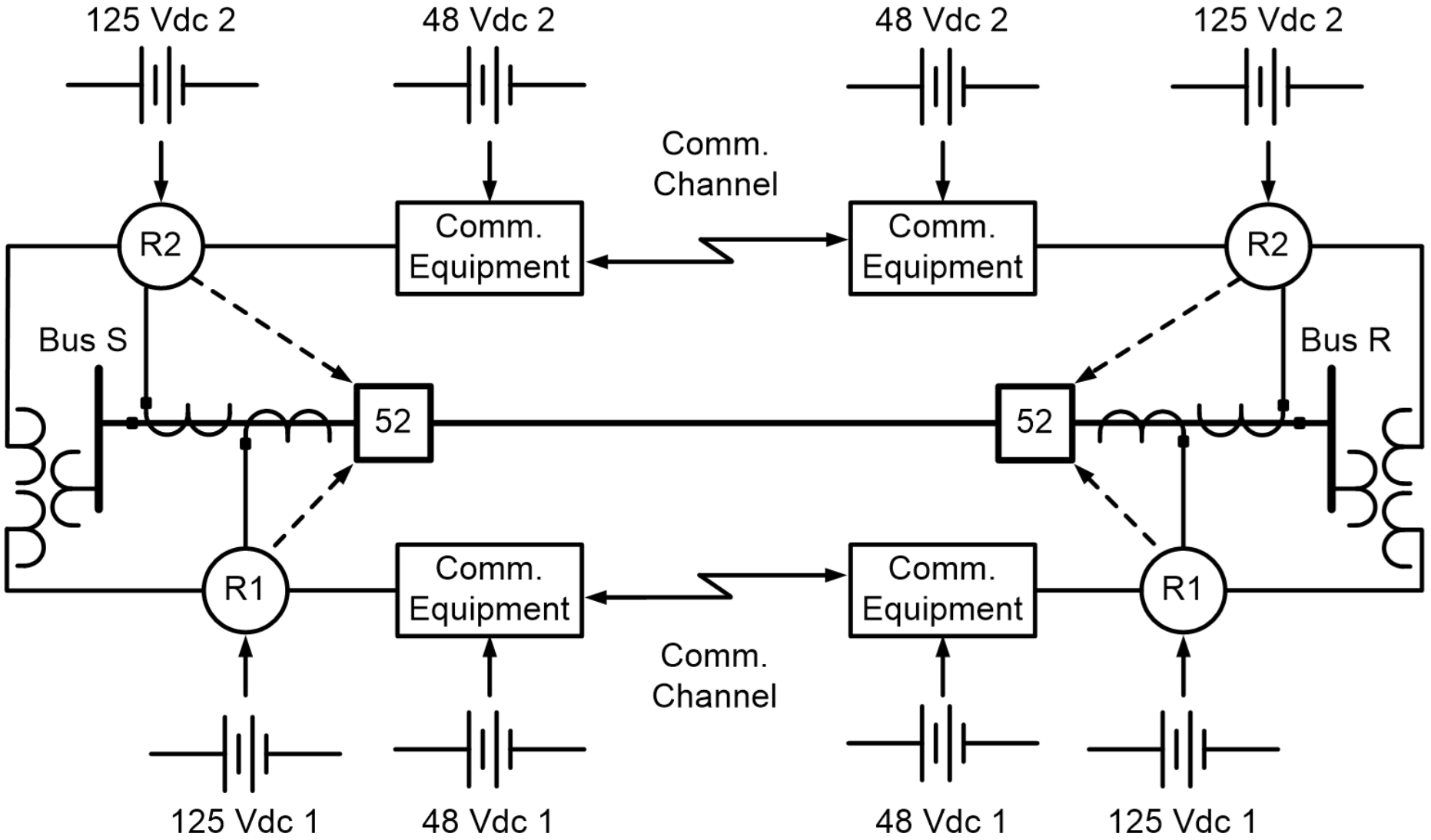
“Redundancy is required to assure that the failure of any single protection component, such as an instrument transformer, relay, breaker, control circuit, or communication channel will not result in the failure to be able to detect and isolate faults. The major objectives of the protective systems must remain intact for the failure of any device associated with a protective system. This constraint typically requires the use of two independent protection schemes for each protected facility on bulk power systems.”

Source: Blackburn , J. Lewis, “Protective Relaying, Principles and Applications”

Basic Line Protection Scheme



Dual-Redundant Protection Scheme



Redundancy principles

- “Workby or massive redundancy, in which redundant components are continuously active and immediately inserted (for instance several energized power supplies, sharing the load and tolerating the failure of one). Workby applies to the network, components, or any resource.”
  - "1+1 redundancy" with two simultaneously active resources.
- “Standby or spare redundancy, in which the redundant component is normally inactive, and it will take a recovery delay to become active in case of fault detection. The recovery delay can be so long as to render redundancy useless.”
  - RSTP

Source: IEC TR 61850-90-12:2020

Redundant Protection Systems

- Dual-redundant schemes use OR tripping logic
- Triple-redundant schemes use two-out-of-three voting logic
- System may use identical or different devices
- Are systems fully redundant?
- Are hidden and common-mode failures considered?

Comms Network Redundancy Protocols

INDUSTRIAL COMMUNICATION NETWORKS –
HIGH AVAILABILITY AUTOMATION NETWORKS –

Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR)

