IEC/TR 61850-90-4

Edition 1.0 2013-08

TECHNICAL REPORT

colour inside

Communication networks and systems for power utility automation – Part 90-4: Network engineering guidelines

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

Useful links:

IEC publications search - www.iec.ch/searchpub

The advanced search enables you to find IEC publications by a variety of criteria (reference number, text, technical committee,…).
It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available on-line and also once a month by email.

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary (IEV) on-line.

Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

IEC/TR 61850-90-4

Edition 1.0 2013-08

TECHNICAL REPORT

colour inside

Communication networks and systems for power utility automation – Part 90-4: Network engineering guidelines

INTERNATIONAL ELECTROTECHNICAL COMMISSION

PRICE CODE XH

ICS 33.200

ISBN 978-2-8322-0903-5

Warning! Make sure that you obtained this publication from an authorized distributor.

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

COMMUNICATION NETWORKS AND SYSTEMS FOR POWER UTILITY AUTOMATION –

Part 90-4: Network engineering guidelines

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

The main task of IEC technical committees is to prepare International Standards. However, a technical committee may propose the publication of a technical report when it has collected data of a different kind from that which is normally published as an International Standard, for example "state of the art".

IEC 61850-90-4, which is a technical report, has been prepared by IEC technical committee 57: Power systems management and associated information exchange.

The text of this technical report is based on the following documents:

Enquiry draft	Report on voting
57/1238/DTR	57/1330/RVC

Full information on the voting for the approval of this technical report can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

A list of all parts in the IEC 61850 series, published under the general title *Communication networks and systems for power utility automation,* can be found on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

A bilingual version of this publication may be issued at a later date.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

The growing success of the IEC 61850 series calls for guidelines for engineering Ethernet networks. The IEC 61850 series specifies the basic requirements for the networks but not how to achieve them. Instead, the IEC 61850 series of standards focuses on data modelling and the interchange of that data, leaving out physical interconnection details that are nevertheless needed for full interoperability.

This Technical Report provides definitions, guidelines and specifications for the network engineering of IEC 61850-based substation automation.

This Technical Report addresses issues such as Ethernet technology, network topology, redundancy, traffic latency and quality of service, traffic management by multicast and VLAN, network-based clock synchronization and testing of the network. It does not address network-based security.

The Technical Report is based on existing standards for semantics, services, protocols, system configuration language and architecture. It is based on work done by IEC TC 57 WG 10 (Power system IED communication and associated data models) and IEC TC 57 WG 15 (Data and communications security), on IEC 61918 (*Industrial communication networks – Installation of communication networks in industrial premises*), IEC 62439 (*Industrial communication networks – High-availability automation networks*) and IEC 61588 (*Precision clock synchronization protocol for networked measurement and control systems*), on the work of the IEEE 802.1 Working Group, the UCA International Users Group 9-2LE and the IEEE Power System Relaying Committee (PSRC), and on contributions by different companies.

The contents of this Technical Report have been coordinated with the Working Groups producing IEC 62439, IEC 62351 and with the IEEE PSRC.

COMMUNICATION NETWORKS AND SYSTEMS FOR POWER UTILITY AUTOMATION –

Part 90-4: Network engineering guidelines

1 Scope

This part of IEC 61850, which is a Technical Report, is intended for an audience familiar with network communication and/or IEC 61850-based systems and particularly for substation protection and control equipment vendors, network equipment vendors and system integrators.

This Technical Report focuses on engineering a local area network limited to the requirements of IEC 61850-based substation automation. It outlines the advantages and disadvantages of different approaches to network topology, redundancy, clock synchronization, etc. so that the network designer can make educated decisions. In addition, this report outlines possible improvements to both substation automation and networking equipment.

This Technical Report addresses the most critical aspects of IEC 61850, such as protection related to tripping over the network. This Technical Report addresses in particular the multicast data transfer of large volumes of sampled values (SV) from merging units (MUs). It also considers the high precision clock synchronization and “seamless” guaranteed transport of data across the network under failure conditions that is central to the process bus concept.

This Technical Report is not a tutorial on networking or on IEC 61850. Rather, it references and summarizes standards and publications to assist the engineers. Many publications discuss the Ethernet technology but do not address the networks in terms of substation automation. Therefore, many technologies and options have been ignored, since they were not considered relevant for a future-proof substation automation network design.

This Technical Report does not address network security.

This Technical Report does not address substation-to-substation communication, or substation to control centre communication. Inter-substation communication involves WAN technologies other than Ethernet, but when it uses Ethernet on layer 2, parts of this report can be applied. For inter-substation communication which uses exclusively the routable Internet Protocol, more adapted guidelines are in discussion within IEC TC 57, especially in documents IEC/TR 61850-90-1, IEC 61850-90-2[1], and IEC/TR 61850-90-5, which will be addressed in the WAN engineering guidelines, IEC 61850-90-12[2].

This Technical Report does not dispense the responsible system integrator from an analysis of the actual application configuration, which is the base for a dependable system.

---

1 Under consideration.

2 Under consideration.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 60050 (all parts), *International Electrotechnical Vocabulary* (<available at: http://www.electropedia.org/>)

IEC 60834-1, *Teleprotection equipment of power systems – Performance and testing – Part 1: Command systems*

IEC 60870-2-2, *Telecontrol equipment and systems – Part 2: Operating conditions – Section 2: Environmental conditions (climatic, mechanical and other non-electrical influences)*

IEC 61000-4-4, *Electromagnetic compatibility (EMC) – Part 4-4: Testing and measurement techniques – Electrical fast transient/burst immunity test*

IEC 61000-4-5, *Electromagnetic compatibility (EMC) – Part 4-5: Testing and measurement techniques – Surge immunity test*

IEC 61000-6-2, *Electromagnetic compatibility (EMC) – Part 6-2: Generic standards – Immunity for industrial environments*

IEC 61508-4, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*

IEC 61588:2009, *Precision clock synchronization protocol for networked measurement and control systems*

IEC 61754-2, *Fibre optic connector interfaces – Part 2: Type BFOC/2,5 connector family*

IEC 61754-20, *Fibre optic interconnecting devices and passive components – Fibre optic connector interfaces – Part 20: Type LC connector family*

IEC 61800-3, *Adjustable speed electrical power drive systems – Part 3: EMC requirements and specific test methods*

IEC 61850-3, *Communication networks and systems for power utility automation – Part 3: General requirements*

IEC 61850-4, *Communication networks and systems for power utility automation – Part 4: System and project management*

IEC 61850-5:2013, *Communication networks and systems for power utility automation – Part 5: Communication requirements for functions and device models*

IEC 61850-6:2009, *Communication networks and systems for power utility automation – Part 6: Configuration description language for communication in electrical substations related to IEDs*

IEC 61850-7-1:2011, *Communication networks and systems for power utility automation – Part 7-1: Basic communication structure – Principles and models*

IEC 61850-7-2:2010, *Communication networks and systems for power utility automation – Part 7-2: Basic information and communication structure – Abstract communication service interface (ACSI)*

IEC 61850-7-3, *Communication networks and systems for power utility automation – Part 7-3: Basic communication structure – Common data classes*

IEC 61850-7-4:2010, *Communication networks and systems for power utility automation – Part 7-4: Basic communication structure – Compatible logical node classes and data object classes*

IEC 61850-8-1:2011, *Communication networks and systems for power utility automation – Part 8-1: Specific communication service mapping (SCSM) – Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3*

IEC 61850-9-2:2011, *Communication networks and systems for power utility automation – Part 9-2: Specific communication service mapping (SCSM) – Sampled values over ISO/IEC 8802-3*

IEC/TR 61850-90-1, *Communication networks and systems for power utility automation – Part 90-1: Use of IEC 61850 for the communication between substations*

IEC/TR 61850-90-5, *Communication networks and systems for power utility automation – Part 90-5: Use of IEC 61850 to transmit synchrophasor information according to IEEE C37.118*

IEC 61869-9:__[3], *Instrument transformers – Part 9: Digital interface for instrument transformers*

IEC 62351 (all parts), *Power systems management and associated information exchange – Data and communications security*

IEC/TS 62351-6, *Power systems management and associated information exchange – Data and communications security – Part 6: Security for IEC 61850*

IEC 62439-1:2010, *Industrial communication networks – High availability automation networks – Part 1: General concepts and calculation methods*
Amendment 1:2012

IEC 62439-3:2012, *Industrial communication networks – High availability automation networks – Part 3: Parallel Redundancy Protocol (PRP) and High availability Seamless Redundancy (HSR)*

IEC 81346 (all parts), *Industrial systems, installations and equipment and industrial products – Structuring principles and reference designations*

ISO/IEC 8326:1996, *Information processing system – Open Systems Interconnection – Session service definition*

ISO/IEC 8649, *Information technology – Open Systems Interconnection – Service definition for the Association Control Service Element*[4]

---

[3] To be published.

[4] Withdrawn.

ISO/IEC 8802-2, *Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 2: Logical link control*

ISO/IEC 8824-1, *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation*

ISO 9506-1:2003*, Industrial automation systems – Manufacturing Message Specification – Part 1: Service definition*

ISO 9506-2:2003, *Industrial automation systems – Manufacturing Message Specification – Part 2: Protocol specification*

IEEE 802.1AB-2005, *IEEE standard for Local and metropolitan area networks – Station and Media Access Control Connectivity Discovery*

IEEE 802.1D-2004, *IEEE standard for Local and metropolitan area networks – Common specifications – Media Access Control (MAC) Bridges*

IEEE 802.1Q-2011, *IEEE standard for Local and metropolitan area networks – Media Access Control (MAC) Bridges and Virtual Bridge Local Area Networks*

IEEE 802.3, *Local Area Network (LAN) protocols*

IEEE 1344, *IEEE Standard for Synchrophasors for Power Systems* (replaced by IEEE C37.118)

IEEE 1613-2009, *IEEE Standard – Environmental and Testing Requirements for Communications Networking Devices Installed in Electric Power Substations*

IEEE C37.118.1-2011, *IEEE Standard for Synchrophasor Measurements for Power Systems*

IEEE C37.118.2-2011, *IEEE Standard for Synchrophasor Data Transfer for Power Systems*

IEEE C37.238-2011, *IEEE Standard Profile for Use of IEEE 1588 Precision Time Protocol in Power System Applications*

RFC 793: 1981, *DARPA Internet Program, Transmission Control Protocol, Protocol Specification, 1981*

RFC 1006: 1987, *Network Working Group, ISO Transport Service on top of the TCP Version:3*

RFC 1305: 1992, *Network Working Group, Network Time Protocol (Version 3)*

RFC 2328: 1998, *The Internet Society, OSPF Version 2*

RFC 2661: 1999, *The Internet Society, Layer Two Tunneling Protocol "L2TP"*

RFC 3416: 2002, *The Internet Society, Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)*

RFC 4330: 2006, *The Internet Society, Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI*

RFC 4836: 2007, *IETF Trust, Definitions of Managed Objects for IEEE 802.3 Medium Attachment Units (MAUs)*

TIA/EIA 568A, *Commercial building telecommunications cabling standard set (contains: TIA-568-C.0, TIA-568-C.1, TIA-568-C.2, TIA-568-C.3 AND TIA-568-C.4 – with addendums and erratas)*

3 Terms, definitions, abbreviations and conventions

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 60050-191:1990, as well as the following, apply.

3.1.1
bridge
network device that connects network segments at the data link layer (layer 2) of the OSI model, according to the principles of IEEE 802.1D Clause 7

Note 1 to entry: A bridge is often referred to as a “layer 2 switch”. In this document, the word “bridge” means the logic used to forward a frame from one port to another at layer 2, while “switch” designates a device with additional functionalities.

3.1.2
broadcast domain
set of all network nodes that receive a layer 2 frame with a broadcast destination address

Note 1 to entry: The broadcast domain is the entire layer 2 subnet.

3.1.3
broadcast storm
condition on a network where there is an abnormally huge broadcast traffic that consumes resources and renders the network unable to transport normal traffic

3.1.4
bus
communication medium that supports broadcast, either physically (e.g. radio, multi-drop cable) or logically (e.g. switched layer 2 network), as opposed to links that are point-to-point connections

3.1.5
cut-through
basic operation of a bridge, in which frames on ingress are forwarded to the appropriate egress port(s) before the whole frame has been received, on the basis of their header

Note 1 to entry: “Cut-through” is in contrast to “store-and-forward”.

3.1.6
doubly attached node
node that has two ports for the purpose of redundant operation

[SOURCE: IEC 62439-1:2010, 3.1.11]

3.1.7
layer 2
data link layer of the OSI model

Note 1 to entry: At layer 2, data packets are encoded and decoded into bits. Layer 2 is divided into sub layers: Media Access Control (MAC) and Logical Link Control (LLC). The MAC sub layer controls how a network node gains access to the media and the LLC sub layer handles flow control and error checking. Ethernet is a layer 2 technology.

[SOURCE: ISO/IEC 7498-1:1994]

3.1.8
layer 3
network layer of the OSI model

Note 1 to entry: At layer 3, data packets are routed depending on their IP address over any layer 2 technology, e.g. Ethernet or wireless. The use of broadcast domains is limited at layer 3.

[SOURCE: ISO/IEC 7498-1:1994]

3.1.9
logical topology
actual path through which data pass through the network from one node to another node

Note 1 to entry: "Logical topology" is in contrast to "physical topology", which is the set of all possible physical paths.

3.1.10
managed switch
bridge that includes the basic bridge functionality as defined in IEEE 802.1D Clause 7.1 plus a variety of configurable features such as: a user interface, SNMP management, redundancy protocols, and VLAN support among others

Note 1 to entry: The IEEE standards use the term "bridge" instead of the more common term "switch" for layer-2 communication.

3.1.11
merging unit
1) logical device, a unit that generates SV traffic for eight process values (four voltage and four currents) in a synchronized way, allowing to correlate these samples [UCA 61850-9-2LE]

merging unit
2) physical device (IED in the meaning of IEC 61850-2) in which logical device merging unit is implemented [IEC 61869-9]

Note 1 to entry: A SAMU is a particular case of a PIA that contains a Merging Unit Logical Device and that uses standardized analog values as an input.

3.1.12
multicast domain
set of all nodes that receive a layer 2 frame with a given multicast destination address

Note 1 to entry: The multicast domain is equal to the broadcast domain unless multicast traffic filtering is applied.

3.1.13
node
network entity connected to one or more links

[SOURCE: IEC 62439-1:2010, 3.1.35]

3.1.14
PHY
physical layer device that interfaces to the media independent interface

Note 1 to entry: PHYs are usually integrated circuits that encode and decode the bit stream of data for transmission and reception on the physical media and can do additional functions such as line supervision and time-stamping.

3.1.15
process interface
physical device that interfaces to the primary technology and that is attached to the process bus

Note 1 to entry: A PI-Analog (PIA) is a measuring device generating synchronized samples for current or voltage.

Note 2 to entry: A PI-Binary (PIB) is an Input/Output device for binary values that can issue control signals to the primary technology such as trip signals or tap changer.

Note 3 to entry: See also: merging unit, 3.1.11.

Note 4 to entry: A PIA is not a SAMU according to IEC 61869-9 since it accepts also non-standard inputs.

3.1.16
physical topology
set of all possible paths between nodes

Note 1 to entry: “Physical topology” is in contrast to “logical topology”, which is the set of all actual paths.

3.1.17
process bus
communication network which connects IEDs at primary equipment level

Note 1 to entry: Originally, the process bus was specified as the carrier of the IEC 61850-9-2 traffic (SV), but it can carry other traffic, such as IEC 61850-8-1 (MMS and GOOSE) or FTP.

3.1.18
QuadBox
four-port layer-2 bridge between two HSR rings

3.1.19
RedBox
layer 2 bridge between singly attached nodes and two PRP LANs or between an HSR LAN and singly attached nodes

Note 1 to entry: RedBox is an abbreviation of “redundancy box”.

3.1.20
router
layer 3 interconnection device

[SOURCE: IEEE 610.7:1995]

3.1.21
singly attached node
node that has only one port to a LAN

[SOURCE: IEC 62439-1:2010, 3.1.55]

3.1.22
spanning tree protocols
family of protocols executed by the bridges which auto-configure a meshed network topology into a tree topology at initialization and upon changes, including RSTP (rapid spanning tree protocol, VLAN unaware) and MSTP (multiple spanning tree protocol, VLAN aware)

3.1.23
station bus
communication network which connects IEDs at bay level and IEDs at station level

Note 1 to entry: Originally, the station bus was specified as the carrier of the IEC 61850-8-1 traffic (MMS and GOOSE), but it can carry IEC 61850-9-2 (SV) and other traffic as well.

3.1.24
store-and-forward
basic operation of a bridge, in which frames on ingress are completely stored before forwarding to the appropriate egress port(s)

Note 1 to entry: "Store-and-forward" is in contrast to "cut-through".

3.1.25
switch
interconnection device between network parts, e.g. a simple repeater (hub), a layer 2 connecting device (bridge) or a layer 3 connecting device (router) or a combination thereof

Note 1 to entry: This document uses "switch" for a complex device, while bridge refers to the IEEE 802.1D functionality. Electrical switches are designated as "switchgear", "circuit breaker" or "disconnector".

3.1.26
switchgear
electrical, high power switching device, circuit breaker or disconnector

3.1.27
unmanaged switch
bridge that only has the basic IEEE 802.1D functionality

Note 1 to entry: An unmanaged switch has typically no configurability, has no SNMP support, has no user interface and is not capable of supporting redundancy protocols, priorities, VLANs, or any other more advanced layer 2 functions.

3.2 Abbreviations

AIS	Air Insulated Switchgear (in open-air substation, as opposed to GIS)
APPID	Application ID in GOOSE and SV messages
ASN.1	Abstract Syntax Notation
AVR	Automatic Voltage Regulator
BC	boundary clock
BCU	Bay Control Unit
BMCA	Best Master Clock Algorithm
BP	Busbar protection
BPDU	Bridge Protocol Data Unit
BPU	Bay Protection Unit
CPU	Central Processing Unit
CT	Current Transformer (for measurement)
DAN	Doubly Attached Node
DANH	Doubly Attached Node using HSR

DANP	Doubly Attached Node using PRP
DANR	Doubly Attached Node using RSTP
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
DMC	Designated Master Clock
ECT	Electronic Current Transformer
EHV	Extra High Voltage
EIT	Electronic Instrument Transformer
EMC	Electro-Magnetic Compatibility
EMI	Electro-Magnetic Interference
EVT	Electronic Voltage Transformer
FEFI	Far End Fault Indication
FMEA	Failure Mode and Effect Analysis
FTP	File Transfer Protocol
GIS	Gas Isolated Switchgear (in underground or compact substation, as opposed to AIS)
GNSS	Global Navigation Satellite System (comprises GPS, GLONASS, Galileo)
GMC	Grandmaster Clock
GMRP	Generic Multicast Registration Protocol
GoID	GOOSE message identifier, string
GVRP	Generic VLAN Registration Protocol
HC	Hybrid Clock
HSR	High-availability Seamless Redundancy HMI Human-Machine Interface
IANA	Internet Assigned Numbers Authority, that manages the IP addresses worldwide
ICD	IED Capability Description, file that describes the objects in an IED
IED	Intelligent Electronic Device
IRIG-B	Inter-Range Instrumentation Group time code B
ICMP	Internet Control Message Protocol
IP	Internet Protocol
LAN	Local Area Network
LLDP	Link Layer Discovery Protocol
MAC	Media Access Control
MC	Multicast

MC	Master Clock
MIB	Management Information Base (used by SNMP)
MMRP	Multiple MAC Registration Protocol
MSTP	Multiple Spanning Tree Protocol
MTBR	Mean Time Between Repairs
MTTR	Mean Time To Repair or Mean Time To Recovery
MTTF	Mean Time To Fail
MU	Merging Unit (Logical Device), merging unit (physical device)
MVRP	Multiple VLAN Registration Protocol
NAT	Network Address Translation
NTP	Network Time Protocol, NTPv4
OC	Ordinary Clock
OAM	Operation, Administration, Maintenance
OSI	Open System Interconnection
PCP	Priority Code Point carried in the tag
PFD	Probability to Fail on Demand
PI	Process Interface (Primary technology to/from process bus)
PIA	Process Interface Analog
PIB	Process Interface Binary
PICS	Protocol Implementation Conformance Statement
PIO	Process Interface Output (to the Primary Technology)
PMC	Protection, Measurement and Control combined IED
PPCP	Port Priority Code Point, default port priority
PPS	Pulse Per Second (1 PPS time synchronization)
PRP	Parallel Redundancy Protocol
PTP	Precision Time Protocol version 2
PVID	Port VLAN identifier
PVMS	Port VLAN member set
QB	QuadBox
RB	RedBox
RSTP	Rapid Spanning Tree Protocol
SAN	Singly Attached Node
SAMU	Stand-Alone Merging Unit

SCADA	Supervisory Control And Data Acquisition
SCD	Substation Configuration Description
SCL	Substation Configuration Language
SLD	Single Line Diagram
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
STP	Spanning Tree Protocol
SSH	Secure SHell
SV	Sampled (measurement) values
TC	transparent clock
TCP	Transmission Control Protocol
TLV	Type-Length-Value, the ASN.1 structuring used e.g. in MMS and PTP messages
UDP	User Datagram Protocol
VID	VLAN identifier
VLAN	Virtual Local Area Network
VT	Voltage Transformer (for measurement)
WAN	Wide Area Network

3.3 Conventions

3.3.1 Network diagram symbols

The symbols shown in Figure 1 are used throughout this document in an effort to provide diagrammatic consistency. These symbols are sometimes combined to create more advanced network nodes. This allows the illustration of fairly complex concepts in a single, uncluttered diagram.

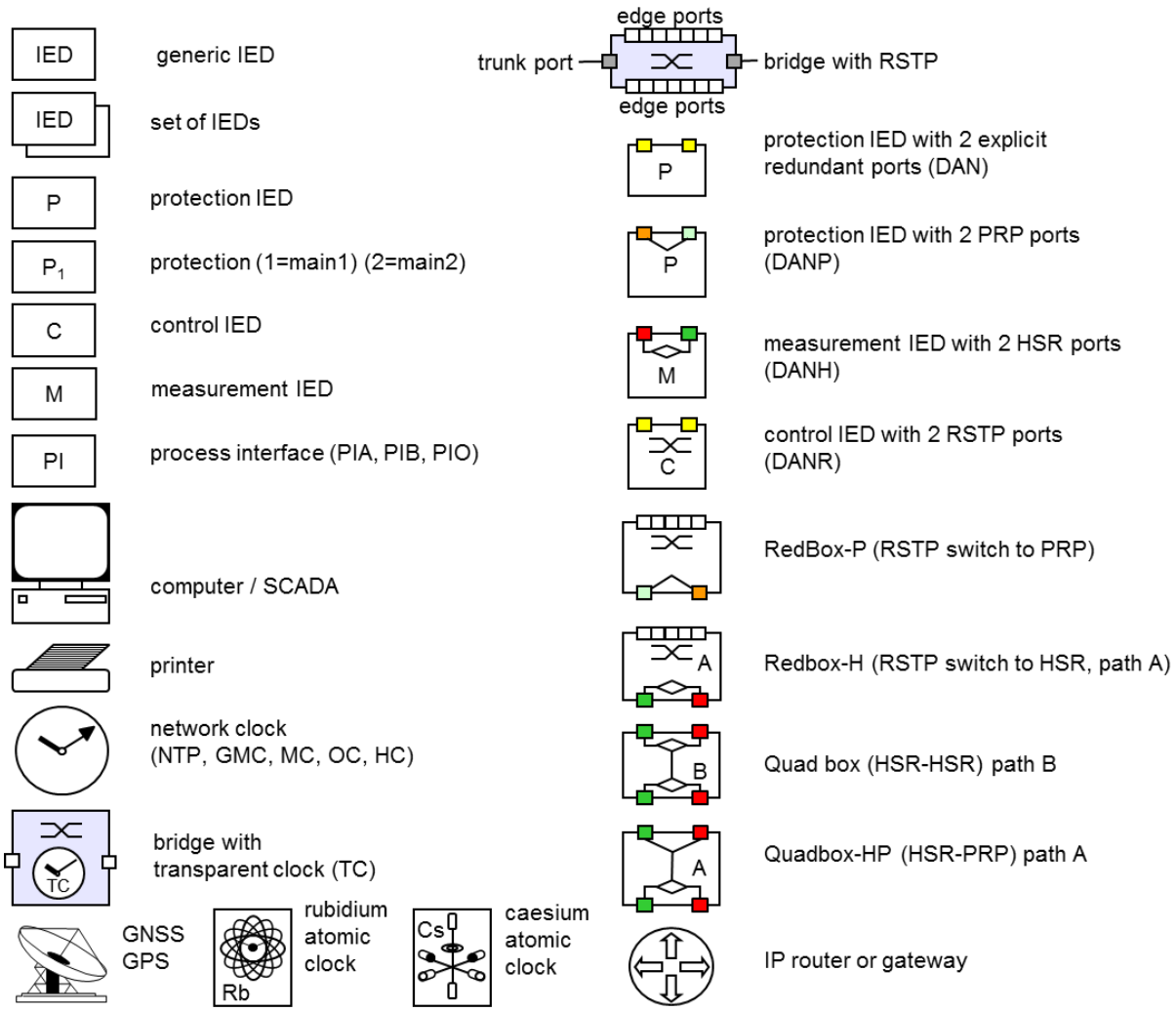


Figure 1 – Network symbols

3.3.2 Port and link symbols

To specify the ports and links, the symbols of Figure 2 are used in this document.

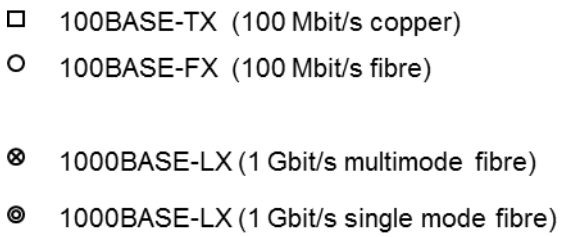


Figure 2 – Port symbols

3.3.3 Bridges symbols

The bridges can be drawn as beams to simplify the drawings, as shown in Figure 3.

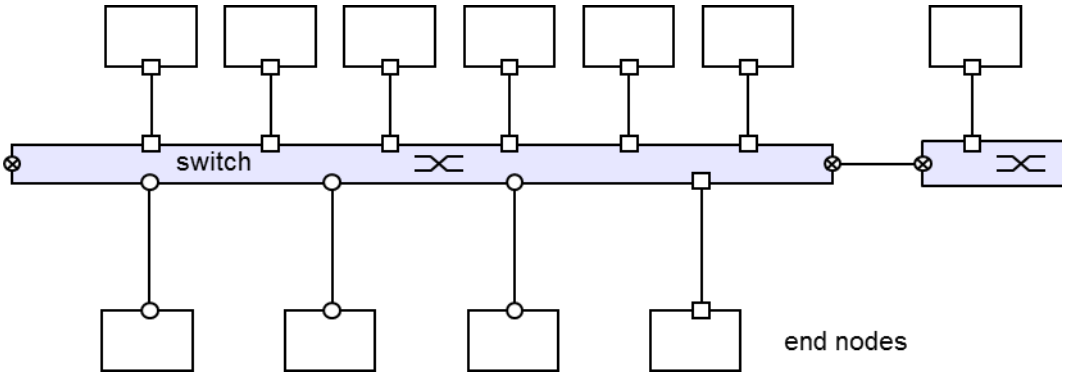


Figure 3 – Bridge symbol as beam

To simplify even more crowded drawings, the bridges can be drawn as a line, although switched Ethernet is not a bussed technology, as shown in Figure 4.

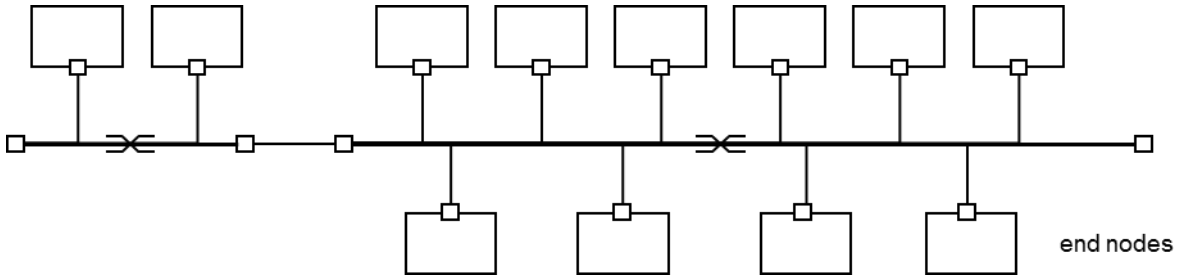


Figure 4 – Bridge symbol as bus

4 Overview of IEC 61850 networks

4.1 Logical allocation of functions and interfaces

IEC 61850-5 defines three different levels (station, bay, process) and the logical allocation of functions and interfaces. This part is repeated here for convenience. Figure 5 depicts these traffic types and flows.

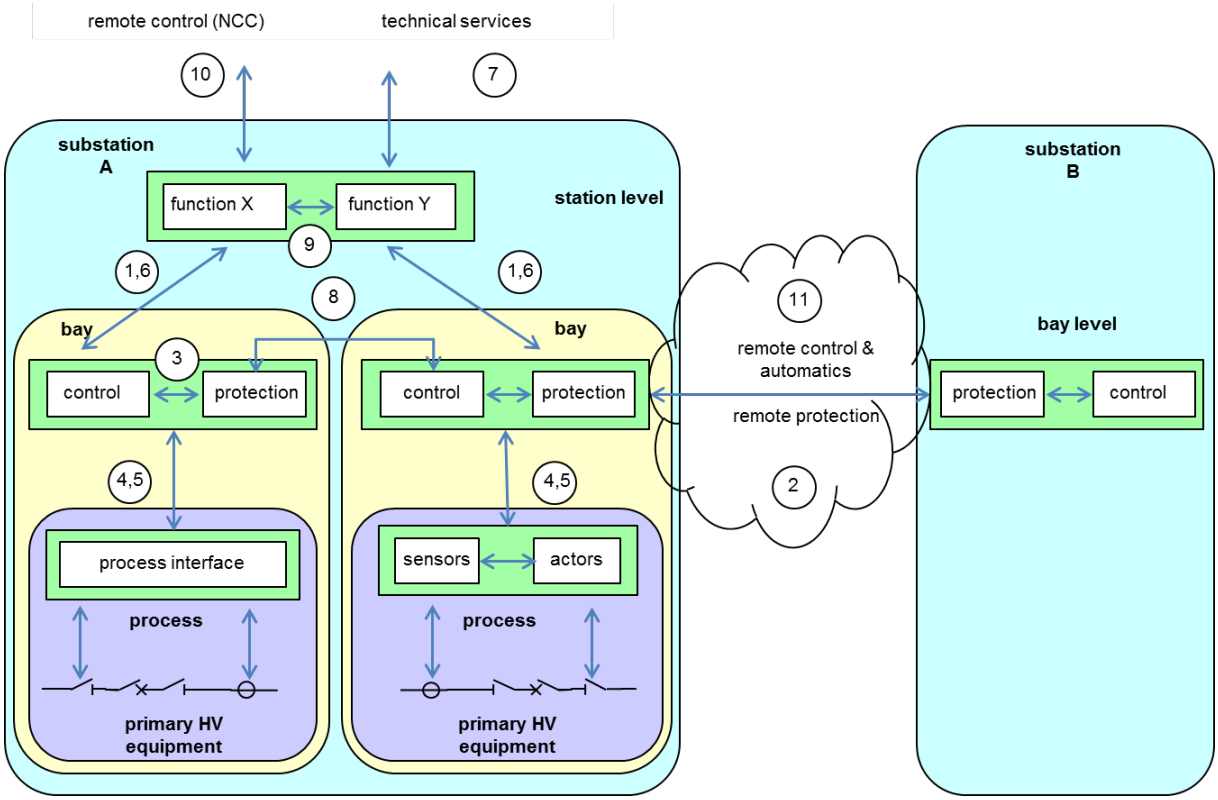


Figure 5 – Levels and logical interfaces in substation automation systems

The cloud in Figure 5 symbolizes a WAN outside of a substation. The meaning of the interfaces is detailed in Table 1.

Table 1 – IEC 61850-5 interface definitions

IF	IEC 61850-5 Definition	Comment
1	Protection-data exchange between bay and station level	The SCADA Gateway / HMI is not involved in protection functions
2	Protection-data exchange between bay level and remote protection (outside the scope of this part of IEC 61850)	Tunnelled GOOSE defined in IEC/TR 61850-90-1
3	Data exchange within bay level	Relates to station bus
4	CT and VT instantaneous data exchange (especially samples) between primary equipment and bay level	Relates to process bus so are not considered for station bus
5	Control-data exchange between primary equipment and bay level	Relates to process bus so are not considered for station bus
6	Control-data exchange between bay and station level	Station bus to SCADA Gateway / HMI communications
7	Data exchange between substation (level) and a remote engineer's workplace	IED and SCADA Gateway / HMI configuration, monitoring from external like engineering PC
8	Direct data exchange between the bays especially for fast functions such as interlocking	Relates to station bus
9	Data exchange within station level	SCADA gateway / HMI communications
10	Control-data exchange between substation (devices) and a remote control centre (outside the scope of this part of IEC 61850)	SCADA gateway / HMI to control centre communications
11	Control-data exchange between substations, e.g. binary signals for interlocking or other inter-substation automatics	Substation to substation, see IEC/TR 61850-90-1

4.2 IEC 61850 protocol stack

4.2.1 General

Figure 6 shows the basic IEC 61850 protocol stack. It is divided into a hard real time stack supporting the services of Sampled Values, GOOSE and the Precision Time Protocol, and a soft real-time stack supporting the network time synchronisation SNTP, the MMS communication and ancillary services mentioned in IEC 61850-8-1. These protocols rely on the services of the MAC layer, which may support 802.1Q VLANs and priorities, redundancy and possibly data security (not shown).

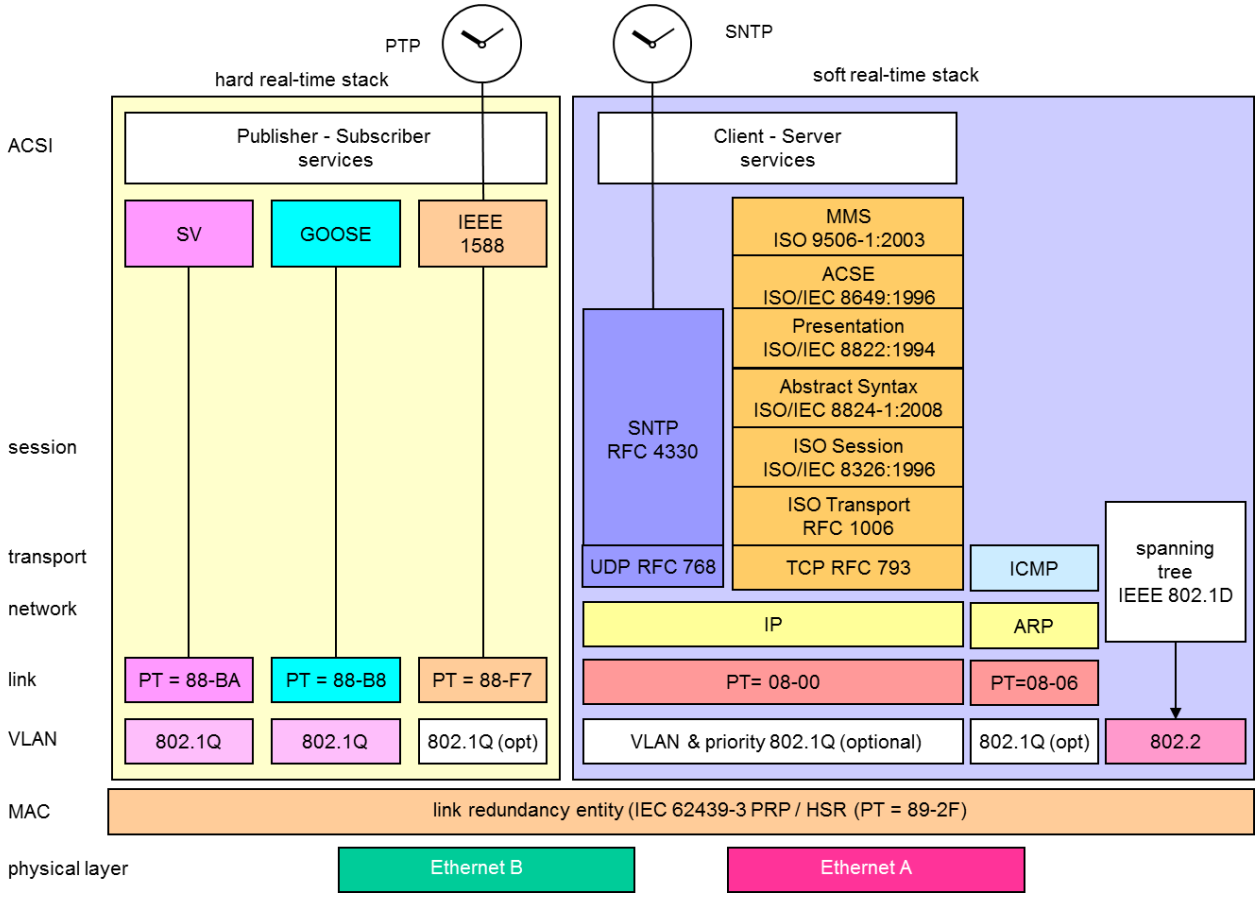


Figure 6 – IEC 61850 protocol stack

4.2.2 IEC 61850 traffic classes

IEC 61850-8-1 and IEC 61850-9-2 define three kinds of traffic:

- MMS traffic defined in IEC 61850-8-1, which allows an MMS client such as the SCADA, an OPC server or a gateway to access “vertically” all IED objects. This traffic flows both on the station bus and on the process bus, although some process bus IEDs do not support MMS.
- GOOSE traffic defined in IEC 61850-8-1, which allows IEDs to exchange data “horizontally” between the bays or “vertically” between process level and bay level, especially for the status signals and tripping signals, and often for interlocking. This traffic flows normally over the station bus and/or the process bus.
- SV traffic defined in IEC 61850-9-2, which carries voltage and current samples. This traffic flows normally on the process bus but can also flow over the station bus, for instance, for busbar protection and phasor measurement.

4.2.3 MMS protocol

The MMS protocol is a client-server (unicast) protocol operating at the network layer (layer 3). Therefore, it operates with IP addresses and can cross routers. In one operating mode, the MMS client (generally the SCADA or the gateway) sends a request for a specific data item to the MMS server of an IED, identified by its IP address. The server returns the requested data in a response message to the IP address of the client. In another mode, the client can instruct the server to send a notification spontaneously upon occurrence of an event (see Figure 7).

To ensure that no event is lost, MMS relies on the TCP protocol for error detection and recovery.

An MMS server can support several clients simultaneously, each client is treated individually.

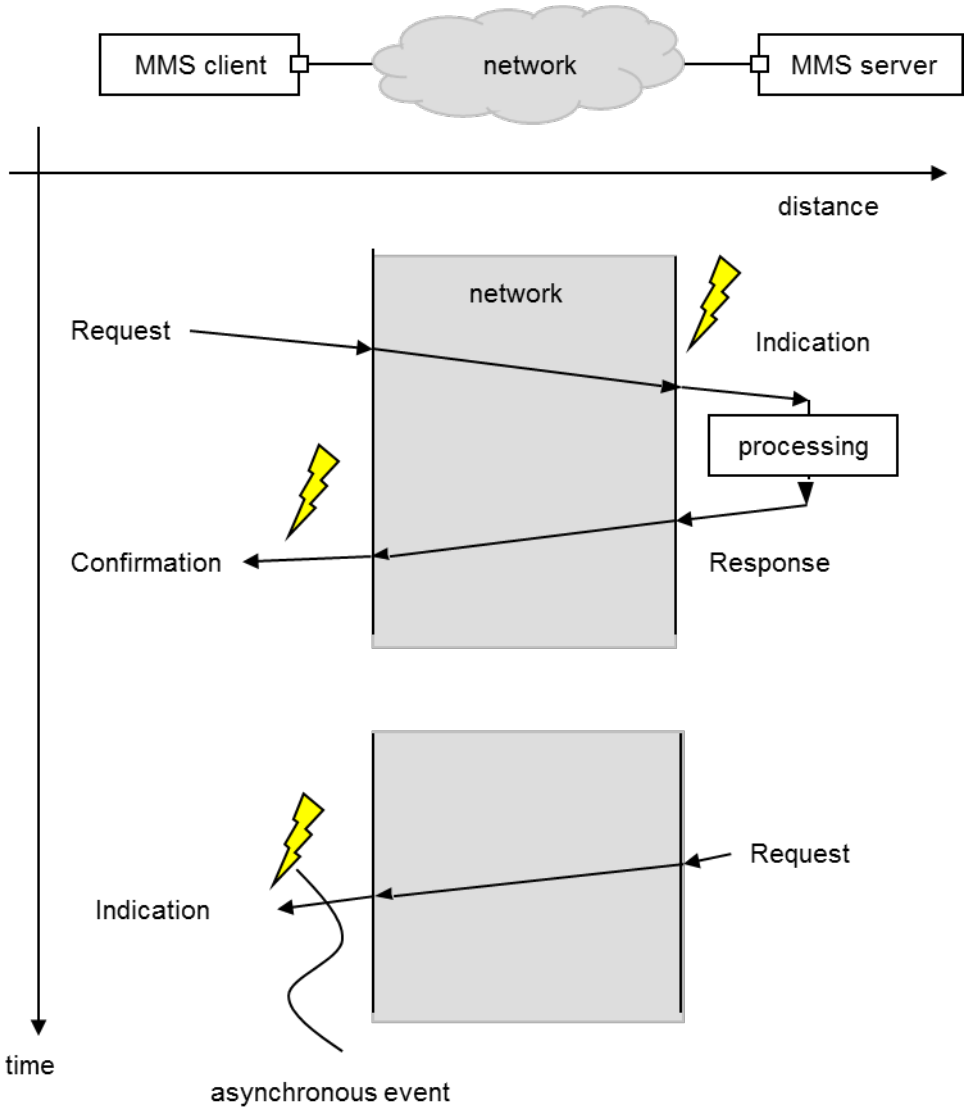


Figure 7 – MMS protocol time/distance chart

4.2.4 GOOSE protocol

GOOSE messages are exchanged at layer 2 (link layer), taking advantage of the multicast functionality provided by Ethernet. The GOOSE communication consists of a fast event-driven transmission and of a slow cyclic transmission as shown in Figure 8 (time/distance chart) and Figure 9 (time chart).

Upon occurrence of a preconfigured event condition, an IED sends immediately a GOOSE message carrying the values of the variables to be communicated for that event.

Since GOOSE messages are multicast, they are not acknowledged by the destination. To overcome transient errors, the same GOOSE message is retransmitted several times in a row, at interval T1, then T2, then T3 (application specific).

To assess the presence of the source, GOOSE messages are retransmitted at low rate T0.

Since GOOSE messages operate on layer 2, they do not leave the LAN and cannot cross routers. They are identified by their source MAC address and an identifier in the message.

GOOSE operates on the publisher/subscriber principle. The new value received replaces the former value, as opposed to being queued if the old value could not be processed in time. However, overwriting is not prescribed, so queuing is also used.

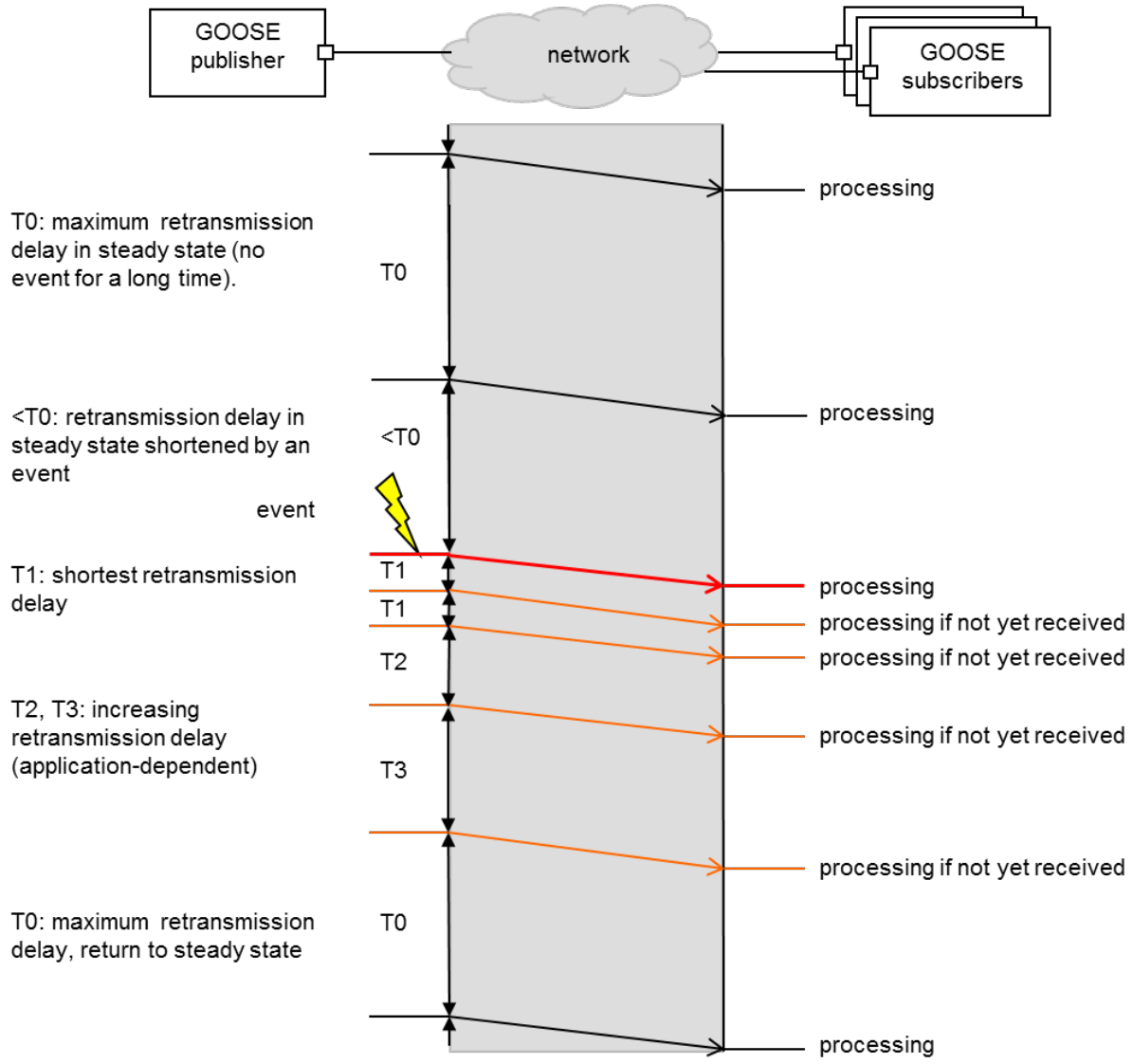


Figure 8 – GOOSE protocol time/distance chart

Figure 9 explains the same GOOSE protocol with a time chart.