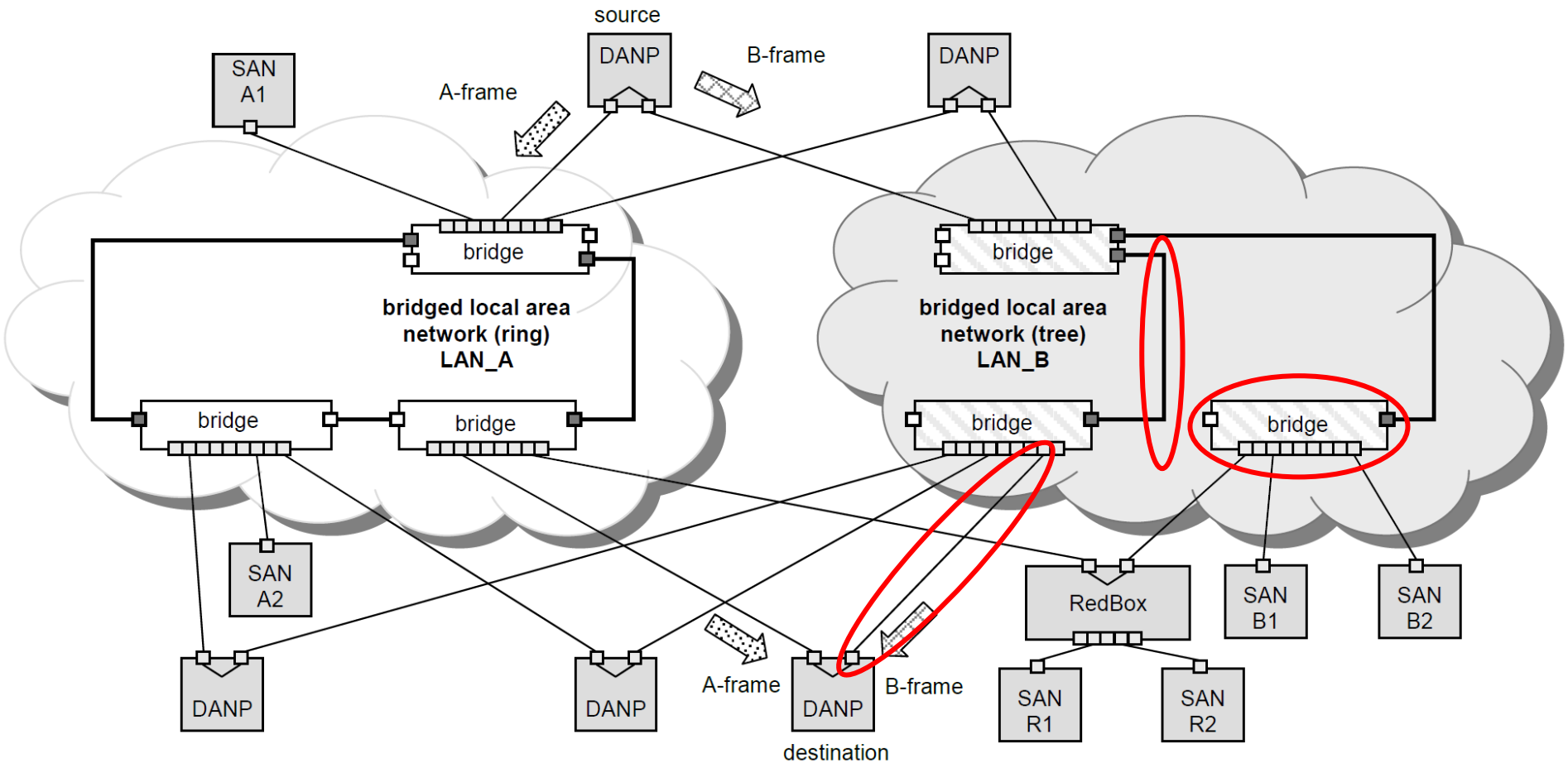
1 Scope

The IEC 62439 series is applicable to high-availability automation networks based on the Ethernet technology.

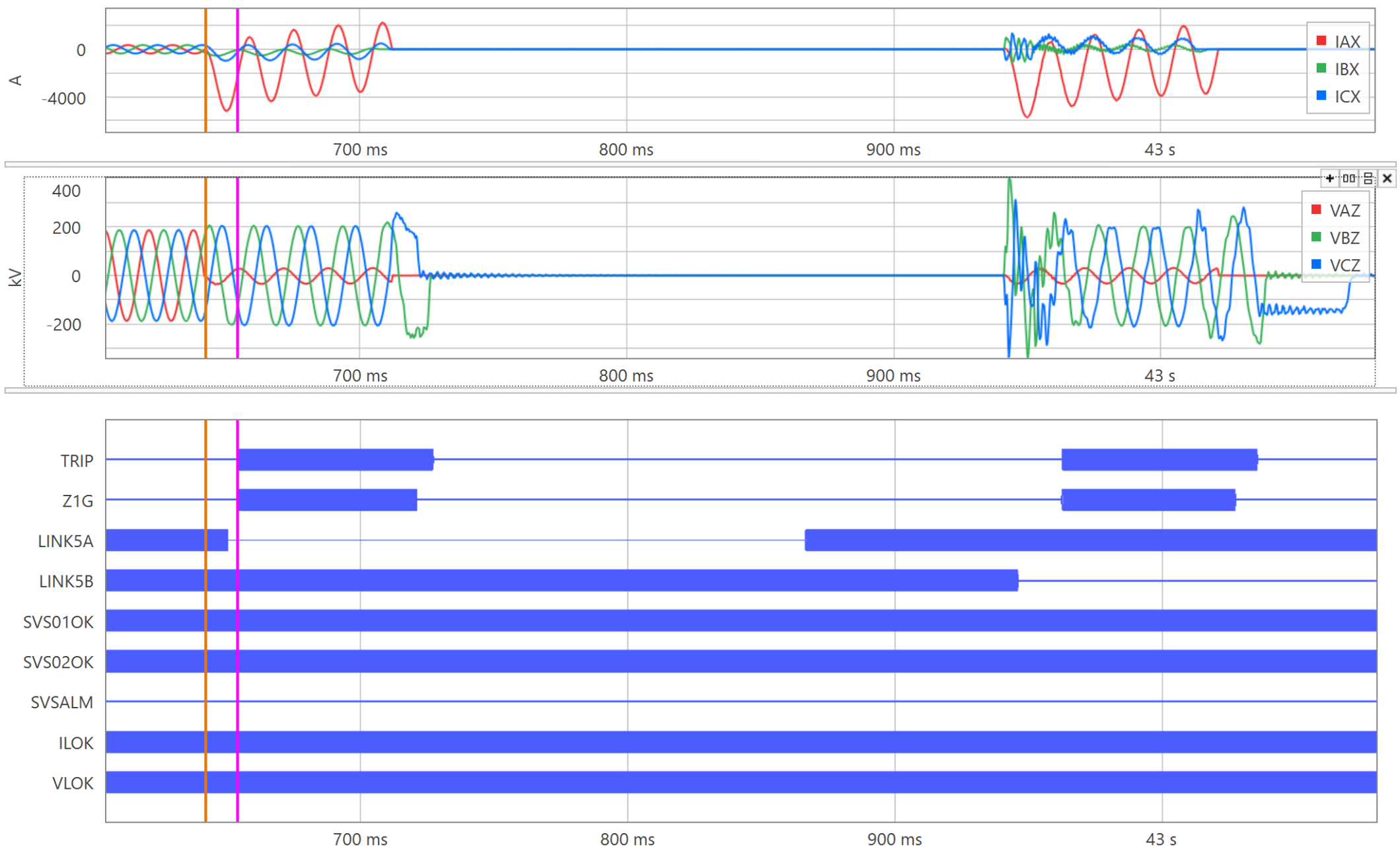
This part of IEC 62439 specifies two redundancy protocols designed to provide seamless recovery in case of single failure of an inter-bridge link or bridge in the network, which are based on the same scheme: parallel transmission of duplicated information.

Source: IEC 62439-3:2018

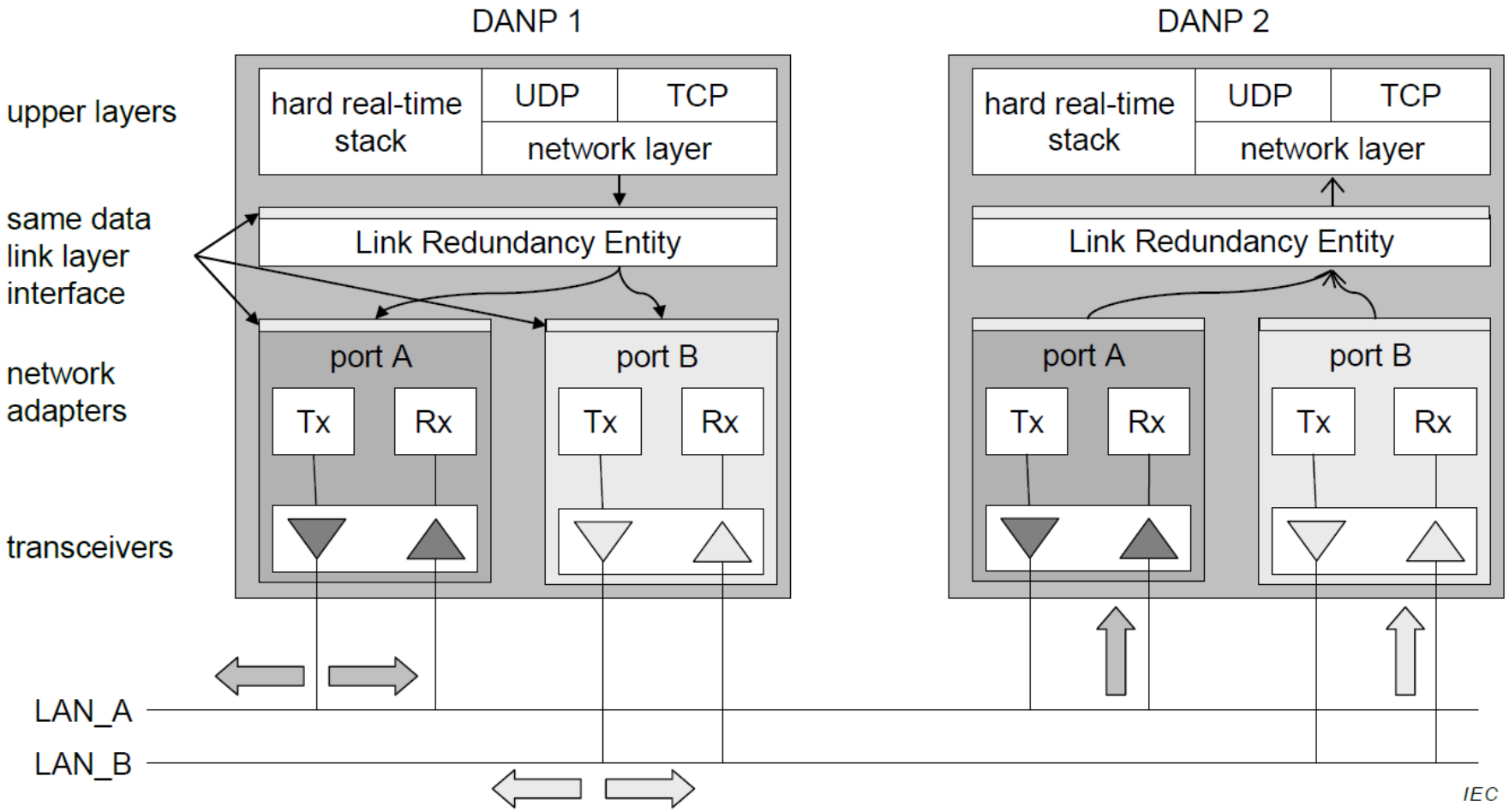
Which Failures are Covered?



Source: IEC 62439-3:2018


A
0
-4000
IAX
IBX
ICX
700 ms
800 ms
900 ms
43 s
kV
400
200
0
-200
VAZ
VBZ
VCZ
700 ms
800 ms
900 ms
43 s
TRIP
Z1G
LINK5A
LINK5B
SVS01OK
SVS02OK
SVSALM
ILOK
VLOK
700 ms
800 ms
900 ms
43 s