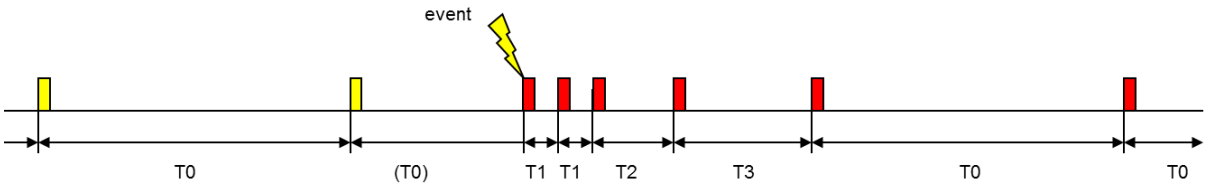


Figure 9 – GOOSE protocol time chart

4.2.5 SV protocol

The Sampled Values protocol (specified in IEC 61850-9-2) is mainly used to transmit analogue values (current and voltage) from the sensors to the IEDs.

The SV protocol, like GOOSE, uses layer 2 multicast, messages are identified by their MAC addresses (and possibly VLAN ID) and an identifier (in the message body).

NOTE IEC 61850-9-2 also foresees a unicast SV transmission, but it is seldom used.

Like for GOOSE, there is no retransmission protocol: a lost sample is overwritten by the next successful one.

The SV messages, unlike GOOSE, are transmitted purely cyclically at high frequency. UCA 61859-9-2LE prescribes a period of 250 μs in a 50 Hz grid, respectively 208,3 μs in a 60 Hz grid.

With a typical size of 160 octets, an SV message takes some 12 μs at 100 Mbit/s (6 % of the bandwidth at 4 800 SV messages per second [15][5]). The period should accommodate a maximum size FTP message of 123 μs at 100 Mbit/s (60 % of the bandwidth at 4 800 SV messages per second), thus limiting the number of attached SV senders on a bus to around 6. Therefore, SV messages must be kept small.

To avoid spurious jamming, all SV sources on the same bus should operate at the same period and preferably implement a time division multiplex scheme as shown in Figure 10.

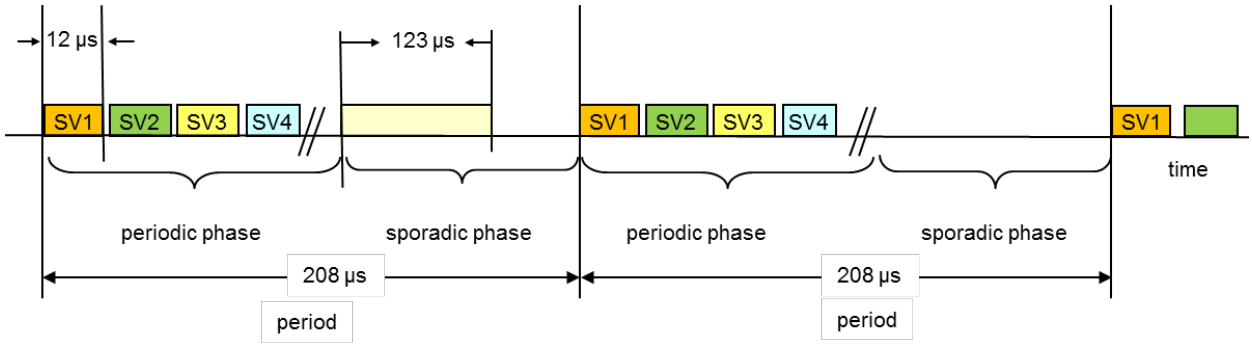


Figure 10 – Example of SV traffic (4 800 Hz)

4.3 Station bus and process bus

The two main interfaces are the station bus and the process bus (see Figure 11). IEC 61850-5 uses the terms “station bus” and “process bus" with no precise definition. Common understanding is:

- The station bus interconnects the whole substation and provides connectivity between central management and the individual bays. It also connects the protection and control devices within a bay, the different bays among themselves, and the bays with the SCADA

[5] Figures in square brackets refer to the Bibliography.

or Grid Control gateway. The station bus connects up to hundreds of IEDs. In large networks, the station bus is segmented, but all segments come together at the station level. Several physically distinct station busses are often used, e.g. one per voltage level, with or without horizontal connection.
The station bus typically carries GOOSE (layer2 multicast) traffic and TCP/UDP (unicast) traffic (MMS, SNTP, SNMP, FTP, etc.), as well as non-IEC 61850 traffic such as video surveillance.
The station bus typically provides only soft real-time quality of service, i.e. some jitter in delivery time is acceptable.

- The station bus can also carry SV traffic (layer 2 multicast) e.g. for busbar protection, and in this case, it provides the same quality of service as a process bus. It could then be beneficial to separate the station bus into two networks, one dedicated to SV traffic and the other to the soft real-time traffic.
- The process bus connects the primary measurement and control equipment to the IEDs. It takes different topologies, from a fan of point-to-point links to a classical network.
  The process bus is generally limited to a bay; in particular applications such as busbar protection and differential protection, it spans several bays.
  The process bus typically carries SV (multicast), GOOSE (multicast) and often MMS (unicast) traffic.
  The process bus is expected to provide hard real-time quality of service, i.e. the transmission guarantees a worst case delivery time. How to provide it is not in the scope of the standard.

NOTE The term “bus” is historical and only reminds that each “bus” is a broadcast domain.

Figure 11 shows a typical structure, the leftmost bay being equipped with a process bus, attached to a Process I/O for analog values (PIA) and a Process I/O for binary values (PIB).

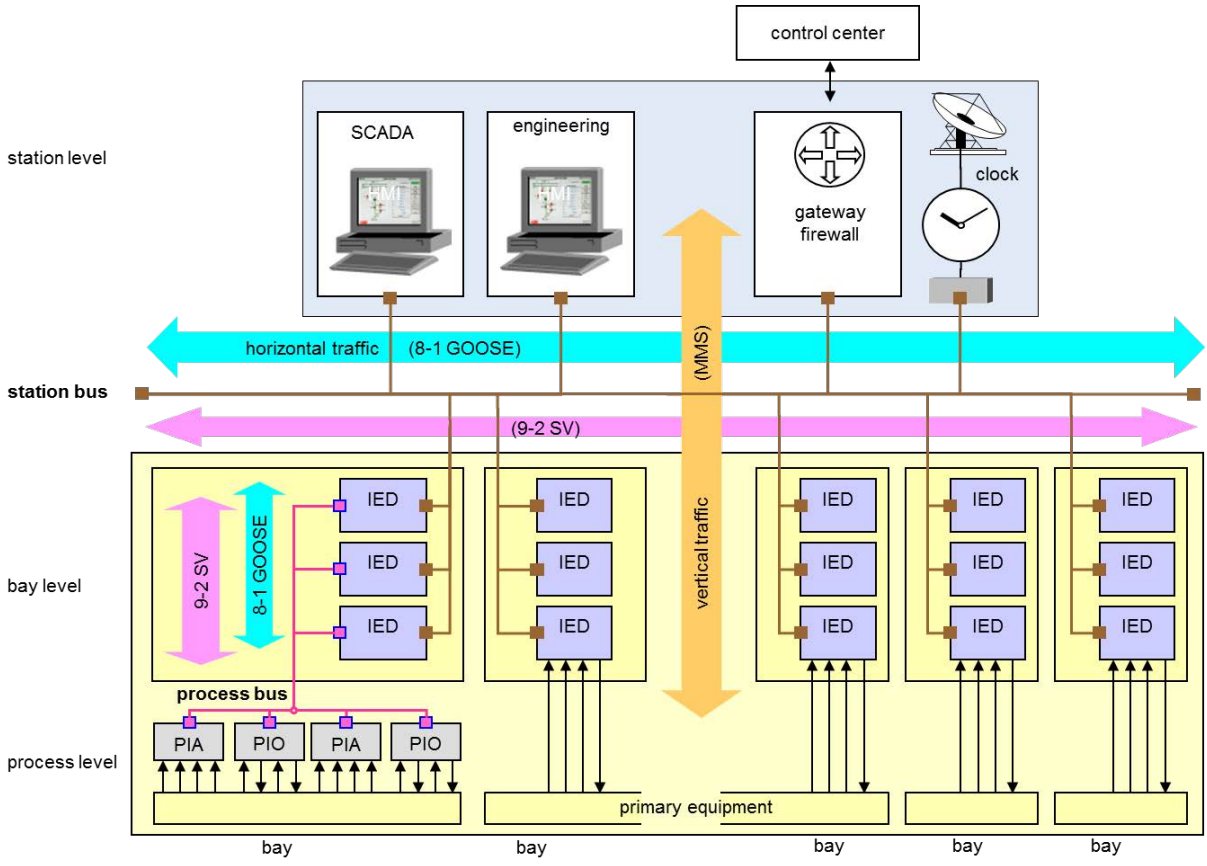


Figure 11 – Station bus, process bus and traffic example

While it is possible to fit station bus and process bus into one network structure if sufficient bandwidth is available (e.g. 1 Gbit/s), it is prudent to separate them for various reasons, e.g.

to reduce the station bus load due to SV traffic or to avoid single points of failure when coupling tightly process bus and station bus.

5 Network design checklist

5.1 Design principles

The network design has to satisfy the high-level system requirements and the detailed design requirements. A suitable network design requires understanding all the functional and non-functional requirements of the system. The network design could be dictated by application requirements such as the mandatory use of GOOSE for the exchange of trip signals between IEDs. The interfacing capability of the IEDs constrains the design. Establishing design principles assists in resolving conflicting requirements (e.g. safety could be rated higher than cost).

5.2 Engineering flow

The engineering process of a substation communication is a balance between the aspects of:

- application requirements;
- topology and design constraints;
- available products;
- costs.

There exist several engineering flows; one example is described in Figure 12. The highlighted parts concern directly the network components.

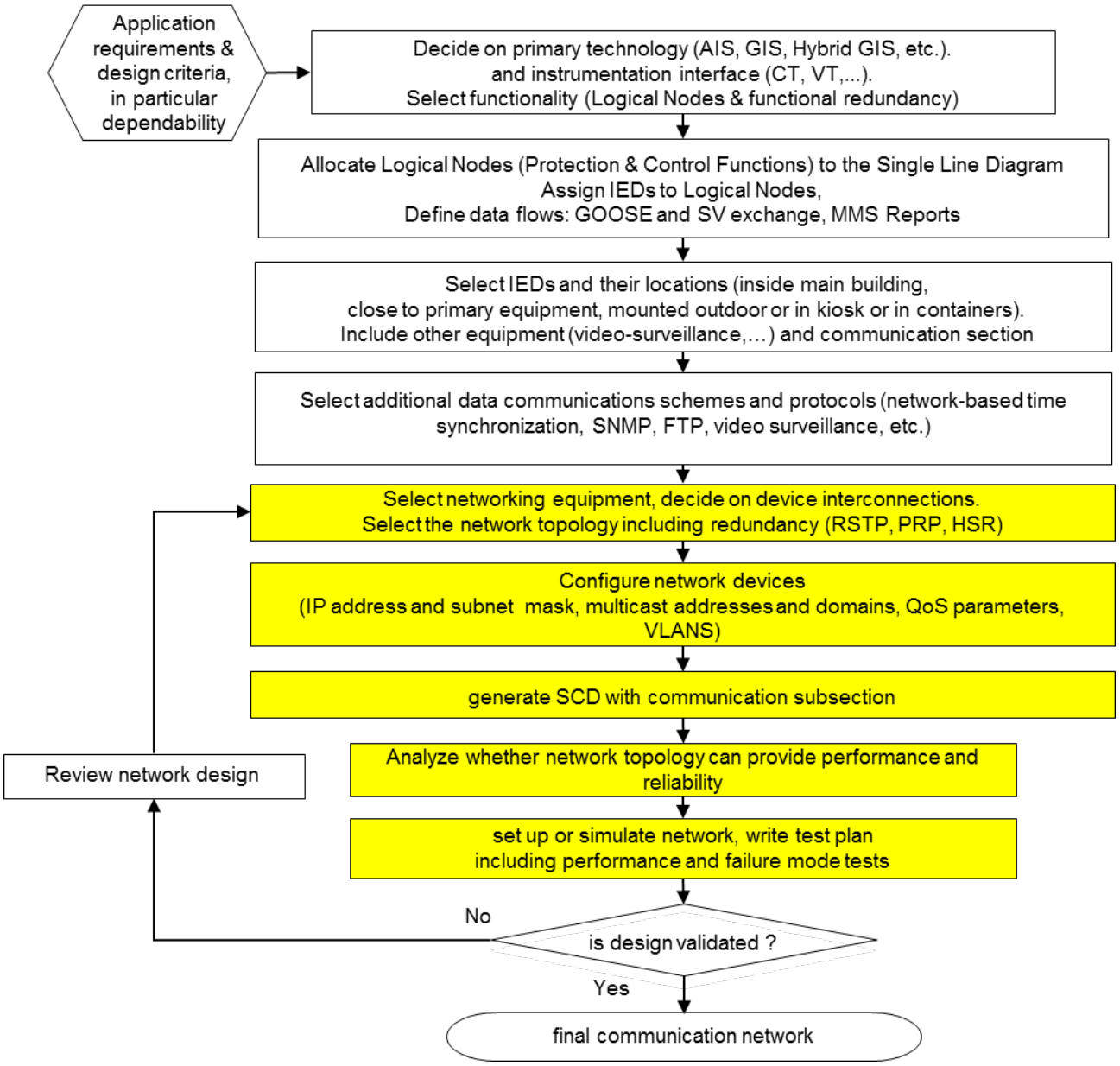


Figure 12 – Example of engineering flow

5.3 Checklist to be observed

5.3.1 Summary

A network for IEC 61850 based substations is designed taking into account several criteria, of which the most important are listed here and detailed in 5.3.2 to 5.3.19:

- environmental issues;
- EMI immunity;
- form factor;
- physical media;
- substation application and network topology;
- redundancy;
- reliability, availability, maintainability;
- logical data flows and traffic patterns;

- latency requirements for different types of traffic;
- performance;
- network management;
- network supervision;
- time synchronization and accuracy;
- remote connectivity;
- cyber security;
- scalability, upgradeability and future-proof;
- testing;
- cost.

These points are developed after the definition of the basic network architectures.

5.3.2 Environmental issues

High levels of pollution, salt, humidity, abrupt temperature changes, etc. impose using hardened networking equipment or adequate protection in cabinets and sheltered locations.

Outdoor devices such as process bus interfaces close to primary equipment require special enclosures or high grade of protection and adequate connectors. This limits the available device choice or imposes relocation. The requirements apply to all involved components, not only network devices.

The environmental conditions valid for substation equipment are defined in IEC 61850-3. This aspect is not further developed.

5.3.3 EMI immunity

Network devices operate under EMI, caused e.g. by inductive load connection, lightning strikes, electrostatic discharges from human contact, radio frequency interference due to personnel using portable telephones, ground potential rise resulting from high current fault conditions, etc. IEC 61850-3 specifies the immunity requirements. This aspect is not further developed.

5.3.4 Form factor

The limitation of the room available for installations of networking equipment asks for devices with small form factor or specific mounting options (DIN rail, etc.), thus limiting the equipment choice. When using 19” rack mounted equipment, enough room needs to be left at the rear of rack mounted equipment to ensure adequate air flow. This aspect is not further developed.

5.3.5 Physical media

The physical medium is chosen based on the EMI conditions, expected traffic, distances to travel and cost. The medium is either copper wiring or optical fibre, while the data rate is either 100 Mbit/s or 1 Gbit/s. Guidance is given in 6.3.

5.3.6 Substation application and network topology

The substation application, in particular the busbar protection, interlocking and inter-tripping, the presence of a local or of a remote substation control system, the attachment method of primary equipment, etc. determine the data flows. The application therefore influences the network choice and topology.

The topology of the substation, number of voltage levels, attachment method of the primary equipment (conventional, merging unit or process interface), the electrical equipment technology (AIS, GIS), the location of the cabinets and control system define the physical topology of the network. Guidance is given in Clause 7 and in the case studies of Annex A, Annex B, Annex C and Annex D.

5.3.7 Redundancy

The value of the protected equipment for the operation dictates the level of redundancy to be observed. A usual requirement is the avoidance of any single point of failure, which implies the introduction of redundancy.

Guidance is given in 7.2 and 13.1.

5.3.8 Reliability, availability, maintainability

Redundancy by itself does not ensure a high availability. Operation can be impaired by long recovery times and lack of maintenance. Equipment must be installed so as to simplify maintenance and reduce the MTTR (Mean Time To Repair).

Utilities want to estimate how often a substation or a bay shuts down due to a failure of the IEDs and how often an electrical element is unable to operate when requested (PFD = Probability to Fail on Demand, see IEC 61508-4).

Utilities want to estimate how often any component of the automation system fails (MTTF = Mean Time To Fail) and how often a repair team must be sent to replace failed parts (MTBR = Mean Time Between Repairs). The MTBR can exceed the MTTF when redundancy is available.

The contribution of the network unavailability to the substation dependability must be evaluated on a function-by-function basis.

Requirements apply to whole or parts of the network are defined as the desired MTTF, MTBR and MTTR.

Methods such as FMEA allow the detection of weak points.

Guidance is given in 13.2.

5.3.9 Logical data flows and traffic patterns

The logical data flows depend on the application, and are defined by the SCD file, which allows defining the steady-state traffic, while typical operations such as busbar transfer define the burst traffic patterns. Guidance is given in 10.1.1.

5.3.10 Latency for different types of traffic

The protection and control application defines the latency requirements. This influences the segmentation of the network and the allowed number of cascaded devices. This is detailed in Clause 11.

5.3.11 Performance

To prevent or minimize overloads, the devices and network elements must handle the foreseen traffic. This influences the choice of elements. Unnecessary traffic can be limited by defining multicast domains or VLANs. Guidance is given in Clause 8.

5.3.12 Network management

Network management concerns the configuration of the network and allocation of addresses, while at the same time limiting the traffic through multicast or VLAN domains.

Network management tools set the bridge parameters, in particular multicast and VLAN filters.

5.3.13 Network supervision

Network supervision tools monitor the network to detect the presence or absence of devices, link failures or degradation of performance. It allows creating network maps and monitoring the status of the devices. Guidance is found in Clause 16.

5.3.14 Time synchronization and accuracy

The method of clock synchronization depends on the accuracy that a given application requires. Timing accuracy for sampled measurement values is much higher than for simple time-stamped events. Further details are found in Clause 14.

5.3.15 Remote connectivity

The substation state and events are communicated to external entities such as the control centre, for instance over dedicated lines or through a public or private data network (out of scope). A gateway maintains an image of the substation, so direct access to the IEDs is not needed.

Some operators require that the IEDs be accessible from outside of the substation for maintenance or upgrade. To this purpose, the IEDs have an external (public) IP address that must be mapped to the internal (private) IP address within the substation. This mapping is preferably performed by a dedicated gateway or router with firewall functionality. Remote connectivity is not further considered in this document.

5.3.16 Cyber security

When the substation network is connected to the corporate WAN or remotely accessed, cyber security must be ensured. The best way is not to allow external access except through controlled gateways where this is needed. Even where the network is completely isolated and no remote equipment is connected, security mechanisms in the networking equipment are recommended, for instance syslogs, security audit trails, passwords, access control, port security, and encryption since they also increase resiliency against configuration and installation errors.

While encryption of messages may be requested outside of the substation, within the relatively well-sheltered environment of a substation, security through authentication is deemed sufficient. An extensive threat assessment is recommended before deploying security measures, given the added complexity in implementation and management that it costs.

Provisions for security exist in IEC 61850-8-1, IEC 61850-9-2, IEC/TR 61850-90-5 and Annex K of IEC 61588:2009, but most work is at the experimental level. A particular problem is to conciliate the overhead due to security with the high communication and short delays required for real-time communication.

Details can be found in IEC/TS 62351-6, cyber-security is not further considered in this document.

5.3.17 Scalability, upgradeability and future-proof

To upgrade firmware or hardware, add new applications or new bays without significant modifications of the core infrastructure, the network must provide reserve capacity (e.g. using 1 Gigabit Ethernet links between bridges where 100 Mbit/s would be sufficient) and must be properly segmented. Selecting equipment with built-in support for upgrades supports future extensions. This aspect is considered in the topologies of Clause 7.

5.3.18 Testing

Once the network has been designed, its compliance to the requirements needs to be tested, first as a design verification, then during factory acceptance tests and finally at site acceptance. Guidance is given in Clause 18.

NOTE Conformance testing is out-of-scope and specified in IEC 61850-10.

5.3.19 Cost

The network cost is conditioned by the available budget. Cost is usually divided into an investment cost and a maintenance cost. The economic calculations need to consider the materials and engineering costs derived from the complexity of the network design and configuration, as well as the maintenance and replacement costs. For instance, saving through cheaper copper cabling can be more than offset by costs of the time spent in fault seeking. This aspect is not further developed.

6 Ethernet technology for substations

6.1 Ethernet subset for substation automation

There exist a large number of tutorials on Ethernet technology and Clause 6 is no replacement for them. Substation automation however contemplates only a subset of the Ethernet and Internet protocols and ignores legacy restrictions.

Therefore, engineers need to be aware only of a few options, which are summarized in Clause 6.

Since most of Clause 6 can be applied to any industrial automation network, the application to IEC 61850 or substations is contained in notes, which point to the corresponding detailed application-specific explanations.

6.2 Topology

Ethernet is a “switched network”, consisting of “nodes” and “switches” connected by point-to-point links, as shown in Figure 13.

Switches operating at layer 2 (only with MAC addresses) are named “bridges”, so “bridge” is used whenever the layer-2 functionality of a switch is meant.

NOTE Hubs are signal repeaters and even simpler than unmanaged bridges, but they are not in use any more since, unlike bridges, they cannot prevent collisions.

In Figure 13, the yellow “LAN” cloud considers the part of the network that is not a node, but includes the bridges. Nodes are attached by edge links, while bridges are connected among themselves with trunk links that carry a higher traffic than edge links and therefore require more bandwidth. Meshing introduces redundant trunk links (as any of the trunk links in Figure 13) and means such as RSTP exist to prevent “loops”, i.e. frames that circulate indefinitely.

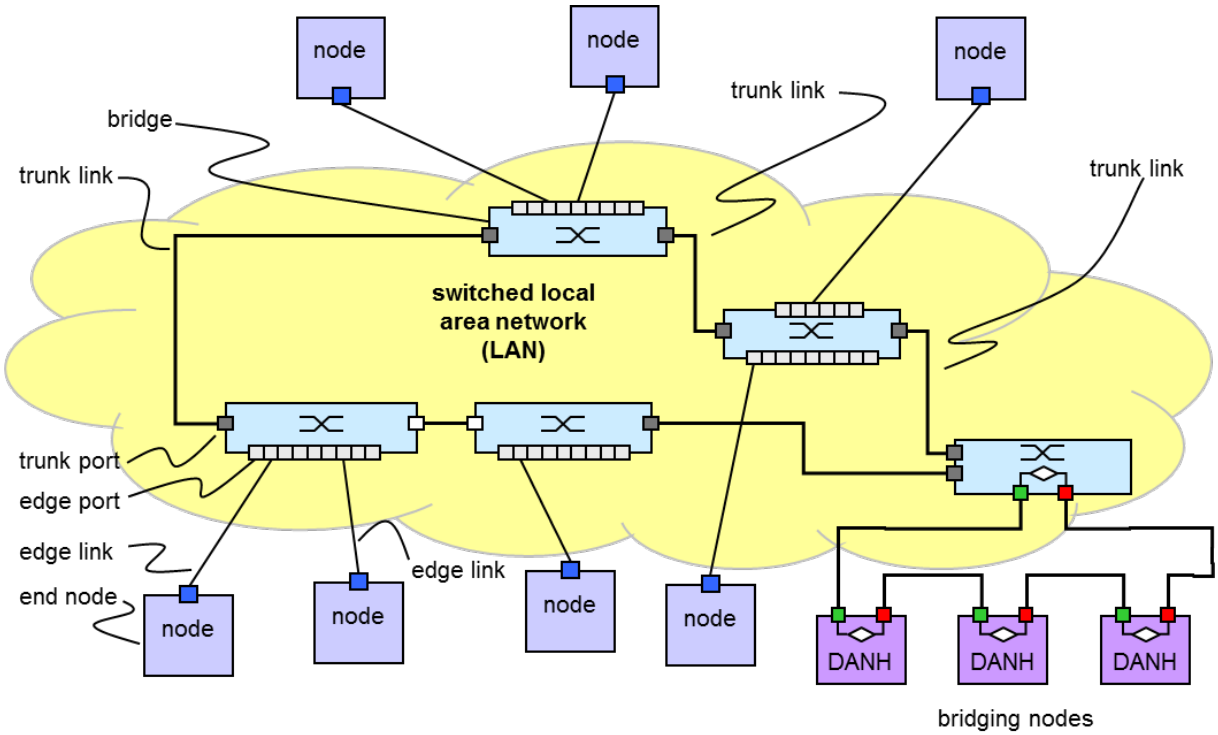


Figure 13 – Ethernet local area network (with redundant links)

Nodes called “bridging nodes” incorporate bridge functionality for a limited number of ports (normally two). These devices, in particular Doubly Attached Nodes in HSR (DANHs), combine the properties of nodes and bridges and allow to daisy-chain the devices, as shown in Figure 13 (right side).

Switches are bridging nodes that have multiple ports and replicate the traffic received from one port to one or more other ports if no filtering applies. They can have additional functionalities, such as SNMP and clock synchronization.

Latency increases with the number of bridges in series multiplied by their forwarding delay, so the number of hops is limited in any network. Some protocols such as RSTP limit the number of bridges to about 40.

Figure 14 shows a bridge with connected links.

Figure 14 – Switch with copper (RJ45) ports)

NOTE IEC 61850 does not precisely define the Ethernet technology in order to account for technical progress, but switched Ethernet is implicit.

6.3 Physical layer

6.3.1 Data rate and medium

A network usually includes links with different speeds. For instance, it makes sense to connect end nodes to bridges with cheaper 100 Mbit/s links and bridges-to-bridge (trunk links) with 1 Gbit/s links. The distance that can be covered decreases with increasing data rate since the product bandwidth × distance is a fundamental limit of each medium (optical fibre or copper).

NOTE IEC 61850 considers two physical layers (copper and fibre) and two bit rates (100 Mbit/s and 1 Gbit/s). Future extensions are possible. Special cases such as substation-to-substation communication require different speeds or even LAN protocols. While copper can be used within cabinets, multimode optical fibres are the choice where galvanic separation is needed. Specific applications characterized by large distances between IEDs, such as substation-to-substation differential protection or wind towers separated by several kilometres require special modems, radio connections or single mode fibre.

6.3.2 Full-duplex communication and auto-negotiation

Ethernet controllers operate in full-duplex mode, meaning that they can simultaneously send and receive over the same link. Some older Ethernet controllers start by default in half-duplex mode, a source of configuration error to be checked.

In full-duplex, the limitation to 100 m in IEEE 802.3 imposed by the signal propagation delays of half-duplex does not apply any more, since no collisions are expected.

Ethernet controllers can detect the bit rate and duplex setting of the other party on a link through auto-negotiation. This functionality is generally bound with the ability to detect correct polarity of the cables, i.e. avoid using crossed cables. Caution is needed, since incorrect settings cause duplex mismatch that leads to frame losses.

NOTE 1 Carrier extension to extend slot size to 512 bytes is only required in 1000BASE-X half duplex and does not apply here.

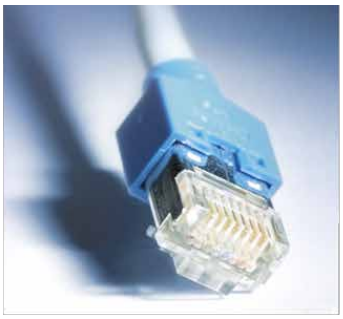
NOTE 2 IEC 61850 assumes that communication is full-duplex and auto-negotiated, i.e. the peer ports are configured to recognize automatically the polarity, the duplex setting and highest common speed.

6.3.3 Copper cabling at 100 Mbit/s

Copper cabling is a cost-effective medium, supported by most PCs, but it can only be used when galvanic separation is not needed. Indeed, the transformer-coupling offers only a limited voltage separation.

The recommended link cable is Cat5e, which contains two twisted pairs and allows spanning about 100 m.

The preferred connector is RJ45 (of which only 4 pins are used) as shown in Figure 15.



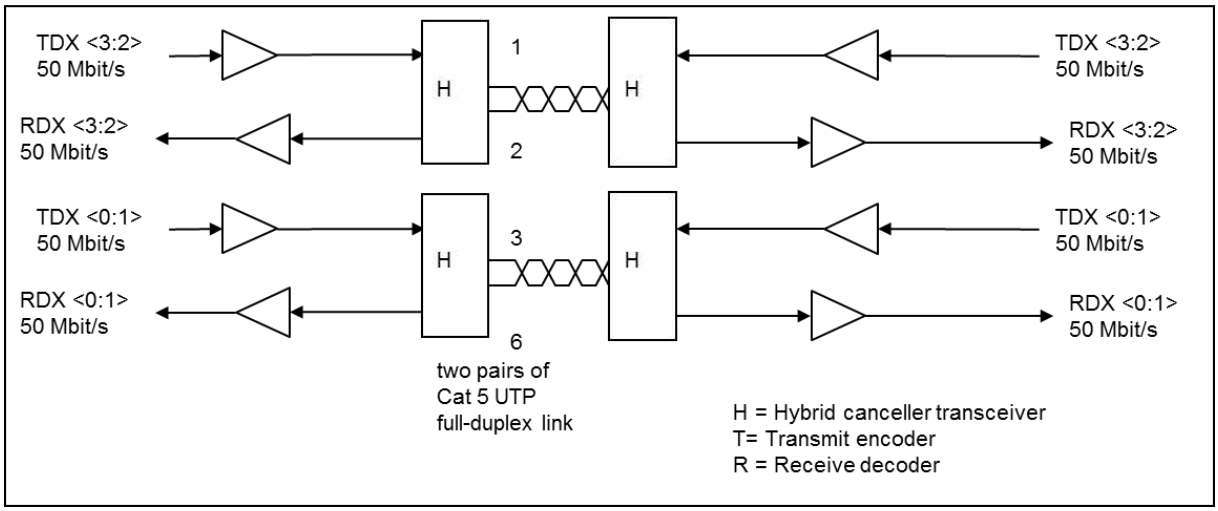


Figure 15 – RJ45 connector

NOTE 1 The RJ45 connector is popular, but not particularly robust, can fall out of the receptacle under vibrations and does not withstand a shoe stepping on it. More robust connectors such as M12 are foreseen for outdoor applications, but could not impose themselves in substations. The practical solution is to fasten the cables by routing them through trays rather than using binders.

Only direct cables should be used (no crossover cables) since most bridges are capable of recognizing the transmitter and receiver pair in the cable, a capability known as Auto-MDI(X).

Over distance less than 100 m, copper cables are more limited by EMC factors than by the cable attenuation. This kind of cabling should only be used between devices that are galvanically connected and where the EM disturbances are low.

There exist two kinds of cables: wires (single wire) for fixed installation on the wall side of the sockets and cables (multi-wire, stranded wire or litz wire) between sockets and moving equipment such as PCs. Wire is cheaper than litz for building installations, but its use is not recommended since it is not vibration-proof and it cannot be inserted into an RJ45 plug.

NOTE 2 In IEC 61850, copper cabling is recommended within cabinets, e.g. to connect bridges directly with IEDs, where disturbances are small and galvanical separation is uncritical.

6.3.4 Optical cabling at 100 Mbit/s (100BASE-FX)

6.3.4.1 Fibre

The 100BASE-FX technology uses a pair of fibres, allowing bridging 2 000 m for multimode fibres and of 10 000 m for single mode fibres.

The recommended optical cable is a paired multimode 50 μm (50/125) fibres.

The colour of the cables is not prescribed. In redundant installations, it is recommended to use cables of different colours and darkness for each LAN, for instance orange and light blue cables. HSR rings have been using yellow cables.

NOTE 1 Individual optical cables using ST connectors are still widely in use, which calls for labelling individually the fibres. The move to paired cables and LC connectors relieves from identifying correctly the fibres.

NOTE 2 62,5 μm (62,5/125) fibres provide a somehow lower bandwidth × distance performance than 50 μm fibres, so they are interchangeable with 50 μm fibres in many, but not all applications. Keeping a homogeneous 50 μm fibre repair stock ensures appropriate fibre replacement.

NOTE 3 Single-mode fibres span 10 km or more, but require that the fibre, sender and receiver be matched. They are typically used for trunk links between remote areas, when conditions dictate it since they are more costly, less reliable and transmitter/receiver are special.

Multiple core fibre optic cables can be advantageous for star topologies and for reserving spares.

6.3.4.2 Connector

The recommended connector type is LC (IEC 61754-20), as shown in Figure 16.

Figure 16 – LC connector

NOTE 1 ST-bayonet (IEC 61754-2) were the preferred connectors of IEEE 802.3 and are still widely used, but LC connectors have a smaller form factor and avoid fibre inversion. Patch fibres with ST connector at one end and LC at the other allow connecting bridges and nodes of different type.

NOTE 2 Apart from ST and LC connector there are also SC and MTRJ connectors which are not recommended. SC has the same issue with identifying fibres as ST. MTRJ connector has more complex mechanical design than LC and therefore is more susceptible to losses and poor performance, especially at higher bit rates such as 1 Gbit/s.

Figure 17 shows an example of a bridge with three ports connected by LC connectors.

Figure 17 – Switch with optical fibres (LC connectors)

NOTE In IEC 61850, optical cables are used whenever galvanic separation is needed, for instance between remote cabinets or between buildings.

6.3.5 Optical cabling at 1 Gbit/s (1000BASE-LX)

1000BASE-LX is the recommended medium for the trunk links.

The 1 000 BASE-LX10 can use the same fibres as 100BASE-FX.

The recommended fibre type is 50 μm (50/125) multimode (up to 550 m) or mono-mode (up to 10 000 m). The two kinds of fibre have different symbols.

6.3.6 Copper cabling at 1 Gbit/s

This cabling is not foreseen in IEC 61850-8-1 or in IEC 61850-9-2.

NOTE Copper wiring for 1 Gbit/s is possible with high-quality cables, but is not encouraged due to practical problems, such as EMC and a link recovery time in the order of 500 ms after a disruption. Also, keeping two cable types on stock which look similar can cause confusion. Use of optical links is encouraged instead.

6.4 Link layer

6.4.1 Unicast and multicast MAC addresses

Each frame carries a 48-bit source and destination address, the latter either unicast (single destination), multicast (group of destinations) or broadcast (sent to all nodes on the local area network). The IEEE allocates the source addresses to the manufacturers and the multicast addresses bands to the standardization bodies.

Multicast addresses are recognized because the least significant bit of the first octet is set, e.g. 01-1B-19-00-00-00 for PTP.

Some multicast addresses are reserved and may not be forwarded by bridges. These addresses are listed in IEEE 802.1Q-2011 Table 8-1, these addresses are mainly reserved for peer-to-peer traffic such as RSTP, LLDP or PTP.

A multicast domain is the set of all devices that receive a certain multicast address.

An Ethernet controller decodes the destination address of a received frame and only passes the frame to its application if the destination address matches its own or if the multicast address belongs to its table of subscribed addresses. However, not all Ethernet controllers implement multicast filtering.

Setting the controller in promiscuous mode (e.g. for traffic monitoring) causes it to receive all traffic, but burdens correspondingly the processor.

NOTE In IEC 61850, as Table 38 shows, the MMS and FTP traffic use unicast addresses; the GOOSE, the SV and the PTP traffic use multicast addresses; few protocols such as ARP use broadcast addresses.

6.4.2 Link layer and bridges

All ports of the bridges are assumed to operate in full-duplex mode.

The bridges operate on the basis of the MAC addresses and partially on the Ethertype.

In principle, a bridge repeats a frame received on one port to all its other ports. This is however restricted by several mechanisms:

- loop prevention (e.g. by executing RSTP);
- MAC address filtering, in which a bridge learns the MAC address of the devices attached to a port and only replicates a unicast frame to that port – this mechanism cannot be disabled;
- multicast or VLAN traffic filtering;
- redundancy control (e.g. HSR or PRP).

6.4.3 Bridging nodes

Bridging nodes implement a subset of the bridges functionality; they at least allow forwarding of the traffic and can sometimes prevent loops.

NOTE In IEC 61850, the bridging nodes protocols considered are RSTP and HSR. PRP is not a bridging protocol.

6.4.4 Loop prevention and RSTP

Switched Ethernet allows more than one path from one source to a destination, creating redundant paths, intentionally or not. This creates physical loops in the network. Such loops would cause a ‘broadcast storm’ where broadcast or multicast frames would circulate endlessly and create copies, consuming all available bandwidth and flooding the network. This would also apply to unicast frames at initialization time. To prevent this, a protocol executed by the bridges maintains a logical tree structure (without loops) and ensures that the best path is used. This protocol also ensures recovery from the failure of a bridge or a link.

RSTP is the most widely used loop breaking protocol.

RSTP is executed by the bridges of the network and not by the end devices.

RSTP converts an arbitrarily meshed network to a logical tree, by blocking ports that would introduce loops on the physical level (see Figure 18).

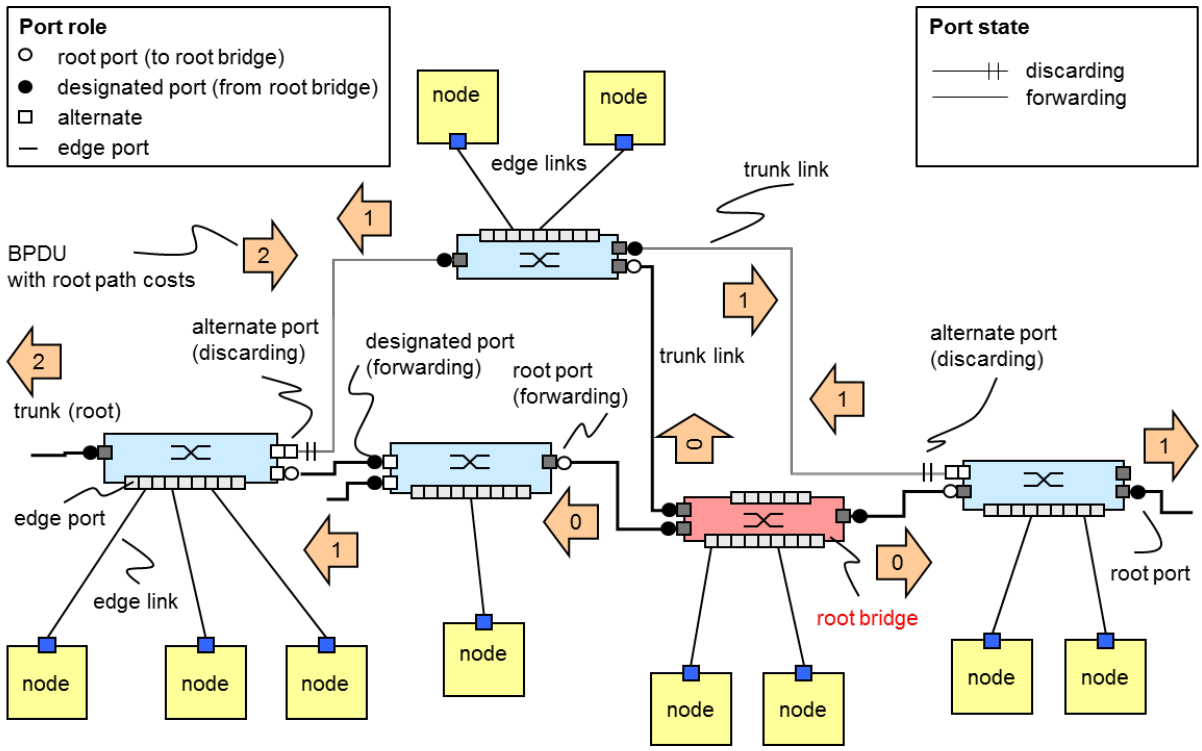


Figure 18 – RSTP principle

To this effect, bridges are assigned priorities and links are assigned costs depending on their speed. Each bridge also has a unique MAC address. Each bridge sends peer-to-peer messages to its neighbours, called BPDUs (Bridge Protocol Data Units) that indicate to its neighbours its priority and the costs to reach the root bridge. BPDUs are periodically exchanged between bridges to detect and correct network topology changes.

Initially, the bridges decide among themselves which bridge plays the role of root. The bridge with the lowest bridge priority will be elected as root. In case two or more bridges have the same priority, the bridge with the lowest MAC address is elected as the root bridge.

The Root Bridge sits at the top of the hierarchy (independently of its physical location).

The path costs consider the number of intermediate bridges to the root, the communication speed of the link between the bridges.

When a bridge can reach the root through several of its ports, it chooses the port with the cheapest costs as root port and blocks the other ports, which become “alternate ports”. The port on the other side of the root port becomes the “designated port”. If path costs are equal, the port number is used to break the tie.

In case a bridge detects that a link to its designated port becomes inactive (no more BPDUs or physical link failure), the bridge unblocks the alternate port with the lowest costs to the root and routes the traffic through this one. However, if the root node fails, a bridge without connection to the root assumes that it is itself the new root and sends BPDUs announcing zero costs to the root (itself). Since several nodes could react the same way at the same time, when two nodes pretend to be root, the one with the lower priority and bridge MAC address demotes the other.

RSTP assumes that the bridges are configurable. Assignment of the root bridge improves performance and lowers the reconfiguration time in case of failure of a link or switch.

The use of RSTP as a redundancy protocol is detailed in 6.4.10.2.

NOTE IEC 61850 considers as loop breaking protocols RSTP and HSR (see 6.4.10.4) which is based on a different principle.

6.4.5 Traffic control in the bridges

Traffic control serves different purposes:

- reducing the traffic that an end device handles, by letting the bridge send only the relevant part of the traffic to the end device. End devices normally do not filter traffic except if their hardware or controller is able to decode the MAC addresses;
- reducing traffic on shared (trunk) links and portions of the network;
- assigning priority to a class of traffic.

6.4.6 Unicast MAC address filtering

To reduce traffic, all bridges filter the unicast traffic towards the egress ports. To this effect, a bridge learns the MAC address of the devices accessible over each port.

When the bridge receives a frame over an ingress port, it registers its MAC address into its “filtering database”. It then searches its filtering database to find out if the MAC destination address of the received frame has been registered and for which port. If it is registered, it directs this unicast frame to that port only; otherwise it sends it to all ports.

Nodes on the other ports are therefore not disturbed by traffic not addressed to them after the first frame exchange. The MAC address filtering is done automatically by the bridges and cannot normally be disabled.

A bridge does not apply MAC address filtering to multicast traffic, since all nodes are the destination.

Address filtering prevents a monitoring device connected to one port to gain access to the whole traffic. For maintenance purpose, port mirroring is used.

NOTE 1 In IEC 61850, the MAC address filtering only reduces the MMS or other IP traffic, since the GOOSE and SV traffic is multicast.

NOTE 2 The performance of MAC address filtering depends on the technology used by the bridge to learn the MAC address of ingressing frames. Bridges that “hash” the 48-bit MAC addresses down to a lower number of bits suffer from occasional hash collisions, causing some frames to be broadcast rather than unicast. Bridges using CAMs (Content Addressable RAMs) or sorted-lists do not have this problem.

6.4.7 Multicast MAC address filtering

6.4.7.1 Principles of multicast filtering

By default, a bridge port forwards all multicast frames.

When multicast traffic is significant, multicast filtering can reduce the processor load of the end devices by letting through only those multicast addresses the end device is interested in. End devices normally have no multicast filtering ability, so the edge port on the bridge does the filtering on their behalf.

To reduce multicast traffic, a port of a managed bridge has a configurable multicast filtering table, which indicates which multicast addresses may egress from that port.

A multicast filter on a port is always associated with a VLAN, since the same multicast address could appear on different VLANs, see 6.4.8. This reminds that a multicast domain is a subset of a VLAN. Multicast filtering however does not require the use of VLANs in the network, and can operate with the default VID =1 (management VLAN) throughout the LAN.

Multicast filtering can also be applied to trunk ports, to limit the traffic to multicast domains.

Therefore, it is important to assign correctly the multicast addresses at the engineering stage.

NOTE The assignment of multicast domains to substation automation regions is described in 12.3. In IEC 61850-6, the multicast addresses an IED is subscribed to can be deduced from the SCD file and from the CID.

6.4.7.2 Static multicast management

In static multicast management, the multicast filters of the ports of the bridges are set explicitly at engineering time.

The bridges are configured using the manufacturer's tools (until generic configuration tools emerge). Configuration loading takes place e.g. via a serial line to the bridge, through a web interface or through the SNMP protocol.

NOTE Clause 19 models bridges as IEC 61850 objects and provides means for a generic bridge configuration. This allows to configure the bridges over MMS. For IEDs that support multicast filtering, the configuration can be loaded through the CID file.

6.4.7.3 Dynamic multicast management

If the end devices are configured with the multicast addresses they are subscribed to, they can claim filtering from the port of the bridge they are attached to using management protocols via GMRP or MMRP, that build a multicast tree.

To this effect, all end devices need to implement at least a "simple applicant" functionality.

While this method allows a certain "plug-and-play", the resulting network traffic can hardly be predicted.

The use of dynamic multicast control protocols is not recommended for inexperienced staff. Indeed, to ensure predictable operation, the whole traffic must be calculated before the plant is ever put into operation. The introduction of dynamic multicast domains could overload the network, especially when the network is being reconfigured after a failure or after reboot. Indeed, such protocols initially operate with all multicast filters removed and establish the traffic limitations as nodes announce their transmission needs.

NOTE Dynamic multicast management offers some benefits for a fast replacement of IEDs or bridges, but is more complex to engineer, less predictive and more difficult to troubleshoot.

6.4.8 Virtual LANs (VLANS) traffic control

VLANs is a method to separate types of traffic that share the medium, for instance:

- Management traffic;
- Substation automation traffic;
- Surveillance camera video traffic;
- Industrial automation traffic in mixed plants.

VLANs just separate traffics, there are not intended to reduce trunk traffic. Usually, trunk links have a higher bandwidth than edge links, so it is not necessary to segment them.

In principle, a device on VLAN 1 cannot even see that a device on VLAN 2 exists. Devices on different VLANs influence each other only by the bandwidth they consume because they nevertheless share the same physical medium. If necessary, communication between VLANs takes place over a layer 3 router.

VLANs divide layer-2 broadcast domains (which define how far broadcast, multicast and unicast traffic travels) and serve as a first security barrier, since the access to the VLAN is entirely governed by the bridges. A device connected inadvertently to the wrong port will not be able to communicate. However, VLANs provide only a weak data security, since any misconfiguration in the network is a potential loophole and configuration is not supervised.

The end devices connected to the edge ports are normally VLAN-unaware.

To support VLANs, the IEEE 802.3 frames carry a header, called the VLAN tag according to IEEE 802.1Q, which has two functions:

- prioritization of traffic;
- logical segregation of traffic.

The VLAN tag is announced by a specific Ethertype (0×8100), followed by a 3 bit priority field called Priority Code Point (PCP), a one-bit canonical format indicator that can be neglected here and a 12-bit field containing the VLAN identifier, or VID (see Figure 19).