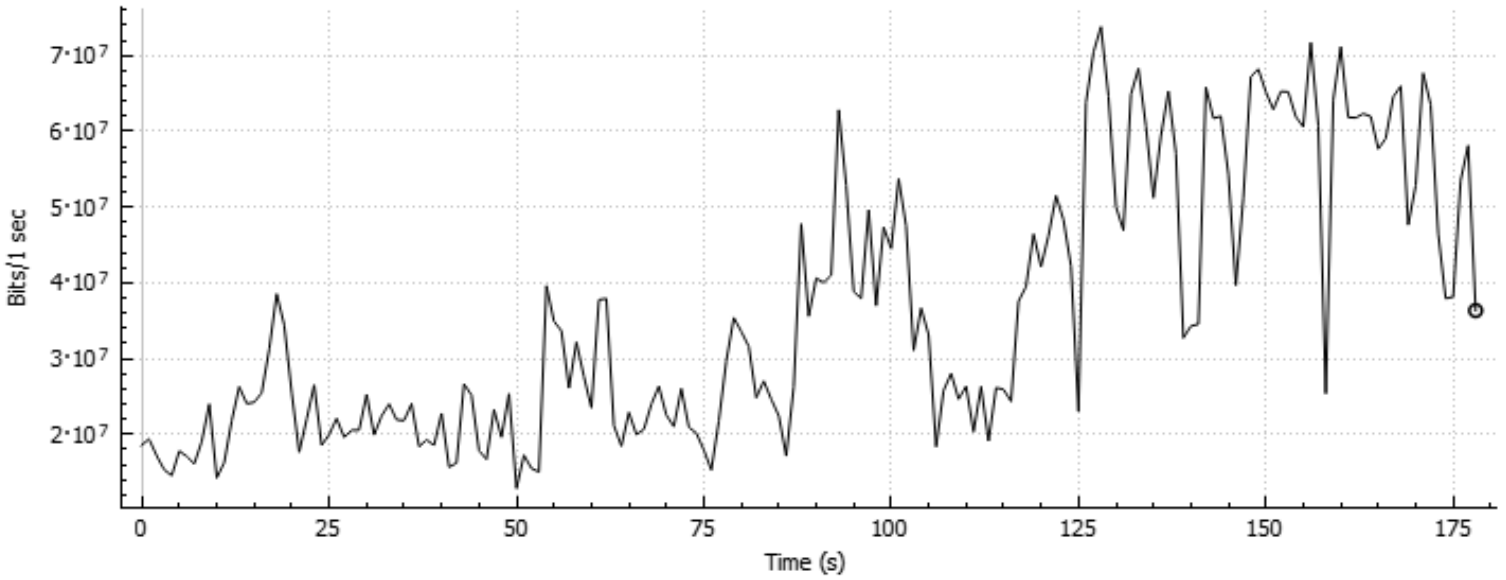
Data Source is the Same



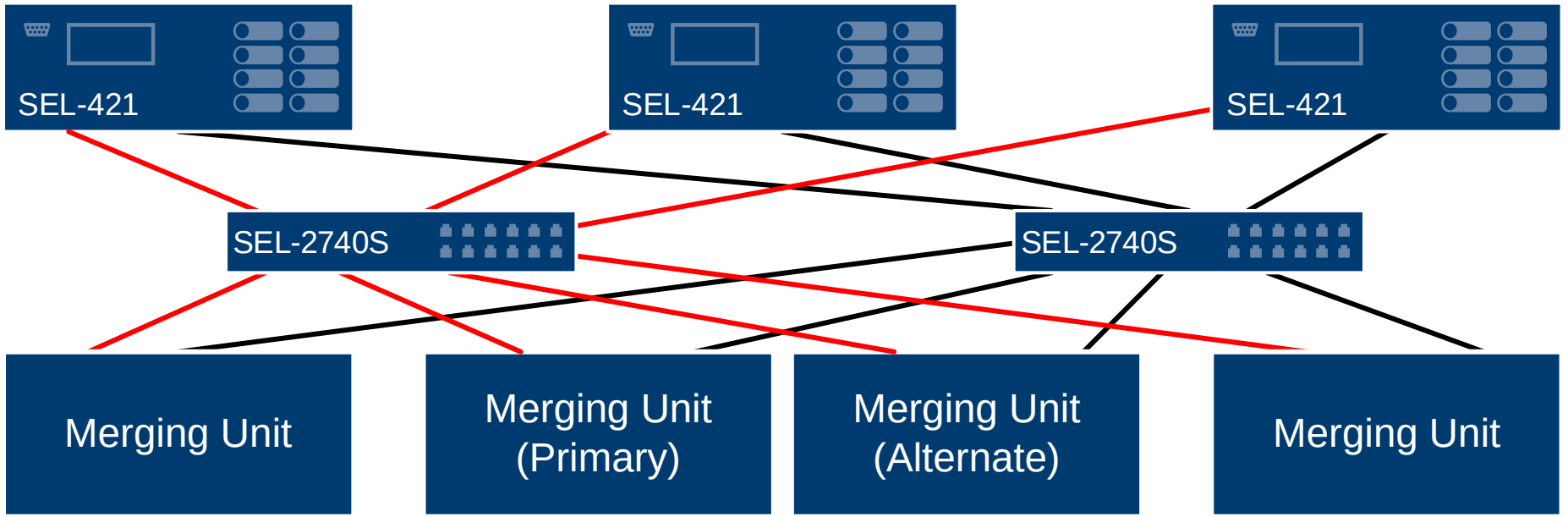
Source: IEC 62439-3:2018

Real Case

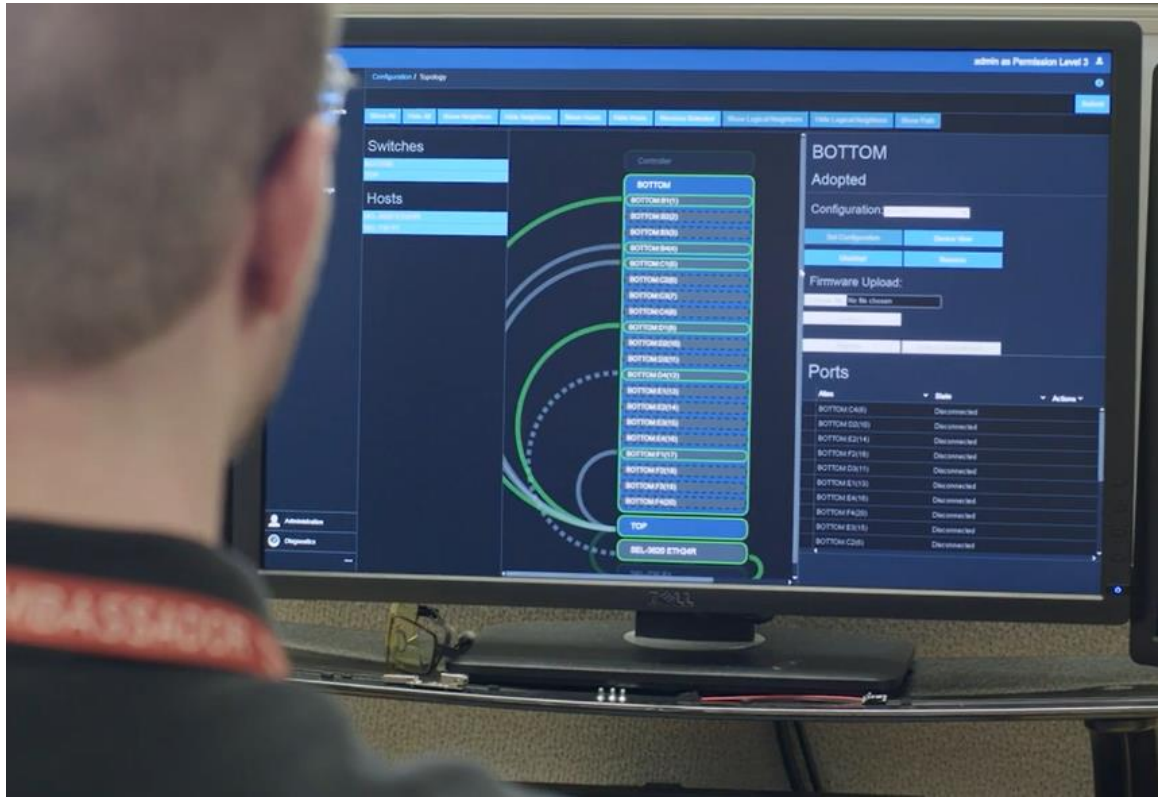
Protocol	Percent Bytes	Bytes
Frame	100.0	809913009
Ethernet	3.9	31340871
GOOSE	96.1	778543358
Address Resolution Protocol	0.0	12434
Internet Protocol Version 6	0.0	8920
Logical-Link Control	0.0	3276
Internet Protocol Version 4	0.0	560
Link Layer Discovery Protocol	0.0	263



SDN Network

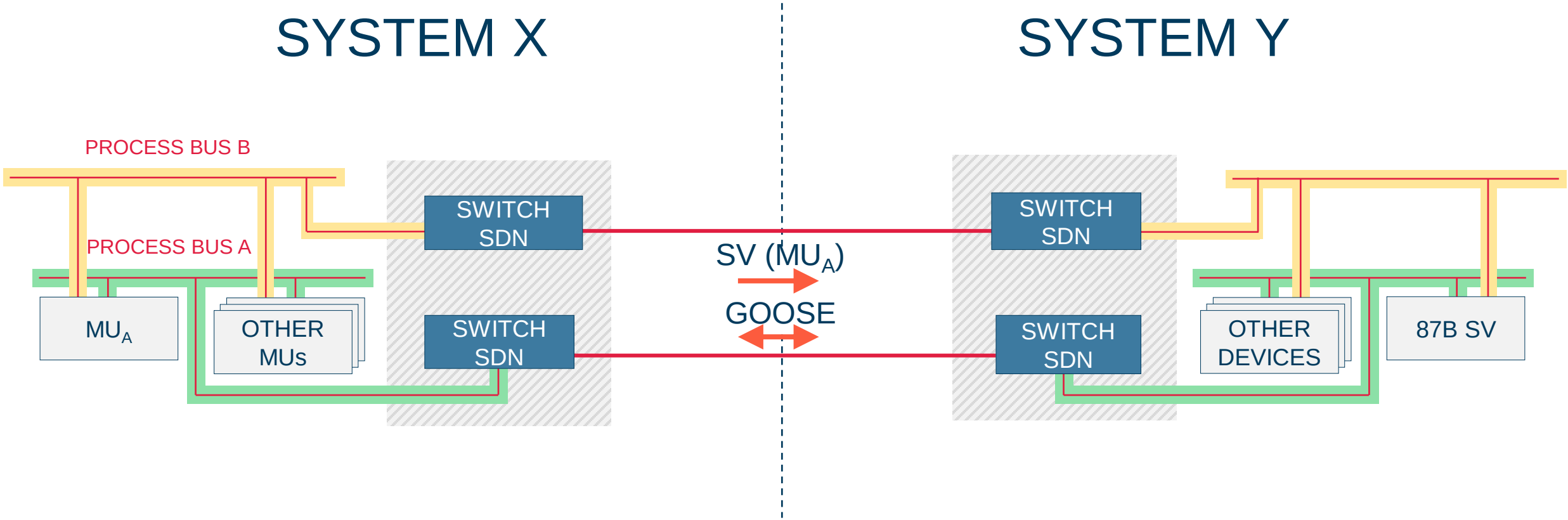

SEL-421
SEL-421
SEL-421
SEL-2740S
SEL-2740S
Merging Unit
Merging Unit (Primary)
Merging Unit (Alternate)
Merging Unit