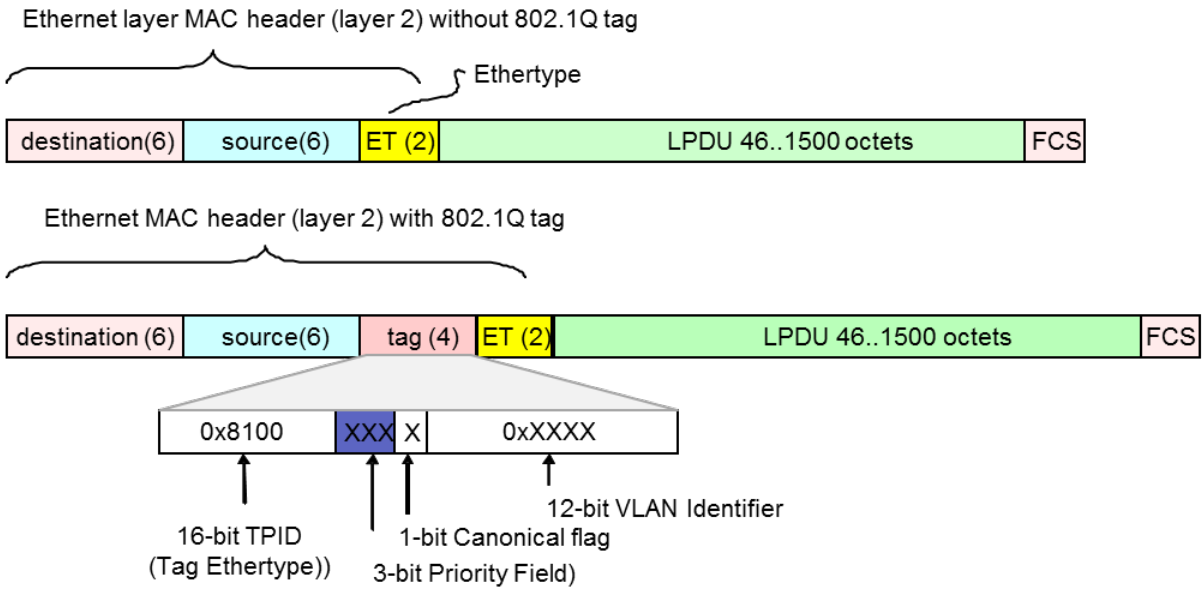


Figure 19 – IEEE 802.3 frame format without and with VLAN tagging

Bridges typically support 64 VLANs, some up to 255 VLANs simultaneously. Several values are reserved:

- VID = 1 is the default management VLAN for VLAN aware bridges. By default, all bridge ports are members in VLAN 1 and are configured to send untagged frames. This enables VLAN aware bridges to work “out of the box” without further configuration. Using VID=1 throughout the LAN yields the same behaviour as if there were no VLANs, except that the bridges supports priority;

- VID = 0 is a particular case, since it means that the frame does not belong to any VLAN, but nevertheless carries a priority. Such frames are called “priority-tagged”;

- VID = 4095 is a reserved VLAN, not to be used.

NOTE 1 In IEC 61850, GOOSE and SV frames are priority-tagged (see 6.4.8.1 and 6.4.8.2).

NOTE 2 The application of these concepts to substation network configuration is described in 12.2.1.

NOTE 3 Double tagging (QinQ) is a special case, in which frames carry two tags, not detailed here, but mentioned in IEC/TR 61850-90-1.

6.4.8.1 Priority and quality of service (QoS)

Giving frames a high priority privileges a certain class of traffic. However, priority alone cannot ensure end-to-end timely delivery, it can only reduce the average delay that a certain traffic suffers. It is a necessary, but not sufficient contribution to the Quality of Service.

Priority means that a bridge that receives several frames simultaneously will forward one frame preferentially, while the others remain queued. To this purpose, bridges use one sending queue per priority per port. Some bridges have one distinct queue per priority. Supporting a large number of queues (8 priorities are allowed by IEEE 802.1Q) imposes a burden on the bridges, so most bridges support only four queues to which the priorities are mapped.

Priority tagging and VLANs are specified in the same standard IEEE 802.1Q, but they are separate concepts that share the same tag. Priority alone is often referred to as IEEE 802.1p (prioritization), an obsolete publication now part of the IEEE 802.1Q-2011 standard.

If the frame carries no IEEE 802.1Q tag, a bridge port assigns it its default priority, the PPCP and its default VLAN PVID.

To give some frames a high-priority without associating them with a VLAN different from the port's default, the source sends them as "priority-tagged", with a PCP value >0 and VID = 0 (see 6.4.8.1 and 6.4.8.2).

NOTE IEC 61850 prescribes that GOOSE and SV frames are priority-tagged, so the bridges treat them preferentially, but it does not prescribe VLANs. The default for GOOSE and SV is therefore VID = 0 (no VLAN). The priorities are assigned at engineering stage and recorded in the SCD file.

6.4.8.2 VLAN bridge behaviour

6.4.8.2.1 Ingress to a bridge

From which VLAN a bridge accepts frames on its ingress ports depends on the port settings. According to IEEE 802.1Q-2011, chapter 6.9, a bridge port implements one of the following modes:

- Admit only VLAN-tagged frames;
- Admit only untagged and priority-tagged frames;
- Admit all frames (not VLAN-aware).

To support IEDs that send a mixed tagged (GOOSE, SV) and untagged (MMS, other) traffic, the default option is "Admit all frames".

The tagging of untagged and priority tagged frames is based on the Port VLAN ID, called the PVID and its default priority PPCP.

NOTE 1 Even if the priority configured at a specific bridge port is 'better' than the PCP received in a frame, the bridge still uses the PCP received in the frame and not the port priority PPCP for VLAN encapsulation.

NOTE 2 An ingress port of a VLAN-aware bridge always tags the internal bridge traffic.

NOTE 3 The IEEE 802.1Q method called "Ingress filtering" allows bridge ports with enabled ingress filtering to discard all frames upon ingress which do not have a VLAN ID that is a member in the PVMS of that port. This feature is used to offload bridges, e.g. prevent VLAN tagged traffic from being introduced into the bridge when the bridge has no member port configured for that particular VLAN, as the introduced traffic would be discarded inside the bridge anyway. This feature has been ignored since most traffic is unacknowledged.

When a VLAN-aware port receives a frame, it considers three cases:

a) The frame is VLAN-tagged with VID ≠ 0. In this case, the port accepts the frame (except if it implements ingress filtering, which is ignored here, see Note 3). This is the normal situation on the trunk ports;

b) The frame is priority tagged only (with VID = 0). The port ignores its own PPCP and inherits the frame's priority and inserts its PVID to form the VLAN tag. This is shown in Figure 57, where both GOOSE and MMS from SAN A are encapsulated into VLAN 3.

c) The frame is untagged. The port prefixes the frame by a VLAN tag with its own PVID and priority PPCP; the frame will now transit with a VLAN tag.

The tagging of untagged and priority tagged frames is based on the Port VLAN ID, called the PVID and its default priority PPCP.

Table 2 shows an example of a bridge ingress table showing the modes and port properties.

Table 2 – Example of port ingress setting table

VID	Ingress	PVID	PPCP
Port 1	Admit all	1	4
Port 2	Admit only tagged	3	6
Port 3	Admit only tagged	3	6
Port 4	Admit only tagged	3	4
Port 5	Admit only tagged	3	5
Port 6	Admit only untagged	2	5
Port 7	Admit all	1	4
Port 8	Admit all	1	4

6.4.8.2.2 Egress from a bridge

Once the frame has entered the bridge, it is forwarded to all other ports of the bridge if the frame has a broadcast or multicast destination address or to one specific port if the frame has a unicast MAC address that the bridge already registered, as explained in 6.4.5.

The egress from a port of a bridge is controlled by the port VLAN member set (PVMS), which defines from which VLANs this port will forward the frames, and if it sends them tagged or untagged.

– An egress port sends the frame only if the VID belongs to the port membership set PVMS. Thus, if no port has been configured to be member of a certain VLAN, network traffic in this VLAN is dropped inside the bridge.

– A port can forward frames either tagged or untagged. If configured to forward tagged, the port sends the frame without a change. If configured to forward untagged, the port removes the VLAN tag including the PCP (and recalculates the frame's FCS).

If VID and priority has to be preserved throughout the network, forwarding untagged should only be used if the port is an edge port linked to a node that cannot interpret VLAN tagged frames.

Usually, the PVMS is defined as a port / VLAN matrix, as shown in Table 3.

Table 3 – Example of port egress settings

VLAN	Traffic	Port 1	Port 2	Port 3	Port 4	Port 5	Port 6	Port 7	Port 8
1	Mgmt	U,D	-	-	-	-	-	T,D	T,D
2	Video	U	-	-	-	-	T,D	T	T
3	App	U	U,D	U,D	U,D	U,D	-	T	T
U: send untagged T: send tagged -: do not send D: default (PVID)									

In the example of Table 3,

- Port 1 is a member of 3 VLANs, PVMS = {1, 2, 3}, its PVID is 1, its default priority is 4. It could be a management device. This device cannot access the video and application traffic.
- Ports 2-5 send App traffic untagged. It does not send Mgnt traffic nor video traffic.
- Port 6 is for video traffic, its traffic is tagged.
- Ports 7 and 8 are trunk ports, they send all traffic tagged and include all VLANs.

6.4.8.3 VLAN configuration

The complexity of the configuration depends on the network topology and the number of nodes and bridges. Assistance through an engineering tool is highly recommended.

Static VLAN configuration using a network management and configuration tool assigns explicitly the priority and VIDs to all device ports. For this, the tool evaluates the (redundant) paths from a publisher to all subscribers (see 12.3.1).

Dynamic VLAN configuration by registration protocols such as GVRP or MVRP avoid the explicit configuration of the bridges, since all devices broadcast their VLAN settings (which have been previously configured by the tools). Therefore replacement of bridges is simplified. Dynamic allocation requires that all bridges and nodes support this protocol. Traffic bursts during initialization and reconfiguration are however hard to predict.

Substation automation should avoid dynamic VLAN assignment. Rules for VLAN configuration are given in 12.2.

6.4.8.4 VLANs and spanning tree protocols

Bridge vendors implement spanning tree in different manners such as one spanning tree for all VLANs or one spanning tree for a defined number of VLANs or a spanning tree per VLAN. Whenever possible, a single spanning tree for all VLANs should be used. A per-VLAN spanning tree, as for instance standardized as MSTP, is useful in special cases, but one must be aware that the loss of one bridge can affect several VLANs, since the VLANs share the same physical hardware.

Substation automation should avoid multiple spanning tree if not mandated by application requirements.

6.4.9 Comparison VLAN versus multicast filtering

Filtering by VLAN and by multicast filtering are complementary concepts, at different levels. Multicast filtering is applied within the broadcast domain of one VLAN.

Table 4 summarizes the pros and cons of VLAN and multicast filtering.

Table 4 – Advantages and drawbacks of VLAN versus multicast filtering

Multicast filtering advantages	VLAN usage advantages
No need for an 802.1Q support in IEDs Works with default switch settings (VID=1, PCP =0). Easy to use and supervise without port mirroring. Multicast addresses are always used and form the bulk of traffic.	Applies to all traffic, including unicast. Separation by VLANs ensures a first level of security, or at least some protection against bad configuration.
Multicast filtering drawbacks	**VLAN usage drawbacks**
Is useful only when a large part of the traffic is multicast traffic.	Rigid network partition. Top level devices such as SCADA must send VLAN-tagged frames to communicate with devices in different VLANs. Large engineering effort.

6.4.10 Layer 2 redundancy protocols

6.4.10.1 Overview

To increase dependability, additional network elements, bridges and links are introduced. These redundant elements would not be needed in the fault-free state, but they impact procurement and maintenance costs.

Redundancy has a strong impact on the network infrastructure, since in the extreme case it implies duplicating all network elements. Redundancy restricts the possible network topology to avoid single point of failure, which also impacts the non-redundant parts of the network.

A network should be designed from the start with full redundancy, but in such a way that redundancy can be removed for the parts that do not need it. The reverse approach requires in most cases a complete reengineering of the network.

Numerous protocols provide partial or full network redundancy; the concepts are described in IEC 62439-1.

The remaining of Clause 6 gives an overview over the different redundancy protocols, which are then applied in Clause 7.

NOTE In IEC 61850-8-1, the redundancy protocols are RSTP, PRP and HSR, in IEC 61850-9-2 these are PRP and HSR.

6.4.10.2 RSTP and IEC 62439-1

Although RSTP is primarily intended for automatic LAN configuration and loop prevention, it provides redundancy against link and bridge failures. It does however not provide resiliency against link failures to end devices. Loss of a bridge usually causes the loss of all attached devices.

Although RSTP does not provide seamless recovery in case of trunk link or bridge failure, it recovers fast enough for most applications that use the station bus.

IEC 62439-1:2010 shows how to calculate the worst case recovery time of RSTP in generalized meshed or tree topologies, knowing the actual topology of the network, the installation diameter (number of participating devices) can be computed at design time and the maximum recovery time can be computed.

IEC 62439-1:2010 shows that RSTP can achieve recovery times upon a root bridge failure that are suitable for the IEC 61850-8-1 traffic in selected topologies, provided that several parameters, in particular the response delay to BPDUs and the deactivation of RSTP on non-ring ports be restricted beyond what IEEE 802.1D-2011 requires.

EXAMPLE RSTP specifies a time-out of 2 s per bridge, which is impracticable for substation automation. However, if all bridges respond to a BPDU in less than 5 ms, as many do today, a ring of such bridges exhibits a recovery time below 200 ms for 40 nodes.

6.4.10.3 PRP and IEC 62439-3

PRP is a layer 2 redundancy protocol that provides seamless operation in case of loss of any link or bridge. PRP is specified in Clause 4 of IEC 62439-3:2012.

PRP relies on complete duplication of the LAN (see Figure 20). Both LANs operate in parallel and each individually can use RSTP.

A PRP node (called a doubly attached node or DANP) has two ports, one for each redundant LAN. Within a node, both ports are merged at the link layer and presents themselves to the upper protocol stack as one single network interface.

A source DANP sends the same frame on both LANs, appending to the payload a six-octet trailer which contains a protocol identifier and a sequence number.

The destination nodes receive the first frame of a pair and discard the duplicate frame on the base of its source address and of its sequence number.

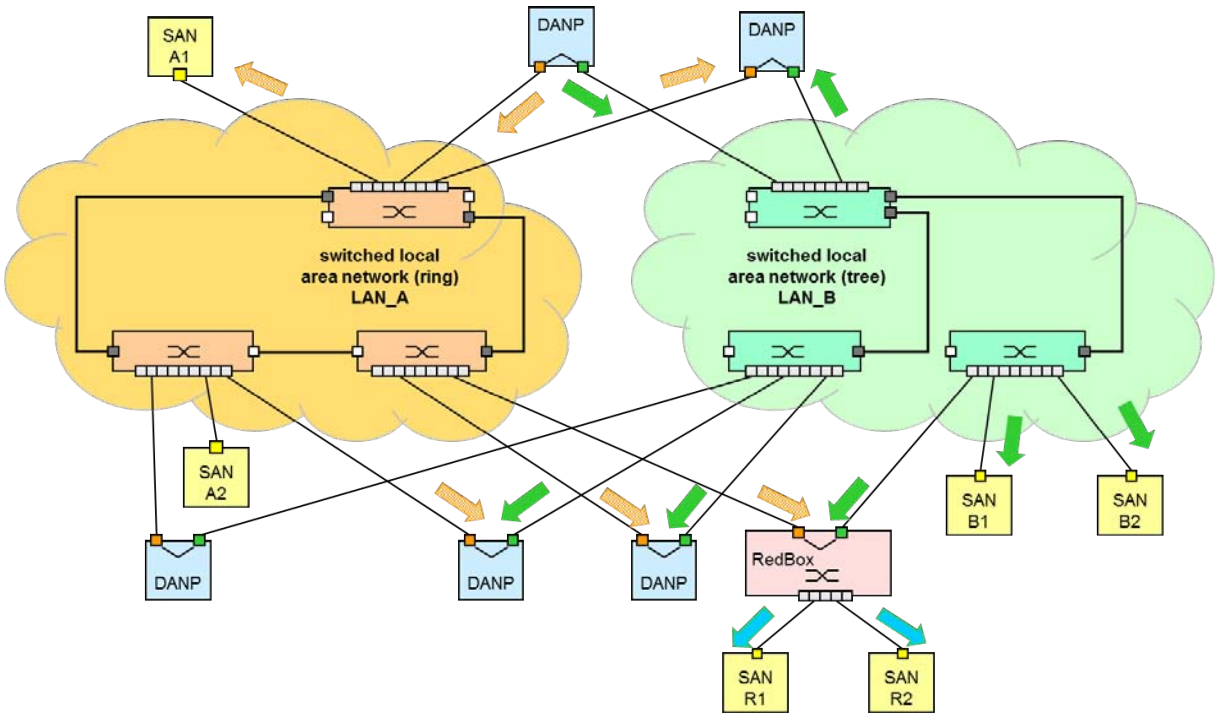


Figure 20 – PRP principle

The 6-octet PRP trailer is ignored by SANs and passed on by bridges. To this effect, all devices in the network must be able to handle oversize frames. Although IEEE 802.3 prescribes a maximum frame size of 1 518 octets, all modern Ethernet controllers and bridges

are able to handle oversize frames of 1 528 and more octets. But some care is needed here for legacy devices.

The protocol is thus transparent to the upper layers. PRP can be implemented in software with two standard Ethernet controllers since a node does not forward frames from port to port.

Since both ports of a DANP use the same MAC address, the two LANs must not be connected, so PRP devices regularly send supervision frames to detect a wrong configuration.

Non-PRP nodes with a single port (Singly Attached Nodes, SAN), e.g. off-the-shelf printers or laptops, can be attached to any LAN and communicate within that LAN with all other devices, but without benefiting from redundancy. Bridges do not need to be PRP-aware.

Non-PRP nodes can be attached to both LANs through one – and only one – RedBox (RB).

NOTE In IEC 61850, PRP is principally applied to the station bus in complex substations, due to the presence of numerous singly-attached nodes, coexistence of duplicated and simplex network segments and extension capability.

6.4.10.4 HSR and IEC 62439-3

HSR is specified in Clause 5 of IEC 62439-3:2012 and provides seamless failover. HSR applies the principle of frame duplication of PRP to a ring of nodes, achieving redundancy through only one single additional link. Nodes in HSR have (at least) two ports, the nodes are daisy-chained, with each one node connected to two neighbour nodes, the last node being connected to the first node and closing the line to a physical ring structure (see Figure 21).

NOTE 1 HSR is not restricted to a ring topology.

To achieve seamless redundancy, a node sends the same frame into both directions on the ring and the destination nodes receive – in the fault-free case – two frame duplicates on both network ports.

To achieve this, an HSR node (called a doubly attached node or DANH) has two ports, one for each direction. Within a node, both ports are merged at the link layer and present themselves to the upper protocol stack as one single network interface. The protocol is thus transparent to the upper layers.

Since HSR forwards frames from port to port in less than 5 μs, it is supported by hardware.

To allow cut-through, HSR frames use a special tag that is not understood by off-the-shelf devices, therefore singly attached nodes (SANs) must be attached through a RedBox.

HSR can operate without dedicated bridges and thus save hardware.

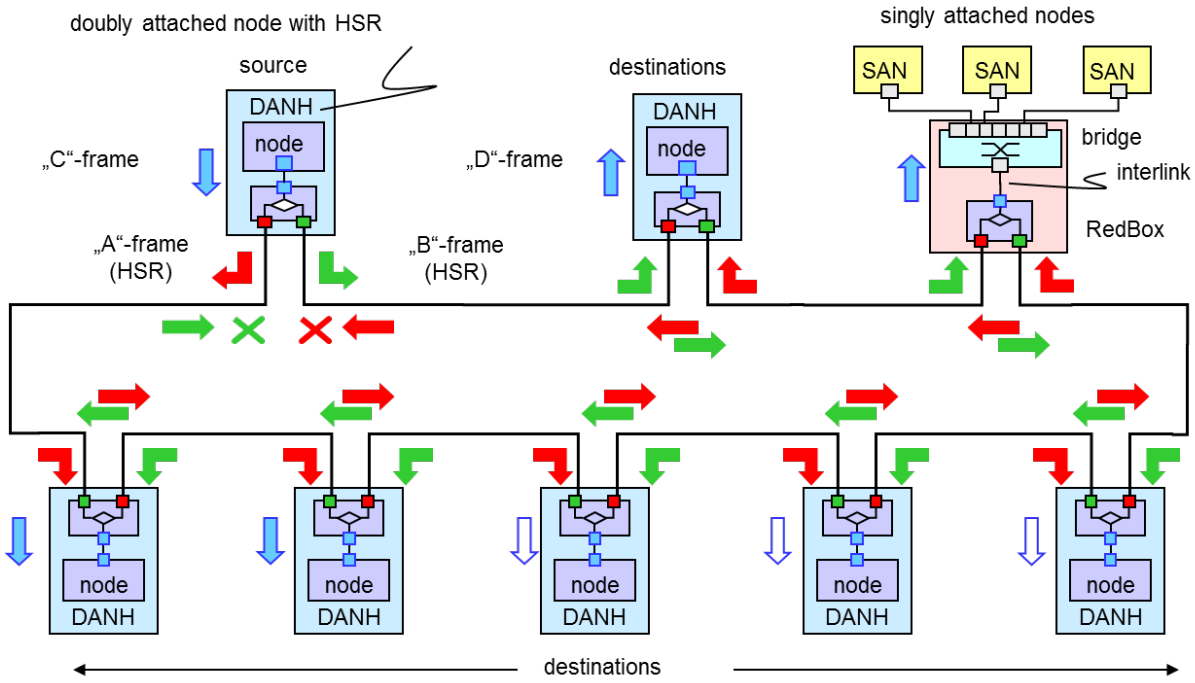


Figure 21 – HSR principle

NOTE 2 In IEC 61850, HSR is principally applied to small substations and to the process bus.

6.4.10.5 HSR/PRP Redundancy Boxes (RedBoxes)

IEC 62439-3:2012 describes how to couple non-redundant network segments to PRP networks and HSR rings through PRP/HSR Redundancy Boxes (RedBoxes). These devices take a delegate function for all non-HSR or non-PRP devices on the networks “behind” the respective RedBox. These devices can also be used to couple HSR to PRP and/or HSR to HSR, as shown in Figure 22.

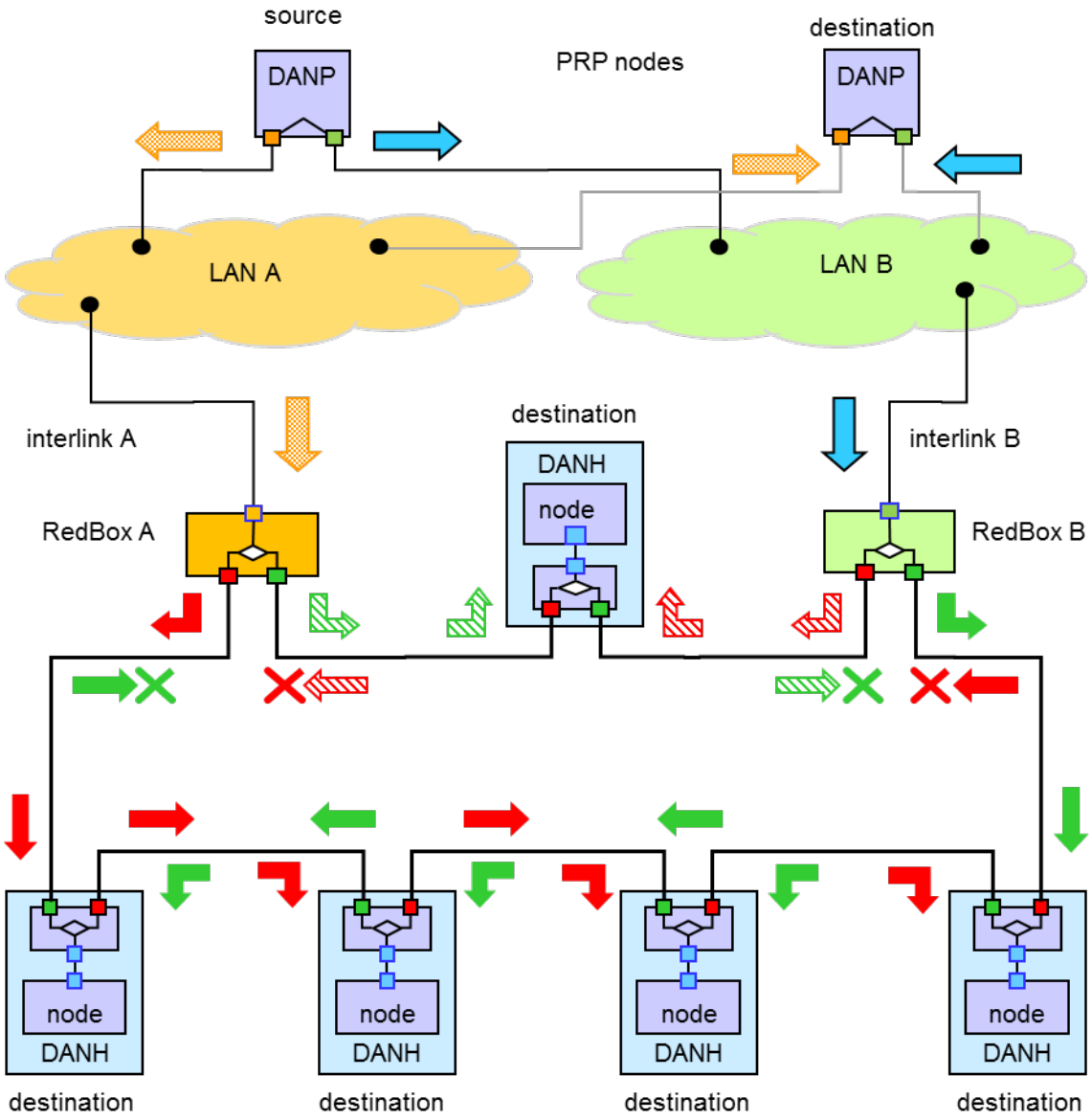


Figure 22 – HSR and PRP coupling (multicast)

6.5 Network layer

6.5.1 Internet protocol

Routers interconnect LANs at layer 3, using the IP addresses. Routers are borders of layer 2 broadcast/multicast domains, thus blocking the transmission of layer 2 multicast messages.

Routers execute the Internet Protocol and route the messages through the internet. The end devices only execute a small subset of the Internet Protocol.

The Internet Protocol version 4 (IPv4) has been the backbone of the internet since 1981. It has an address size of 32 bits. It is being replaced by IPv6 which offers a wider address space and additional services such as cyber-security.

NOTE Within a substation, IPv4 is sufficient. IPv6 is only considered outside of the substation, see 8.3.

6.5.2 IP public and private addresses

IPv4 addresses have a size of 32 bits. IPv4 distinguishes public (internet) addresses and private (intranet) addresses. Private addresses are reusable in several places, but are not

recognized over the internet, while public addresses are unique worldwide and registered with IANA. IPv4 public addresses are now exhausted, IANA only allocates IPv6 addresses.

Private IP addresses are taken from the block allocated by IANA, as specified in RFC 1918 (Table 5).

Table 5 – IANA private IP address blocks (copied from RFC 1918)

Block	Range	Block type	Device quantity
A	10.0.0.0 to 10.255.255.255	24-bit block	16 777 214
B	172.16.0.0 to 172.31.255.255	20-bit block	1 114 111
C	192.168.0.0 to 192.168.255.255	16-bit block	65 535

The size of the private address block depends on the number of devices that need to be connected:

A block C type is sufficient for most installations, but since many companies use a 10.X.X.X address for their intranet, development environments frequently use block A addresses, although this is not recommended if the production part is to be kept separated from the administrative part.

NOTE IEC 61850 specifies the MMS protocol which based in IP / TCP and uses layer 3 addresses. The IP address is selected to match the partition of the network, see 8.1.

6.5.3 Subnet masks

IPv4 subnet masks are used to determine whether the target IP address is within the same subnet (layer 2 multicast domain), in which case frames are sent directly to the MAC address of that device, or if the frame is sent to a router, in which case the frame is sent to the MAC address of the router.

A mask is a bit pattern that acts as a filter for ingoing and outgoing traffic. Devices can only directly communicate (via layer 2 MAC addresses) if the bits of the IP address that correspond to the “1”s in the mask are identical.

Since the mask is a local issue, all devices that need to communicate must be configured with the same subnet mask. Devices on different subnets can only communicate over a router, whose address must belong to the same subnet.

As an example, Table 6 shows that Device X can ping Device Y, but not Device Z.

Table 6 – IP address and mask example

Device	IP address (decimal)	IP address (hex)	IP address (binary)
Device X			
IP address	192.168.1.15	C0.A8.01.0F	11000000 10101000 00000001 00001111
Net mask	255.255.255.224	FF.FF.FF.E0	11111111 11111111 11111111 11100000
Device Y			
IP address	192.168.1.16	C0.A8.01.10	11000000 10101000 00000001 00010000
Net mask	255.255.255.224	FF.FF.FF.E0	11111111 11111111 11111111 11100000
Device Z			
IP address	192.168.1.128	C0.A8.01.40	11000000 10101000 00000001 01000000
Net mask	255.255.255.224	FF.FF.FF.E0	11111111 11111111 11111111 11100000

NOTE In a substation, the subnet mask is selected to match the partition of the network, see 8.1.

6.5.4 Network address translation

If a subnet uses private addresses, they can only be accessed from the outside by introducing between the intranet and the internet a router that performs Network Address Translation (NAT), i.e. maps the intranet address to a temporary extranet address.

NAT and DHCP were originally introduced to allow reuse of IPv4 addresses, which are in short supply, assuming that only few users in a subnet would need to access the internet at the same time. This limitation does not exist anymore in IPv6.

NAT allows separating the addresses used within the private subnet from the address visible outside of the substation. For instance, two substations could use exactly the same private IP addresses internally, while engineering tools access them over different public addresses from the outside. The mapping is done by the router.

However, users are warned that such a router presents a security threat and that it should be used only if necessary and if used, be secured by firewalls and other intrusion protections. Proxy gateways allow to limit access to authorized users and roles and aggregate data.

NOTE Use of proxy gateways and security in substation is addressed in IEC/TR 61850-90-1 and IEC 62351-6.

7 Network and substation topologies

7.1 General rule

The substation electrical topology is related with the voltage level and the protection application. The primary equipment layout and the physical location of IEDs make certain network topologies more suitable.

Although Ethernet can be configured freely, the topology of the communication system mirrors in general the topology of the electrical substation. For instance, there is ideally one group of IEDs per bay attached to a bridge and one network segment for each voltage level, as Figure 23 shows as an example.

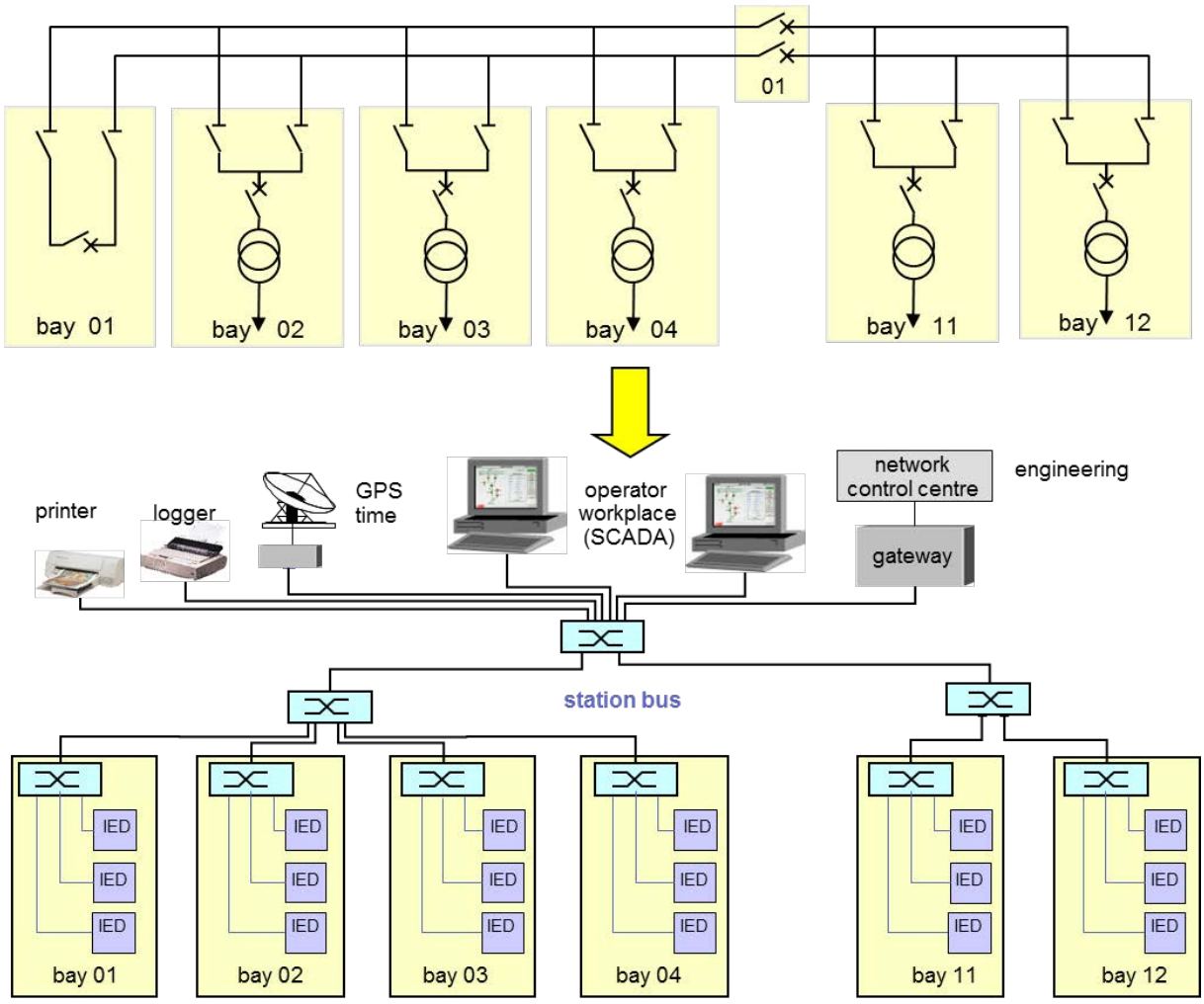


Figure 23 – Mapping of electrical grid to data network topology

Exceptions to this rule are however numerous, the most common being that several voltage levels can be handled by the same subnet and IEDs can serve several bays.

The interconnection between IEDs varies between the extremes of a star topology to a daisy-chain or ring, with several variants. Usually, IEDs located in cabinets are connected star-wise to bridges, while the bridges are connected to form a ring.

In an extreme case of a wind farm, the geographical placement of wind towers favours daisy-chain or ring topologies. Sometimes, the physical topology is not externally visible, for instance in the case of multi-core fibre optical cables which are laid out like a bus, but provide a star connection to a central device.

7.2 Reference topologies and network redundancy

As a framework for network engineering, 7.3 analyses several reference network topologies for the station bus, the process bus and the connection of station bus with the process bus(es).

These reference topologies were chosen based on common practice in substation automation systems ranging from small distribution systems to large multi-voltage level substations. They are representative of the various networking issues described in this document.

Countless other topologies can be realized in actual IEC 61850 networks. There is no ‘best’ network topology and no ‘best’ redundancy protocol. They all have strengths and weaknesses and the correct choice for a given application depends on many factors.

Each reference topology depicts the network graphically as well as various characteristics of the topology including:

- benefits and disadvantages;
- ability to withstand points of failure;
- application suitability;
- protocol dependencies;
- relative cost;
- administration issues;
- redundancy.

Table 7 lists the reference topologies in terms of:

- simplicity of topology (configuration, number of nodes and links);
- traffic control;
- latency;
- redundancy;
- specificity (peculiarity) of a device or protocol;
- limitations.

NOTE The advantages are stated in relative terms, all of these architectures have been successfully used.

Table 8 lists the reference topologies detailed in 7.3 in terms of redundancy protocols.

Table 7 – Summary of reference topologies

Topology		Ease of traffic control	Low latency	Availability	Low cost (from simplicity and specificity)
station bus	station bus as single bridge (7.3.1.1.1)	+	+	–	+
	station bus as hierarchical star (7.3.1.1.2)	+	+	–	+
	station bus as dual star with PRP and RSTP (7.3.1.1.3)	+	+	+	–
	station bus as ring of RSTP bridges (7.3.1.2.1)	0	0	0	0
	station bus as separated bridges for Main 1 and Main 2 protection (7.3.1.2.2)	0	0	+	0
	station bus as ring of bridging nodes (7.3.1.2.3)	–	0	+	+
	station bus as ring and subrings with RSTP (7.3.1.3.1)	0	0	0	0
	station bus as parallel rings (7.3.1.3.2)	0	+	+	0
	station bus as ring of rings (7.3.1.3.3)	0	+	+	0
	station bus as ring and subrings with HSR (7.3.1.3.6)	0	0	+	+
process bus	process bus as connection of merging units (7.3.2.3.4)	+	+	–	+
	process bus as a single star (7.3.2.3.5)	+	+	–	0
	process bus as single bridge (7.3.2.3.5)	+	+	–	+
	process bus as separated LANs for Main 1 and Main 2 (7.3.2.3.8)	+	+	+	–
	process bus as dual redundant stars (7.3.2.3.6)	+	+	+	–
	process bus as ring of HSR (7.3.2.3.9)	–	–	+	0

"+" means that this topology has a relative advantage in target column.

"0" means that this topology has characteristics similar to those of other topologies.

"–" means that this topology has a relative disadvantage in target column.

NOTE 1 Costs reflect capital expenditures, not operational expenditures or maintainability.

Table 8 – Reference topologies and redundancy protocols used

Topology		Redundancy	Remarks
station bus	station bus as single bridge (7.3.1.1.1)	none	No redundancy.
	station bus as hierarchical star (7.3.1.1.2)	none	No redundancy.
	station bus as dual star with PRP and RSTP (7.3.1.1.3)	RSTP	RSTP not needed in a star topology.
		PRP	Devices without PRP interface use PRP RedBoxes for communication to both LANs.
	station bus as ring of bridges (7.3.1.2.1)	RSTP	Deterministic reconfiguration according to IEC 62439-1:2010.
	station bus as separated bridges for Main 1 and Main 2 protection (7.3.1.2.2)	RSTP	Deterministic reconfiguration according to IEC 62439-1:2010.
	station bus as ring of bridging nodes (7.3.1.2.3)	RSTP	Deterministic reconfiguration according to IEC 62439-1:2010.
		HSR	Non HSR devices need to be connected via RedBoxes.
	station bus as ring and subrings with RSTP (7.3.1.3.1)	RSTP	See IEC 62439-1:2010 for network engineering aspects and recovery time.
	station bus as parallel rings (7.3.1.3.2)	RSTP	See IEC 62439-1:2010 for network engineering aspects and recovery time.
	station bus as ring of rings (7.3.1.3.3)	RSTP	See IEC 62439-1:2010 for network engineering aspects and recovery time.
	station bus as ring and subrings with HSR (7.3.1.3.6)	HSR	Coupling of rings must be done with QuadBoxes.
process bus	process bus as connection of merging units (7.3.2.3.4)	NA	No redundancy.
	process bus as single star topology (7.3.2.3.5)	NA	No redundancy.
	process bus as single bridge (7.3.2.3.7)	NA	No redundancy.
	process bus as separated LANs for Main 1 and Main 2 (7.3.2.3.8)	application redundancy	Redundancy is provided by duplication of sensors, IEDs, Ethernet bridges and links.
	process bus as dual redundant stars (7.3.2.3.6)	application redundancy	Redundancy is provided by duplication of sensors, IEDs and links.
	process bus as ring of HSR (7.3.2.3.9)	HSR	Non HSR devices need to be connected via RedBoxes (RSTP bridging nodes do not provide zero failover time).
station bus and process bus	station bus Ring and separated process bus based on multiple point-to-point links (7.3.3.1)	RSTP	Can be used on the station bus ring. See IEC 62439-1:2010 for RSTP engineering and recovery time.
		HSR	Can be used on the station bus ring.
	Separated station bus and process bus rings (7.3.3.3)	RSTP	See IEC 62439-1:2010 for network engineering aspects and recovery time.
		HSR	Process bus segments may be isolated by QuadBoxes.
	Combined station bus and process bus by coupled HSR rings (7.3.3.4)	HSR	Rings must be coupled with QuadBoxes (RSTP bridging nodes do not provide zero failover time).
		PRP	PRP can be used to redundantly connect single devices to the HSR network.
	station bus as dual ring and process bus as HSR ring (7.3.3.5)	RSTP	Only as redundancy protocol in the station bus rings.
		HSR	Devices without HSR interface need to use HSR RedBoxes to communicate to both LANs.
		PRP	Devices without PRP interface need PRP RedBoxes for communication to both LANs. Can be used for redundant station bus rings.

7.3 Reference topologies

7.3.1 Station bus topologies

7.3.1.1 Station bus star topologies

7.3.1.1.1 Station bus as single bridge

The most basic station bus topology is the one-level bridge as shown in Figure 24, which can be applied only to very simple substations. Even simpler, the bridge could be implemented in a multiport SCADA device, resulting in a single-level star topology.

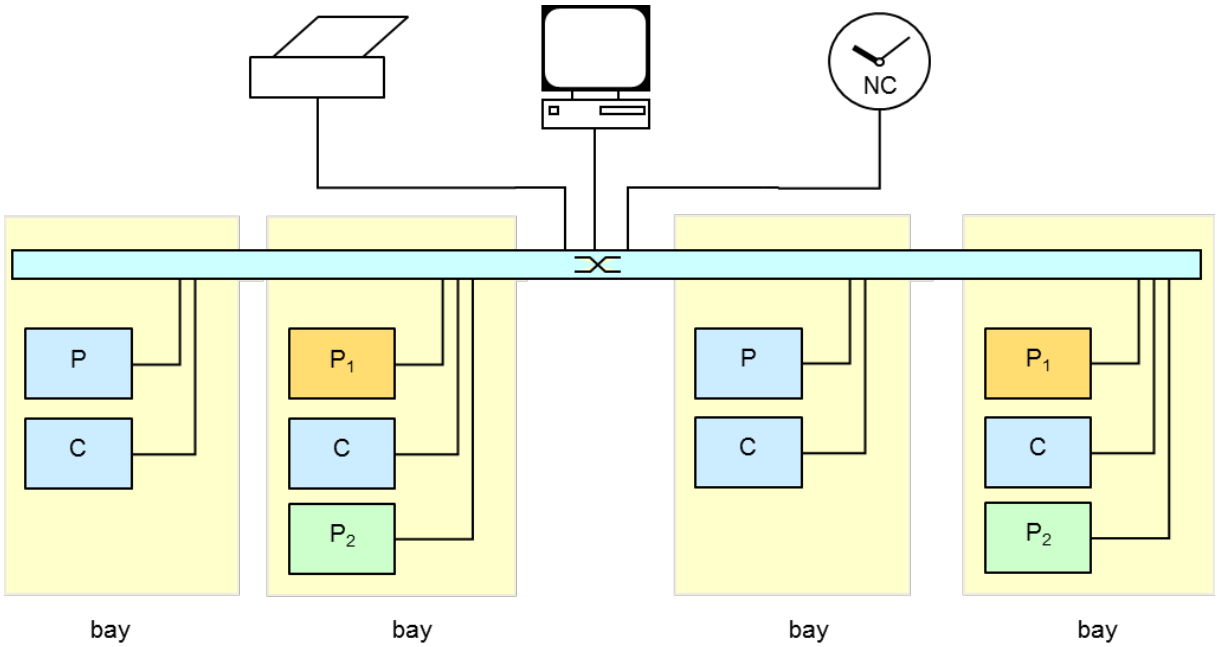


Figure 24 – Station bus as single bridge

The characteristics of this topology are summarized in Table 9.

Table 9 – Station bus as single bridge

Property	Characteristics
Simplicity	Very simple topology with a single bridge. The number of links to the bridge is equal to the number of end nodes.
Traffic control	Easy to ensure adequate bandwidth. Except during the initial network discovery, inter-bay communication is not affected by other inter-bay communication. Within a subnetwork, end-to-end communication is not affected by other end-to-end communication. However, the bridge becomes a bottleneck when the number of IEDs is large because traffic converges on a particular port.
Latency	Very low latency, because the number of bridge hops is one.
Redundancy	No redundancy. A single fault of a link, a bridge or an end node disrupts communication.
Specificity of a device/protocol	No special communication equipment.
Limitations	The bridge becomes a bottleneck when the number of IEDs is large. The number of ports per bridge is limited.

7.3.1.1.2 Station bus as hierarchical star

A star network as shown in Figure 25 has no redundant physical paths or loops in the network; its physical structure is identical to its logical structure.

The key benefit of a star topology is its simplicity. Simple applications operate with unmanaged bridges, reducing costs and engineering, and increasing reliability. However, large networks require means to limit traffic, and need managed bridges.

The disadvantage of a simple star topology is the lack of network path redundancy. Any single point of failure of a cable, bridge port, or entire bridge interrupts a network path with subsequent loss of automation functionality. Because of the lack of redundancy, the simple star is only used when the downtime of the communication system is tolerable, e.g. in uncritical SCADA applications.

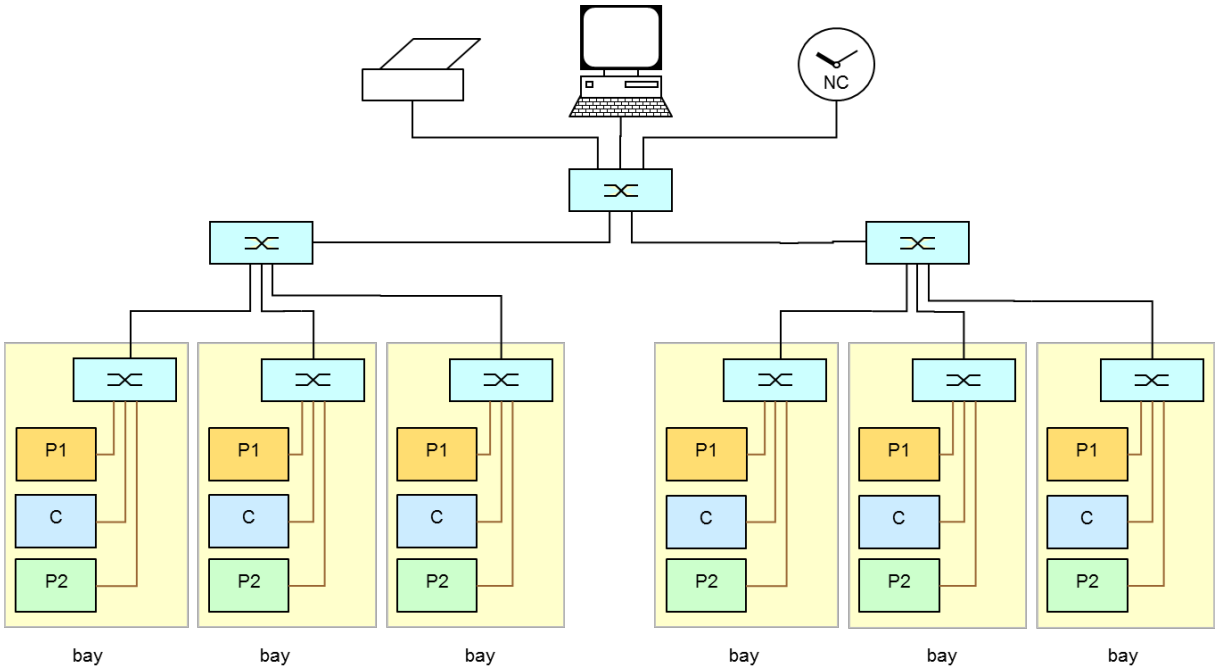


Figure 25 – Station bus as hierarchical star

The characteristics of this topology are summarized in Table 10.