Flow Monitoring

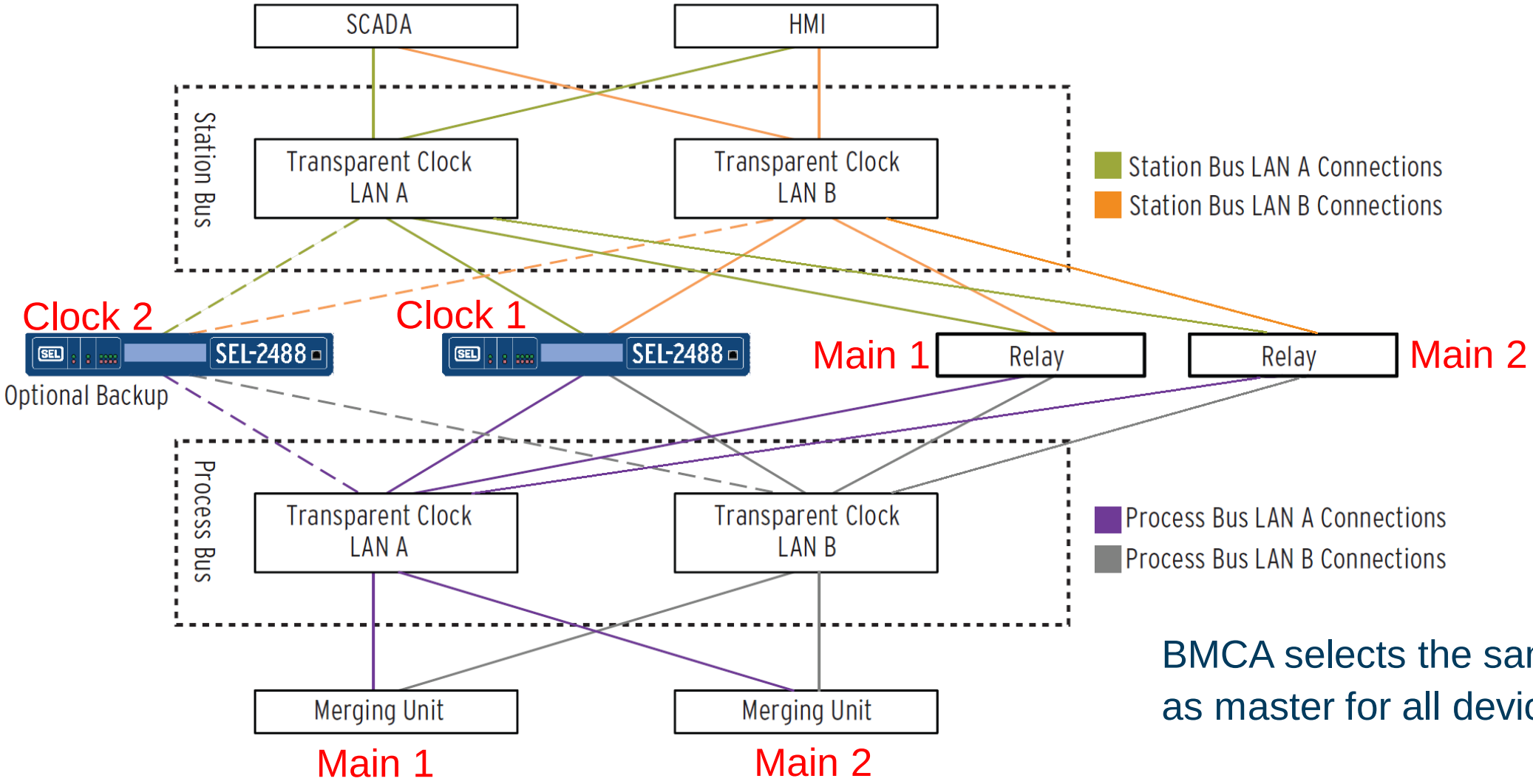


- Monitor each flow individually
- Limit the available bandwidth for each flow individually
- See communications flow in context of application

Isolate Networks



PRP and PTP Redundancy



BMCA selects the same clock as master for all devices

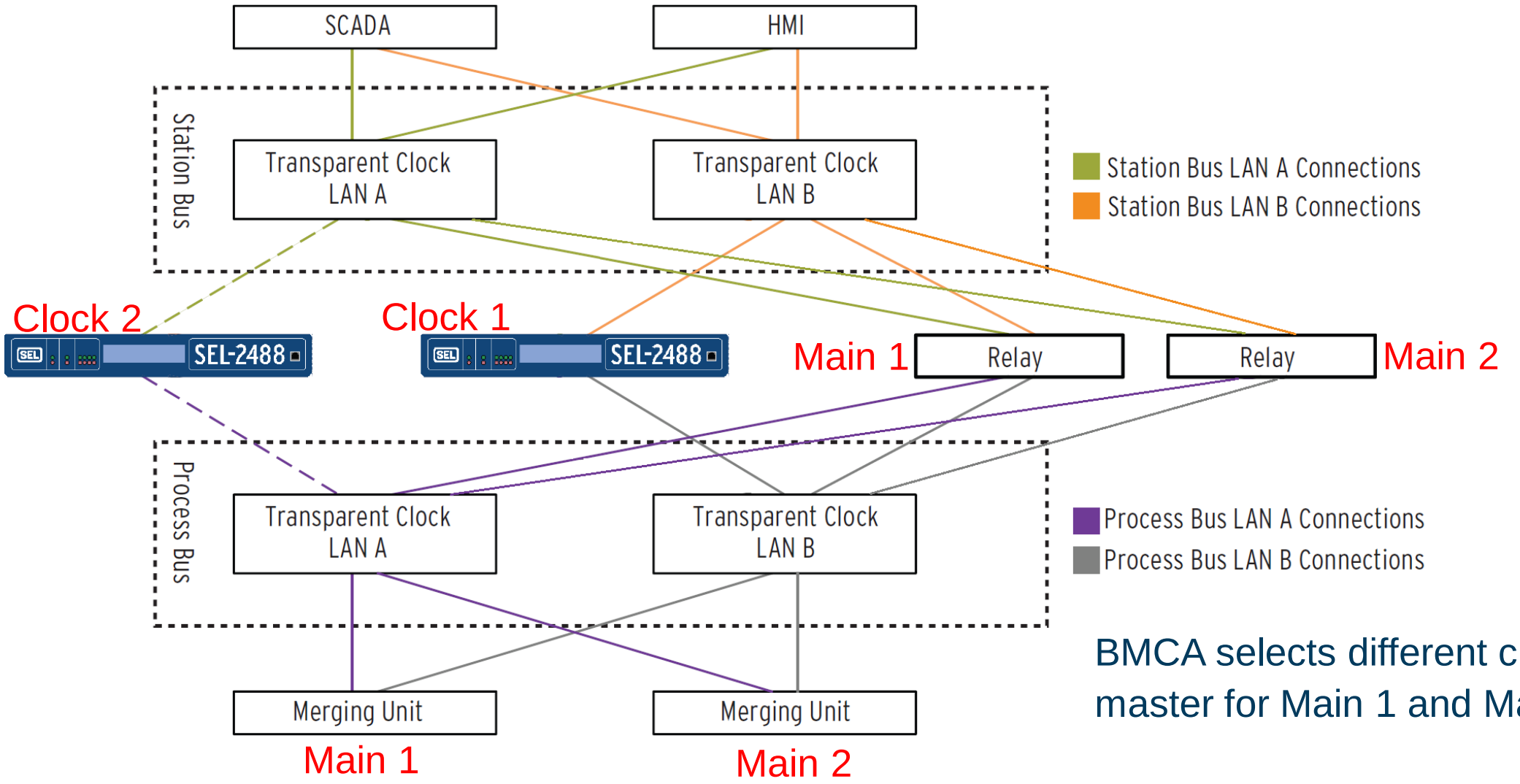
PTP Redundancy

- to one LAN only as a singly attached clock (see OC3, OC4 in Figure A.4) without the benefit of redundancy;
- through a RedBox as specified in A.4.5 (see OC5, OC6 in Figure A.4).