Table 10 – Station bus as hierarchical star

Property	Characteristics
Simplicity	Simple topology. Fits well the cabinet structure. Bays can be easily disconnected. The number of links approximately equals to the number of end nodes plus the number of bridges.
Traffic control	Easy to ensure adequate bandwidth. Unmanaged bridges are used in small networks. In large networks, traffic can be reduced by multicast islands.
Latency	Low latency. The number of hops is not affected by the number of end nodes, unlike ring topologies.
Redundancy	No path redundancy. A single fault of a link, a bridge or an end node disrupts communication.
Specificity	No special communication equipment.
Limitations	Large number of bridges is required because the number of bridges is proportional to the number of subnetworks.

7.3.1.1.3 Station bus as duplicated star

When the network requests a very high availability (no single point of failure), each critical device should be attached to two independent LANs, preferably using the PRP protocol. Each of these networks must comply with the propagation requirements that would exist if only one network would be in use. Non-critical devices can be attached to one LAN only. It is also

possible to attach the main protection to one LAN and the back-up protection to the other LAN to achieve fail-independence, as shown in Figure 26.

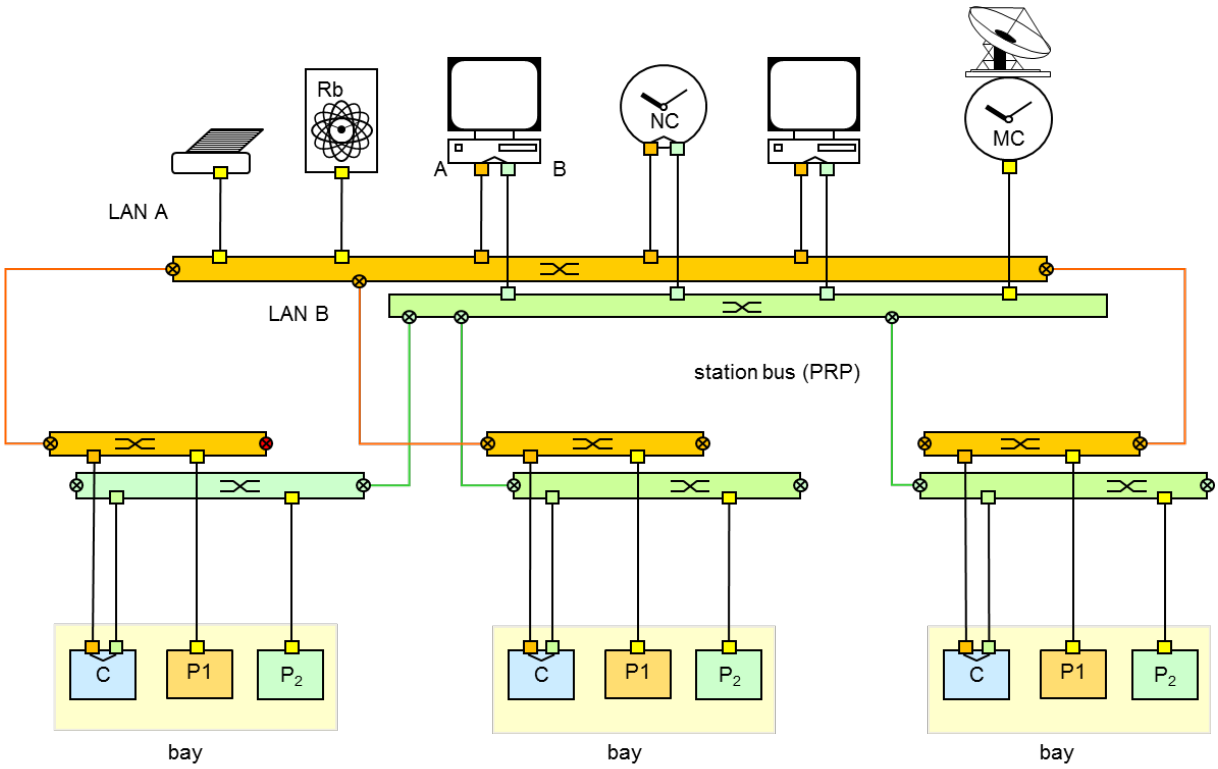


Figure 26 – Station bus as dual star with PRP

The characteristics of this topology are summarized in Table 11.

Table 11 – Station bus as dual star

Property	Characteristics
Simplicity	Simple configuration (each PRP LAN is configured as a simple LAN). Singly attached devices can be attached to different LANs. Duplicate and non-duplicated segments coexist.
Traffic control	Since LAN A and LAN B are independent, the traffic characteristics are not affected by redundancy. The individual LANs can be operated with RSTP when redundant paths are used.
Latency	Same as for a hierarchical bridge topology. Redundancy marginally speeds-up communication in the average, since one path is faster than the other.
Redundancy	Bumpless failover between DANP; SANs can provide redundancy through device redundancy, as the clocks in Figure 26.
Specificity	DANPs or RedBoxes are needed for redundancy.
Limitations	Doubles the network infrastructure for full redundancy, requires PRP-equipped devices.

7.3.1.2 Single ring topologies

7.3.1.2.1 Station bus as ring of RSTP bridges

In a ring, each bridge is connected to two and only two neighbour bridges to form a physical loop (see Figure 27). Rings offer full redundancy against link failures, but not against edge port or bridge failure, unless each device is dual ported and connected to two different bridges.

A redundancy protocol such as RSTP ensures that frames do not circulate indefinitely.

A topology with a bridge per bay is a common arrangement.

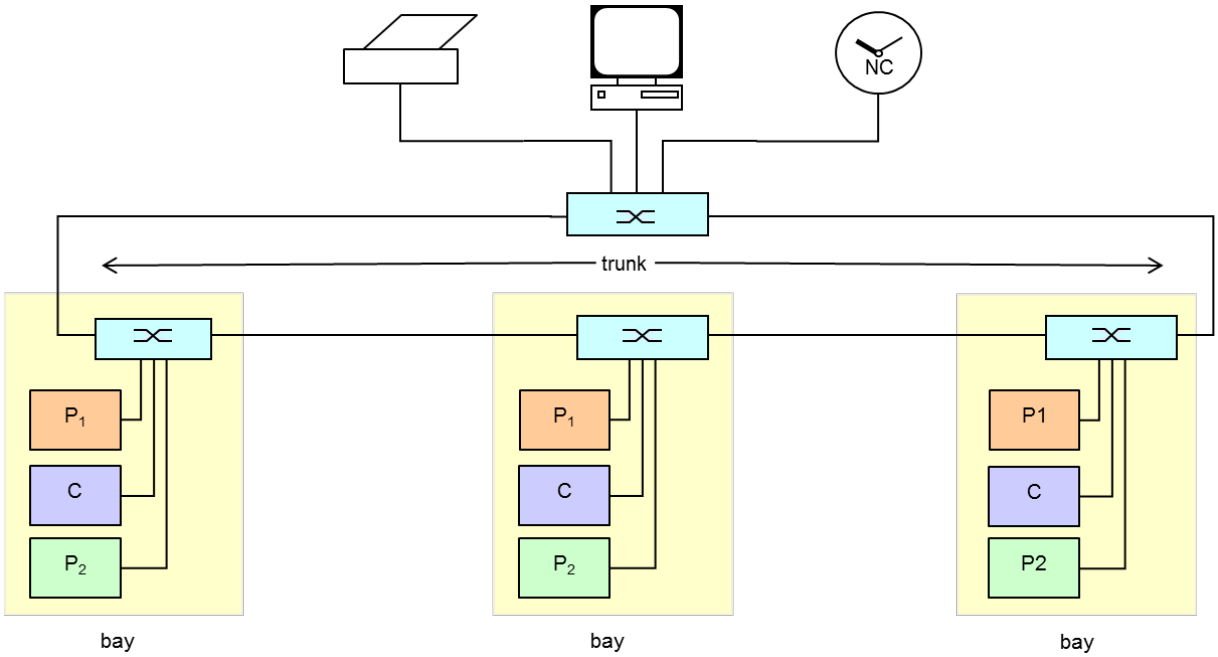


Figure 27 – Station bus as ring of RSTP bridges

The characteristics of this topology are summarized in Table 12.

Table 12 – Station bus as ring

Property	Characteristics
Simplicity	Simple topology. The number of bridges is proportional to the number of bays. The number of links is determined by the number of end nodes and the number of bridges. Maps well to the cabinet arrangement. A bay can be removed from the network for maintenance with minimal effect to other bays.
Traffic control	Slightly difficult to ensure adequate bandwidth. Inter-bay communication is affected by other inter-bay communication because the traffic is forwarded over shared links. The number of subnetwork has an impact to ensure bandwidth.
Latency	Latency increases with the number of bridges in series, in the worst case the number of hops will be N-1 the number of bridges. Unlike rings with DANH, the number of hops does not depend on the number of end nodes.
Redundancy	Provides redundancy against trunk link failures in the ring. However, as IEC 62439-1:2010 shows, the availability increase is negligible since the unavailability of the links to the end devices and of the bridges dominates.
Specificity	To reduce latency, bridges with cut-through are required, although this only improves the average, not the worst-case latency.
Limitations	Not flexible when cable routing demands another topology.

7.3.1.2.2 Station bus as separated bridges for Main 1 and Main 2 protection

Demanding applications require redundant protection devices (1 = Main 1 and 2 = Main 2) that do not present a single point of failure. To ensure fail-independence of the Main 1 and Main 2 protections, they are attached to different LANs and to different bridges, as shown in Figure 28.

NOTE Bus 1 and Bus 2 refer to application redundancy with each its network (see Figure 28), LAN A and LAN B refer to the redundant path within the same PRP network, see Figure 26.

Such separation reduces considerably common mode failures, but some connection between Bus 1 and Bus 2 still exist, since both Main 1 and Main 2 devices are controllable from the same SCADA and receive the same GOOSE messages. Bus 1 and Bus 2 should be treated like different bays.

Figure 28 assumes that Bus 1 and Bus 2 are connected at layer 2 by different bridges, which themselves are connected through the station bus, introducing a possible single point of failure.

This represents a limit case between network redundancy (through the redundant link in the ring) and device redundancy (through the presence of a second bridge). It also presents a boundary case of a process bus since Bus 1 and Bus 2 can carry process bus traffic (note the PI in Figure 28).

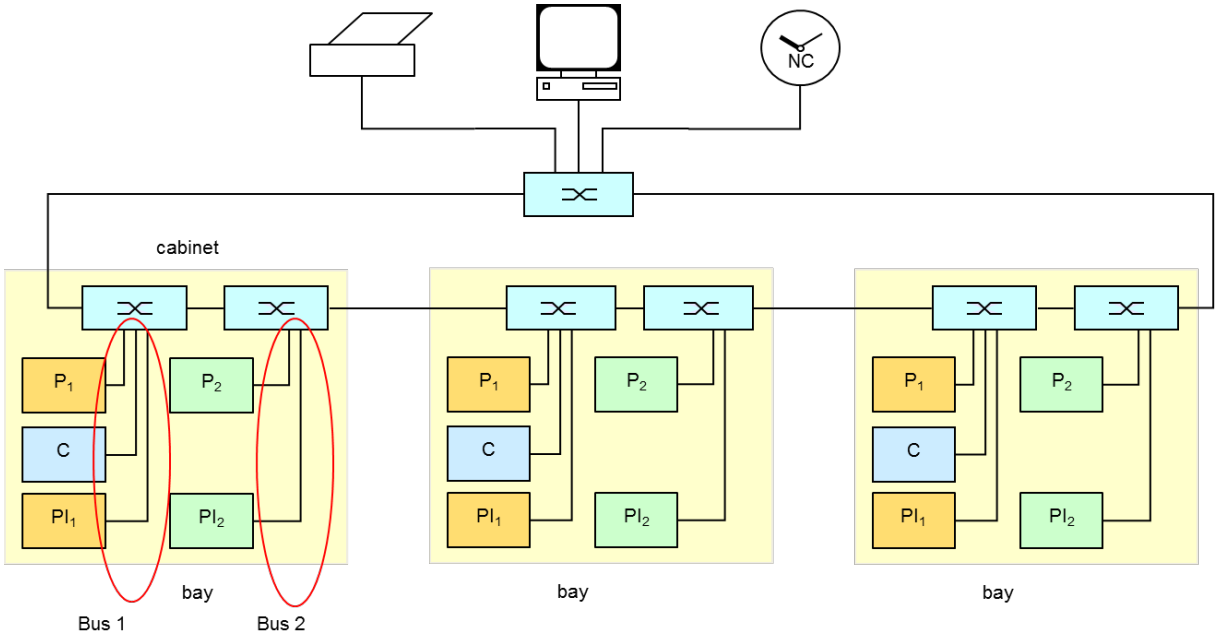


Figure 28 – Station bus as separated Main 1 (Bus 1) and Main 2 (Bus 2) LANs

The characteristics of this topology are summarized in Table 13.

Table 13 – Station bus as separated Main 1 and Main 2 protection

Property	Characteristics
Simplicity	Same as 7.3.1.2, using only two bridges per bay.
Traffic control	Similar to 7.3.1.2, but worst-case traffic in the trunk is more difficult to evaluate, since the bridges carry process bus traffic.
Latency	More latency than 7.3.1.2 since the number of bridges in series is doubled.
Redundancy	Same as 7.3.1.2, with the additional advantage that the separation of Bus 1 and Bus 2 provides a high availability of the protection function.
Specificity	Same as 7.3.1.2.
Limitations	Same as 7.3.1.2. Needs cautious engineering of the connection between Bus 1 and Bus 2.

7.3.1.2.3 Station bus as ring of bridging nodes

A ring structure saves wiring and bridges; it is not used primarily for redundancy. It is well suited for medium-voltage substations with typically one IED per bay.

Bridging nodes, for instance using HSR, reduces the number of bridges and still provides full network redundancy, as shown in Figure 29.

Bridging nodes that use cut-through reduce the average forwarding delay of a frame, although cut-through does not improve the worst case, which occurs when all bridges are forwarding long frames at the same time. Cut-through needs hardware support.

The number of nodes per ring is limited by the cumulative latency introduced by the bridging nodes, the maximum being defined by the application.

For instance, if every node introduces a worst-case forwarding delay of 123 μs (maximum length frame in transit at 100 Mbit/s), putting 50 nodes in series results in a worst case delay of 6,159 ms, which is acceptable only for devices complying with transfer time class TT4 or lower (see 11.1.3 of IEC 61850-5:2013).

Since each node introduces a forwarding delay from port to port, the number of nodes per ring should be kept small.

In medium voltage substations, one IED can combine the protection, measurement and control functions usually found in several devices in high-voltage substations, thus reducing the number of devices in the ring.

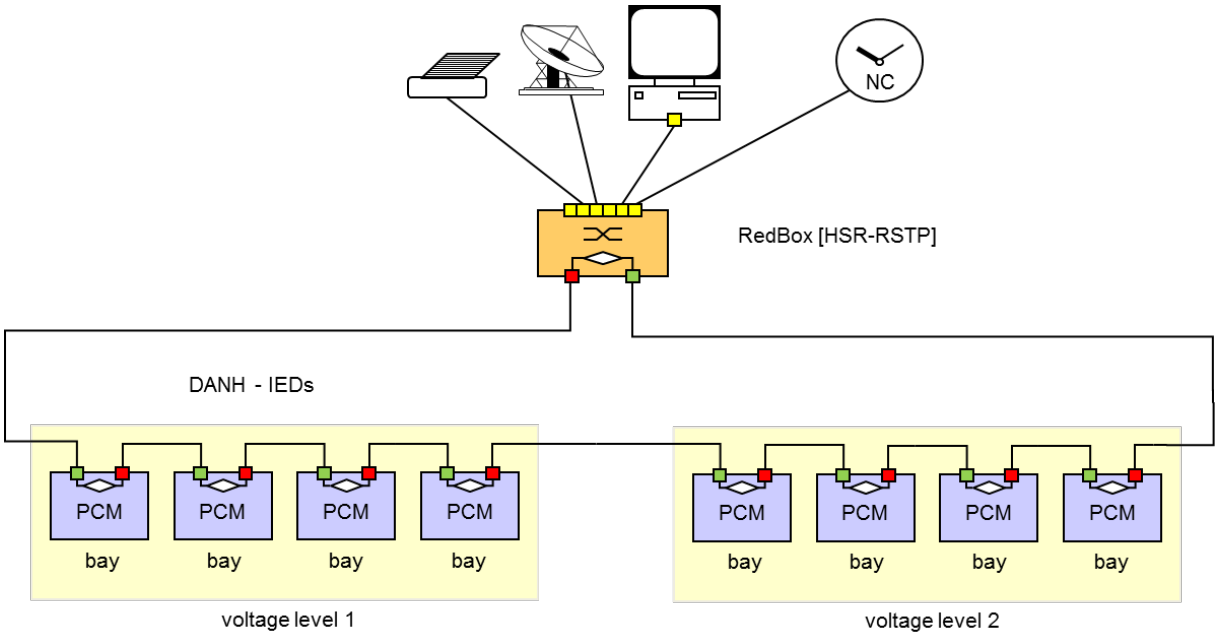


Figure 29 – Station bus as ring of HSR bridging nodes

The characteristics of this topology are summarized in Table 14.

Table 14 – Station bus as ring of bridging nodes

Property	Characteristics
Simplicity	Simple topology. Reduced number of dedicated bridges. Reduced wiring. Maps well to the cabinet arrangement. A bay or voltage level can be disconnected from the substation network for maintenance if loss of redundancy during that time is tolerable. Small number of nodes and links. The number of links is determined by the number of DANs and RedBoxes (or bridges with RSTP).
Traffic control	Difficult to evaluate bandwidth. Traffic of DANs and RedBoxes on the ring is shared. Inter-bay communication and intra-bay communication are affected by communication of other bays and nodes. The number of DANs has critical impact to ensure bandwidth.
Latency	Latency increases with the number of bridges in series, but this is not critical for a station bus. Using cut-through reduces average latency but does not improve its worst case.
Redundancy	Resilient against any single link failure and some bridge failures. A RedBox is a single point of failure, but a pair of them can be used.
Specificity	Requires IEDs with double attachment, hardware support to keep latency low and possibly a by-pass relay. In the case of HSR, HSR RedBoxes are necessary to connect SANs.
Limitations	Not flexible when cable routing demands another topology. Splitting of rings is recommended when the number of bays becomes large, e.g. one ring per voltage level. When more than one IED per bay is used, the ring bridges would be replaced by HSR RedBoxes with multiple ports, and the ring would carry HSR traffic.

NOTE Bridging nodes at the station bus, where longer recovery time is tolerated, could use RSTP as well, but bridging IEDs using RSTP are more complex than those using HSR.

7.3.1.3 Station bus as multiple ring topology

7.3.1.3.1 Station bus as ring and subrings with RSTP topology

A hierarchy of two rings uses one ring at the station level (primary ring) and a ring for each voltage level (secondary rings). Figure 30 shows such a topology implemented with RSTP.

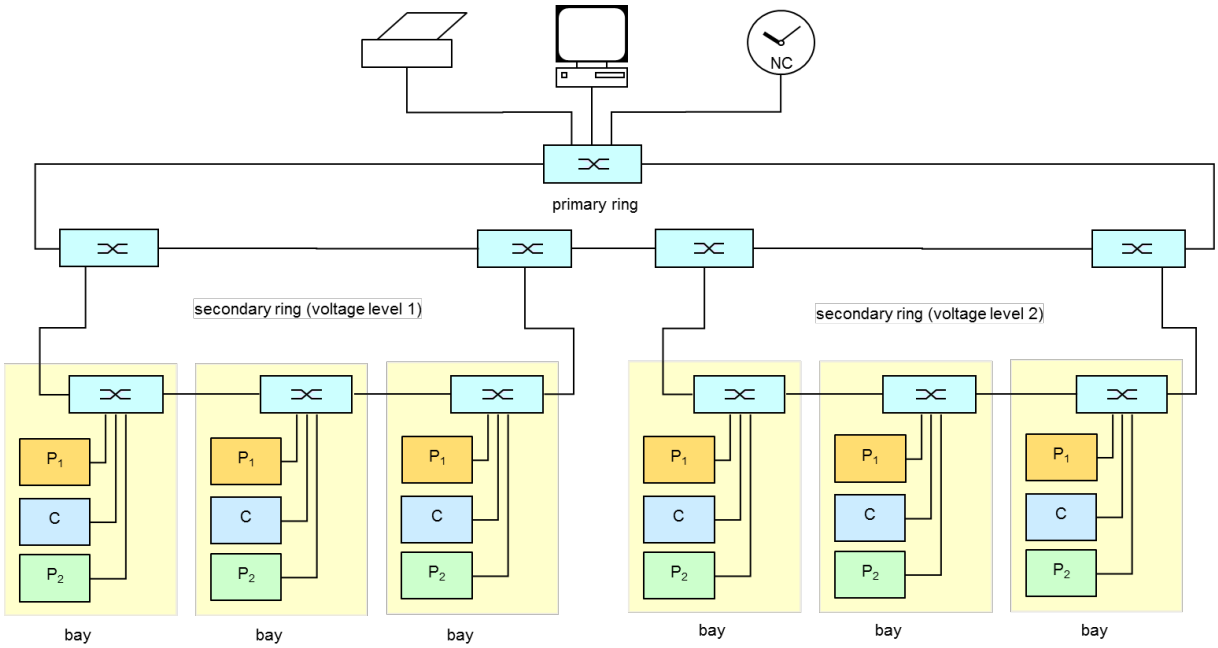


Figure 30 – Station bus as ring and subrings with RSTP

The characteristics of this topology are summarized in Table 15.

Table 15 – Station bus as ring and subrings

Property	Characteristics
Simplicity	Moderate complexity, conventional layout with one bridge per bay. Large number of bridges. The number of bridges in secondary ring is the number of bays plus two. The total number of bridges is the number of bridges of secondary rings plus the number of other bridges in the primary ring. The number of links is approximately the number of end nodes plus the number of bridges plus the number of subrings.
Traffic control	Traffic is segmented by the bridges (multicast filters). Bridge priority should be configured to ensure the root bridge is on the upper ring. Slightly easy to ensure adequate bandwidth unless traffic of numerous secondary rings is forwarded to the primary ring. Inter-bay communication on each secondary ring is affected by unrelated inter-bay communication on the same secondary ring.
Latency	Slightly low latency if the number of bridges which construct primary ring or secondary ring is small and the traffic is not detoured.
Redundancy	One path redundancy on the rings. It is advantageous to use two bridges per bay to connect main 1 and main 2 independently to the station bus.
Specificity	Cut-through bridges help reducing latency.
Limitations	Engineering the connection between the voltage levels is difficult. Location of bridges is not obvious.

7.3.1.3.2 Station bus as parallel rings

This topology extends the single ring and provides multiple ring redundancy with two external bridges and integrated IED bridges using optical links, as shown in Figure 31.

The two main bridges ensure a short propagation delay. If RSTP is used, the main bridges should be designated as Root Bridge 1 and Root Bridge 2 to lower recovery time from root bridge failure. The main bridges can be directly connected to lower delays.

In real applications, the subrings are smaller due to installation arrangement restrictions.

The network structure and therefore the ring size are determined by the physical/logical structure of the application. Rings can be set up suiting the bay structure or the voltage level of a substation. Some mix the IEDs between the bays, so that at the loss of one ring, parts of the bay are still visible.

The SCADA and the back-up SCADA are also DANs, implementing RSTP or a subset thereof.

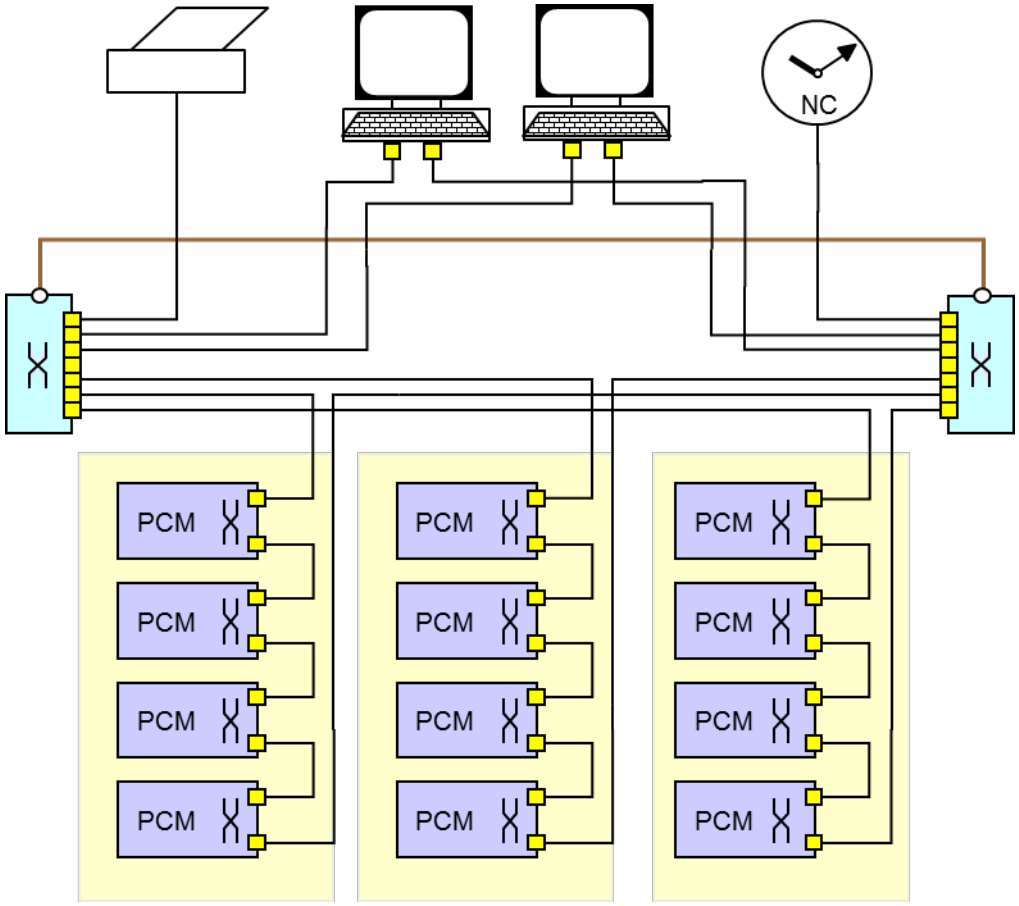


Figure 31 – Station bus as parallel rings with bridging nodes

The characteristics of this topology are summarized in Table 16.

Table 16 – Station bus as parallel rings

Property	Characteristics
Simplicity	Moderately complex topology. The number of bridges is two. The number of links equals the number of end nodes plus the number of bridges. Reduces total installed cost by using IEDs with embedded bridge functionality. Supports several rings.
Traffic control	Difficult to evaluate, since part of the ring traffic is routed between the bridges over the common high-speed link, creating a dependency between the rings.
Latency	Latency increases with the number of DANs in a ring.
Redundancy	One path redundancy with dependence on one backup link.
Specificity	Needs doubly attached nodes in the ring with a support for at least an RSTP subset. To reduce latency, DANs can benefit from cut-through hardware support.
Limitations	Although the extremity bridges can be connected by high capacity links, they can become a bottleneck.

7.3.1.3.3 Station bus as parallel HSR rings

Figure 32 shows a station bus structure in which one HSR ring serves each bay. To reduce the worst-case latency, both ring halves should have the same number of IEDs.

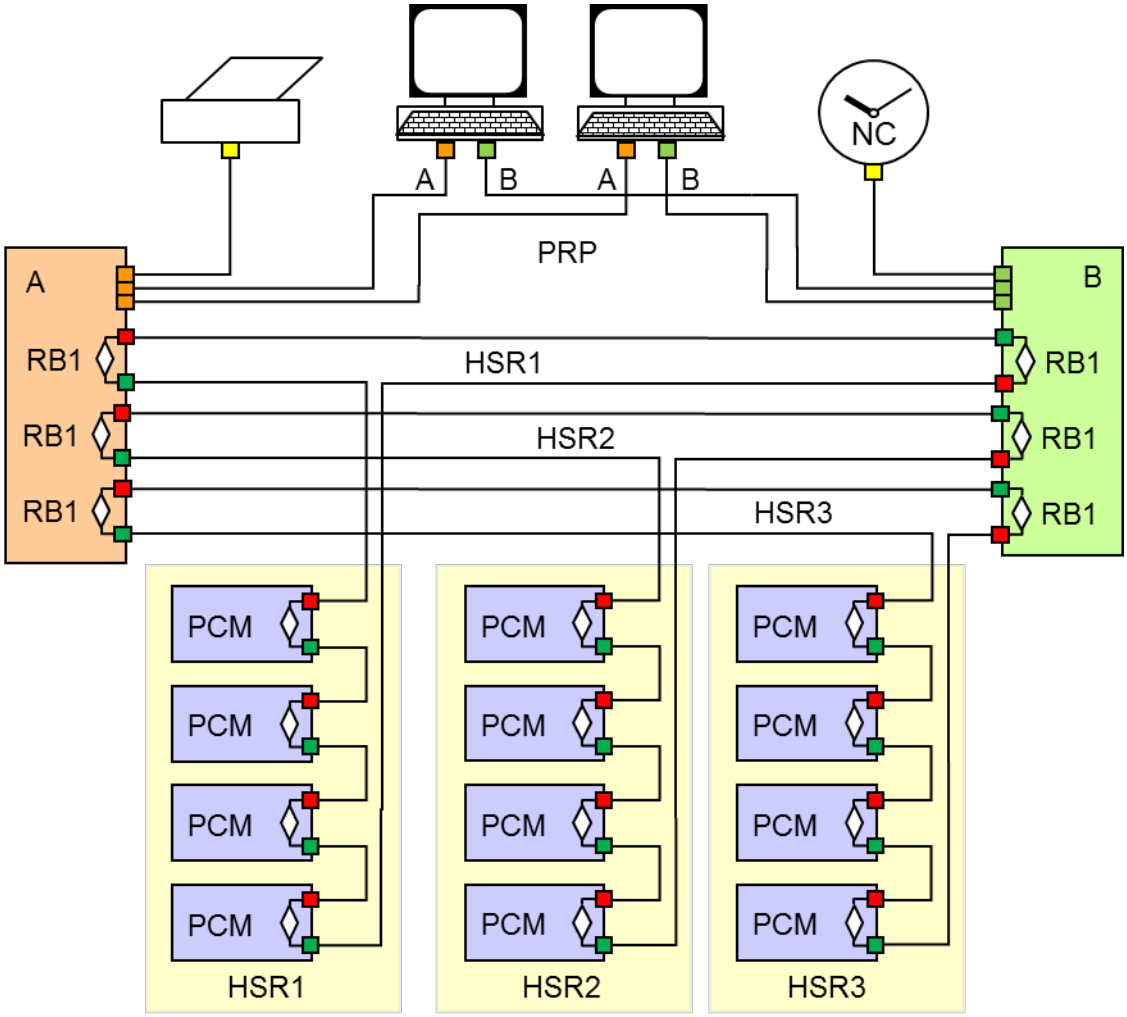


Figure 32 – Station bus as parallel HSR rings

The characteristics of this topology are summarized in Table 17.

Table 17 – Station bus as parallel HSR rings

Property	Characteristics
Simplicity	Moderately complex topology. The number of bridges / redboxes is two. The number of links equals the number of end nodes plus two for each ring, plus twice the number of end devices in PRP. Reduces total installed cost by using IEDs with embedded bridge functionality. Supports several rings.
Traffic control	Difficult to evaluate, since part of the ring traffic is routed between the bridges over the common high-speed link, creating a dependency between the rings.
Latency	Latency increases with the number of DANHs in a ring, but is kept low by HSR cut-through.
Redundancy	Full redundancy within the rings.
Specificity	Needs DANHs in the ring.
Limitations	Although the extremity bridges can be connected by high capacity links, they can become a bottleneck.

7.3.1.3.4 Station bus as ring of rings

The Ring-Ring topology in Figure 33 shows a network with a primary ring and secondary rings connected to the primary ring. This can also be considered a meshed topology and illustrates one of the possible variants of this topology.

This topology follows the way a traditional protection and control system is installed in electrical substations, i.e. bay by bay. Each sub-ring can represent a bay of the substation.

The Ring-Ring provides additional redundancy beyond the simple ring. The Ring-Ring topology is more adaptable than simple ring since it can map to physical wiring constraints of any application.

The Ring-Ring is a more complicated topology requiring a more sophisticated redundancy protocol to manage it, when deterministic network recovery times need to be achieved.

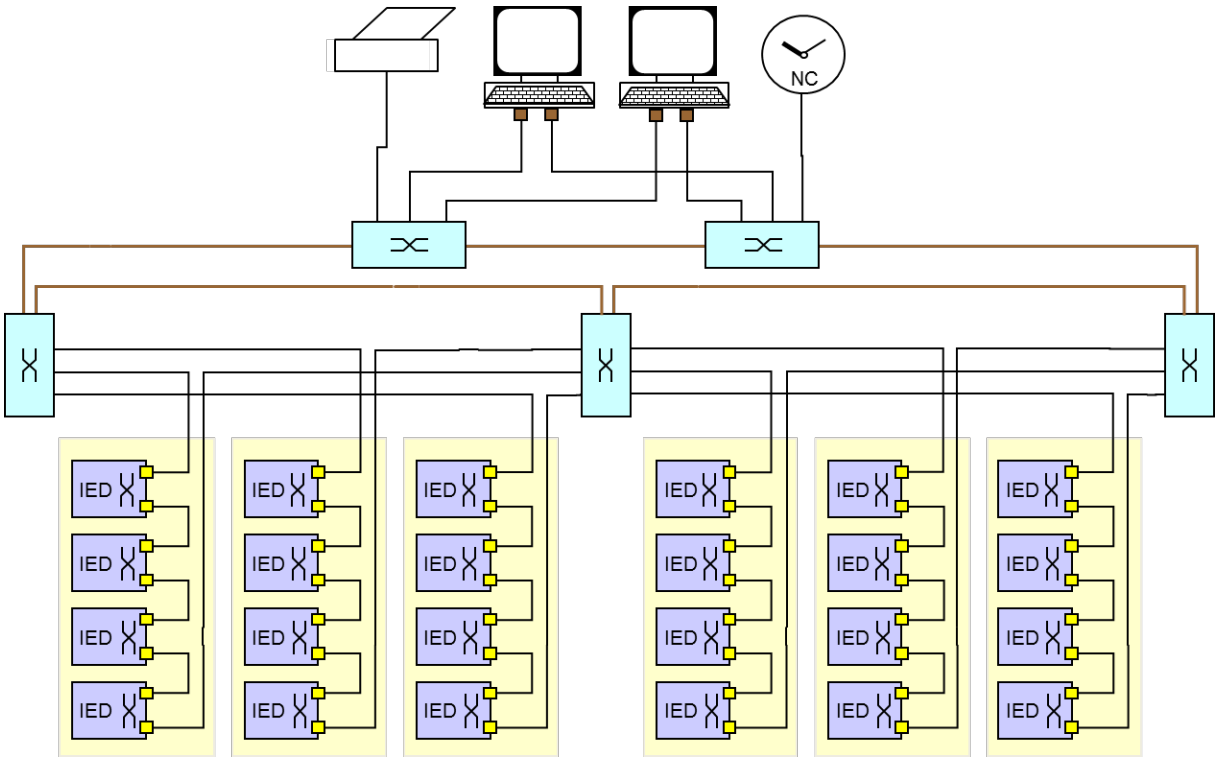


Figure 33 – Station bus as hierarchical rings with RSTP bridging nodes

The characteristics of this topology are summarized in Table 18.

Table 18 – Station bus as ring of rings with RSTP

Property	Characteristics
Simplicity	This topology can map to physical wiring constraints of any application and is suitable for very large substations. Complex topology. Some bridges are needed for constructing primary ring and secondary rings. The number of links is approximately determined by the number of end nodes plus the number of links forming the primary ring.
Traffic control	Multicast filtering in the bridges. Evaluation of bandwidth is difficult since inter-bay communication is affected by non-related inter-bay communication.
Latency	Latency low if the number of DANs is small.
Redundancy	Tolerates a single failure at least, tolerates some multiple failures with no loss of connectivity.
Specificity	DANs with cut-through hardware support are needed to reduce average latency.
Limitations	Needs special care to achieve a deterministic recovery time with RSTP. If RSTP is applied to the primary ring, the protocol has to be deactivated on the links connecting the secondary rings, since otherwise this would introduce loops in the network. If RSTP was active on the links to the secondary ring and the RSTP domain would stretch out from the primary ring to the secondary rings, the network reconfiguration time would only be determinable as an upper bound value as described in IEC 62439-1:2010. There are several vendor-specific solutions which allow the implementation of a topology as shown in Figure 33 with deterministic recovery times, but relying on them complicates engineering of heterogeneous systems.

7.3.1.3.5 Station bus as ring of rings with HSR

The Ring-Ring topology of Figure 33 can be applied to HSR bridging nodes. See Figure 34.

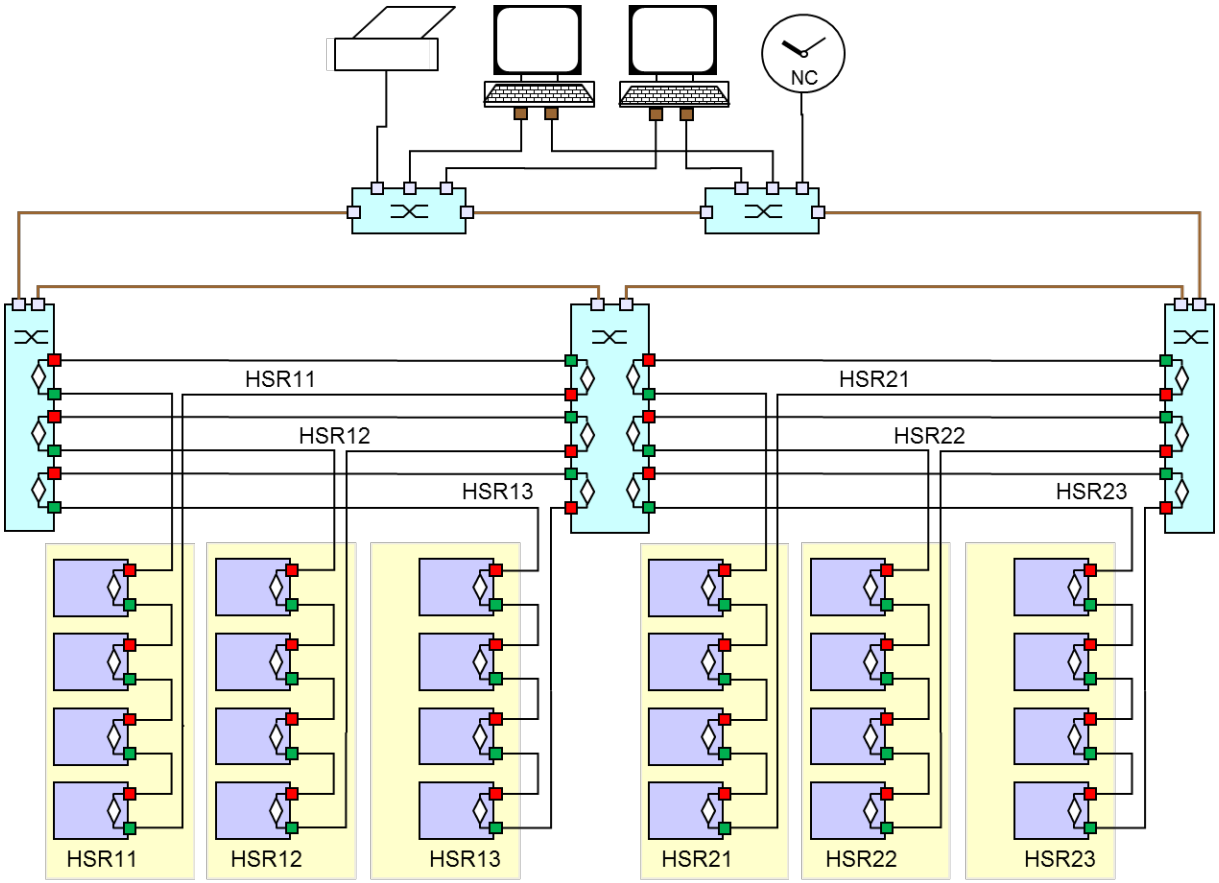


Figure 34 – Station bus as hierarchical rings with HSR bridging nodes

The characteristics of this topology are summarized in Table 19.

Table 19 – Station bus as ring of rings with HSR

Property	Characteristics
Simplicity	This topology can map to physical wiring constraints of any application and is suitable for very large substations. Complex topology. Bridges combined with RedBoxes are needed for constructing primary ring and secondary rings. The number of links is approximately determined by the number of end nodes plus the number of links forming the primary ring.
Traffic control	Multicast filtering in the bridges. Evaluation of bandwidth is difficult since inter-bay communication is affected by non-related inter-bay communication.
Latency	Latency low if the number of DANHs is small.
Redundancy	Tolerates a single failure at least, tolerates some multiple failures with no loss of connectivity.
Specificity	DANHs with cut-through hardware support allow to reduce average latency.
Limitations	Availability of special bridges with modular HSR support.

7.3.1.3.6 Station bus as ring and subrings with HSR

Figure 35 shows a three-level ring hierarchy with HSR rings and RedBoxes / QuadBoxes as coupling elements. The upper level is station-wide, the second voltage level specific, while the third is confined to a bay.

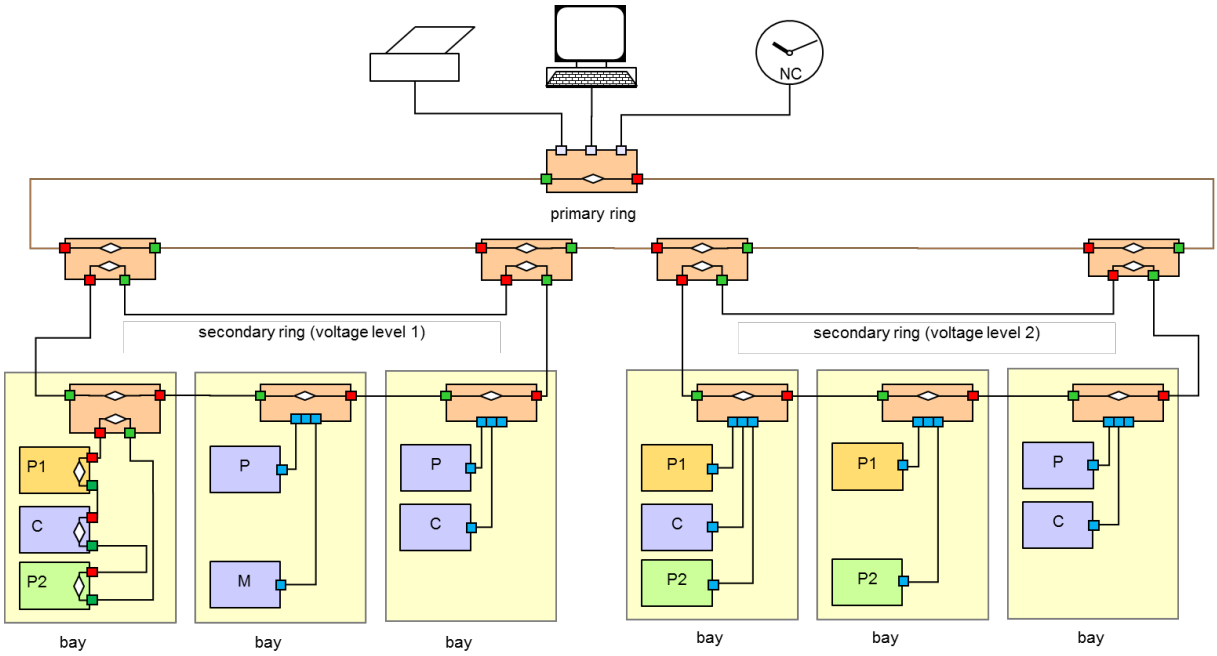


Figure 35 – Station bus as ring and subrings with HSR

The characteristics of this topology are summarized in Table 20.

Table 20 – Station bus as ring and subrings with HSR

Property	Characteristics
Simplicity	Topology suitable for large substations. Large number of QuadBoxes.
Traffic control	Allows segmentation of the traffic and confinement of traffic to a ring. Easy to ensure adequate bandwidth unless huge amount of traffic is forwarded to secondary rings or primary ring.
Latency	Relatively low latency if the number of DANHs is small.
Redundancy	Provides redundancy at all levels. It is advantageous to connect main 1 and main 2 to different QuadBoxes
Specificity	DANHs and RedBoxes are needed.
Limitations	Uses conventional architecture (one bridge per bay). Complicated engineering of the connection between the voltage levels.

7.3.2 Process bus and attachment of primary equipment

7.3.2.1 Process bus peculiarities

The process bus architectures are still under study and a variety of pilot projects exist. Therefore, 7.3.2 describes a number of possible architectures for the process bus with a higher level of detail than for the station bus.

The process bus structure can be quite different from the station bus due to the much higher traffic it has to carry. As 10.2 and Annex A show, a 100 Mbit/s Ethernet segment can only sustain about 6 devices producing SV traffic at 4 800 kHz transmission rate.

For the special case of busbar protection, the process bus follows the structure of the station bus: To detect busbar faults, the instantaneous value of the current of all bays is summed and this sum should normally be zero. The process bus interconnects all bays attached to the

same busbar and uses the same medium as the station bus or uses a parallel wiring. When the number of bays becomes large, the process bus must be segmented, and the different segments connected either hierarchically with a busbar protection unit at the hub, or horizontally, in which case the different zones preferably exchange phasors information rather than sampled values. This application is not considered further here since interoperability is not easy to achieve.

First the double busbar, single bay is described as an introduction, and then the more complex 1 ½ circuit breaker arrangement is detailed.

7.3.2.2 Double busbar arrangement

7.3.2.2.1 Double busbar bay without process bus (conventional)

Conventional bays use voltage and current transformers that usually have multiple, independent cores, each core being used for a separate function as shown in Figure 36. The conventional attachment is by direct cabling.