NOTE A PRP topology in which one MC is located on LAN A and another MC on LAN B is considered a degraded situation, since a grandmaster clock (GMC) on one LAN ignores another master on the other LAN and cannot serve as a back-up. This situation happens when links are lost and ordinary clocks take over as master for lack of a better alternative. This situation can be avoided if at least one device according to A.7.3. exists. However, this can also be an intentional way of providing independent redundant clocks.

Source: IEC 62439-3:2018

Changing PTP Priority Per Device



BMCA selects different clocks as master for Main 1 and Main 2

Changing PTP Priority Per Device

- If the ALTPRIn (alternate priority 1 for master n) setting is set to a positive value, the priority1 value in received Announce messages from the corresponding master clock will be replaced by the ALTPRIn value before applying the BMCA. The ALTPRIn values reprioritize the master clocks locally.

PTP Settings

Search PTP Settings

Filters

Name	Value	Range	Description	Group
ALTPRI1	0	0 to 255	PTP Alternate Priority1 for Master 1	Port 5
ALTPRI2	0	0 to 255	PTP Alternate Priority1 for Master 2	Port 5
ALTPRI3	0	0 to 255	PTP Alternate Priority1 for Master 3	Port 5
ALTPRI4	0	0 to 255	PTP Alternate Priority1 for Master 4	Port 5
ALTPRI5	0	0 to 255	PTP Alternate Priority1 for Master 5	Port 5

Merging Unit 1

TIME SYNC | MU1

Application	Reference	Value
	LTMS.TmAcc.stVal (ST)	20 Significant bits in the second fraction
	LTMS.PortSta5A.strVal (ST)	ACTIVE - GM ID 20
	LTMS.PortSta5B.strVal (ST)	PASSIVE - GM ID 30
	LTMS.GmIncry5A (ST)	23.0000 ns
	LTMS.GmIncry5B (ST)	21.0000 ns
	LTMS.NtwIncry5A (ST)	49.0000 ns
	LTMS.NtwIncry5B (ST)	49.0000 ns
	LTMS.TmSrc.stVal (ST)	GPS
	LTMS.TmSrcTyp.stVal (ST)	PTP
	LTMS.TmSyn.stVal (ST)	GlobalAreaClock
	LTMS.TmSynLkd.stVal (ST)	Locked
	LTMS.TmTosPer.instMag.f (MX)	999.9999 ms

Merging Unit 2

TIME SYNC | MU2

Application	Reference	Value
	LTMS.TmAcc.stVal (ST)	20 Significant bits in the second fraction
	LTMS.PortSta5A.strVal (ST)	PASSIVE - GM ID 20
	LTMS.PortSta5B.strVal (ST)	ACTIVE - GM ID 30
	LTMS.GmIncry5A (ST)	36.0000 ns
	LTMS.GmIncry5B (ST)	21.0000 ns
	LTMS.NtwIncry5A (ST)	49.0000 ns
	LTMS.NtwIncry5B (ST)	49.0000 ns
	LTMS.TmSrc.stVal (ST)	GPS
	LTMS.TmSrcTyp.stVal (ST)	PTP
	LTMS.TmSyn.stVal (ST)	GlobalAreaClock
	LTMS.TmSynLkd.stVal (ST)	Locked
	LTMS.TmTosPer.instMag.f (MX)	999.9999 ms

PTP Network Engineering

C.8 Network engineering

To achieve the required network time inaccuracy, careful network design is required, considering the placement of masters and redundant masters and possible network topology changes because of reconfigurations so as not to exceed the number of allowed TCs and BCs.

The network designer should only select network elements knowing their contribution to network time inaccuracy and dependencies on the operating conditions. The network designer should estimate the network time inaccuracy for all slave clocks.

The network designer should use network elements with stricter specifications in more demanding applications or larger networks.

Source: IEC 62439-3:2018

Network Time Innacuracy

$$NTI = \varepsilon_{GM} + \varepsilon_{TC} N_{TC} + \varepsilon_{BC} N_{BC} + \varepsilon_{MC} N_{MC}$$

ε_{GM} - worst-case grandmaster time inaccuracy

ε_{TC} - worst-case Transparent Clock time inaccuracy

ε_{BC} - worst-case Boundary Clock time inaccuracy

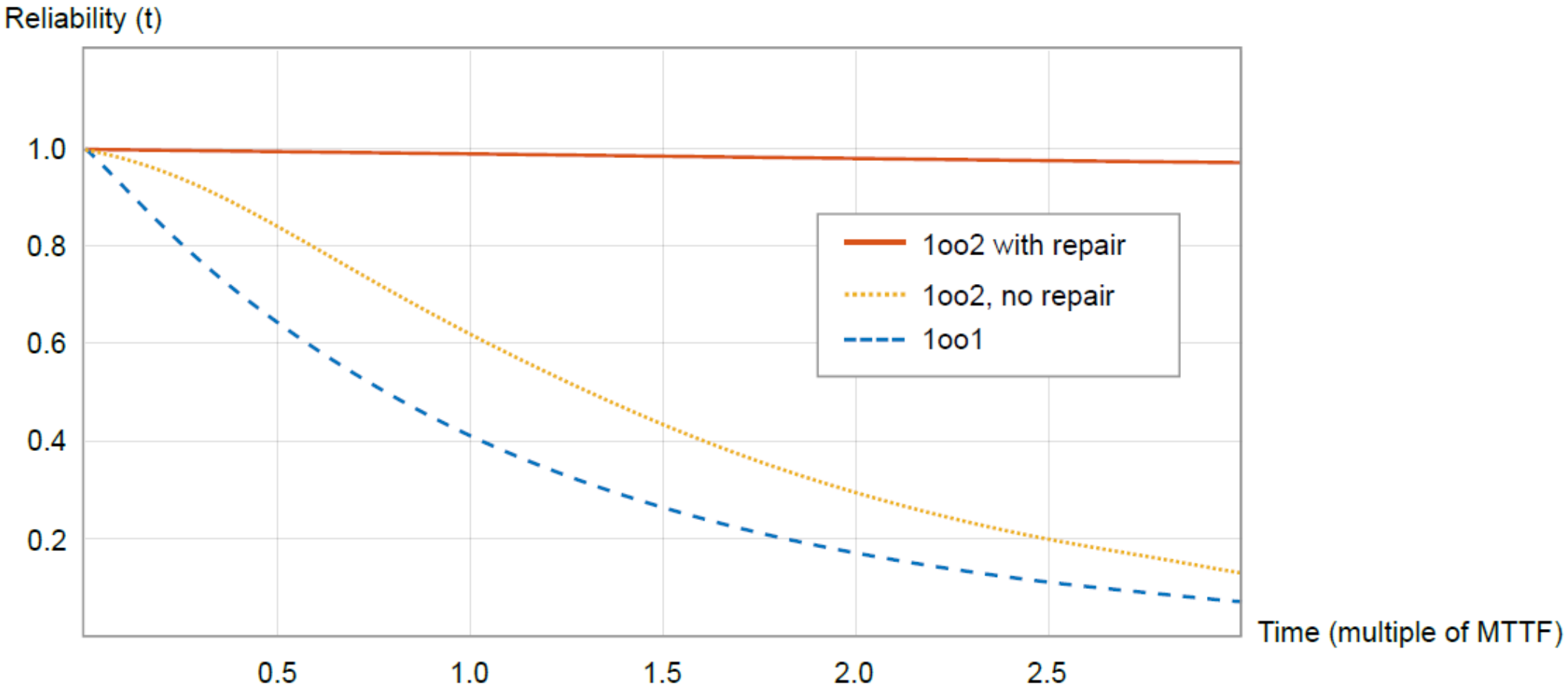
ε_{MC} - worst-case media converter time inaccuracy

N_{TC} - number of TCs in series on the longest path to this clock

N_{BC} - number of BCs in the path on the longest path to this clock

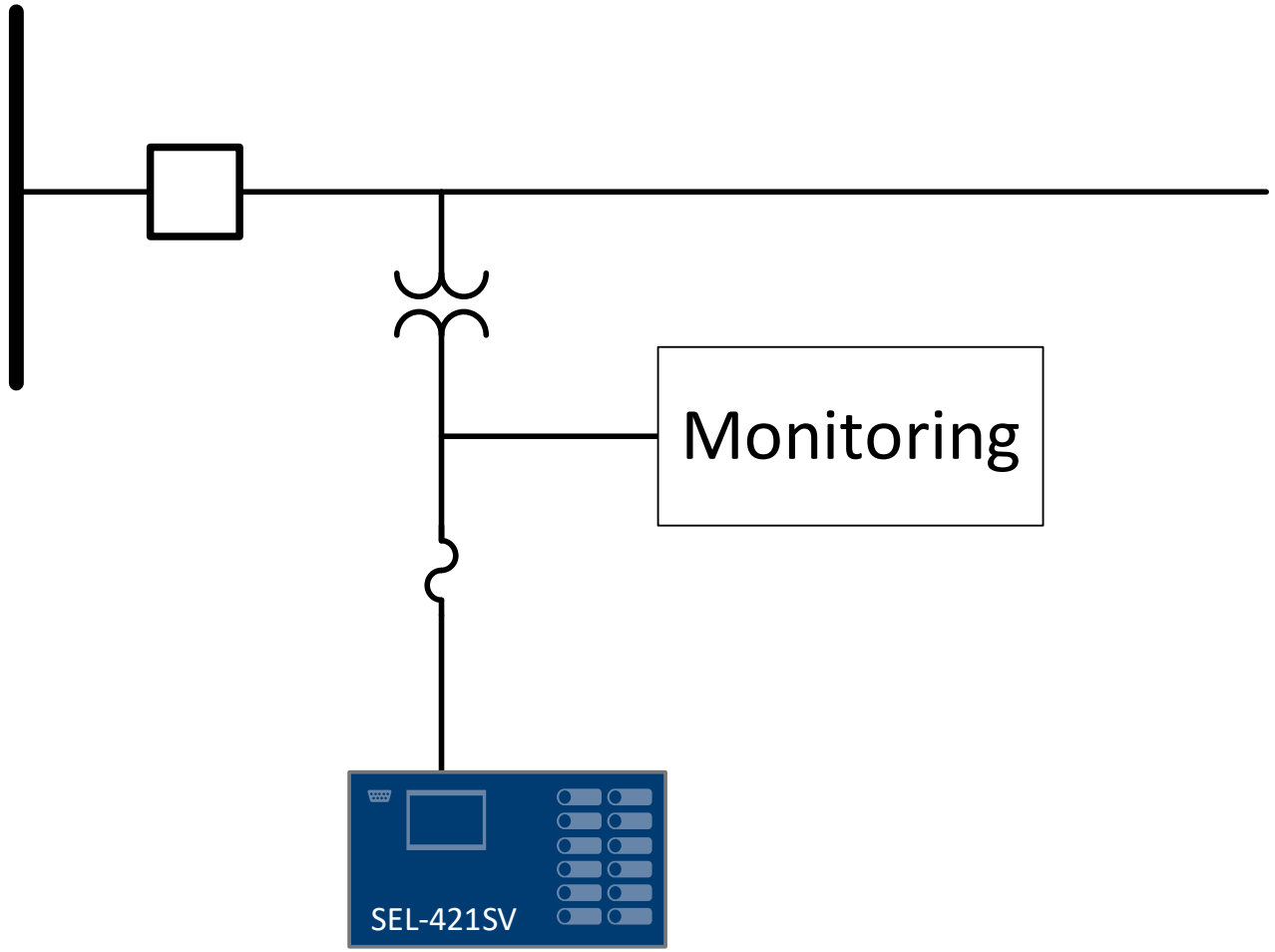
N_{MC} - number of media converters in the path on the longest path to this clock

Redundancy May not Be Effective



Source: IEC TR 61850-90-12:2020

Are You Monitoring Properly?



Conclusions

- Common-mode failures affect redundant scheme dependability and security – settings and design reviews improve reliability
- Comprehensive monitoring systems improves dependability and security of redundancy
- Fundamental requirements of protection systems cannot be left behind

Thank you

SCHWEITZER ENGINEERING LABORATORIES