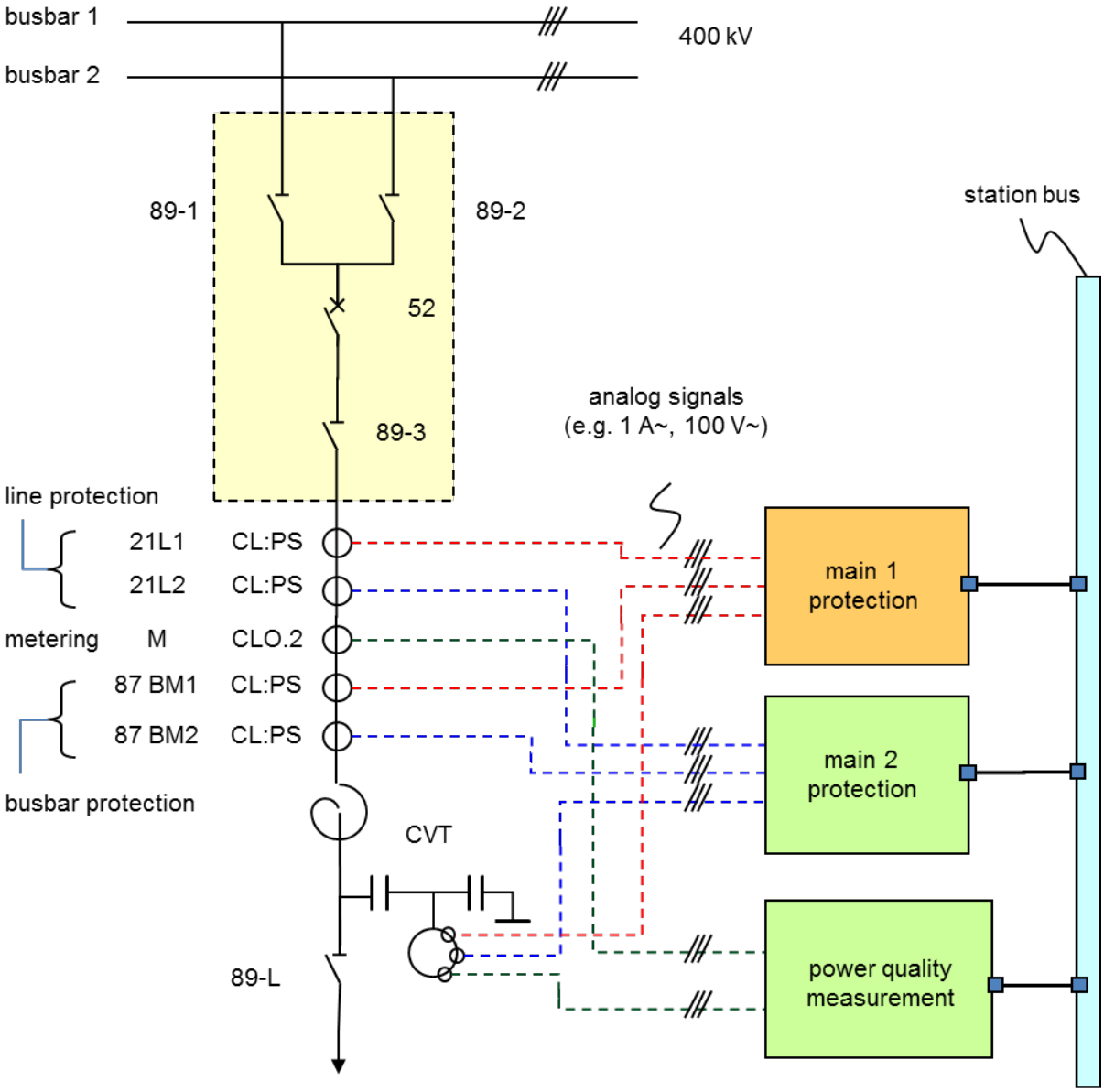


Figure 36 – Double busbar bay with directly attached sensors

7.3.2.2.2 Double busbar bay with merging units and main 1 / main 2 protection

To allow a retrofit from analog to digital measurement, IEC 61869-9 proposes to attach the analog output of the instrument transformers to SAMUs as shown in Figure 37.

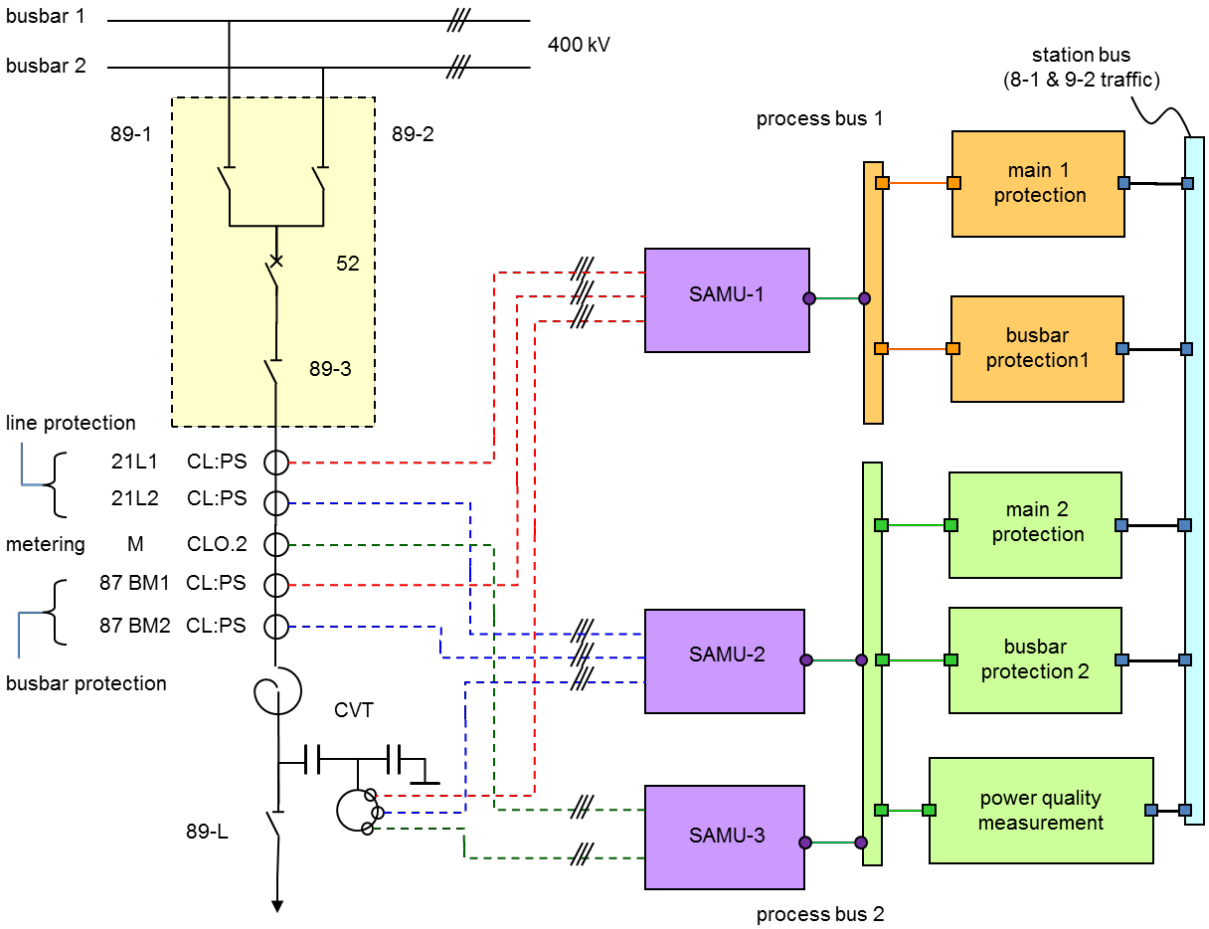


Figure 37 – Double busbar bay with SAMUs and process bus

There are two process busses, one for main 1 and one for main 2; the process buses themselves are not duplicated, their traffics are distinct.

Figure 37 shows the connection to the busbar protection, which is attached here to the station bus.

Due to the small number of ports, it is feasible to attach the SAMU directly to the IEDs, for instance with multiport SAMUs, thereby saving the bridges.

7.3.2.2.3 Double busbar bay with electronic current and voltage transformers

Electronic current transformers (ECTs) and electronic voltage transformers (EVTs) can be attached directly to the process bus, as shown in Figure 38 if they are PIAs.

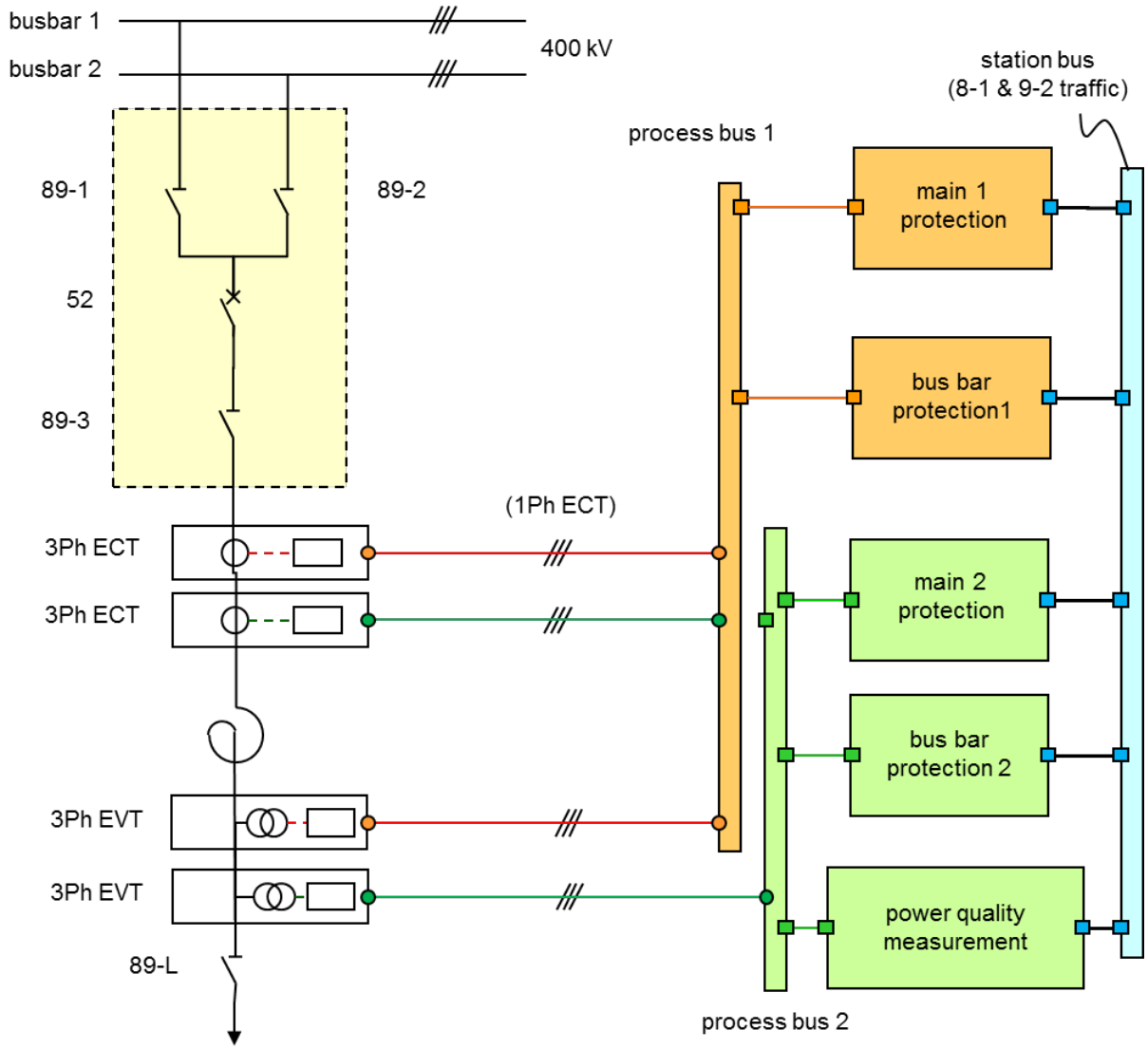


Figure 38 – Double busbar bay with ECT/EVTs and process bus

If three-phase EVT/ECTs are used, the number of connections to the IEDs is small, so it would be feasible to move the bridge into the IED. If single phase attachment is used, the number of PIAs connected to the process bus is six per bridge.

7.3.2.3 One-and a half circuit breaker instrument attachment

7.3.2.3.1 1 ½ CB conventional IED attachment (no process bus, no protection redundancy)

The reference is a 1 ½ circuit breaker diameter (2 lines). This configuration is considered as the worst case for the attachment of instrument transformers.

The conventional protection consists of two line protection and one busbar protection. Due to the coupling, IEDs need the current and voltage values of two feeders. The control signals (trip) of the circuit breakers are not shown.

Figure 39 shows the structure for a non-redundant protection to explain the basic data flows. For a fair comparison with the former and later topologies, the measurement cores should be detailed and the IEDs should be duplicated, as in Figure 40.

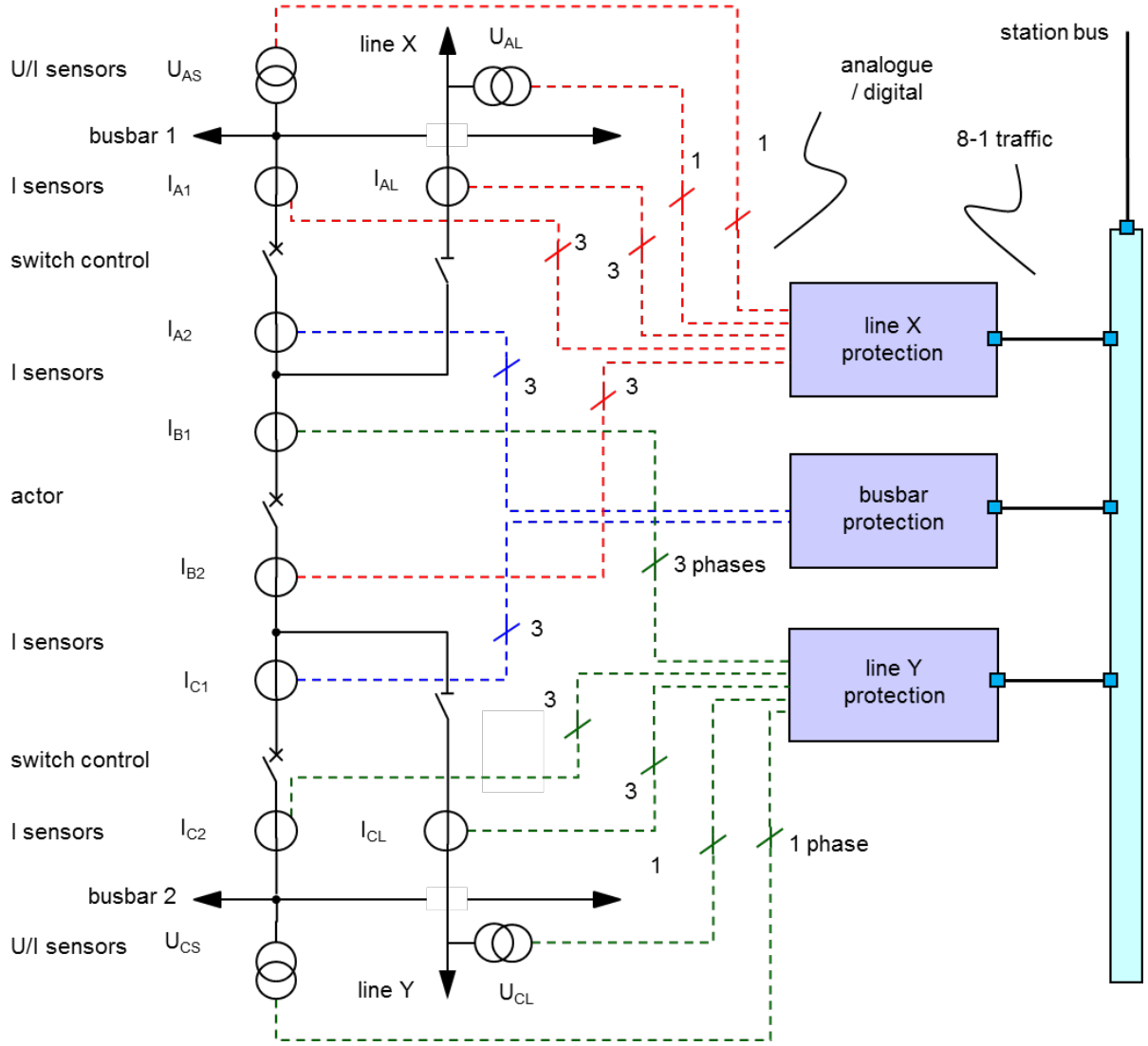


Figure 39 – 1 ½ CB diameter with conventional, non-redundant attachment

7.3.2.3.2 1 ½ CB SAMUs with main 1 & main 2 redundancy

To attach legacy instrument transformers, SAMUs can be attached to a different process bus for main 1 and main 2 protections (see Figure 40).

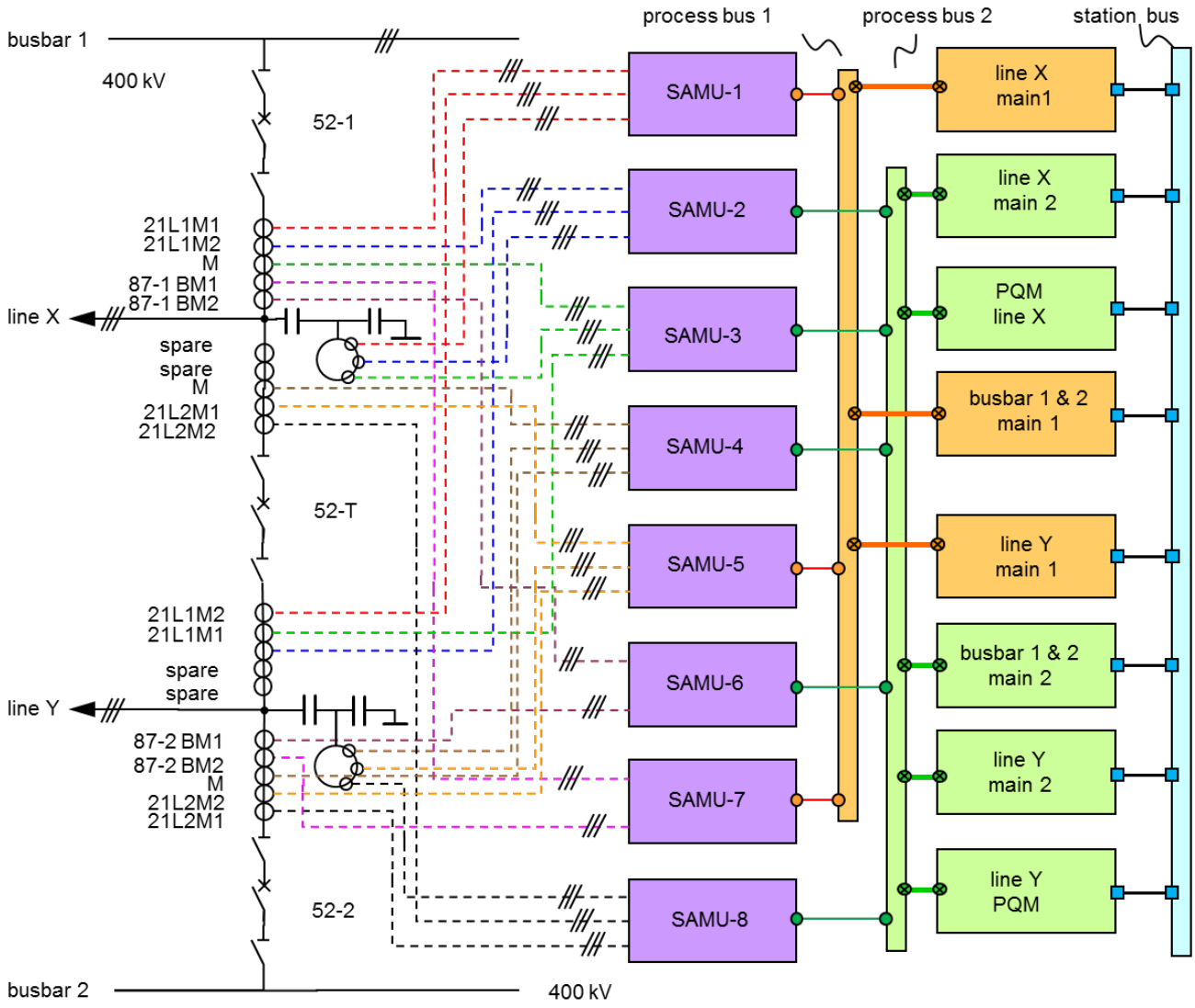


Figure 40 – 1 ½ CB diameter with SAMUs and process bus

NOTE If there were one SAMU per IED, there would be no need for busses or bridges.

7.3.2.3.3 1 ½ CB with ECT/EVTs and main 1 & main 2 redundancy

Figure 41 shows the arrangement when Electronic Instrument Transformers are used. The wiring with respect to Figure 40 is simplified, Electronic Instrument Transformers are duplicated for redundancy.

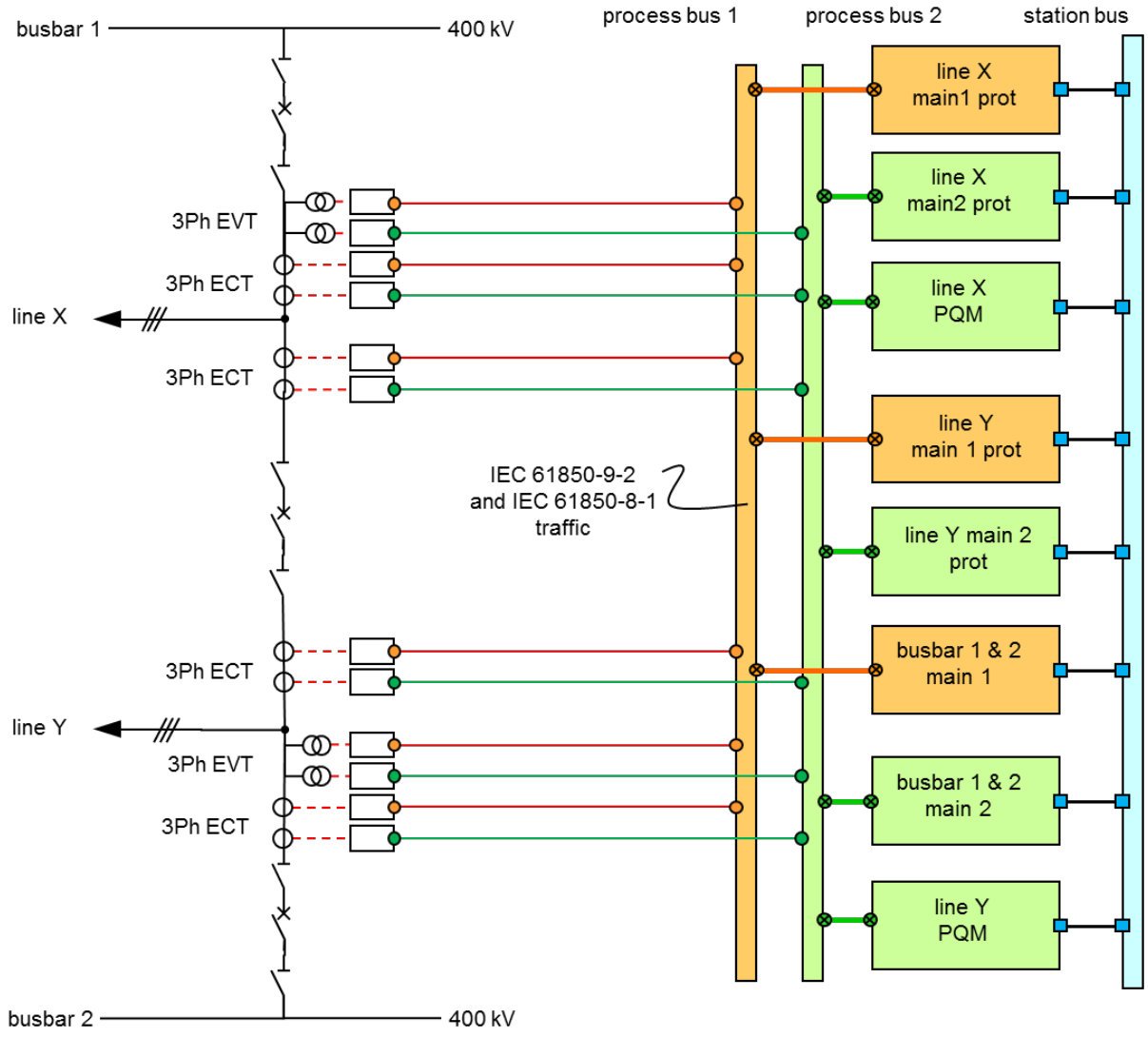
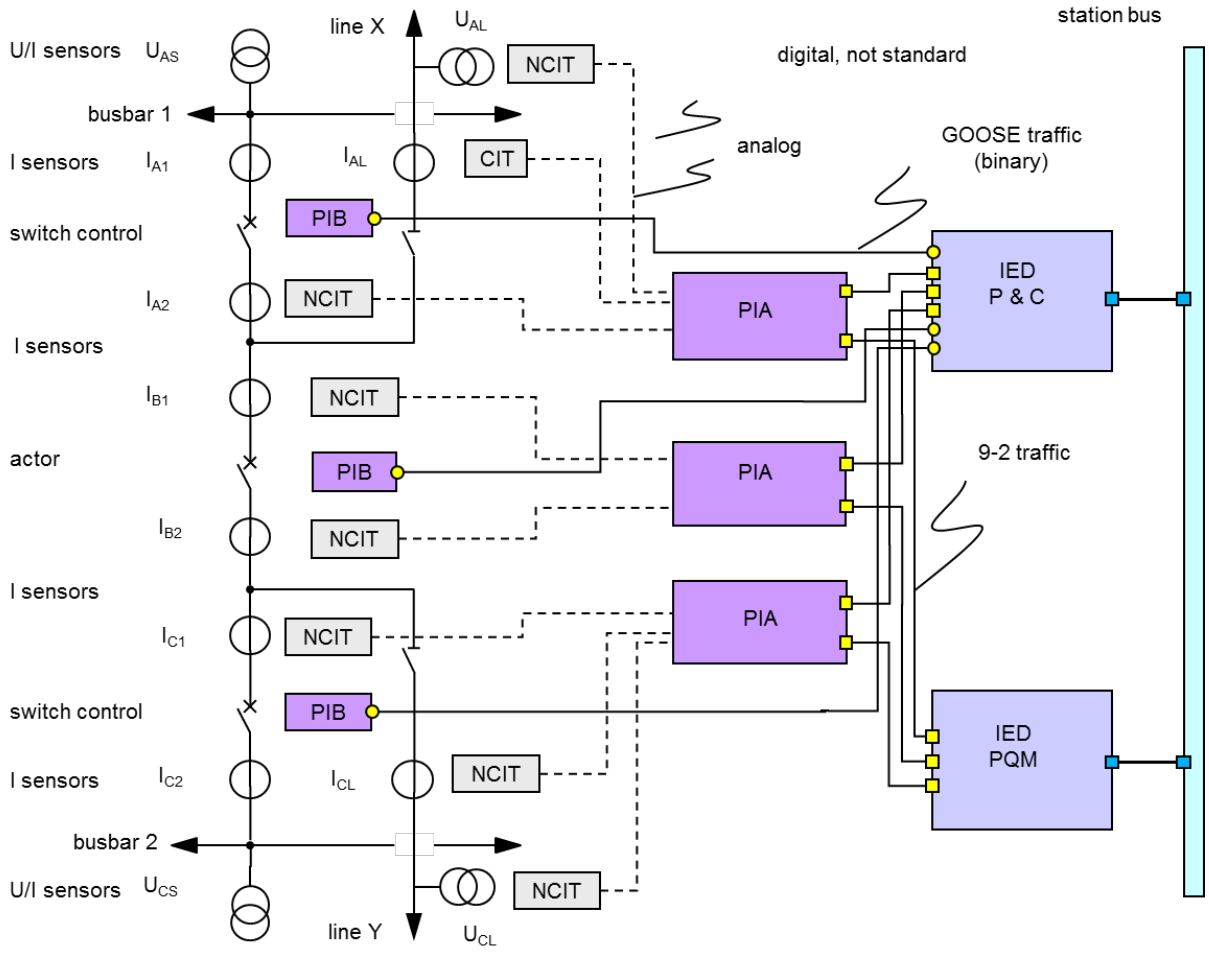


Figure 41 – 1 ½ CB diameter with ECT/EVT and process bus

7.3.2.3.4 1 ½ CB process bus as star with PI

The simplest version of the process bus is a direct connection of PIs to the IEDs, as shown in Figure 42. Conventional (CIT) as well as non-conventional instrument transformers (NCIT) are attached to the PIAs. The PIAs have a process bus output connected directly to the IEDs, which serve as bridge. The PIAs are located close to the primary technology and convert analogue signals from the current and voltage sensors into SV frames. PIBs understand and generate GOOSE frames. No traffic expected from PIA to PIA and little traffic from PIB to PIB.



Key

CIT Conventional instrument transformer

NCIT Non-conventional instrument transformer

PIA Process Interface, Analog (voltage and current measurement)

PIB Process Interface, Binary (circuit breaker and disconnector control)

Figure 42 – Process bus as connection of PIA and PIB (non-redundant protection)

The characteristics of this topology are summarized in Table 21.

Table 21 – Process bus as connection of PIA and PIB

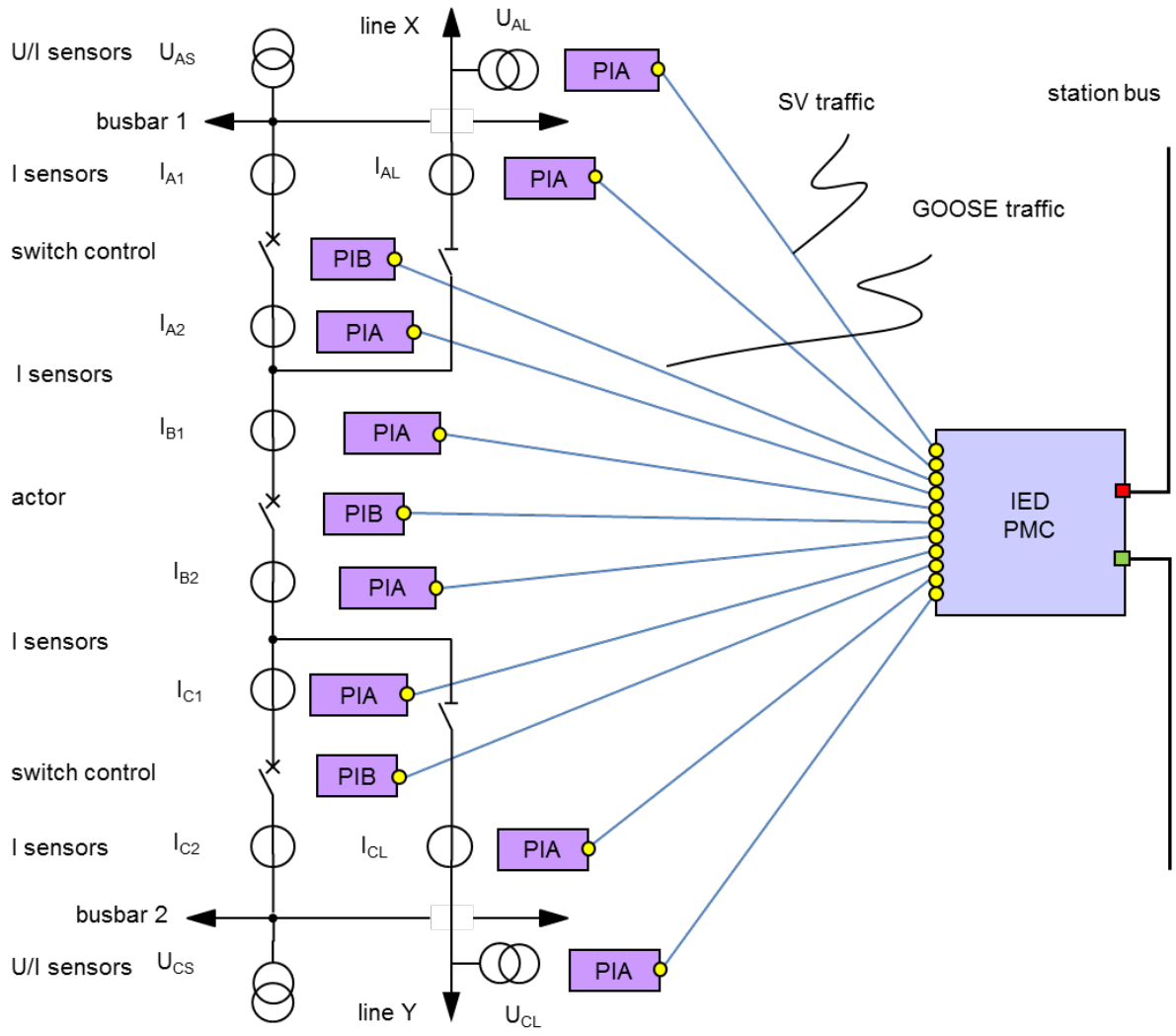
Property	Characteristics
Simplicity	Simple topology. Simple retrofit, since the current and voltage transformers can be replaced by non-conventional instrument transformers without change of the interface. With three-phase attachment, the number of ports in the IEDs is small and it is feasible to put the bridges into the IEDs, reducing costs.
Traffic control	Allows 100 Mbit/s links between MUs and IEDs. Easy to evaluate bandwidth.
Latency	Low latency. No bridges exist between process-level devices and bay-level devices.
Redundancy	No redundancy.
Specificity	IEDs needed with a large number of ports and high processing power. All process interfaces (PIA, PIB) are specific.

Property	Characteristics
Limitations	Physical location of devices on the primary technology dictates the topology. Number of devices limited by the SV traffic. Single phase devices require a large number of ports.

7.3.2.3.5 1 ½ CB process bus as single star (point-to-point)

The topology can be simplified if the PIAs and PIBs can be integrated into the instrument transformers and moved close to the primary technology (e.g. directly mounted on a circuit breaker).

As shown in Figure 43, if IED is a combined Protection, Measurement and Control (PMC) device, a PI needs only a single link to that IED and the process bus is reduced to multiple point-to-point links. The IED performs the bridge function, since there is little horizontal traffic between the PIs.



Key

PMC Protection, Measurement and Control IED

Figure 43 – Process bus as single star (not redundant protection)

The characteristics of this topology are summarized in Table 22.

Table 22 – Process bus as single star

Property	Characteristics
Simplicity	Simple topology. No need for standalone bridges in the process bus.
Traffic control	Easy to ensure adequate bandwidth. Allows 100 Mbit/s links between PIs and IEDs. The product of the number of PIs and the sampling rate is only limited by the capacity of the IEDs to absorb the traffic.
Latency	Very low latency. No bridges exist between process-level devices and bay-level devices.
Redundancy	No redundancy.
Specificity	IED needs a large number of Ethernet ports and becomes quite complex. Only one IED per bay, protection and control merged into the same device (not always accepted). IED must perform the function of a bridge and filter multicast traffic. If PIs are simple devices, the IED must act as their proxy, which increases complexity.
Limitations	The number of ports per IED is limited. Connection of single-phase devices is difficult. Acceptance of PMC devices is limited, since some prefer independent devices for protection, measurement and control.

7.3.2.3.6 1 ½ CB process bus as dual star (Main 1 and Main 2)

This topology differs from 7.3.2.3.6 by the separation of Main 1 protection and Main 2 protection into independent channels connected to two separate redundant IEDs, as shown in Figure 44.

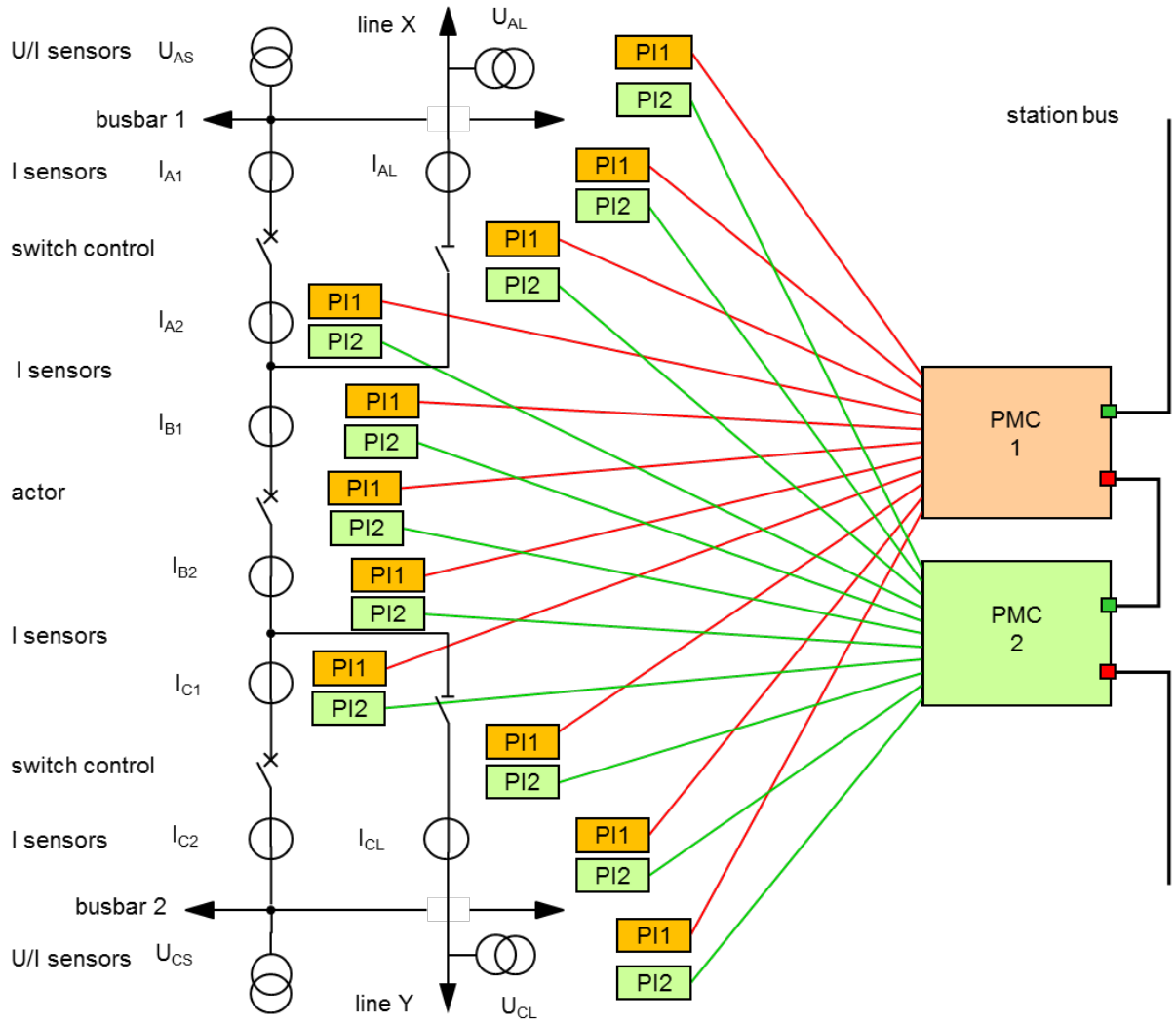


Figure 44 – Process bus as dual star

The characteristics of this topology are summarized in Table 23.

Table 23 – Process bus as dual star

Property	Characteristics
Simplicity	Same as 7.3.2.3.5.
Traffic control	Same as 7.3.2.3.5.
Latency	Same as 7.3.2.3.5.
Redundancy	Full, independent redundancy at the application level.
Specificity	Same as 7.3.2.3.5, application-specific failover for control.
Limitations	Same as 7.3.2.3.5. Communication between process bus1 and process bus 2 must be carefully engineered, since it involves communication between PMC1 and PMC2.

7.3.2.3.7 1 ½ CB process bus as single bridge

When customer do not accept PMCs and when the number of ports on the IEDs becomes large, a bridge structure is advantageous, as shown in Figure 45. The process bus is restricted to the connection between the protection and control devices and the PIOs. The SCADA access the PI devices directly or otherwise using the IEDs as proxies.

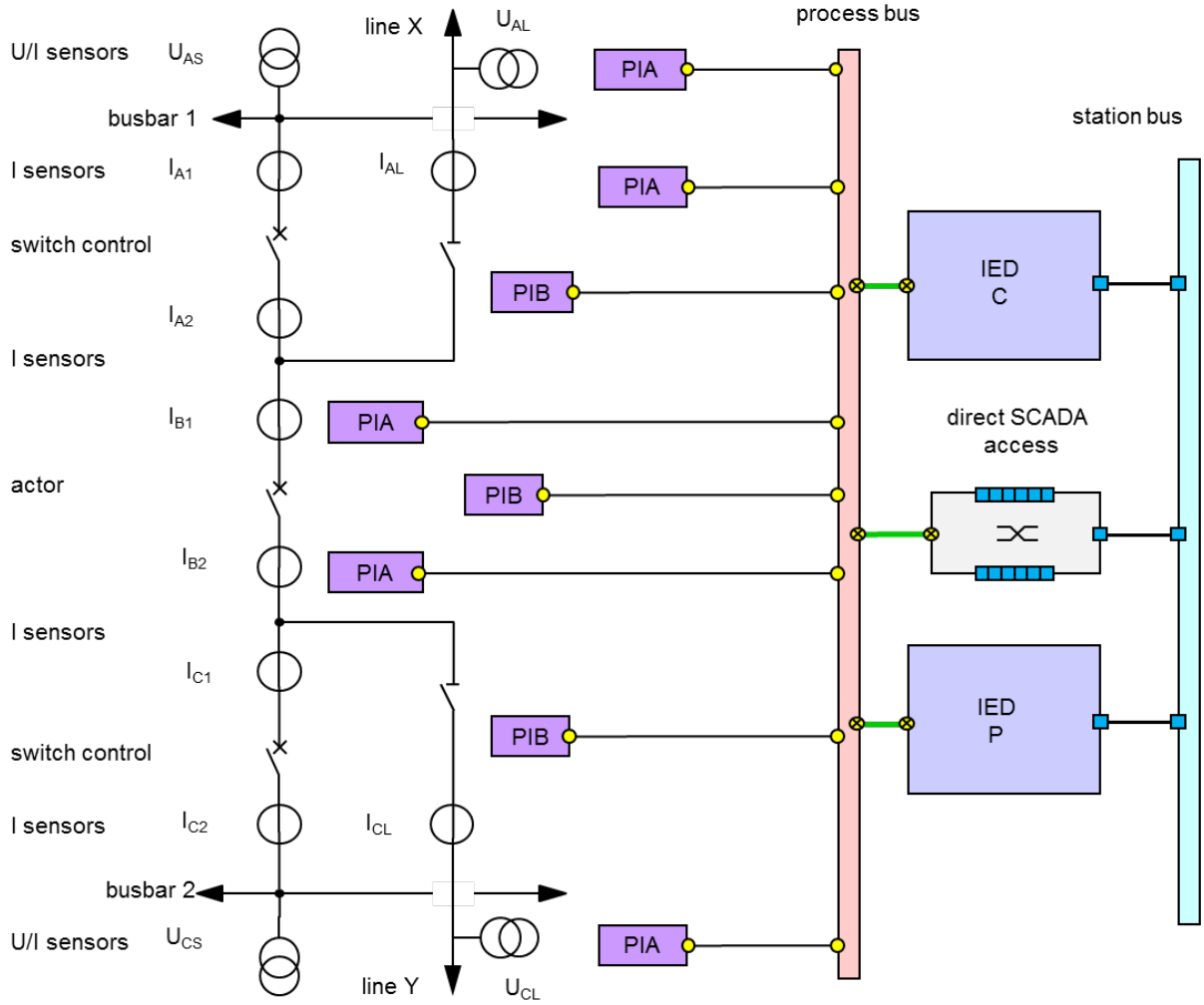


Figure 45 – Process bus as a single bridge (no protection redundancy)

The characteristics of this topology are summarized in Table 24.

Table 24 – Process bus as single bridge

Property	Characteristics
Simplicity	Simple topology, a single bridge is sufficient. Bridge allows a variable number of ports.
Traffic control	Easy to evaluate bandwidth. Since the bulk of traffic is from the PIs to the IEDs, PIs can be attached with 100 Mbit/s links if multicast is filtered properly. The product of the number of PIs and the sampling rate is limited by the bridge's capacity and if this one is sufficient, by the capacity of the IEDs to absorb the traffic. The bridge can connect process bus and station bus if proper multicast filtering is applied.
Latency	Low latency – one single bridge hop.
Redundancy	No redundancy – the bridge is a single point of failure (but this can be addressed with a Main 1 / Main 2 scheme as 7.3.2.3.8 shows).
Specificity	PIAs and PIBs are specific to the primary technology. If the IEDs are acting as their proxies, they must be adapted.
Limitations	In case of significant number of PIs, especially with single-phase attachment of PIAs, IEDs require 1 Gbit/s connection. The multicast filtering must be effective during initialization and / or recovery. If PIs are simple devices, IEDs must act as their proxy, which increases the complexity.

7.3.2.3.8 1 ½ CB process bus as dual bridge (Main 1 and Main 2)

This topology is similar to the one described 7.3.2 with the difference that Main 1 protection and Main 2 protection each have their own network, bridge and sensors as shown in Figure 46. With duplicated protection, there is no incentive to duplicate each process bus.

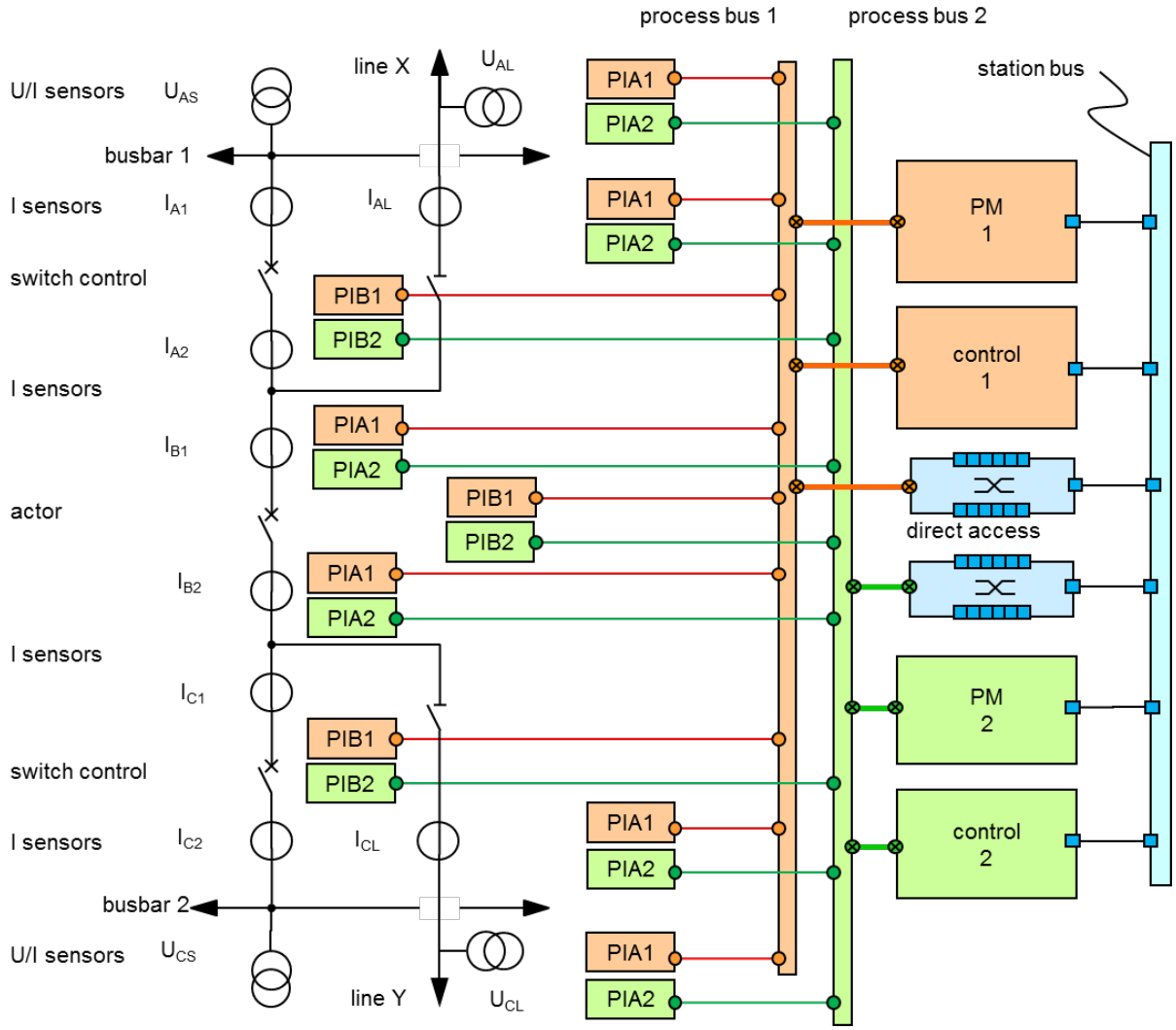


Figure 46 – Process bus as separated LANs for main 1 and main 2

The characteristics of this topology are summarized in Table 25.

Table 25 – Process bus as separated LANs

Property	Characteristics
Simplicity	Duplicates the topology of 7.3.2.3.7. Duplication of sensors, duplication of bridges and links
Traffic control	Same as 7.3.2.3.7.
Latency	Same as 7.3.2.3.7.
Redundancy	Complete independence of Main 1 and Main 2 protection ensures application-level availability.
Specificity	Same as 7.3.2.3.7.
Limitations	Connection of the LAN1 and LAN2 traffic and failover operation are difficult to engineer, since this is application-specific.

7.3.2.3.9 Process bus as single ring

The process bus can be built as an HSR ring, as shown in Figure 47. In this case, all PI units support the IEC 61850-9-2 protocol. A process bus HSR ring can be connected to the station bus by an IED or by an HSR RedBox.

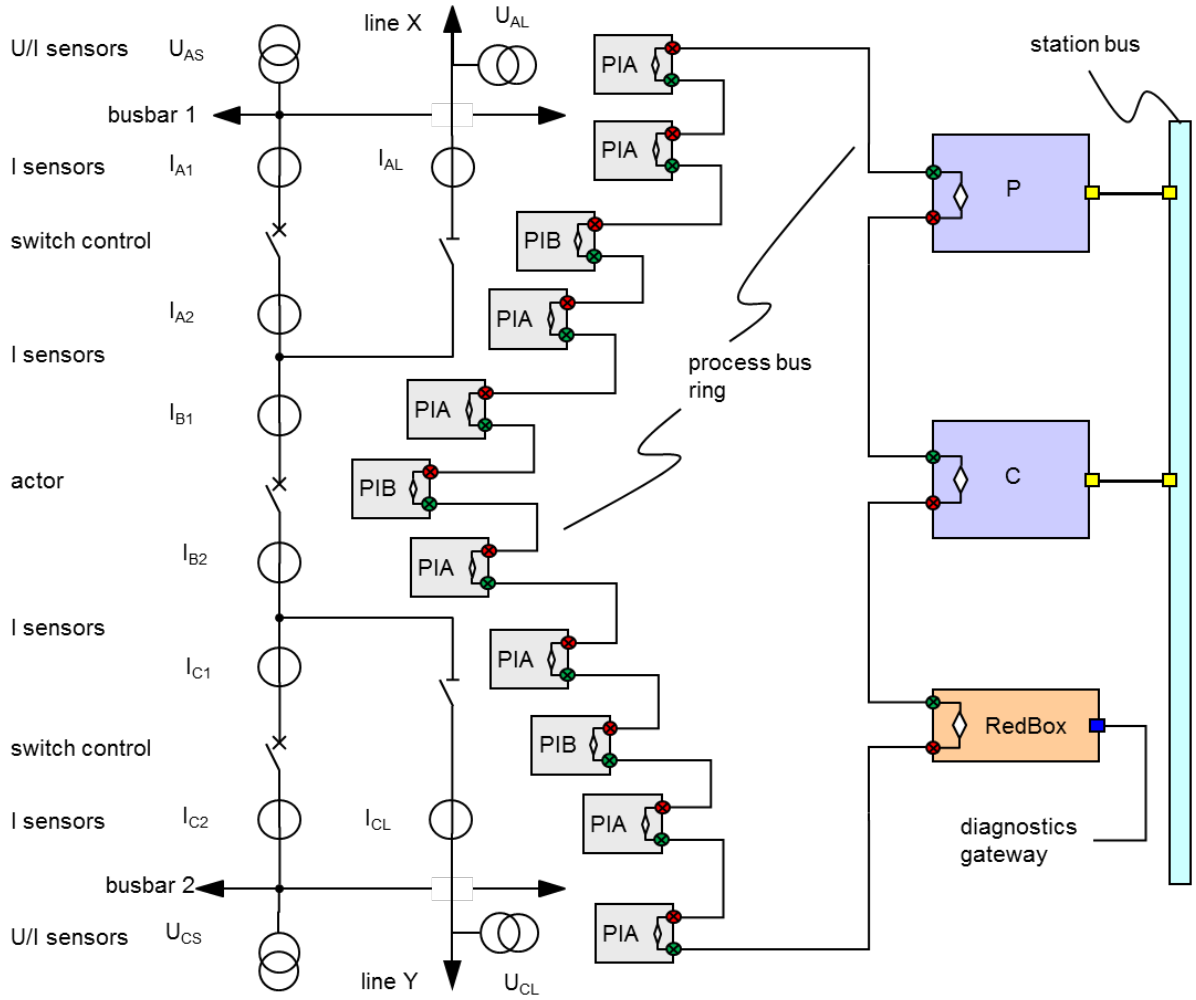


Figure 47 – Process bus as ring of HSR nodes

The characteristics of this topology are summarized in Table 26.

Table 26 – Process bus as simple ring

Property	Characteristics
Simplicity	Simple topology. No bridges.
Traffic control	Difficult to evaluate bandwidth. The product of the number of PIs and the sampling rate limits the number of PIs or MUs in the ring, since the whole traffic flows through each device, see 10.2. To comply with the sampling rate of UCA 9-2LE, some 6 devices are supported at 100 Mbit/s; otherwise, a 1 Gbit/s connection is needed, except if the sampling rate is lowered.
Latency	Latency increases with the number of PIs in the ring.
Redundancy	Provides redundancy with only one additional link.
Specificity	Doubly attached IEDs and PIs needed. IEDs must perform the function of a bridge and do multicast filtering. If PIs do not support MMS, the IED must act as their proxy, which increases its complexity.
Limitations	The number of devices in the ring is limited by the SV traffic. Careful design must exclude common mode failures such as malfunctioning devices producing high traffic.

7.3.3 Station bus and process bus connection

7.3.3.1 Separating versus connecting the station bus and the process bus

The main reasons to separate the station bus and the process bus are as follows.

- Except in very small substations, the station bus is unable to carry the sum of the SV traffic of all process busses connected to it.
- Segmenting the network into multiple redundancy domains increases the resiliency of the network. A ring tolerates one failure, but not a second failure, which becomes more probable as the number of devices and links in the ring increases. If the network is separated into several rings, each ring being its own redundancy domain, a second failure won't affect the other rings.

Station bus and process bus can be separated physically or logically:

- Physical separation means that there exist two separate communication networks with no connectivity. The process bus becomes a private domain of some IEDs and the SCADA cannot access directly the process bus devices. To give the SCADA some control over these devices, an IED can implement a Proxy Logical Node which maps the data model of process bus devices to IEC 61850-7-4:2010 objects. This solution is useful in case of merging units and process interfaces with no MMS stack but also increases the complexity of the proxy IED. Pros and Cons are summarized in Table 27.

Table 27 – Advantages and drawbacks of physical separation

Advantages	Drawbacks
Fail-independence Process bus devices can be very simple	Proxy IED needed. No interoperable access to download firmware. Difficult to introduce a redundant proxy. No standardized procedure if one proxy represents several devices or several proxies exist.

- Logical separation means that the process bus and the station bus belong to one communication network. Bridges filter the traffic between station bus and process bus domains, allowing some devices to exchange specific traffic between the domains. A bridge is needed when GOOSE or SV messages are to be exchanged. A bridge with multicast filtering ability or a layer 3 router separates the process bus and station bus domains and by default prevents GOOSE and SV messages from transiting, except through a protocol gateway. The layer 3 solution requires that all process bus devices are capable of layer 3 communication, which rules out simple PIs. Pros and Cons are summarized in Table 28.

Table 28 – Advantages and drawbacks of logical separation

Advantages	Drawbacks
Simpler IED Operates also when IED is down	Process bus devices must implement an IP stack Process bus devices and bridges or routers need careful configuration

7.3.3.2 Station bus ring and process bus with point-to-point links

The process bus can be implemented as multiple point-to-point links as shown in Figure 48. One MU with multiple ports can be connected to several IEDs, which allows the reception by multiple IEDs of the SV data sent by each MU. The MUs must not implement an internal bridge, since this would create loops.

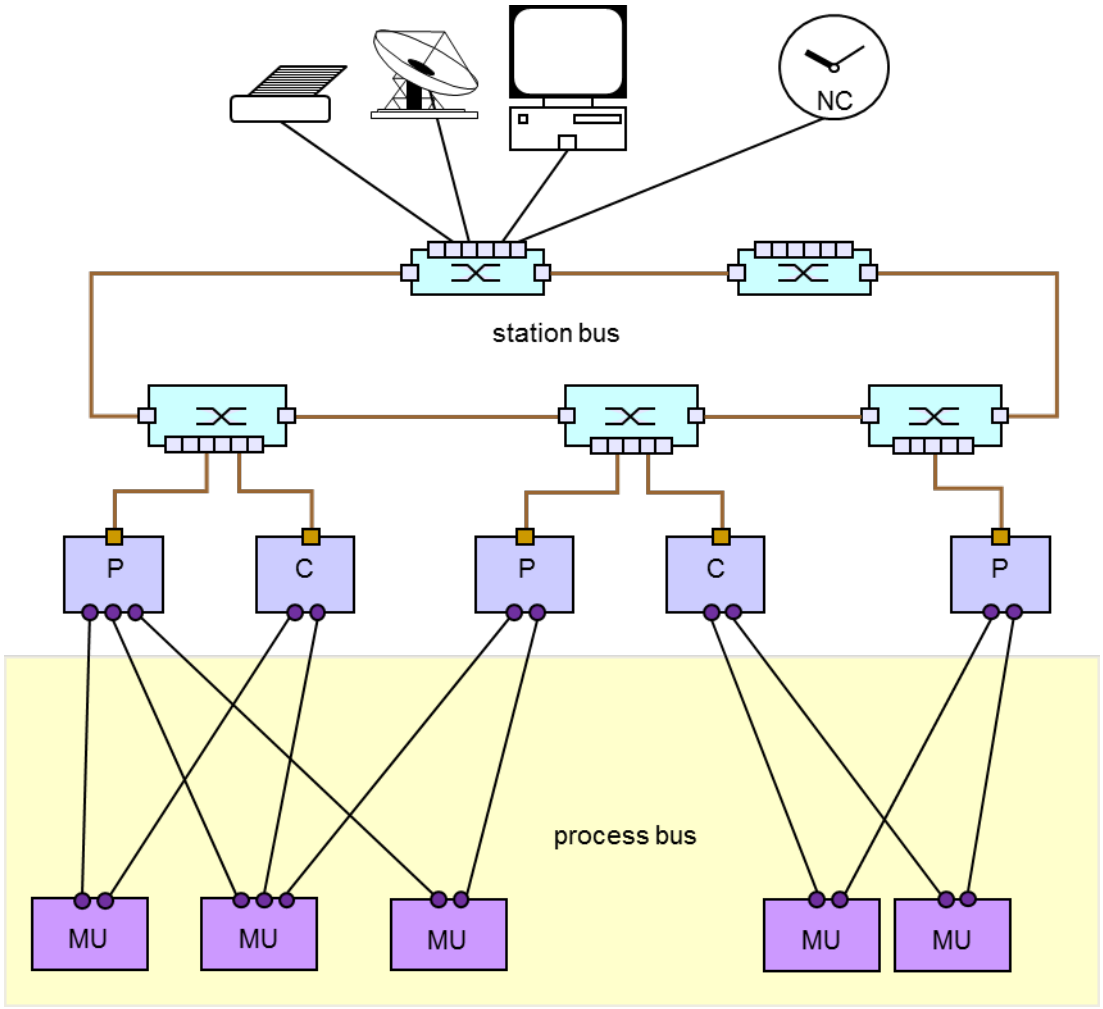


Figure 48 – Process bus as star to merging units and station bus as RSTP ring

The characteristics of this topology are summarized in Table 29.

Table 29 – Process bus as star to merging units

Property	Characteristics
Simplicity	Slightly complicated topology. Point-to-point connections require more links.
Traffic control	Easy to ensure adequate bandwidth. 100 Mbit/s links are sufficient for attaching MUs. High performance even in very large applications since point-to-point links are deterministic. Not sensitive to sampling rate.
Latency	Very low latency between process-level devices and bay-level devices.
Redundancy	If needed, the redundancy of the process bus can be changed by connecting additional MUs or IEDs to them with multiple point-to-point links. However, MUs or IEDs need to have more interfaces of multiple point-to-point links. In the station bus, one path redundancy is provided by the ring topology.
Specificity	The number of ports and point-to-point links is limited, which makes such topology of limited flexibility. Needs multiport IEDs and MUs.
Limitations	Number of connections limited by the number of ports.

7.3.3.3 Separated station bus and process bus rings

This is a use case that combines a station bus network and a process bus network as rings.

Separation of station bus and process bus rings avoids flooding the station bus with high traffic generated by SV publishers such as merging units. The IEDs have separate ports for station bus and for process bus. The internal implementation of both interfaces in each IED is vendor specific. The two interfaces of the IED must not bridge frames, since this would create loops in the network. If they would bridge the bus – assuming they implement RSTP on both the station bus and/or process bus side, these integrated bridges would couple the process bus and the station bus rings and increase reconfiguration time possibly beyond tolerable values.

This network setup effectively separates the station bus and process bus into two completely separate physical networks. To enable a reach-through (if needed) from the SCADA, engineering or other layer 3 application to devices on the process bus, e.g. the MUs, an IP router connects the two layer 2 networks through a layer 3 connection. In Figure 49, an IP router is included into the topology design via dotted lines. The dotted lines represent the connection of the router into the two LANs. These connections and the router can be designed redundantly (utilizing e.g. the Virtual Router Redundancy Protocol VRRP) to provide fault tolerance, if desired. Alternatively, multicast filtering bridges can be used.

station bus: RSTP is recommended.

process bus: Use HSR, either connect nodes via RedBoxes or use dedicated HSR client interfaces on the process bus side of the protection/control IEDs. Figure 50 shows a setup with HSR RedBoxes with integrated bridges. The merging units and protection/control units are connected to the HSR ring with single, non-redundant links. To enable link redundancy for a MU, the MU must implement the HSR interface and must be integrated directly into the ring.

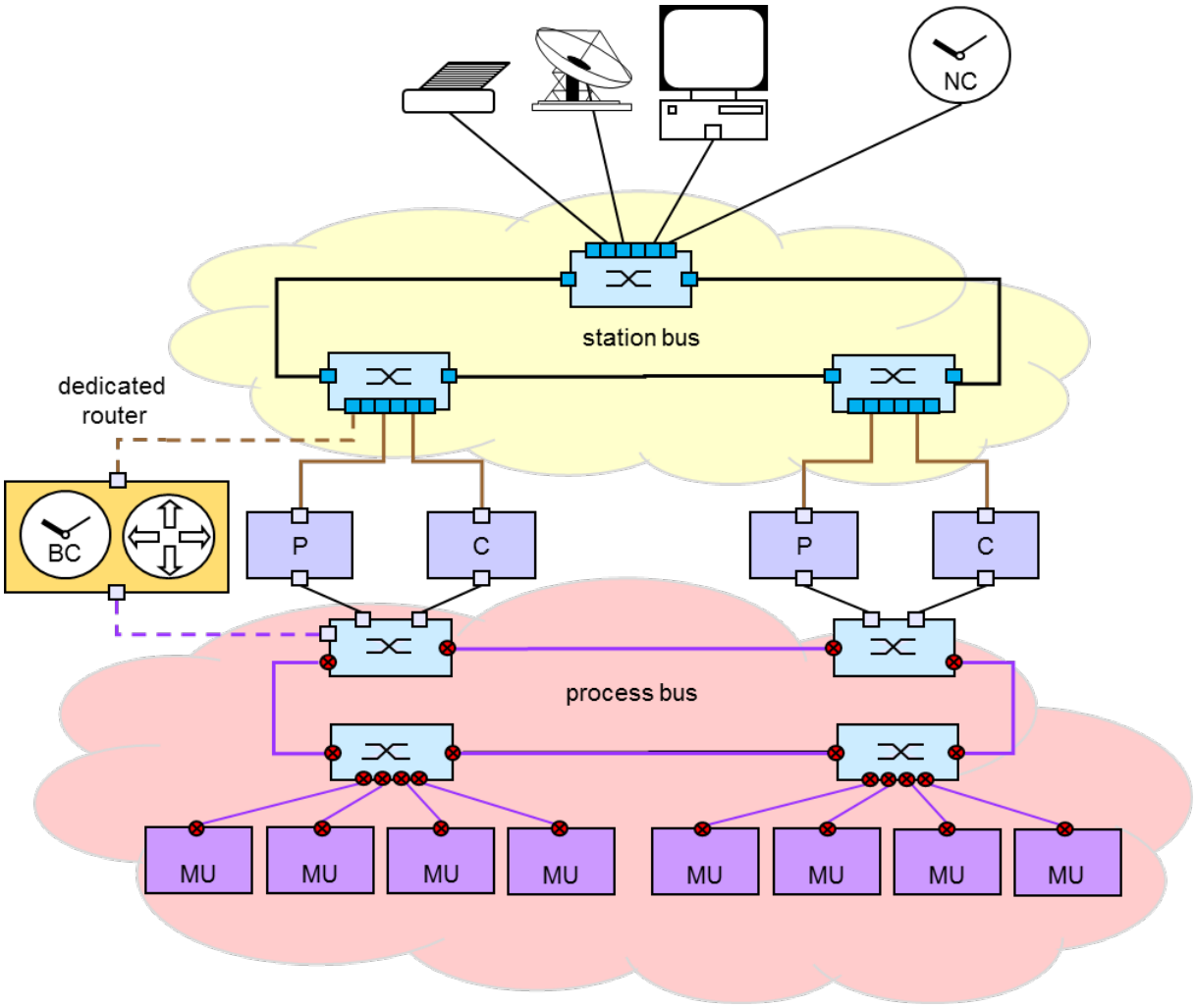


Figure 49 – Station bus and process bus as rings connected by a router

The characteristics of this topology are summarized in Table 30.

Table 30 – Connection of station bus to process bus by routers

Property	Characteristics
Traffic control	Difficult to ensure adequate bandwidth in the process bus because all traffic is shared in the ring. In the station bus, easy to ensure adequate bandwidth unless huge amount of traffic such as SV traffic are forwarded between bridges.
Latency	Low latency if the number of bridges in series in the ring is small.
Redundancy	One path redundancy in the rings of the process bus and the station bus. However, application-level redundancy needs redundant MUs, Circuit Breaker IEDs and IEDs.
Simplicity	Moderate complexity. Some bridges are needed for constructing rings.
Specificity	IEDs equipped with a port for process bus and a port for station bus are needed. MUs are needed. Needs a router to inter-connect both levels. (Multicast filtering can produce the same level of features)
Others	Supports differential protection schema (2 to N bays). Allows transmitting the voltage SV to many bays.

7.3.3.4 Combined process bus and station bus by coupled HSR rings

The basic structure from 7.3.3.4 is retained, with the exception that this topology is specifically designed for HSR usage both in the station bus and in the process bus. The process bus HSR rings and the station bus HSR ring are interconnected via QuadBoxes in a redundant manner.

- Station bus network: For attachment of the DANs on the station bus, HSR and PRP can be used. Depending on the client interface of e.g. the NTP server in Figure 50, the connecting Bridge/RedBox components have to be either RedBoxes in HSR mode of operation or in PRP mode of operation. The SANs can be connected to the RedBoxes. Choosing HSR attachments for the DANs on the station level provides no drawback, only the advantage of flexibility of usage, either as PRP style node or HSR style node.
- Process bus network: Only HSR nodes are present on the process bus HSR rings. The QuadBoxes interconnecting the individual rings must implement multicast filters to prevent unnecessary flooding of traffic to the whole network.

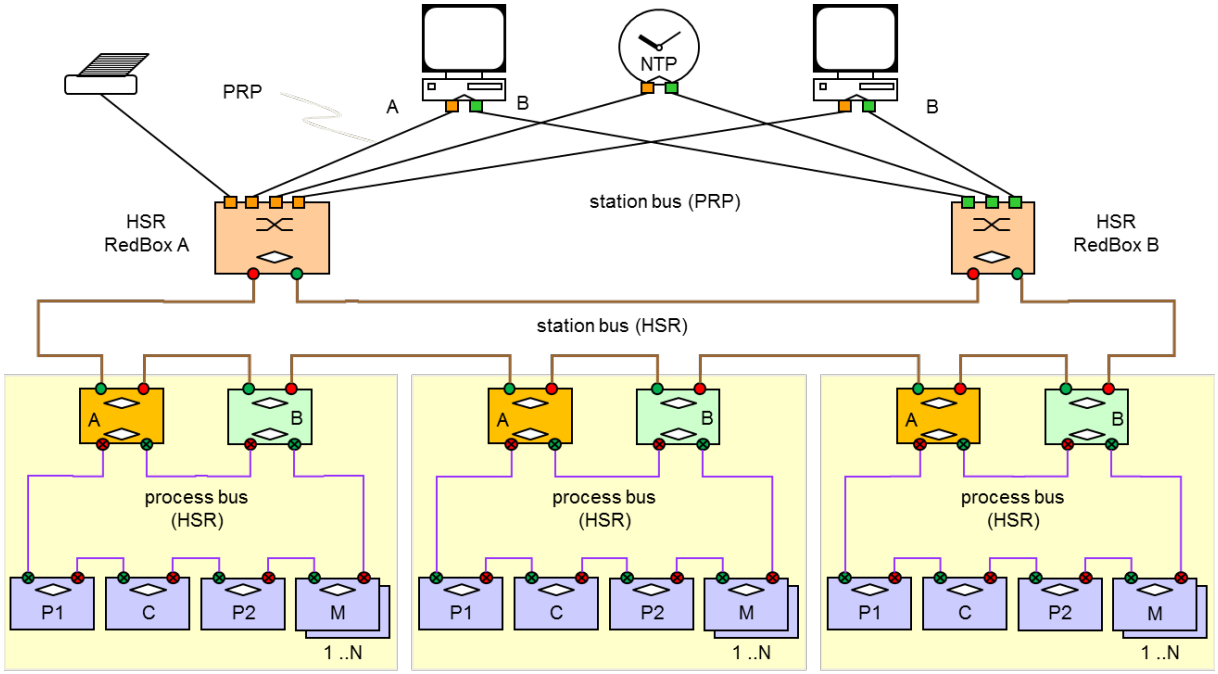


Figure 50 – Station bus ring and process bus ring with HSR

NOTE SCADA do not need seamless redundancy; in Figure 50 dual links (warm standby) are shown.

The HSR bridge is combined with an integrated RedBox, working in either PRP A/B or HSR mode of operation, depending on the network interfaces on the client devices on the network, depicted as SCADA and NTP devices in this example.

For this topology to work efficiently, it has to ensure that SV traffic from the process bus is not unnecessarily propagated into the station bus. This can be done with multicast filtering on the QuadBoxes.

The characteristics of this topology are summarized in Table 31.

Table 31 – Connection of station bus to process bus by RedBoxes

Property	Characteristics
Traffic control	In HSR rings, to ensure adequate bandwidth multicast filtering is needed. In PRP network of station bus, easy to ensure adequate bandwidth.
Latency	Relatively high latency unless the number of nodes in the ring are small.
Redundancy	One path redundancy is provided by HSR or PRP.
Simplicity	Slightly simple topology. The number of QuadBoxes is determined by twice the number of bays.
Specificity	DANs are needed. QuadBoxes are needed. For connecting SANs to the ring, RedBoxes are required. Multicast filtering allows to separate the GOOSE and SV traffic.
Others	Fits mainly the differential protection scheme (2 to N bays). Fits also the case for transmitting the voltage SV to many bays.

7.3.3.5 Hierarchy with different redundancy principles

This topology shows a combination of a station bus and process bus network, but it could also be a second-level station bus.

High availability throughout both the station and the process bus network is achieved using a double LAN network on the station bus and a ring of bridging end nodes according to the HSR protocol (IEC 62439-3:2012) on the process bus, as shown in Figure 51.

The redundant networks A and B may be closed into a ring structure using RSTP (but the added complexity is not justified). They are connected to the rings through redundancy boxes working in PRP “A” and “B” mode.

NOTE With the RedBoxes connecting the station bus and the process bus networks working in HSR-PRP mode, the looping of frames originating from a SAN in either LAN A or LAN B is prevented through the configuration of the HSR-PRP RedBoxes as a coupled RedBox pair. Frames injected into the ring from the station bus via RedBox A will not be reflected back to the station bus via RedBox B and vice-versa.

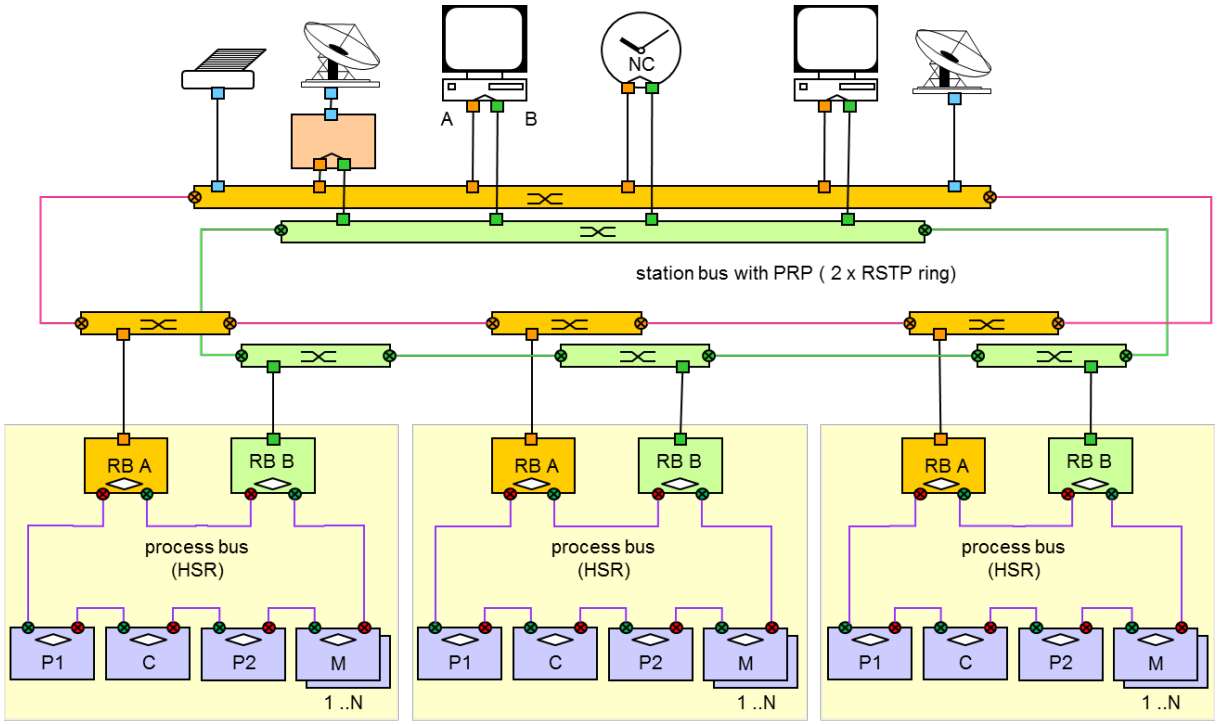


Figure 51 – Station bus as dual PRP ring and process bus as HSR ring

Variants: The LAN A and LAN B can also be merged into one HSR ring, as shown in Figure 50.

The characteristics of this topology are summarized in Table 32.

Table 32 – Connection of duplicated station bus to process bus by RedBoxes

Property	Characteristics
Simplicity	Simple topology. One link plus one in the process bus, no bridges. Two RedBoxes per bay. For the station bus, PRP can be used.
Traffic control	Adequate bandwidth multicast filtering in the RedBoxes is needed to prevent the SV traffic from the process bus from being unnecessarily injected into the station bus. The RedBoxes operate in “HSR-PRP” mode to prevent loops originating from single attached nodes in the station bus rings.
Latency	Relatively high latency if the number of nodes in the ring is small.
Redundancy	In the case of DANs, one path redundancy is provided.
Specificity	For redundancy, nodes need to have two Ethernet ports being compliant with HSR protocol or PRP protocol. RedBoxes are needed.
Limitations	Sharing of sensor values require a signification portion of the process bus traffic.

8 Addressing in the substation

8.1 Network IP address plan for substations

8.1.1 General structure

Within a substation, only private IP addresses are used. This allows to set up an address plan and assigns the IP addresses according to the same scheme in all substations.

The allocation of IP addresses should take place after assignment of names to primary objects according to IEC 81346. It is the first measure to organize and partition the network. The wiring of the devices according to the structures given in Clause 7 is deduced from this network structure.

The scheme proposed here does not apply to all topologies.

The IP addresses and IP masks are a property of each device. In case of device failure, the replacement device receives the same IP address.

The IP addresses are registered in the SCD and in the CIDs; they should not be allocated dynamically.

The IP address should be structured to reflect the physical plant as follows:

172.NET.BAY.DEVICE

NOTE Methods such as DHCP and Domain Name Servers are widely used to assign IP addresses dynamically, address the devices by their names, and deduce their IP address from the name for further data exchanges. Dynamic IP address assignment is however not used in IEC 61850 for several reasons:

a) IEDs are servers. DHCP applies to clients, not to servers to which administrators assign a fixed IP address, such as printers or data storages. DHCP requires a Domain Name Server. There is however no unique identifier or URL for IEDs.

b) IEC 61850's SCD assigns a fixed IP address to the devices. This allows finding a device according to its location. It also facilitates debugging and replacement of failed devices.

c) An IP address plan such as suggested in this document would not be possible with dynamic IP address assignment. It allows the maintenance staff to locate the devices.

d) Substation automation is not dynamic in nature; configuration changes are seldom and must be planed, approved and accepted.

8.1.2 IP address allocation of NET

The NET field is allocated according to the example of Table 33, using the rules:

- the IEDs are allocated to the different NETs depending on the voltage level;
- the first NET starts by the highest voltage level available in the related substation;
- the different NETs are assumed to be physically independent (even if cross-connections exist).

Table 33 – Example IP address allocation of NET

IP address	Network
172.16.xxx.xxx	Voltage level 1, C1
172.17.xxx.xxx	Voltage level 1, D1
172.18.xxx.xxx	Voltage level 2, E1
172.19.xxx.xxx	Voltage level 3, H1
172.20.xxx.xxx	Voltage level 4, K1
172.30.xxx.xxx	Station-wide traffic (non-IEC 61850 communication)

In small substations, the SCADA uses a single Ethernet board and a mask of 255.240.0.0.

In larger substations, the SCADA keeps the networks separate by using different Ethernet boards with distinct addresses, for instance 172.16.xxx.xxx, 172.17,xxx.xxx, etc., all using the same mask 255.255.0.0.

8.1.3 IP address allocation of BAY

The BAY field is allocated according to the example of Table 34:

- Bay address 0 is used for station level or system function dedicated devices;
- Bay addresses 201 up to 250 are used for station level IEC 61850 switches;
- Bay addresses 170 up to 179 are used for "virtual bays" (substitution of actual devices by simulation or calculation, see IEC 61850-6.

Table 34 – Example IP address allocation of BAY

IP address	Bay
172.16.0.xxx*	Voltage level 1, Station level (PCs, etc.)
172.16.201.xxx	Voltage level 1, Bay 201 (station level IEC 61850 bridge)
172.16.1.xxx	Voltage level 1, Bay 1 -> D1Q01
172.16.2.xxx	Voltage level 1, Bay 2 -> D1Q02
172.16.x.xxx	Voltage level 1, Bay x -> D1Q0x
172.17.0.xxx*	Voltage level 2, Station level (PCs, etc.)
172.17.1.xxx	Voltage level 2, Bay 1 -> E1Q01
172.17.2.xxx	Voltage level 2, Bay 2 -> E1Q02
172.18.n.xxx	Voltage level 3, Bay n -> E1Q0n
172.30.0.xxx*	Station LAN (non IEC 61850 communication)
* Bay address 0 is reserved for station level communication equipment.	

8.1.4 IP address allocation of device

The device address is allocated according to the example of Table 35.

The address is related to the functionality of an IED in the following order:

- Control IEDs, AVRs or Feeder terminals;
- Main Protection;
- Backup Protection;
- The device address of a bay or station level switch is 100.

Table 35 – Example IP address allocation of device

IP address	Device
172.16.1.100	Voltage level 1, Bay 1, bay level Switch-> D1Q01
172.16.1.1	Voltage level 1, Bay 1, 1. Control IED -> D1Q01A1
172.16.1.2	Voltage level 1, Bay 1, Main Protection IED -> D1Q01FP1
172.16.1.3	Voltage level 1, Bay 1, Backup Protection IED -> D1Q01FP2
172.16.2.100	Voltage level 1, Bay 2, bay level Switch-> D1Q02
172.16.2.1	Voltage level 1, Bay 2, 1. Control IED -> D1Q02A1
172.16.2.2	Voltage level 1, Bay 2, 2. Control IED -> D1Q02A2
172.16.2.3	Voltage level 1, Bay 2, Main Protection IED -> D1Q02FP1
172.16.2.4	Voltage level 1, Bay 2, Backup Protection IED -> D1Q02FP2
172.17.1.100	Voltage level 2, Bay 1, bay level Switch-> H1Q01
172.17.201.100	Voltage level 2, Bay 201, station level IEC 61850 switch

The least significant octet of a host address should not be set to “0” to avoid confusion with network addresses.

8.1.5 IP address allocation of devices with PRP

In PRP, two separate, similar LANs operate in parallel.

Each doubly attached device has the same IP address as it would use for a non-redundant network over both its ports.

The components present in one LAN only, in particular the bridges and RedBoxes, must have a distinct IP address.

The general rule is to add 100 to the unit number of the LAN A switch, as in the example of Table 36.

Table 36 – Example IP address allocation of switches in PRP

IP address	Switch
172.16.1.100	Voltage level 1, Bay 1, bay level Switch-> D1Q01 -> LANA
172.16.1.200	Voltage level 1, Bay 1, bay level Switch-> D1Q01 -> LANB
172.17.1.100	Voltage level 2, Bay 1, bay level Switch-> H1Q01-> LANA
172.17.1.200	Voltage level 2, Bay 1, bay level Switch-> H1Q01-> LANB
172.17.201.100	Voltage level 2, Bay 201 (station level IEC 61850 switch) ->LANA
172.17.201.200	Voltage level 2, Bay 201 (station level IEC 61850 switch) ->LANB
172.17.202.100	Voltage level 2, Bay 202 (station level IEC 61850 switch) ->LANA
172.17.202.200	Voltage level 2, Bay 202 (station level IEC 61850 switch) ->LANB

8.2 Routers and GOOSE / SV traffic

GOOSE and SV operate uniquely on the base of MAC addresses (layer 2). Only very simple devices operate only with GOOSE or SV traffic, e.g. Process Interface nodes.

However, GOOSE and/or SV may be intentionally distributed over the station bus. To allow GOOSE and SV traffic to bypass the router, a layer 2 network bridge (IEEE 802.1D) could be used in parallel to a router (see 7.3.3). Such a bridge possibly provides filtering capabilities.

Therefore, using a router only for limiting the broadcast domains and having a bridge in parallel for GOOSE/SV is more complicated than simply using a managed switch. The efforts for managing the MAC filters in the switch are comparable to the filter setup in the bridge.

8.3 Communication outside the substation

A substation communicates with the outside world at the network layer through one or more routers or gateways. IEC 61850 contemplates several kinds of communication of a substation towards the outside world:

a) Substation to substation communication using layer 2 and layer 3 communication, described in IEC/TR 61850-90-1;

b) Communication between Phasor Measurement Units and Phasor Data Concentrators, as described in IEC/TR 61850-90-5;

c) Communication for remote configuration, monitoring and asset management. To this effect, IEDs may act in addition to MMS as a web server.

For communication outside of the substation, both IPv4 (legacy) and IPv6 are considered.

Layer 2 traffic (GOOSE and SV) can be sent directly on layer 2 if a dedicated path exists or tunnelled over layer 3.

When protocols other than Ethernet are involved, methods such as layer-2 tunnelling can be applied, e.g. with RFC 2661 L2TP.

9 Application parameters

9.1 MMS parameters

It is recommended to use only the default value of the parameters.

A set of recommended parameters (SCL file representation) is:

```
<P type = "OSI-AP-Title">1,3,9999,23</P>
<P type = "OSI-AE-Qualifier">23</P>
<P type = "OSI-PSEL">00000001</P>
<P type = "OSI-SSEL">0001</P>
<P type = "OSI-TSEL">0001</P>
```

9.2 GOOSE parameters

GOOSE messages have a fixed structure indicated in the SCD file. To reduce encoding and decoding overhead, it is recommended to use fixed-length fields (always encode values with the maximum number of octets).

GOOSE messages have several identifiers:

- Multicast addresses follow Annex B of IEC 61850-8-1:2011, they should be allocated so as to allow multicast filtering.
- APPID (16 bits) identifies the application that generates the message. IEC 61850-8-1 defines only its two most significant bits. The APPID should be unique within a substation (see Annex C of IEC 61850-8-1:2011). It can be used as a 14-bit filter to select the relevant GOOSE messages, thereby offloading the processor.
- datSet (VisibleString 129) identifies the data set whose values are transmitted, as defined in the SCD.
- goCBRef (VisibleString 129) references the GOOSE control block as defined in the SCD.
- goID (VisibleString 129) is a system wide, unique identification of the application to which the GOOSE message belongs (e.g. ”interlocking”), see IEC 61850-7-2 and IEC 61850-8-1. Its value is called “appID” in the SCD (see IEC 61850-6) and GOOSEID in the GOOSE control block (see IEC 61850-7-2). Its usage is left to the user, but since it is mandatory, at least a placeholder is inserted. It is redundant with the 16-bit APPID which is also unique system-wide.

9.3 SV parameters

SV messages have several identifiers:

- Multicast addresses follow Annex B of IEC 61850-9-2:2011 (which is the same as Annex B of IEC 61850-8-1:2011), they should be allocated so as to allow multicast filtering.
- APPID (16 bits) identifies the application that generates the message. IEC 61850-9-2 defines only its two most significant bits. The APPID should be unique within a sub-network (see Table 8 and 5.3.3.4.2 of IEC 61850-9-2:2011). It can be used as a 14-bit filter to select the relevant SV messages, thereby offloading the processor.
- DatSet (VisibleString 129) identifies the data set whose values are transmitted, as defined in the SCD. It is optional.

- MsvID (VisibleString 129) is a system wide, unique identification of the sampled value message to be used as a handle for the receiving application (see IEC 61850-9-2). It is mapped to MulticastSampleValueID (see 6.4.3.5 in 61850-7-1).

The SV frames carry a high overhead in form of application strings. These should be reduced to the minimum size that allows to distinguish the SV frames system-wide, for instance by leaving out the optional DatSet, reducing the mandatory MsvID to a few characters and using the APPID to uniquely identify the SV message.

10 Performance

10.1 Station bus performance

10.1.1 Logical data flows and traffic patterns

Knowledge of data flows and traffic patterns allows detecting bottlenecks and planning the network segmentation, filtering and segregation of traffic.

Logical data flows are determined by the protection and control application. Engineering defines the communication relationships between Logical Devices and IEDs, in particular:

- which data sets are used for GOOSE, for SV and for MMS reports;
- which IEDs communicate with which IEC 61850 clients;
- which IEDs are subscribed to each of the GOOSE publishers; and
- which IEDs are subscribed to each of the SV publishers in the process bus.

This information extracted from the SCD file allows determining the traffic base load in the steady state. In addition, the traffic peaks can be estimated for certain conditions, such as busbar fault or general update.

Table 37 shows the expected IEC 61850 traffic.

Table 37 – IEC 61850-5 interface traffic

Function Type/Message		Interface (Table 1)	Protocol	Max. delay ms	Bandwidth	Priority	Application
1A. Trip	GOOSE	3,8	L2 Multicast	3	Low	High	Protection
1B. Other	GOOSE	3,8	L2 Multicast	10 to100	Low	Medium High	Protection
2. Medium Speed	MMS	6	IP/TCP	<100	Low	Medium Low	Control
3. Low Speed	MMS	6	IP/TCP	<500	Low	Medium Low	Control
4. Raw Data	SV	4	L2 Multicast	4	High	High	process bus
5. File Transfer	MMS	6,7	IP/TCP/FTP	>1 000	Medium	Low	Management
6. Time Sync	Time Sync		IP (SNTP) L2 (PTP)		Low	Medium High	General Phasors, SVs
7. Command	MMS	6	IP		Low	Medium Low	Control

However, non-IEC 61850 traffic is not modelled nor considered in the SCD files. Other applications can be present in the network, for example for disturbance recording, network management, clock synchronization, video surveillance, etc. Part-time devices (e.g. for maintenance) can influence the performance of the network. Table 38 summarizes the expected traffic mentioned in IEC 61850 documents in a substation, other traffics also coexist.

Table 38 – Message types and addresses

Traffic	Type	Ethertype/ length (hex)	Addressing	Description
GOOSE	IEEE 802.3/ Multicast	88B8	01-0C-CD-01-00-00 to 01-0C-CD-01-01-FF	
SV	IEEE 802.3/ Multicast	88BA	01-0C-CD-04-00-00 to 01-0C-CD-04-01-FF	
MMS	TCP/IP	0800	TCP/102	Uses
Time Sync – SNTP	UDP/IP	0800	UDP/123	
Time Sync – PTP	IEEE 802.3 /Multicast	88F7	01-1B-19-00-00-00 01-80-C2-00-00-0E	IEC 61588 over layer 2
Monitoring – Ping	ARP ICMP	0806 0800	ICMP/Echo ICMP Echo-Reply	Ping bridges and IEDs
RSTP	IEEE 802.2	length / LLC		BPDUs for configuration
Monitoring – SNMP	UDP/IP	0800	UDP/161	Device management
Monitoring – SNMPTRAP	UDP/IP	0800	UDP/162	Events from bridges
Monitoring – SYSLOG	UDP/IP	0800	UDP/514	Logs from bridges
File transfer	IP/TCP/FTP	0800	TCP/20	Event logs from IED
Administration – SSH	TCP/IP	0800	TCP/22	Bridge management
HSR	IEEE 802.3	892F	NA	HSR tag
PRP – HSR Supervision	IEEE 802.3	88FB	NA	IEC 62439-3:2012

10.1.2 GOOSE traffic estimation

Although GOOSE messages are smaller than MMS messages, GOOSE traffic impacts more the station bus. GOOSE transmits messages cyclically and retransmits spontaneous messages, usually two times, to overcome possible frame losses. This increases traffic over what is actually needed. Since links have a very low loss rate, the recovery mechanism of GOOSE actually increases the probability of losing frames due to congestion in the switches. The buffer size in the bridges must be sized accordingly.

A “short” GOOSE message handling just one digital status information (one Boolean value and the related Quality bit string) in the data set has an approximate size of 124 octets. The actual size depends on the configured parameters in the GOOSE Control Block such as GoID, name of the data set and the reference object of the GOOSE Control Block. Typically the size of GOOSE messages is within 92 octets to 250 octets.

One GOOSE application in an IED generates about 1 kbit/s in steady-state and about 1 Mbit/s during bursts. Bursts are often correlated since one switching operation can trigger several GOOSE frames.

10.1.3 MMS traffic estimation

The MMS traffic generated by IEDs consists of a polling part from the SCADA and an event-driven part that depend on reports the MMS servers send to the MMS clients. An IED sends digital values and data counters using reports triggered by data change, quality change or data update. The IEDs can also be configured to send integrity reports with digital values as an additional data check mechanism, the interval of such reports is normally in the range of 60 s to 300 s.

Measurements are commonly sent predictably via Integrity Reports with an interval of approximately 1 s, but the IEDs can also be configured to send measurements triggered by data changes. The latter method is less often used as it requires configuration of deadbands for each analogue value. The size of reports sent via MMS depends on the number of elements in the data set as well as on the configuration of report control block parameters such as OptFlds, RptID and the lengths of object references.

10.1.4 station bus measurements

Figure 52 shows a typical station bus interconnecting 10 bays.

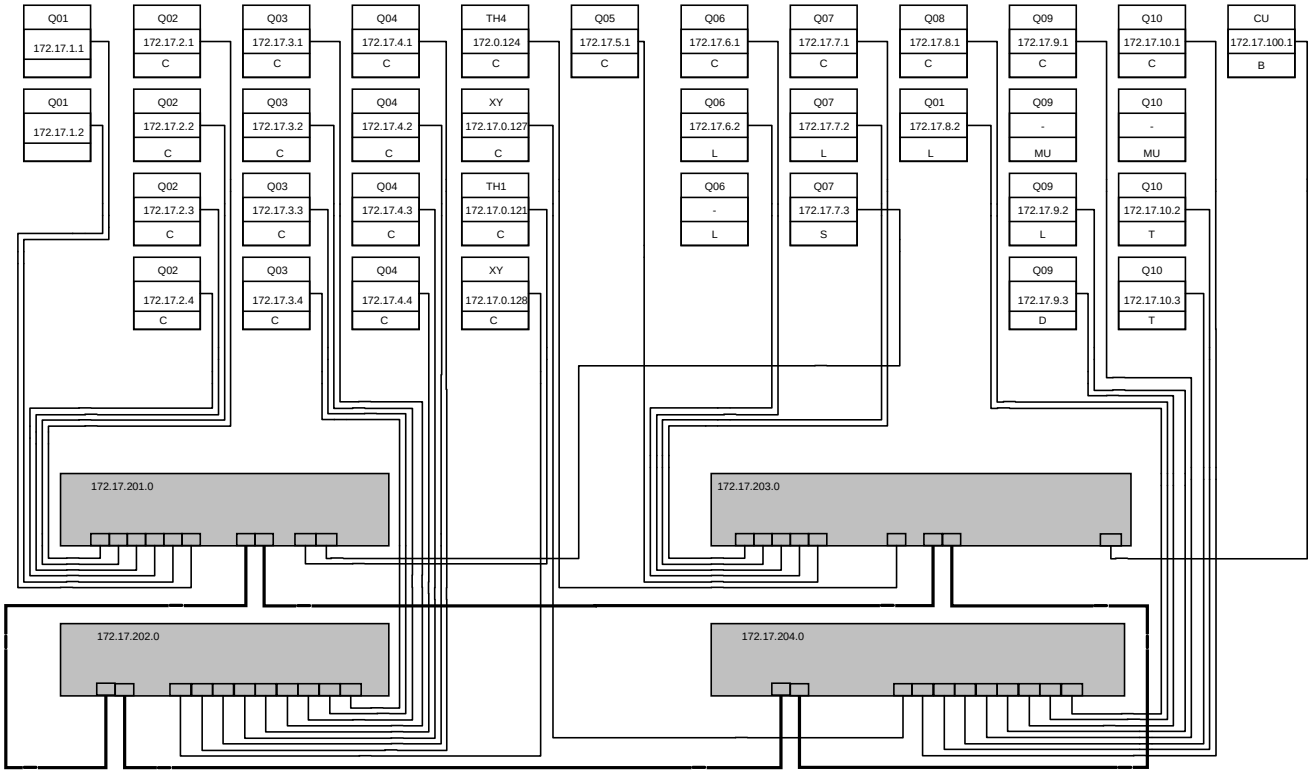


Figure 52 – Station bus used for the measurements

The traffic of that substation under steady-state (no switching operation) and burst conditions (simulated busbar transfer) is shown in Figure 53.

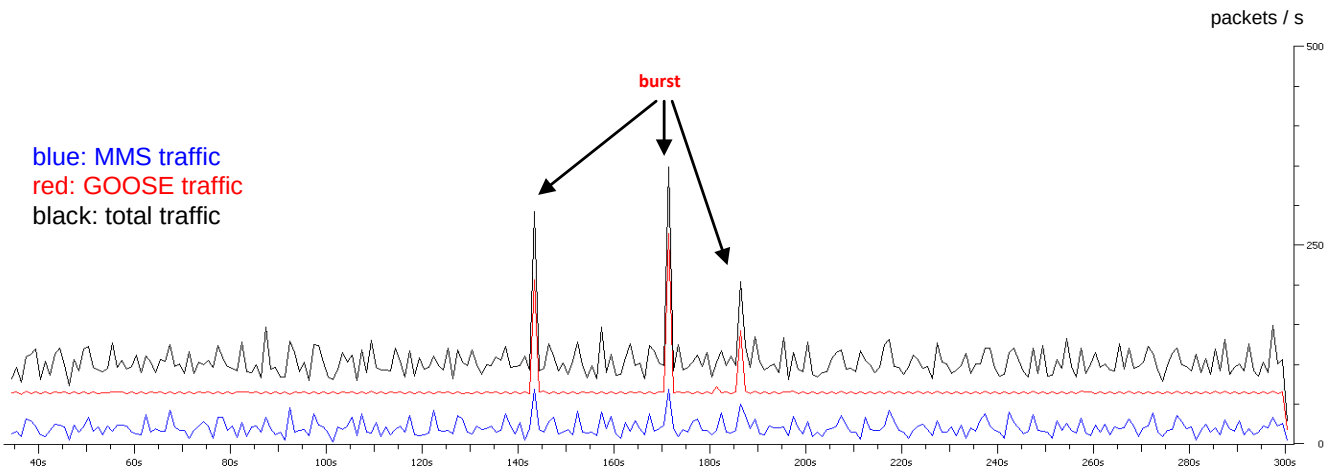


Figure 53 – Typical traffic (packet/s) on the station bus

This shows that the network hardly becomes a bottleneck in this configuration and that no special measures must be taken in this case.

As a rule of thumb, the MMS traffic generated by a single IED on the station bus in the steady state is below 10 kbit/s. Since MMS traffic is not multicast, it only influences the bandwidth on the network links between the MMS server and the MMS client and it does not influence the edge links to other IEDs.

10.2 Process bus performance

The process bus interconnects I/O devices like sensors and merging units on the field level, e.g. in one individual bay. Each bay usually has its own process bus network, coupled to the station bus network. Typical traffic consists of IEC 61850 SV and GOOSE multicast traffic, MMS and PTP.

While GOOSE and MMS put similar requirements on the process bus network as on the station bus network, SV traffic is even more demanding, but it is easily predictable.

As an example, an SV frame as specified in UCA Guideline 9-2LE [15] with a sampling rate of 80 samples per cycle transmitted at 4,0 kHz (for a 50 Hz grid) or at 4,8 kHz (for a 60 Hz grid) have an approximate size of 140 bytes, consuming a bandwidth of approximately 5 Mbit/s (50 Hz) or 6 Mbit/s (60 Hz) per source IED.

NOTE The actual size depends on MsvID and OptFlds values as well as on the lengths of reference objects of Multicast Sampled Value Control Block (MSVCB) and data set name.

Therefore, a process bus at 100 Mbit/s hardly supports more than six devices if time should be left for the longest MMS messages (123 μs). Up to 20 devices can be accommodated if the 100 Mbit/s process bus is dedicated to SV traffic. This shows that the process bus must have an own multicast or VLAN domain to separate its SV traffic from the station bus traffic.

For the process bus, some form of source throughput limitation (rate limiting in bridges) must be applied to the real-time traffic since because of its high priority, it could monopolize the network. This is a requirement on the IEDs rather than a requirement on the network.

In applications where the station bus also carries SV traffic, it must provide the same quality of service as the process bus.

Annex A shows an estimation of the traffic for a process bus used in busbar protection.

11 Latency

11.1 Application requirements

If an IEC 61850 frame is not received in a timely manner, it loses its usefulness; and being late could be worse than being lost. Delays – especially jitters – also affect the clock synchronization.

Three metrics are to be observed:

- Latency of communication, which is the delay between the instant data are ready for transmission and the moment they have been completely received at their destination(s). This is the worst delay of all possible associations.
- Throughput, which is the quantity of data that can be transported by unit of time, while retaining a certain quality of service, for any association, and under worst-case load conditions.
- Reliability, which is the probability that the frame gets lost because of congestion, not because of physical failure. Indeed, physical failures can be dealt with through redundancy, while overload can affect both redundant paths.

For this performance metric, the term dependability has been traditionally used for protection communications, whereas the term QoS (for Quality of Service) is commonly used now by the network community, so it is used here.

The required delivery time depends on the application, with the most demanding being the few milliseconds needed for protection applications. E.g. IEC 60834-1 requires that 99,99 % of commands for inter-tripping protection schemes are delivered within 10 ms.

The correct design of a network to be used for IEC 61850 communications requires knowledge of the application's requirements, plus knowledge of the latencies through the various network elements.

11.2 Latency requirements for different types of traffic

11.2.1 Latency requirements in IEC 61850-5

IEC 61850-5:2013 provides performance requirements for different types of messages and specifies basic performance requirements for each type of message, which are reproduced for convenience in Table 39.

Table 39 – Transfer time requirements of IEC 61850-5

Transfer time class	Transfer time ms	Application example, transfer of
TT0	> 1 000	Files, events, log contents
TT1	1 000	Events, alarms
TT2	500	Operator commands
TT3	100	Slow automatic interactions
TT4	20	Fast automatic interactions
TT5	10	Releases, Status changes
TT6	3	Trips, Blockings

11.2.2 Latencies of physical paths

A path delay is caused by the finite speed of the electromagnetic waves through the medium: copper cables, optical fibres or wireless links. To this, media converter delays must be added as shown in Table 40.

Table 40 – Elapsed time for an IEEE 802.3 frame to traverse the physical medium

Medium	Time to traverse a link
CAT-5 and CAT-6 cables	0,55 μs per 100 m (5,5 μs/km)
Glass-Fibre cables (Corning smf28)	0,49 μs per 100 m (4,9 μs/km)
Free air (wireless)	0,33 μs per 100 m (3,3 μs/km)

11.2.3 Latencies of bridges

Whenever a frame arrives at a bridge's ingress port, most bridges wait for the complete frame to be received to check its integrity (using its FCS (CRC) field) before it is forwarded. This technology is called "store-and-forward". A less-frequently used technology called "cut-through" avoids this delay, but requires hardware support.

Store-and-forward bridge latency includes elapsed time of ingress and egress ports (depending on link speed), internal processing delay, in particular protocol processing, and

queuing delays. The delays for various frame lengths and port speeds are shown in Table 41, to which the internal delay is to be added.

Table 41 – Delay for an IEEE 802.3 frame to ingress or to egress a port

Frame length	Frame duration at 100 Mbit/s	Frame duration at 1 Gbit/s
64 Octets (minimum allowed)	7 μs	0,7 μs
300 Octets (e.g. compact GOOSE frame)	25 μs	2,5 μs
800 Octets (e.g. large GOOSE frame)	64 μs	6,4 μs
1 530 Octets (maximum)	124 μs	12,4 μs

In cut-through, the delay in Table 41 does not apply, it is replaced by the fixed delay that the bridge needs to recognize the VLAN tag, which is about 1 μs at 100 Mbit/s or 0,1 μs at 1 Gbit/s.

Whenever a frame arrives at a bridge's egress port that is busy outputting another frame, the frame must be held in a buffer. All bridges have egress queues for this buffering with some bridges having separated queues for frames with different priority levels (usually 2, 4, or 8 priority levels are supported).

For each frame buffered in the egress port's queue at the same or higher priority levels, the elapsed time for the waiting frame increases by the time shown in Table 41.

11.2.4 Latency and hop counts

In a non-congested network, the minimum bridge hop latency at 100 Mbit/s is estimated to 32 μs.

NOTE The 32 μs latency is calculated as follows. The bridges usually operate in a store-and-forward mode, which means the whole frame is received before it is forwarded. A typical GOOSE message of 300 octets has 2 400 bits, and causes at 100 Mbit/s a delay of 24 μs. With a minimum bridge latency of 8 μs + frame delay, the latency is 8 μs + 24 μs = 32 μs. To this must be added the queuing latency, which is a variable depending on load and QoS settings on the network bridges.

GOOSE and SV frames could be allocated a high priority on the network and therefore have a minimum wait time of the largest possible frame.

Network latency is caused primarily by egress queuing, the amount of time a frame has to wait before it is transmitted. Forwarding latency is affected by QoS and frame sizes. If no QoS is used then frames are forwarded in a FIFO (first in first out) method, with the assistance of QoS frames can be prioritized and forwarded based on this priority. So if a low priority packet is being transferred at the time a high priority GOOSE packet is sent, the high priority packet can in essence jump the egress queue and be the next frame to be sent, but it must await the end of the current transmission. The worst case latency per bridge, providing the high priority queue is empty, is 124 μs based on a 1 530 octet frame at 100 Mbit/s.

11.2.5 Network latency budget

Table 42 records the best and worst case latencies based on a 300 octet frame that receives a high priority on the network and the same with a delay of a 1 530 octet frame queuing wait for each hop. The worst case for the total chain occurs when a 1 530 octet frame waits at each bridge, but the probability that this happens is low.

Table 42 – Latencies caused by waiting for a lower-priority frame to egress a port

Bridge hops	Min. latency (no waiting)	Max. latency, congestion at only one bridge	Average latency with variable congestion	Max. latency, congestion at every bridge
1	32 µs	156 µs	156 µs	156 µs
2	64 µs	188 µs	250 µs	312 µs
3	96 µs	220 µs	344 µs	468 µs
4	128 µs	252 µs	438 µs	624 µs
5	160 µs	284 µs	532 µs	780 µs
6	192 µs	316 µs	626 µs	936 µs
7	224 µs	348 µs	720 µs	1 092 µs
8	256 µs	380 µs	814 µs	1 248 µs
9	288 µs	412 µs	908 µs	1 404 µs

The total budget for a fast trip is 3 ms as per IEC 61850-5 Class TT6. Assuming a maximum processing time for each IED of 1,2 ms, and two IEDs concerned, this leaves the network with a maximum budget of 3 ms – (2 × 1,2 ms) = 0,6 ms of latency. Hence, for a fast trip, the number of hops in the network between the concerned IEDs should be lower or equal to 5 according to Table 42.

NOTE The minimum latency would improve using cut-through in the bridges, but not the maximum latency.

11.2.6 Example of traffic delays

At each egress bridge port, a high-priority frame has to wait in the worst-case for a maximum-length lower-priority frame to egress.

If one hop delay is 124 µs at 100 Mbit/s (12,4 µs at 1 Gbit/s), a potential 2 ms extra delay could therefore be incurred in a network path comprising 16 hops at 100 Mbit/s (160 hops at 1 Gbit/s).

11.2.7 Engineering a network for IEC 61850 protection

A protection engineer needs to know what latencies to use for the various protection events so that they can be correctly coordinated.

To meet the IEC 60834-1 standard, the network must be designed so that the latencies of the critical protection GOOSE frames be less than 10 ms 99,99 % of the time. This requires the following:

- Identification of all bridge egress ports in the circuit paths carrying critical protection GOOSE traffic.
- Identification of all other circuits sharing these critical egress ports (e.g. SCADA, surveillance, corporate).
- Classification of all circuits as known-pattern or unknown-pattern (pattern being the frame length(s) and inter-frame gap statistics).
- If any circuits are unknown-pattern, these must be assigned a lower-priority.
- Unless its pattern is known, MMS traffic should be assigned a priority lower than that of critical protection traffic.
- For the known-pattern circuits, use Table 40, Table 41 and Table 42 to calculate the probability that a frame latency exceeds 10 ms; if worse than 99,99 %, then:

– assign several priority levels to the known-pattern circuits (e.g. critical protection GOOSE traffic to the highest priority), or

– use (more) VLANs to restrict multicast and broadcast frames to only the network paths needed, or

– rearrange the network;

– implement a policy to ensure that the performance is not compromised by future changes to the network (new traffic sources, network topology changes etc.).

12 Network traffic control

12.1 Factors that affect performance

12.1.1 Influencing factors

Performance and real time response from end to end are affected by:

- Number of hops (bridges and routers) and amount of traffic in the layer 2 network, which affects latency and jitter;
- Ratio of edge ports to trunk ports based on traffic load patterns. E.g. 100 Mbit/s for devices to bridge and 1 Gbit/s for inter-bridge communication;
- Use of multicast filtering to confine traffic within multicast domains and VLANs to segregate traffic;
- Use of QoS parameters to meet the real-time requirements of various traffic flows;
- Capacity of the end devices to deal with the traffic. This last point is not considered as a network issue, see 6.4.7.

12.1.2 Traffic reduction

Removing bottlenecks on the trunk links requires a careful analysis to configure correctly the bridges in the network.

Client/Server traffic (C/S, unicast) can only be reduced by VLANs and by the natural filtering of the bridges through MAC source address filtering.

The bulk of IEC 61850 traffic however consists of multicast GOOSE and SV messages.

Multicast traffic can be filtered or restricted to specific domains in the network by VLAN and Multicast filtering, in the generic scheme of Figure 54. This will be detailed in the sequel.

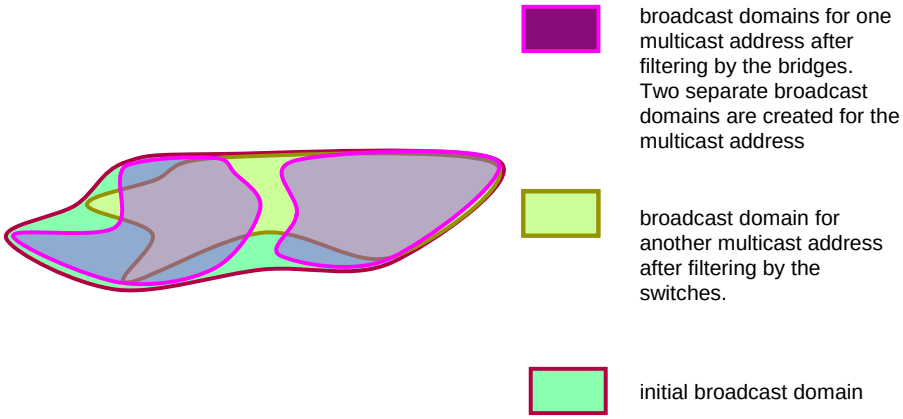


Figure 54 – Generic multicast domains

12.1.3 Example of traffic reduction scheme

Figure 55 shows a "full blown" scenario utilizing all communication mechanisms of IEC 61850: MMS Client/Server (C/S), GOOSE (GO), and Sampled Values (SV). The substation communication network is segregated into a dedicated station bus and a dedicated process bus.

The station bus carries primarily C/S traffic between the station control and bay devices (IEDs) for SCADA purposes and GOOSE messages between the bays.

The process bus carries the real time communication, which are the SVs from the merging units (MUs) to the bay devices and the GOOSE messages. GOOSE messages are exchanged between the bay devices within the bay level and between the bay devices and the process close IEDs (PIBs). The bay devices (protection IEDs) publish e.g. trip commands by GOOSE for the PIBs, which in turn publish their breaker positions by GOOSE as well.

When SVs are not utilized, the dedicated process bus possibly does not exist and the peer-to-peer communication via GOOSE between the bay devices also runs over the station bus.

In case of high load due to SVs, it might be necessary to limit the broadcast domains in the process bus. This is indicated in Figure 55 by the segmented process bus, which is connected by bridge 2 and bridge 3. The link between is permeable for GOOSE messages, while filters are applied for SVs to separate the streams crossing the link from those confined to a process bus segment.

The PIBs communicate not only with the bay devices by GOOSE, but also with the station control by C/S communication. Typical tasks are to send reports with the CB position to the station control while the station control commands the PIBs to trip or close the CBs.

Thus, C/S communication must traverse vertically from the station control to the process level through all layers. To accommodate this, the link between bridge 1 and bridge 2, respectively bridge 3 is provided. This link can be implemented in different ways.

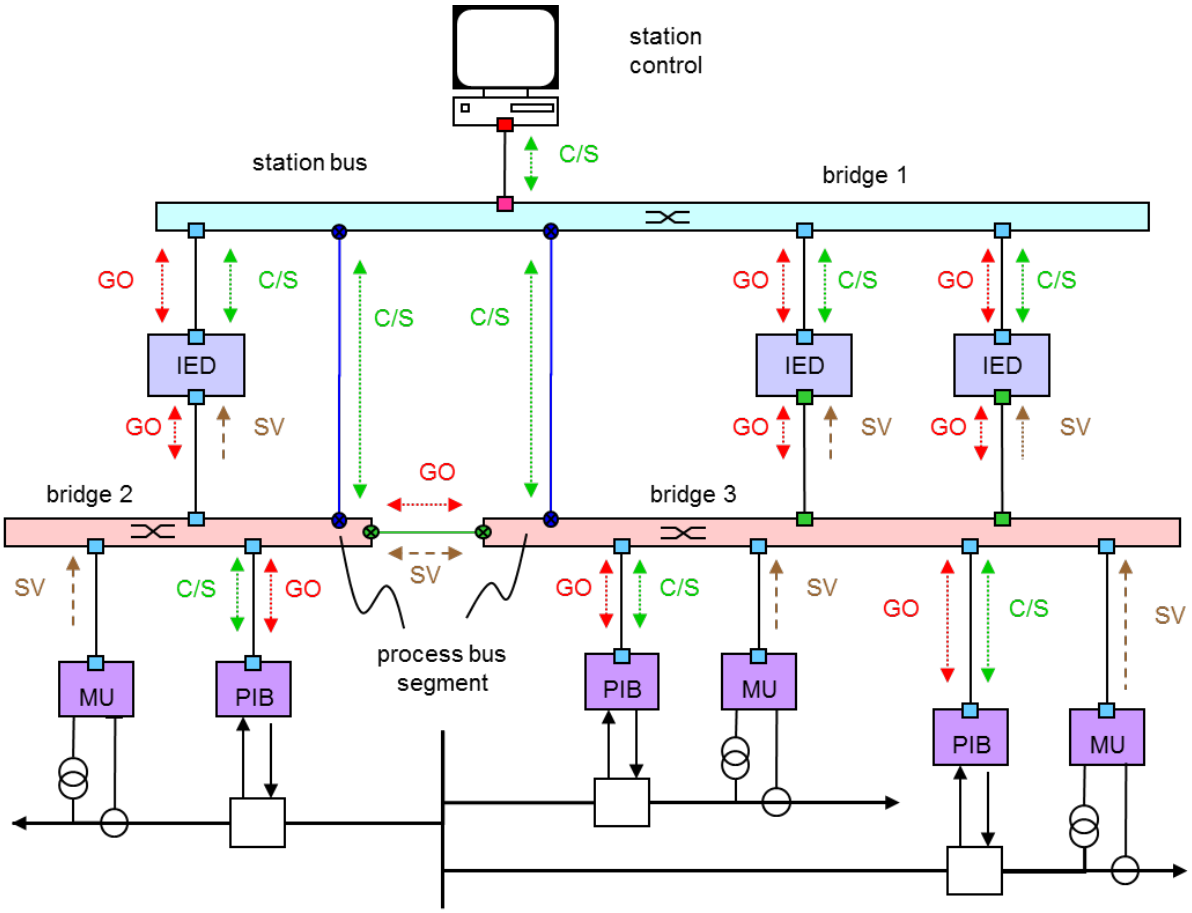


Figure 55 – Traffic patterns

12.1.4 Multicast domains in a combined station bus and process bus network

A filtering or segregation mechanism in the bridges allows to restrict multicast traffic only to those IEDs that are subscribers of the GOOSE or SV traffic. If this filtering is not applied, the network is flooded by multicast messages which results in excessive bandwidth consumption and overhead of IEDs by unnecessary processing of unwanted traffic. Figure 56 shows a representation of the multicast domains in a combined station bus and process bus network.

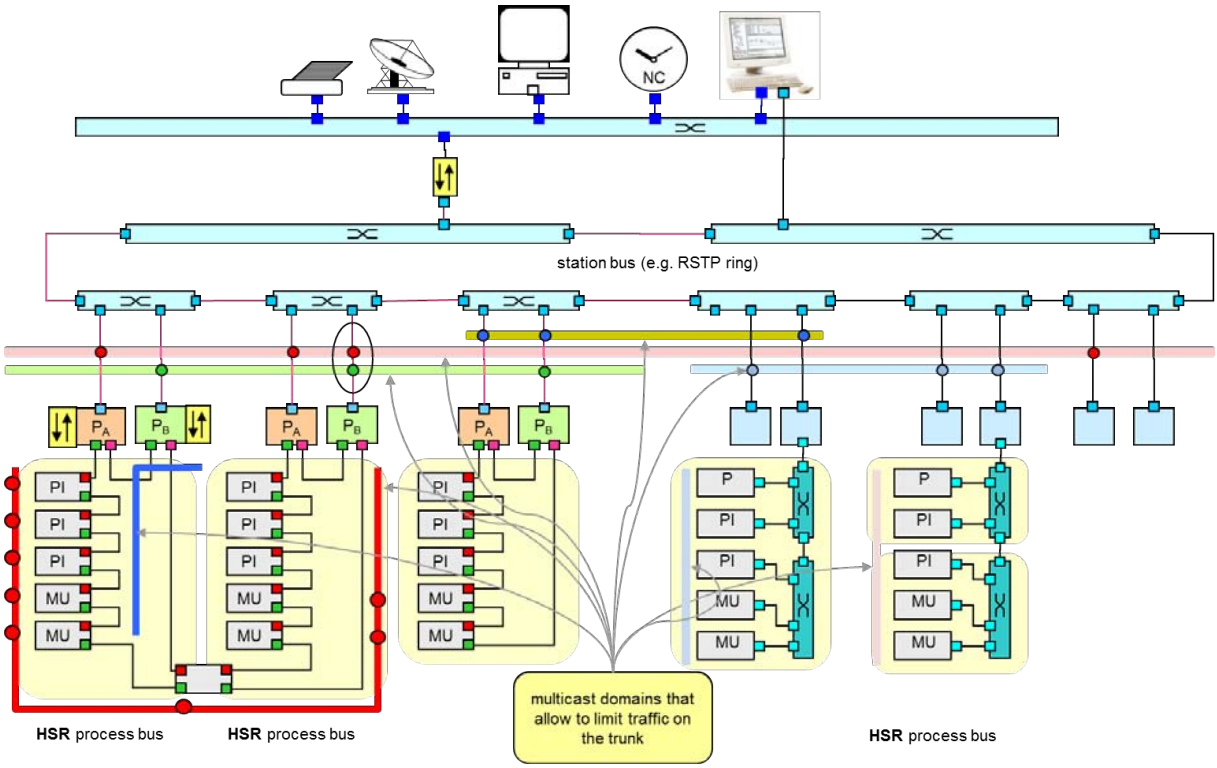


Figure 56 – Multicast domains for a combined process bus and station bus

NOTE PI (Process Interfaces) are explained in 7.3.2.

Flooding the whole network with multicasts like SV could overload bridges and devices that cannot handle this traffic. If e.g. SV traffic has to pass through the station bus, e.g. from one process bus network to another, it is rigorously restricted to the network path it has to travel. If several such traffics use the station bus segment, they can overload the station bus.

In large substations, it becomes necessary to limit the multicast domain to devices that must communicate with each other.

The bridges between the multicast domains should segregate the GOOSE traffic based on the multicast address of the frames.

Typically, the IEDs of a voltage level form one specific multicast domain.

When used for communication between multicast domains, GOOSE frames should be configured with one specific global multicast domain address.

12.2 Traffic control by VLANs

12.2.1 Trunk traffic reduction by VLANs

NOTE VLANs are introduced in 6.4.8.

VLANs can reduce the amount of messages that the end devices must process, but this is not a network traffic issue.

VLANs reduce the network traffic only when distinct zones can be built. This requires careful analysis, since the network can reconfigure itself upon failure of a link, and restrictive VLAN filtering could hamper communication.

12.2.2 VLAN usage

VLANs require careful engineering and deployment, they should be avoided unless justified.

IEC 61850 does not mention nor does it mandate the use of VLANs. It requires to send the GOOSE and SV frames as priority-tagged frames to ensure priorities. Preserving these priorities requires at least default VLAN support.

IEC/TR 61850-90-1 suggests using VLANs for tunnelling substation-to-substation communication, to prevent burst situations from propagating to another substation.

To reduce the traffic load on end devices, multicast filtering is often sufficient since the bulk of IEC 61850 communication is multicast.

12.2.3 VLAN handling at the IEDs

IEC 61850-8-1:2011 requests that an IED sends the GOOSE and SV messages with a 802.1Q tag; it may send MMS messages untagged. The other traffic is unspecified.

An IED may also send messages with VLAN tags, in which case the bridge will treat it as explained in 6.4.8.2.

At reception, the edge port of the bridge to which the IED is connected is expected to be configured to remove the 802.1Q tags, but this is not required.

An IED is requested to accept VLAN tagged frames regardless of the VLAN tag for any message, while it may use the priority field internally.

12.2.4 Example of correct VLAN configuration

Figure 57 shows a properly configured network where priority is preserved, in which node A2 sends MMS traffic as untagged and GOOSE traffic as priority-tagged (VID = 0; PCP = 4) to a port at bridge A with (PVID = 3; PPCP = 0) and configured with ‘Admit all frames’ and ingress filtering turned off.

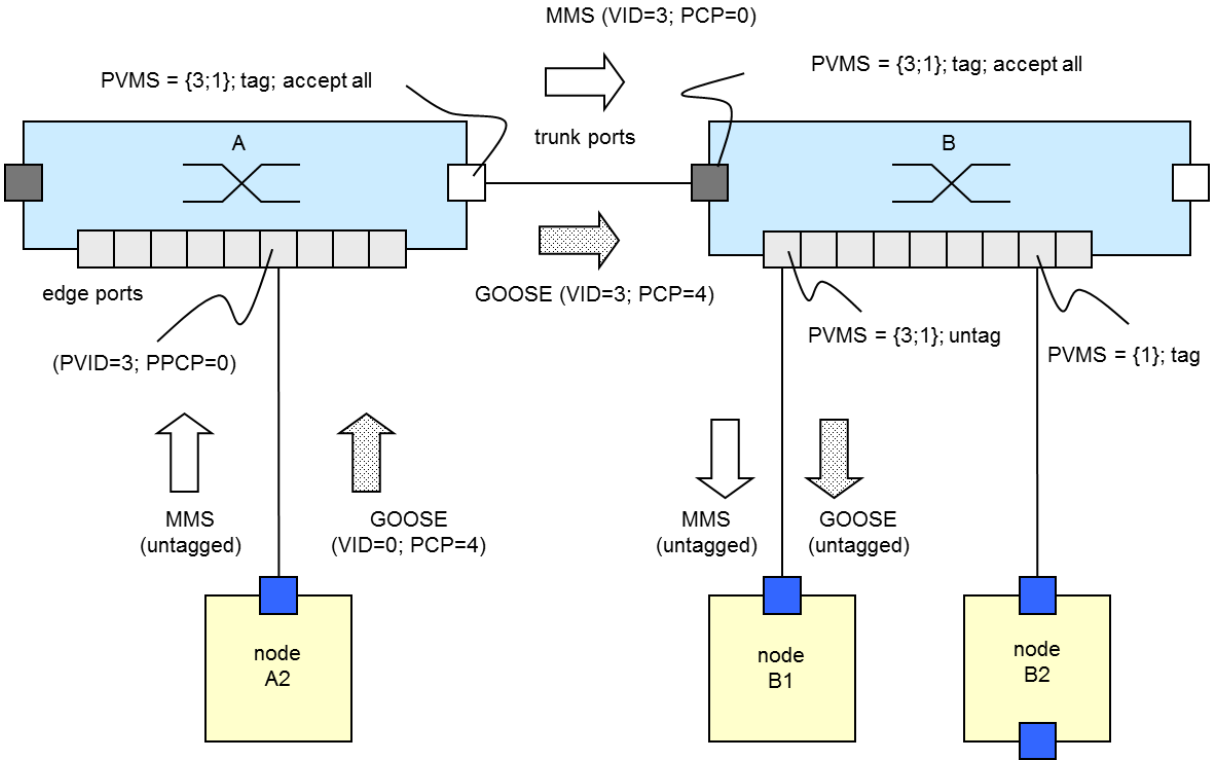


Figure 57 – Bridges with correct VLAN configuration

The ingress port encapsulates the frame carrying MMS traffic with a VLAN tag with (VID = 3; PCP = 0), inheriting the port's configuration. The port encapsulates the frame carrying GOOSE traffic with (VID = 3; PCP = 4), preserving the priority.

Bridge A forwards both the GOOSE and the MMS frame through the trunk port towards bridge B. This port is configured to keep the frame tagged. Thus both frames (MMS and GOOSE) retain the VLAN tag with their respective VIDs and PCP. The port is also member in VLAN 3, but this is irrelevant when ingress filtering is not used.

The receiving trunk port on bridge B is configured as "accept all frames". It thus accepts both frames, regardless of their tag. Bridge B internally forwards the frames towards the edge port to which node B1 is connected. This port is a member of VLAN 3 and is configured to untag frames.

Thus, the egress port removes the VLAN tag from both the MMS and the GOOSE frames. These frames lose their priority information, but it only would matter if the node is able to forward frames like node B2 in Figure 57, which forwards frames of the default VID as tagged.

12.2.5 Example of incorrect VLAN configuration

Several misconfigured parameters could prevent the correct reception of the frames from node A at SAN B. An example is shown in Figure 58.

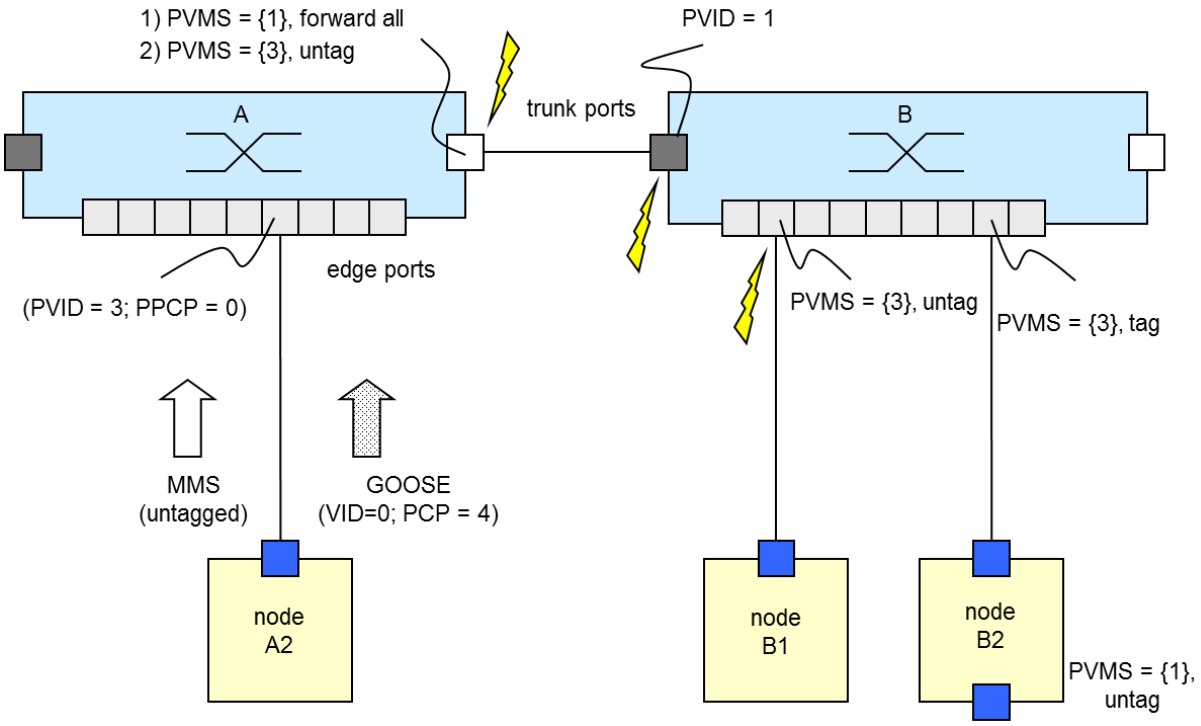


Figure 58 – Bridges with poor VLAN configuration

The first configuration error appears at the trunk port of bridge A. The port is not a member port of VLAN 3. This means that the MMS and GOOSE frames from SAN A will not be forwarded by that port.

A second configuration error assumes that trunk port is correctly configured to be member of VLAN 3, but also to untag all frames. This removes all VLAN information (VID and PCP) on all frames sent from that port and also the priority information of GOOSE messages. The ingress port would tag both GOOSE and MMS frames entering the bridge with its PVID and PPCP (VID = 1; PCP = 0). The bridge port towards SAN B1 however is still configured to be a member port of VLAN 3 only, which means that frames will be discarded, thus preventing end-to-end communication between SANs A2 and B1.

Other errors could be as follows (this list is not exhaustive):

- the bridge port connected to node A2 could be configured to accept frame types with ‘Admit only VLAN tagged’. In this case, the bridge discards both the MMS and the GOOSE frame, since it considers priority-tagged frames with a VID different from zero as “untagged”;
- the trunk port on bridge B connected to the bridge A could be configured as ‘Admit untagged only’. In that case, bridge B would discard all tagged frames from bridge A;
- the port on the bridge B connected to the end node B2 could be configured to be a member port in VLAN 3 and sends frames with VLAN tag instead of “untagged”. However, if the second port of node B2 is not capable of interpreting frames with a VLAN tag of 3, it will not forward them.

To prevent this kind of bad configurations, configuration guidelines should be observed. Such guidelines should distinguish:

– enabling end-to-end connectivity while preserving priorities (e.g. to expedite GOOSE frame delivery compared to MMS);

– restricting traffic flows by VLANs.

12.2.6 Retaining priority throughout the network

The following design rules allow to send the traffic from the IEDs within the same VLAN X and to preserve the priority of multicast GOOSE frames throughout the network:

- Choose one VID = X which is to be used by all devices for all network traffic (e.g. VID=1);
- Configure all edge ports to which IEDs are connected to as:
  - "accept all frames";
  - PVID = X;
  - PPCP = 0 (default).
- Configure all bridge trunk ports connected to other bridges in the network:
  - to be member ports of VLAN X;
  - to "accept all frames";
  - to keep tags on egress.
- Configure all bridge ports to which IEDs are connected to send frames untagged. The only exception to this rule should be if a specific IED can only interpret VLAN tagged traffic, in which case the port should be configured to send frames tagged.
- Configure the IEDs connected to the ports of VLAN-aware bridges to send high priority traffic either with VID = X or priority tagged (with VID = 0) and with the PCP values as needed according to the traffic (e.g. PCP = 4 for GOOSE). Low priority traffic should be sent untagged.

The PCP value within each frame is given by the IED. High priority traffic should be sent tagged (either priority or VLAN), low priority traffic should be sent untagged.

NOTE If an IED is not capable of sending either VLAN or priority tagged frames, all its traffic will be automatically mapped to the best effort class. Configuring port priority could be used to map the whole traffic of that IED to a higher priority upon ingress at a bridge, but this could have a negative impact on overall performance.

12.2.7 Traffic filtering with VLANs

In addition to allowing priorities to be retained throughout the network, VLANs can also be used to segregate traffic flow throughout the network. Traffic filtering cannot however be applied to the ring ports of a ring since a ring reconfiguration would make parts unreachable.

Mapping specific traffic from different GOOSE control blocks to individual VLANs and then configuring these VLANs only on bridges that need to forward these frames can be an effective means of limiting traffic to specific parts of a network.

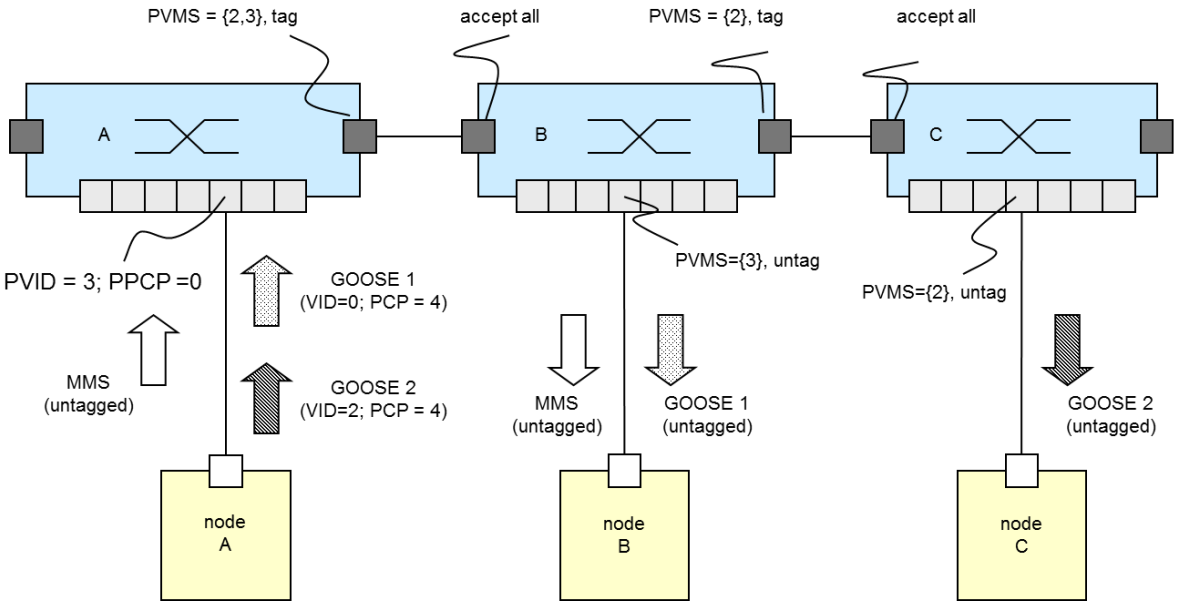


Figure 59 – Bridges with traffic segmentation through VLAN configuration

Figure 59 shows such an example configuration. Node A is connected to bridge A, which has its connecting bridge port configured to PVID = 3 and the default PPCP. Node A sends MMS traffic untagged and traffic for two GOOSE control blocks, GOOSE 1 and 2. GOOSE 1 is priority tagged, while GOOSE 2 is VLAN tagged. After ingress at the bridge, the three frames will have the following configuration:

- MMS: (VID = 3, PCP = 0)
- GOOSE 1: (VID = 3, PCP = 4)
- GOOSE 2: (VID = 2, PCP = 4

The bridge port connecting bridge A to bridge B therefore has to be configured to be a member in both VLANs 2 and 3 in order to make it possible for GOOSE 1 and 2 to travel to bridge B.

In bridge B, the MMS traffic and the GOOSE 1 traffic are forwarded only to the edge port that is connected to node B. The trunk port connecting bridge B to bridge C is configured to be a member port only of VLAN 2. Thus, GOOSE 1 multicast traffic is restricted to bridges A and B without consuming bandwidth on bridge C. GOOSE 2 traffic is forwarded to bridge C and subsequently to node C.

NOTE If VLANs are to be used for GOOSE/SV multicast filtering, IEDs need the ability to transmit different kinds of traffic with different VLAN encapsulation, e.g. one distinct VLAN ID for every GOOSE control block. If this cannot be guaranteed, traffic control through multicast filters is preferred.

12.3 Traffic control by multicast filtering

12.3.1 Trunk traffic reduction by multicast filtering

IEC 61850 uses 802.1Q priority tagging to privilege time critical bus traffic for protection relevant applications over low priority MMS and management traffic.

GOOSE and SV traffic use layer 2 multicast. This traffic propagates across the whole network reaching all bridges and all IEDs. It impacts the bandwidth of all links in the network and adds latency to processing times in all bridges and all IEDs.

Therefore, when the station bus extends to numerous devices, it is advisable to divide it into segments separated by bridges that can filter out multicast traffic. A natural way is to split the station bus according to the different voltage levels, as shown in Figure 60.

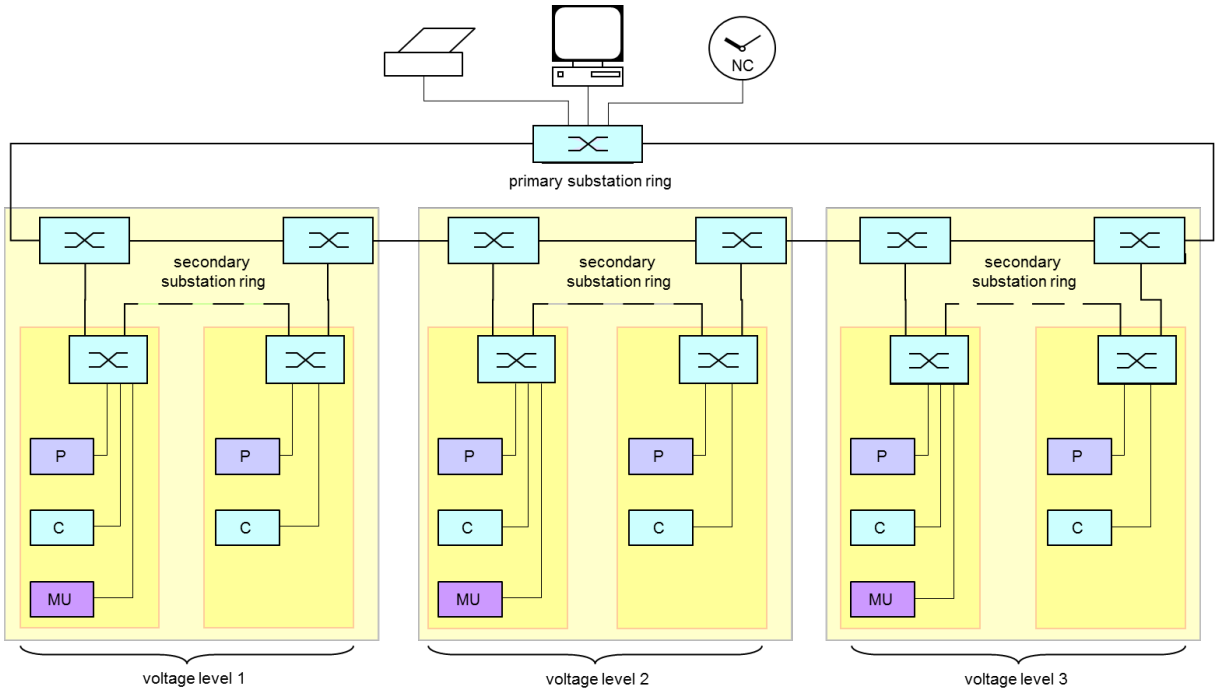


Figure 60 – Station bus separated into multicast domains by voltage level

12.3.2 Multicast/VLAN management and redundancy protocol reconfiguration

When multicast traffic is restricted via multicast control and/or VLANs, a network redundancy reconfiguration could decouple devices or whole network segments from e.g. a multicast tree.

For both VLAN and multicast control, the transition points between station bus and process bus need to be identified. Transition points are most likely redundant network elements like e.g. HSR Redundancy Boxes or network bridges which employ redundant coupling, which have to be fitted with the same multicast control information. Furthermore, the actual physical topologies need to be taken into account, as is explained in 12.4.

12.3.3 Physical topologies and multicast management implications

12.3.3.1 Ring

On a ring, multicast cannot be controlled on the ring ports, as a multicast publisher cannot determine where in the physical ring a network port has been blocked by a redundancy control protocol. Therefore, it has to send the multicast traffic in both directions inside the ring to reach all possible subscribers (see Figure 61).

For actual implementation, this means that specific MAC multicast filtering cannot be done on the ring ports of ring devices. If multicast management is done via VLANs, all VLANs containing multicast groups must be configured on all ring ports of the ring devices (analogous for dynamic MC management via GMRP/MMRP, forward-all must be implemented on ring ports).

This applies to RSTP rings, while on HSR rings the frame transmission is done automatically. As each frame is already being transmitted over two network paths by the HSR protocol itself, only VLANs need to be configured. Multicast management is done on the non-ring ports, connecting single subscribing devices or attached network segments.

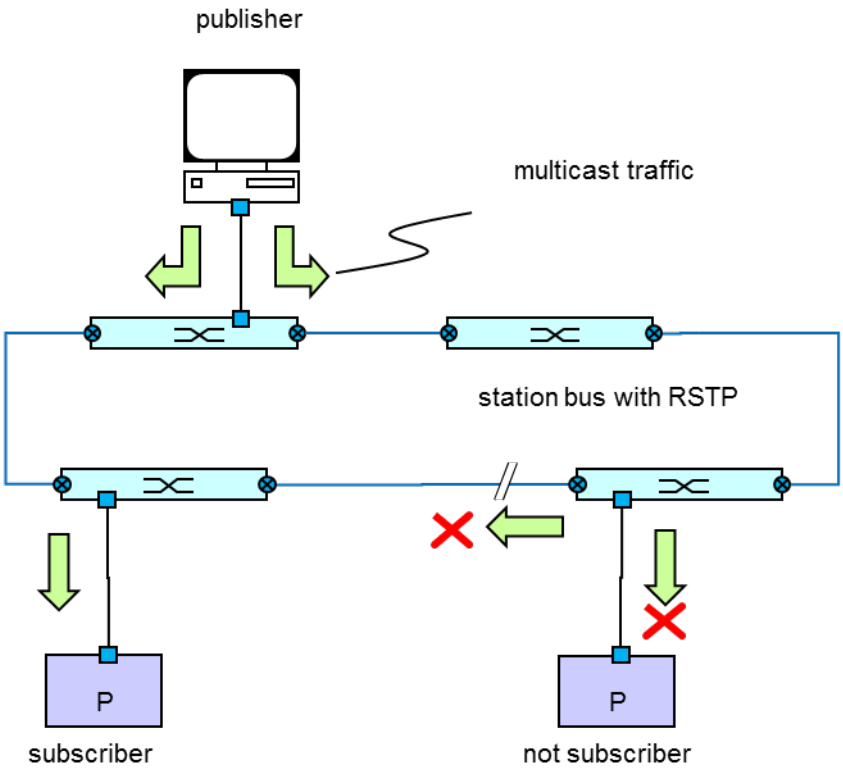


Figure 61 – Multicast traffic on an RSTP ring

12.3.3.2 Parallel topology

In parallel topologies, two distinct, independent networks provide redundant paths from source to sink. In the case of PRP, the networks are operated completely in parallel. This means that the redundant networks need to be configured identically regarding multicast filtering at the junction points to other network systems and regarding subscribed end nodes.

E.g. the transition point from the process bus to LAN A is configured identically to the other transition point to LAN B in terms of multicast filtering. LAN A and LAN B themselves just must ensure that the transmission of multicast or VLAN tagged messages is transparent to the outer networks and to the publishers/subscribers. In case the parallel networks are not identical, the multicast configuration must still ascertain that a subscribing doubly attached end node receives the multicast messages from a MC group over both networks on both interfaces.

12.3.3.3 Separation of process bus and station bus

Figure 62 shows a generic network structure: On the station level, an RSTP ring is used and on the primary equipment level, a HSR ring is redundantly connected via two HSR Redundancy Boxes that are part of the RSTP ring structure and at the same time are participants in the HSR ring. The HSR redundancy boxes are therefore the points of interconnection between the process bus and the station bus and therefore, a multicast configuration has to be made on these devices.

For instance, SV multicast traffic from the process bus HSR network must not be transmitted into the station bus RSTP network. Therefore, for all configured multicast addresses, filtering entries need to be added into the configuration of both Redundancy Boxes. If the multicast configuration is done via VLANs, the corresponding VIDs can only be configured on the HSR ring interfaces, not on the RSTP ring interfaces, thus restricting SV traffic to the HSR ring. On the other hand, GOOSE traffic from the protection devices on the station bus need not be forwarded to the HSR ring.

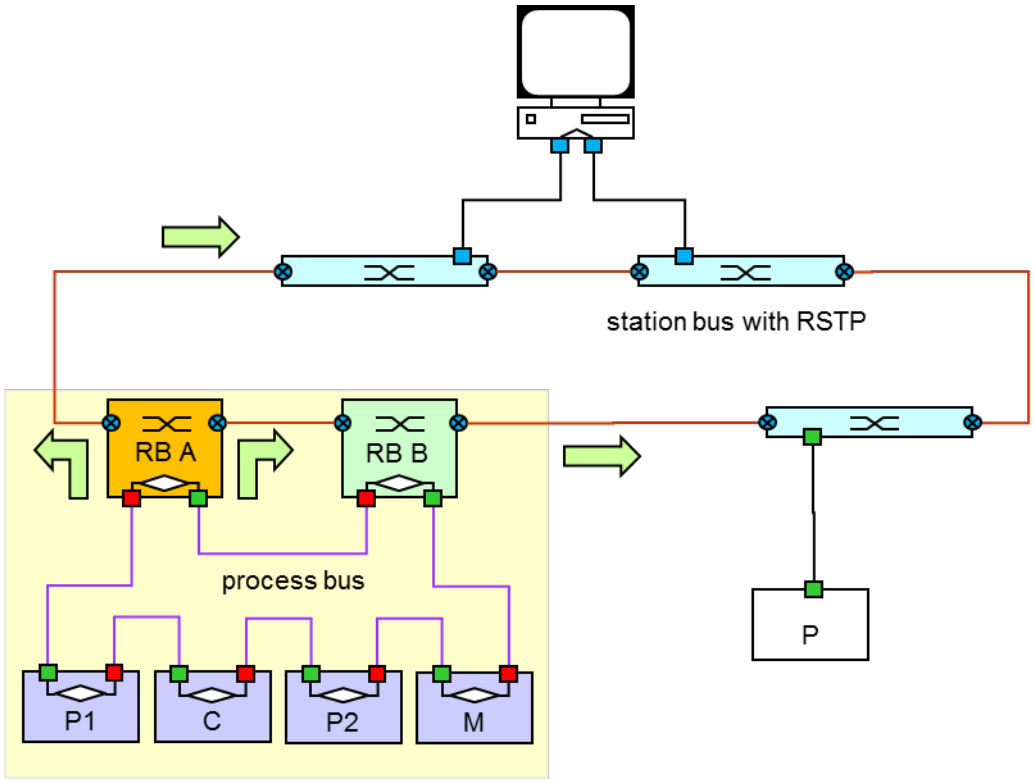


Figure 62 – RSTP station bus and HSR ring

Figure 63 shows a top level station bus network with RSTP (doubly attached using the SRP protocol to two switches) and two redundantly coupled HSR Rings on the process bus. SV data from HSR 1 needs to be transmitted to HSR 2. This means that a strict segmentation of multicasts into transmission on station bus and on process bus is not possible. Therefore, a strict multicast configuration on the RSTP station bus level ring needs to be implemented for the SV traffic. The SV traffic does not leave the top level redundant ring.

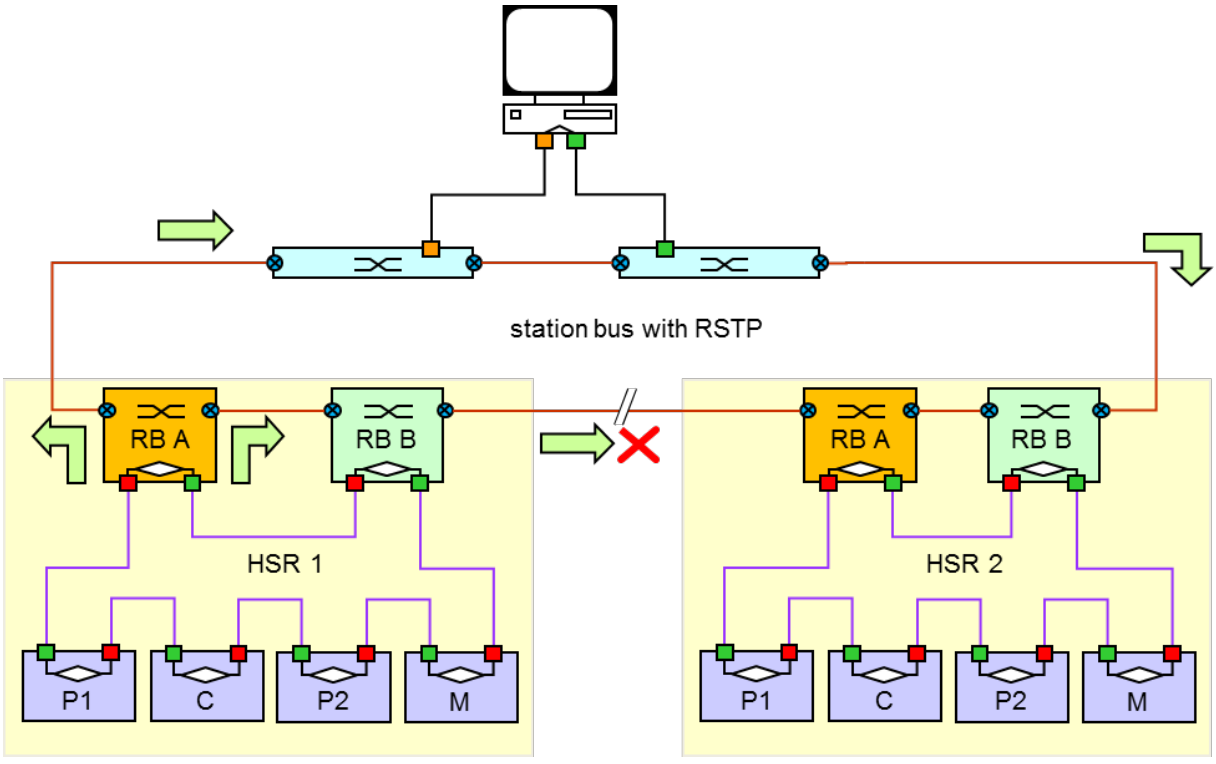


Figure 63 – RSTP station bus and HSR process bus

The junction points between individual rings are the only place to evaluate whether a specific multicast group has to pass from one network segment into another. Which multicast group has to be transmitted to which segment depends on the devices situated at each segment. With this information, the junction points between the network segments can be configured to not forward multicast traffic to network segments where there are no subscribers. The network configuration could be done e.g. with a network management tool which visualizes the network structure.

NOTE Caution is needed in network structures with multiple rings that are chained and not all directly interconnected, for instance when one or several rings do not contain subscribers for a specific multicast group, but a ring further downstream does. In this case, the intermediate rings are transit rings; multicast configuration has to be done accordingly.

12.4 Configuration support from tools and SCD files

Traffic control can be engineered with Network Engineering Tools that can graphically visualize or edit a network topology, can evaluate and modify SCD files and extract which IEDs are subscribed to which multicast groups. If the SCD file does not already contain a communication section with physical topology, the engineer wires bridges and IEDs, graphically, identifying the ports and completing the communication section of the SCD file.

The tool can configure the bridging devices (VLANs or Multicast Addresses) automatically based solely on the SCD file.

To this purpose, the SCD file should include the following:

- The topology of the network in the communication section;
- “Inputs” section in the LLN0 and other Logical Nodes as described in 9.3.13 of IEC 61850-6:2009 (not necessary if all control blocks have a complete subscriber list);
- for each control block, the subscriber list (can be deduced from the input section of all other IEDs if not present);
- for each “GSEControl” and “SampledValueControl” block defined in the IED section, the “P” elements of the type “MAC-Address”, “APPID” , “VLAN-PRIORITY” and “VLAN-ID” in the communication section.

13 Dependability

13.1 Resiliency requirements

The required behaviour of a substation automation system upon a failure of one of its parts depends on the consequence of that failure. In general, the voltage level and the importance of the connected loads dictate the dependability requirements.

A common criterion is “N-1”, meaning that complete functionality is sustained when any single component fails. The “N-1” requirement applied to the network as a whole says that the network connectivity is maintained in spite of any single failure.

A finer analysis identifies failure-prone individual functions of the automation system and how long their outage is tolerated, and which loss of production results.

For instance, a less stringent network resiliency requirement is that the loss of any single element affects only one bay.

The consequence of an unintended function is a safety issue.

This analysis yields the level of redundancy expected in the network to overcome the failure of a component.

Redundancy of the network must be separated from redundancy of the end devices. Failure of an end device can only be overcome by a back-up device. Device redundancy allows e.g. for the protection of a valuable circuit breaker by two independent IEDs (Main 1 / Main 2 protection). This is not required when enough redundancy exists in the protection hierarchy, so that another IED can trip a circuit breaker if the IED in charge is momentarily incapacitated.

The fail-independence of the two application devices must not be impaired by any network failure.

Typically, the level of redundancy required for the station bus and the process bus are different, depending on the consequences of a loss of communication on the application.

All permanent failures should be detected and reported to SCADA and network management.

13.2 Availability and reliability requirements

Utilities rarely prescribe reliability and availability figures for the network alone. Concrete figures must be derived from the functional dependability requirements.

Sometimes, only a redundant layout of the network is required.

The dependability requirements in substations are described in IEC 61850-5.

See Clause 13 for more details.

13.3 Recovery time requirements

A key parameter is how long a substation application tolerates an interruption of the communication due to recovery from a failure without consequences on the plant.

Failure to deliver in time because of traffic congestion is treated as a performance (or security) issue.

IEC 61850-5 specifies in particular the different requirements on recovery time between station bus (and more precisely IEC 61850-8-1 traffic) and process bus (or more precisely IEC 61850-9-2 traffic).

On the station bus, recovery from a failure needs to complete within a time short enough for GOOSE traffic not to be delayed beyond a critical threshold. In an engineered network, an upper bound for this recovery time must be calculable and low enough to meet IEC 61850-5. RSTP is a widely used protocol that fulfils most requirements when engineered with restrictions specified in IEC 62439-1:2010. The PRP and HSR protocols provide seamless recovery and therefore can be used on the station bus for demanding applications.

On the process bus, the tolerated disruption time must be short enough that the flow of SV is not disturbed. This calls for a redundancy scheme that provides seamless failover. For the process bus, network redundancy needs to be approached not on a basis of failover times at all but on the basis of a seamless redundancy concept with no failover time at all. Both PRP and HSR are redundancy protocols fulfil these requirements.

13.4 Maintainability requirements

Maintenance is a prerequisite to achieve dependability. According to the N-1 criteria, dependability calculations are dominated by the probability that a faulty device is not yet repaired at the time a second device fails.

Therefore, a comprehensive failure detection and maintenance strategy allows minimizing repair time.

The maintenance cost of substations depends on the criticality of the application and on the geographical constraints. For example, maintenance of remote sites or offshore wind farms is typically ten times more expensive than in case of substations where staff is on stand-by. For such applications, remote maintenance of networking equipment is highly recommended. Also modular design of equipment, field replaceable or hot-swappable modules are recommended.

13.5 Dependability calculations

Clause 7 of IEC 62439-1:2010 defines availability models and calculation methods for communication networks. These models and calculation methods can be applied to networks for energy and power utility automation.

The following issues must be addressed when calculating reliability:

- Which are the criteria for declaring the network operational in case not all elements are redundant (the N-1 criteria only holds strictly only if all elements are redundant)?
- Are degraded modes allowed (e.g. losing one bay is less severe than losing the whole substation or a voltage level)?
- Is there on the contrary a higher dependability requirement that calls for an N-2 criterion for parts of the system?
- Are the availability / reliability to be calculated on a per-function basis (protection / control) or on a per-network device basis (bridge, link, IED)?
- Are the IEDs specified as IEC 61508 devices with a Safety Integrity Level and a PFD (Probability to Fail on Demand)?
- To which extend is the critical traffic mixed with non-critical, but unpredictable traffic such as HTTP while still keeping the risk of malfunction calculable?
- What are the offered capabilities to detect a network failure? How long does it take?
- What is the typical maintenance reactivity to be considered on field for repairing a faulty device, once the failure has been detected?

These questions must be answered in the frame of an actual implementation and contract.

13.6 Risk analysis attached to "unwanted events"

The level of reliability required for the communication network depends also on the accepted level of risk attached to "unwanted events".

The "unwanted events" the system faces must be clearly specified according to the level of risk the user accepts (probability of occurrence).

The result of such risk analysis influences the level of reliability to allocate to each part of the system, including:

- the reliability requirement attached to the communication network as a whole, and the failure modes;
- the reliability requirement attached to the link of dedicated devices to the communication network and the failure modes;
- the reliability requirement of the device itself and the failure modes.

14 Time services

14.1 Clock synchronization and accuracy requirements

There is a number of precise clocks at many levels of the substation automation, in particular for time-stamped measurements, sequence-of-events and transient recorders. These clocks need to be synchronized.

Protection functions such as busbar protection and differential protection require a relative clock synchronization. Synchrophasors however require an absolute synchronization to a global time reference.

A clock is characterized by its

- accuracy, which is the mean error from the reference clock expressed in time units, e.g. 1 μs;
- precision, which is the deviation of the error from the mean, also expressed in time units, e.g. 1 ns (the clock could have an offset of 1 μs ± 1 ns);
- stability, which is the variation of the precision in time expressed in μs/s.

IEC 61850-5 defines classes of clock synchronization for different applications. The classes are summarized in Table 43, copied from IEC 61850-5 for convenience:

Table 43 – Synchronization classes of IEC 61850-5

Class	Accuracy	Usage
T1	±1 ms	Event logging.
T2	±100 μs	Zero crossing for the distributed synchrocheck.
T3	±25 μs	Class P1 protection functions.
T4	±4 μs	Class P2 protection functions (e.g. busbar protection function) and class M1. This is the class of accuracy specified in [15].
T5	±1 μs	Class P3 protection functions and classes M2/3.

The accuracy in Table 43 includes the inaccuracy within the device. For instance, IEC 61869-6 defines instrument transformer accuracy classes that comprise the whole measurement chain from the transformer to the digital output, assuming that the network clock messages applied to the device have an accuracy better than 1 μs.

14.2 Global time sources

The primary time source (called stratum 0 in NTP) relies on time broadcast by atomic clocks.

A dedicated time server within the substation receives the time signal from the outside, e.g. over long-wave radio WVBB (USA), DCF77 (Germany), MSF-60 (UK), short wave (WWV) or microwaves (GNNS: GPS, GLONASS, Galileo) satellites, which provide the highest accuracy.

When absolute time distribution is critical, a substation should rely on two redundant time servers. Some substations loose the reference signal for a longer period due to their geographical location (e.g. in a deep valley). Also, GNNS jamming (intentional or not) can occur. Solar storms have disabled GPS satellites. Therefore, the two time servers should be of different types and it is recommended to use an atomic clock as a backup. Rubidium clocks are available at affordable prices. Several clock types can be used, provided the hierarchy between the clocks is the same for all devices.

The local clock in a device keeps the time within tolerance after an outage of the reference clock only during a certain time, called the holdover time. This time depends on the quality of the quartz and the environmental conditions.

To increase the holdover time, clocks in each node need to be syntonized (tuned to the same frequency) and not only synchronized (set to the same time). This gives a longer grace time for the activation of the back-up clock upon loss of the clock master. For IEC 61850-9-2 (SV) applications, a holdover time of about 5 s is sufficient to overcome a failure of the time server, assuming that a hot standby is available.

For relative clock synchronization, absolute time is not critical as long as all clocks are synchronized to the same master clock.

Most applications do not need a high accuracy and a cost/benefit analysis is recommended.

14.3 Time scales and leap seconds

There exist several absolute time scales, in particular TAI and UTC.

TAI is the scientific time scale. It is continuously incrementing and will never be reset or discontinued.

UTC is the legal time. It is the base for the clocks of all countries. It indicates approximately 12:00:00 at solar noon in Greenwich at the spring equinox (it was formerly called Greenwich Mean Time). The Bureau International des Poids et Mesures, Paris, is responsible for the definition of UTC.

UTC and TAI proceed at exactly the same rate; both were identical some time back in 1961. Since 1961, the earth rotation slightly slowed down, days became longer. Additional fractions of seconds were regularly inserted until 1972, when it was decided to insert only full seconds, called leap seconds. Since then, when the difference between UTC and solar noon exceeds 0,9 s, which happens after some years, the Bureau International des Poids et Mesures adjusts UTC by letting all clocks insert a leap second, so the last minute of a day (in principle the 31st of December or the 30th of June) lasts 61 s. The reverse case is theoretically possible, but is very unlikely that the Earth starts spinning faster.

Leap seconds insertion cannot be anticipated, since irregularities of the earth's rotation are unpredictable. After 2012, June 30th, UTC lagged behind TAI by 35 s, so when TAI time says it is 2012-10-17 12:00:00, UTC says it is only 2011-10-17 11:59:25.

When a leap second is introduced, the time counter is set back by one second (or the second counter is not incremented at the end of the last second of a minute). Thus, during one leap second, time stamps can have the same value as in the second before. This means that a measurement taken a few milliseconds before the leap second was inserted will have a time stamp that is later than a measurement taken a few milliseconds after insertion.

To deduce TAI time from UTC time, a table of all elapsed leap seconds is needed. UTC cannot be predicted for a given TAI, since introduction of a leap second is an arbitrary decision. The system of leap seconds is still subject to discussion and could be revised in 2015, according to a decision of the ITU in January 2012.

Some protocols such as NTP/SNTP and IRIG-B transmit UTC time and indicate if a leap second will take place at the end of the current minute. Unfortunately, they do indicate the number of accumulated leap seconds so the calculation of time differences over a long period of time requires an up-to-date table containing all elapsed leap seconds and the date at which they were introduced. Also, a clock that was not connected during some minutes before the leap second will not be informed of the jump and will experience a delay in synchronizing.

Recent protocols such as PTP and GPS use the TAI time scale (with different, but constant offsets). They both indicate the accumulated number of leap seconds and if a leap second is pending, so that UTC can be deduced from TAI.

14.4 Epoch

When expressed in digital form, time is counted since an arbitrary date, called the epoch. For instance, in a Unix machine, the epoch of the time counter is 1970, January 1st, 00:00:00. Since the size of the time counter is limited, at some point in time, the time value wraps around, and a new epoch starts.

For instance, Unix uses a signed 32-bit counter for the seconds which will wrap around 19th of January 2038 around 03:14:08 UTC. NTP is represented by an unsigned 32-bit integer for the seconds and an unsigned 32-bit integer for the binary fractions of a second. NTP has an epoch of 1900, January 1st, 0 h and its 32-bit second counter will wrap around 2036, February 7th, i.e. before the Unix wrap.

NOTE In fact, NTP specifies TAI with an epoch of 1st of January 1900, but informatics engineers interpreted this as UTC. Some ask to go back to TAI.

The IRIG-B protocol carries the date in BCD form, so the epoch is day zero of the Julian Calendar.

PTP's epoch is 1970, January 1st 0 h while GPS's epoch is 1980, January 6th, 0 h, the day the first satellite was launched.

14.5 Time scales in IEC 61850

When engineering a substation, it is critical to use only one time base, preferably TAI, since only TAI allows an unambiguous time-stamping also during leap seconds and the building of time differences across leap seconds. Any other should be derived from TAI.

The UTC time scale should be used for human displays, but not for time-stamping or sequence-of-events recorders. The UTC time transmitted by IEC 61850 messages should be corrected by the amount of leap seconds (indicated by the clock synchronization protocols). Indeed, wide-area systems using phasors or differential protection schemes could suffer disruptions when the clocks of the different measurement units leap at about the same time.

IEC 61850-7-2:2010, defines two time representations:

- TimeStamp counts seconds and binary fraction of seconds in a 56-bit counter since 1970-01-01 00:00:00, plus an 8-bit indication of time quality, which tells if the UTC or the TAI scale (LeapSecondsKnown=false) is in use, if the clock is in operation, if the clock is synchronized to a global reference, and which accuracy (number of significant digits) it has.
- EntryTime which is assumed to be an internal time representation with an epoch of 1984-01-01 00:00:00. This representation is used only for log entries. It carries no time quality.

Annex E of IEC 61850-8-1:2011 describes the mapping of

- TimeStamp to MMS type UtcTime (ASN.1 Type OCTET STRING [8]) which is a 64-bit counter which counts multiples of 2^{-32} s since 1970-01-01 00:00:00, but leaves the use of the least significant 8 bits undefined, possibly random.
- EntryTime to MMS type TimeOfDay (ASN.1 Type Btime6 or OCTET STRING [6]) which counts milliseconds since midnight and days since 1984-01-01 on the GMT scale.

IEC/TR 61850-90-5 (Synchrophasor transmission) and IEC/TR 61850-90-1 use TimeStamp.

NOTE UtcTime is an extension of ISO 9506-1 and ISO 9506-2 defined in IEC 61850-8-1. TimeOfDay is defined in ISO 9506-1 and ISO 9506-2.

Measurement synchronization according to IEEE C37.118-1 and IEEE C37.118-2 uses a representation similar to TimeStamp, but the scale is always UTC and the quality information is coded differently and at another place in the message.

The IRIG-B time representation is complex since it carries the number of seconds since midnight and the same time quality field as IEEE C37.118. There is no fraction of second since IRIG-B is sent always exactly when a second starts. The reception of the header indicates the second.

Table 44 compares the different time representations used in utility automation.

Table 44 – Time representations

Protocol	Scale	Time representation	Epoch	Ends
RFC 1305 (NTP)	UTC (TAI)	time of reception contained in the message, expressed as 32-bit signed integer: seconds since epoch 32-bit signed integer: binary fractions of second	1900-01-01	2036
Unix	UTC (TAI)	32-bit signed integer: seconds since epoch	1970-01-01	2038
IEC 61588 (PTP)	TAI	time of reception contained in the message, expressed as 48-bit unsigned integer: seconds since epoch 32-bit unsigned integer: scaled nanosecond counter	1970-01-01	9 Mio years
IEC 61850-7-2 IEC 61850-8-1 TimeStamp	UTC & TAI	32-bit unsigned integer: seconds since epoch 24-bit unsigned integer: binary fractions of second 8-bit TimeQuality (UTC/TAI, locked, significant digits) 'sssssssssssssssssssssssssssssssssffffffffffffffffffffffffqqqqqqqq'B	1970-01-01	2106
IEC 61850-8-1 UtcTime mapping of TimeStamp	UTC & TAI	32-bit unsigned integer: seconds since epoch; 32-bit unsigned integer: binary fractions of second (use of least significant 8 bits undefined) ASN.1 Octet String [8]	1970-01-01	2106
IEC 61850-7-2 EntryTime	UTC	32-bit unsigned integer: millisecond counter: 16-bit unsigned integer: day counter	1984-01-01	2163
ISO 9506-1 ISO 9506-2 TimeOfDay BINARY-TIME	UTC	32-bit millisecond counter; 16-bit day counter (optional) '0000ttttttttttttttttttttttttttt'B or '0000ttttttttttttttttttttttttttddddddddddddddd'B ASN.1 Octet String [4|6]	1984-01-01	2163
IEC 61850-8-1 TimeOfDay mapping of EntryTime	UTC	32-bit millisecond counter 16-bit day counter (optional) Octet String [6] '0000ttttttttttttttttttttttttttddddddddddddddd'B	1984-01-01	2163
IEEE C37.118 Synchrophasor Measurement and transmission	UTC	32-bit unsigned integer: SOC seconds since epoch 8-bit time quality (special format). 24-bit unsigned integer: FRACSEC fraction of second 'sssssssssssssssssssssssssssssssqqqqqqqqfffffffffffffffffffffff'B	1970-01-01	2106
IRIG-B	UTC	Second defined by reception of the signal, time expressed BCD representation of date and straight number of seconds	none	none
ISO 8824-1 ASN.1 UTCtime	any	Visible String not to be confounded with UtcTime	none	none

14.6 Synchronization mechanisms in IEC 61850

14.6.1 Clock synchronization protocols

IEC 61850-8-1 and UCA 61850-9-2LE [15] respectively recommend these clock synchronization protocols:

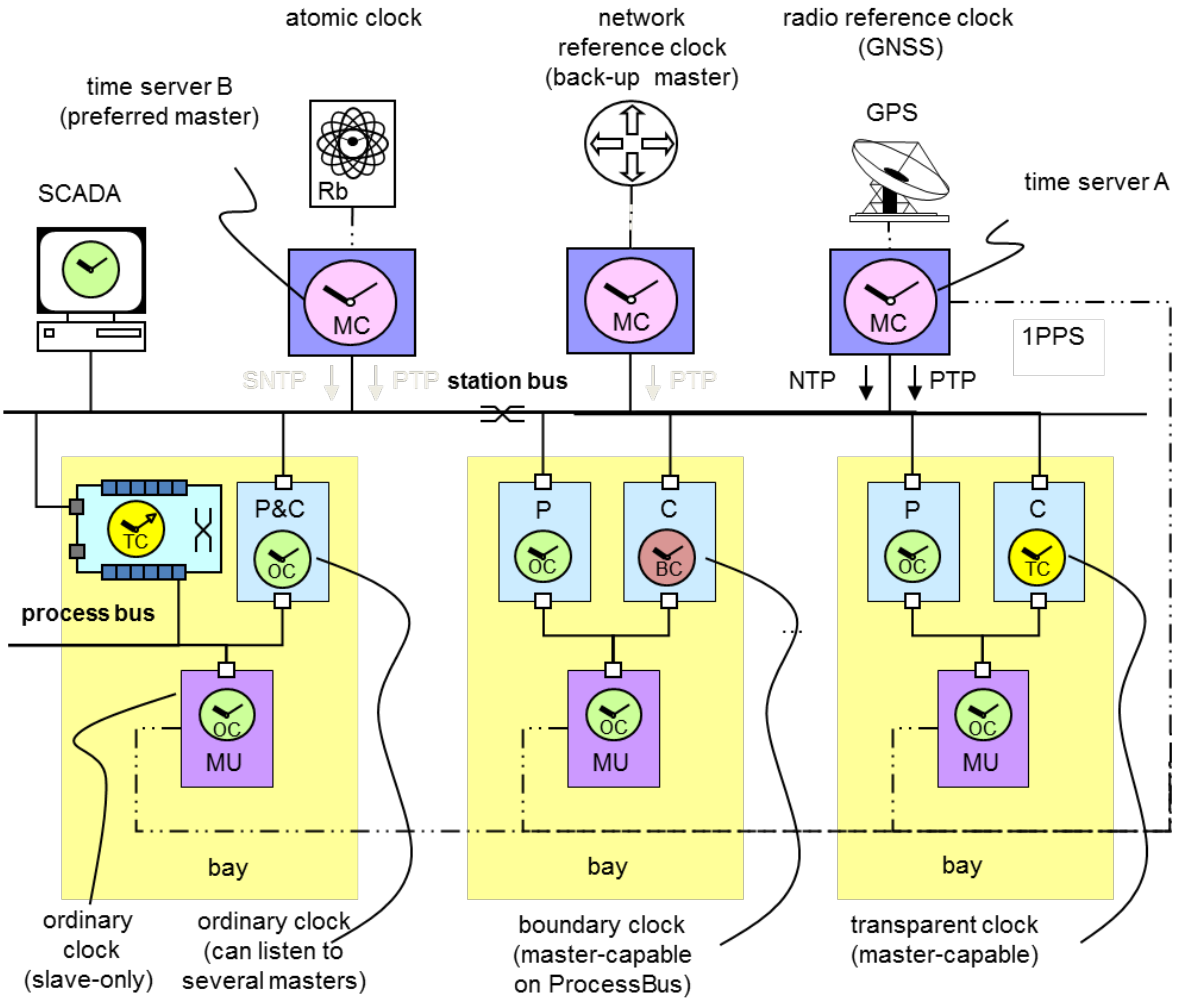
- 1 PPS (see 14.6.2);
- IRIG-B (see 14.6.3);
- SNTP (see 14.6.4);
- PTP (see 14.6.5).

Figure 64 shows an example of several arrangements of the clock synchronization within in a substation.

The GPS receivers indicate the absolute time, a back-up atomic clock protects against GPS loss. These clocks can generate a 1 PPS signal over a dedicated wiring, and/or send the time information over SNTP or PTP.

The merging units on the process bus are synchronized by 1 PPS, using dedicated wiring, as UCA 61850-9-2LE foresees.

IEC 61869-9 foresees that the merging units are synchronized over PTP through a transparent clock or a boundary clock in the IED that bridges the station bus and the process bus. This IED can become the time source in case the station bus time distribution becomes unavailable. Instead, a dedicated bridge may be used (left device in Figure 64).



Key

BC	boundary clock (master-capable)
MC	master-capable clock
OC	ordinary clock
TC	transparent clock

Figure 64 – Clock synchronization channels

14.6.2 1 PPS

1 PPS is a frequently used synchronization that sends a continuous train of pulses at a frequency of one pulse per second over a twisted wire pair or an optical fibre. 1 PPS does not carry the absolute time. The rising edge and duration are specified in 6.2 of IEC 60044-8:2002, as shown in Figure 65.

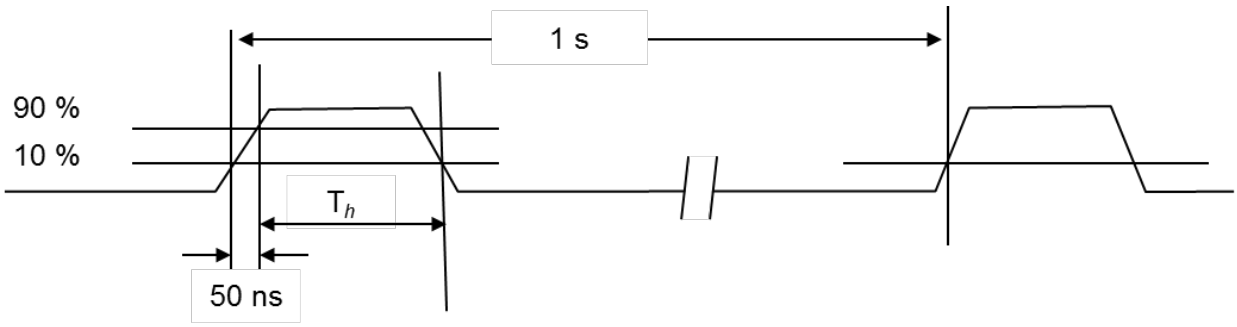


Figure 65 – 1 PPS synchronisation

UCA 61850-9-2LE [15] specifies an accuracy class of T4 and the synchronization by a 1 PPS signal generated by a GPS receiver and possibly carried by a dedicated network, e.g. direct fibre links to each device that needs precise synchronization (e.g. merging units).

UCA 61850-9-2LE makes a distinction between the accuracy of the source of synchronization, which is 1 μs, and the accuracy of the actual time stamping of the data, which is 4 μs.

IEC 61869-9 defines that the synchronization by 1 PPS may not exhibit more than ±2 μs of inaccuracy. It also specifies that a pulse width T_h longer than 5 μs implies that the source is a global reference clock while a pulse width T_h shorter than 1,1 μs indicates a local reference clock.

14.6.3 IRIG-B

IRIG-B is a time synchronisation protocol which defines a train of pulses encoding the UTC date as BCD numbers, with additional indication of the clock traceability and quality. This train of pulses can be modulated over a radio signal, or sent as baseband over a simple twisted wire pair or optical fibre. Bus topologies and point-to-point are used with different kinds of links.

There exist several variants of IRIG-B. The synchrophasor measurement and transmission standards C37.118-1 and C37.118-2 (formerly IEEE 1344) define the use of IRIG-B 200-04 with the addition of a continuous time quality field that indicates the inaccuracy when the reference signal is lost. These documents contain an extensive description of the protocol.

UCA 61850-9-2LE [15] mentions IRIG-B as an alternative to 1 PPS.

14.6.4 NTP/SNTP clock synchronization for IEC 61850-8-1 (station bus)

IEC 61850-8-1 specifies that synchronization is to be achieved through SNTP. SNTP is a simplified version of NTP; both use the same message formats.

SNTP uses a clock hierarchy of several levels, called stratum. The highest stratum is linked to a reference atomic clock.

SNTP is implemented in most PCs as part of the communication stack. Usual implementations provide a precision of about 1 ms within a substation LAN.

SNTP carries UTC, although some interpret it as TAI. The 64-bit timestamps used by NTP consist of a 32-bit seconds counter and a 32-bit fractional second part, giving NTP a time scale that rolls over every 2^{32} s (136 years) and a theoretical resolution of 2^{-32} s (233 ps). SNTP has an epoch of 1st of January 1900. The first rollover will occur in the year 2036, prior to the UNIX year 2038 problem (see IETF RFC 4330), introducing a 200 ps interval in which time is invalid (all zero).

This rollover will occur within the lifespan of presently delivered devices. Therefore, unless a NTPv.4 protocol is used, testing and workaround is recommended.

NOTE As there exist probably no archived NTP timestamps before bit 0 was set in 1968, a convenient way to extend the useful life of NTP timestamps is the following convention: If bit 0 (MSB) is set, the UTC time is in the range [1968..2036], and UTC time is reckoned from 0 h 0 m 0 s UTC on 1 January 1900. If bit 0 is not set, the time is in the range [2036..2104] and UTC time is reckoned from 6 h 28 m 16 s UTC on 7 February 2036.

SNTP operates over UDP/IP (layer 3) using port 123, and therefore crosses routers.

The SNTP clock synchronization is initiated by the client (slave clock), who sends a time request to the server (master clock, higher stratum), which responds with the current time, as shown in Figure 66.

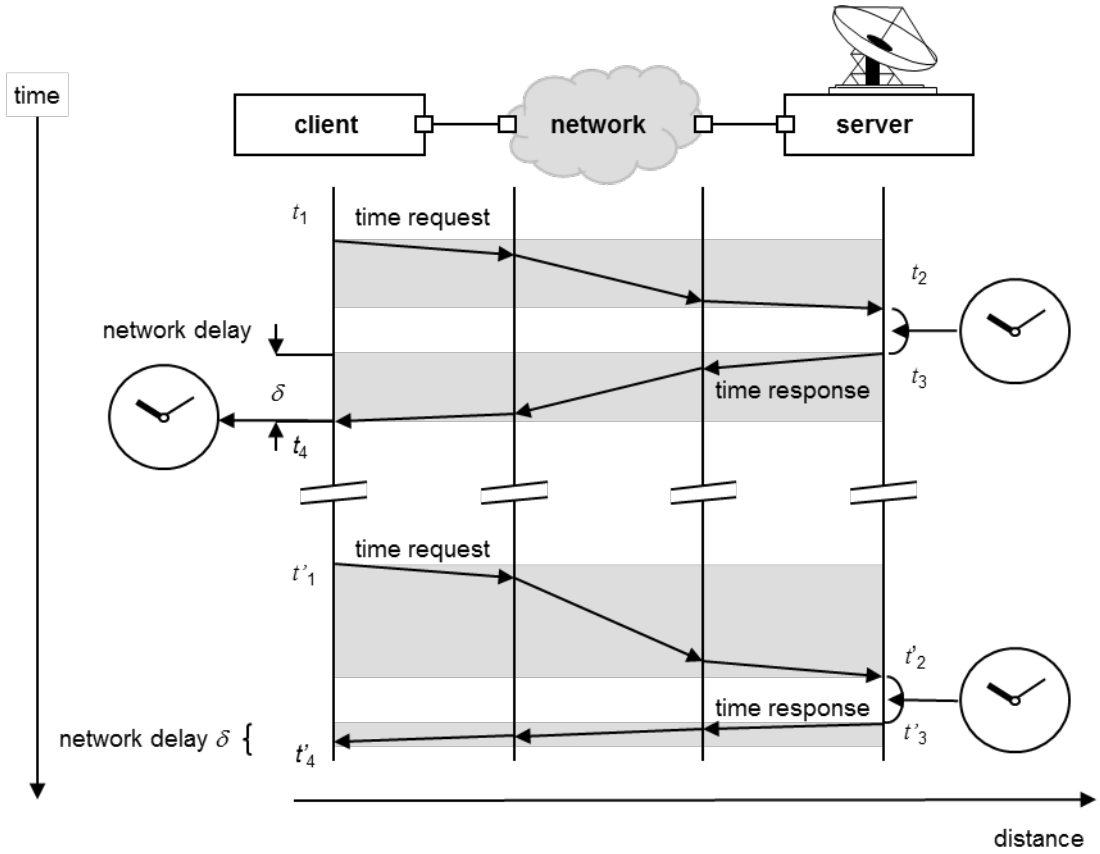


Figure 66 – SNTP clock synchronization and delay measurement

The client needs to compensate for the delays in the network by calculating the round-trip delay between the clock server and itself. To this effect, the client registers its local time when sending the request (transmit timestamp) and registers its local time when receiving the response (receive timestamp). The server also registers its local time when it received the request and includes this time in the response, together with the time at which it sent the response. The client adds to the clock time the network delay δ, which it estimates as:

$$\partial = \frac{(t_4 - t_1) - (t_3 - t_2)}{2}$$

where

t_1 is the time the client sent the request;

t_2 is the time the server received the request;

t_3 is the time the server sent the response;

t_4 is the time at which the client received the response.

This calculation assumes that the delays in the network are symmetrical, i.e. the request and the response take the same path and that each router takes the same amount of time to treat each message. For instance, the lower part of Figure 66 shows an asymmetrical round trip delay which then leads to an incorrect estimation of the network delay. Cleverer algorithms consider the average over several measurements and known asymmetries. This method is limited by uncertainty due to asymmetrical transmission and varying residence delays in the routers and bridges, possibly due to overload. This uncertainty cumulates with the number of hops. The residence delays in NTP are imprecise, because the NTP protocol is handled in software at layer three and the time-stamping is done with no hardware support.

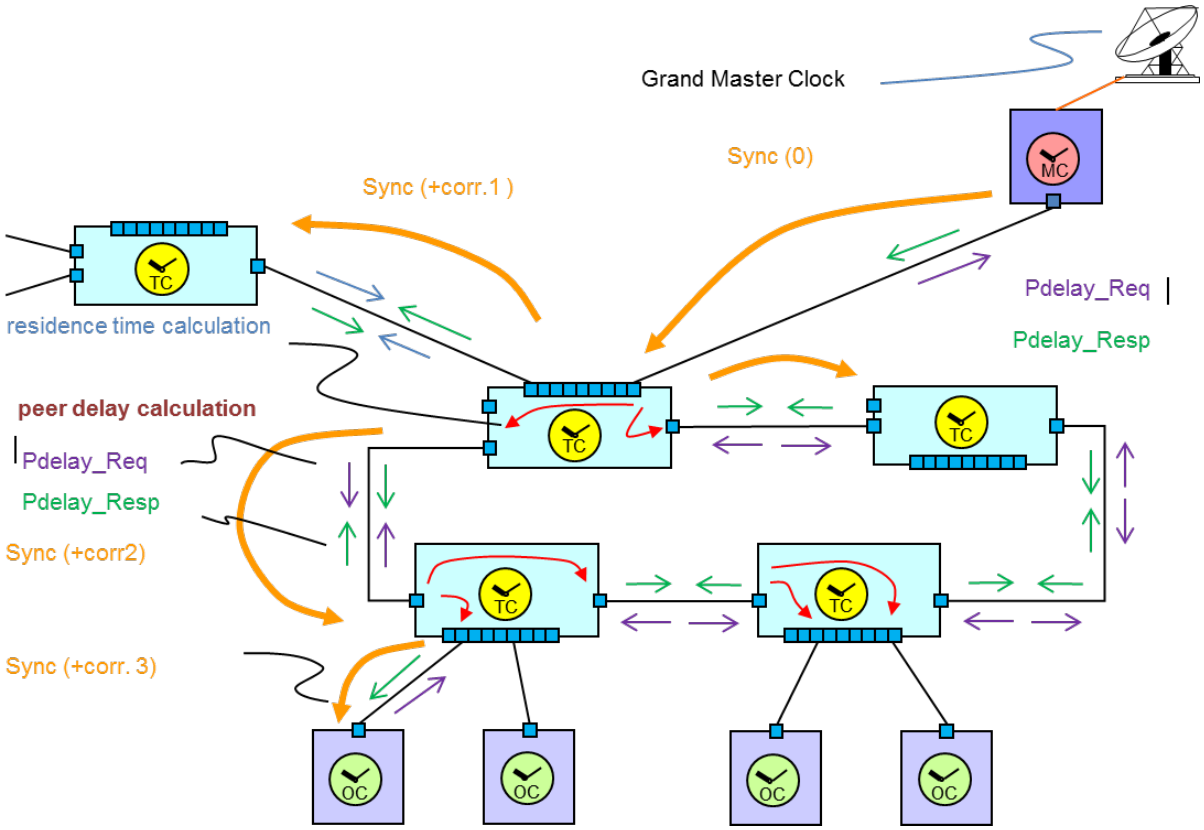
For precise synchronization using SNTP, network engineers should care that the network presents a symmetrical behaviour regarding the path that a time request and time response take. This is best ensured if the routers use pre-established routes rather than routes chosen depending on the network load.

14.6.5 PTP (IEC 61588) synchronization

14.6.5.1 PTP elements

PTP distinguishes the following elements as shown in Figure 67:

- Grand master clock (GMC), that is the top-level master clock controlling a time domain and which is usually connected to a reference signal (GPS or atomic clock).
- Master clocks (MC), that is the clock that is sending the time synchronization message Sync within a subdomain, either as grand master or as a boundary clock (on behalf of the Grand Master).
- Ordinary clocks (OC), that can be either slave or master clocks. Master-capable clocks can become master (of a subdomain) or grand-master (of the top subdomain).
- Transparent clocks (TC), that forward the Sync messages and correct the time by evaluating the peer delay and residence delay of Sync messages.
- Hybrid clocks (HC), that combine a transparent clock and an Ordinary Clock
- Boundary clocks (BC), that have a slave port synchronized by a master clock and a master port that controls a time sub-domain. Even if it is a bridge, it does not forward the messages it receives from the upper-level master to its sub-domain, but sends its own PTP messages, possibly with a different period.



Key

MC	master clock
OC	ordinary clock
TC	transparent clock

Figure 67 – PTP elements

14.6.5.2 PTP operation

Contrarily to SNTP, which relies on a client-server scheme in which the client takes the initiative of asking the server time, PTP relies on a master-slave scheme, in which the time master takes the initiative of time transmission, with no knowledge of the slaves.

The time master broadcasts periodically (e.g. every 1 s) a Sync message containing its reference time. This Sync message transits through the network and suffers a network delay consisting of the link delays λ and of the residence delays ρ in the bridges, before it reaches the slave clocks. Figure 68 shows the (one-step) PTP clock to explain the principle.

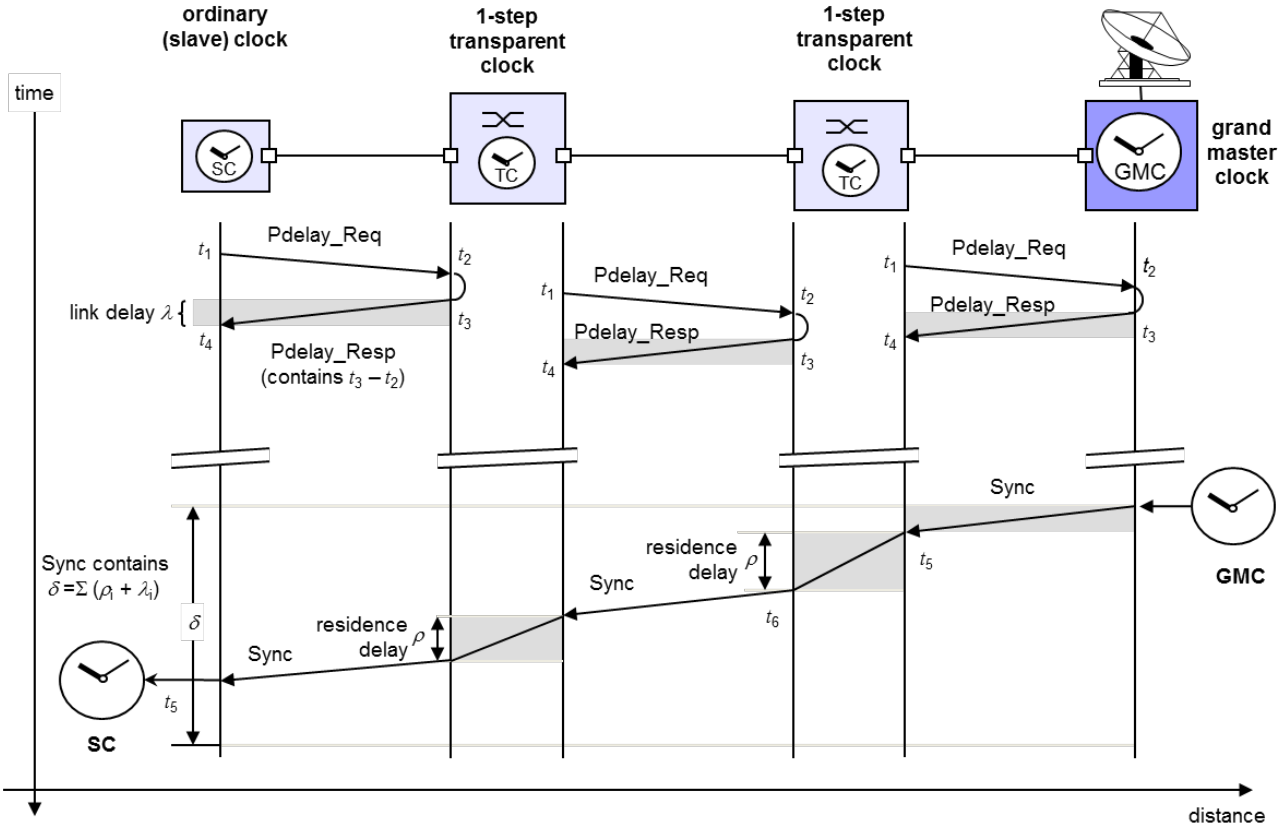


Figure 68 – PTP one-step clock synchronization and delay measurement

While SNTP communicates at layer 4 (UDP), the profile of PTP for utility automation uses only layer 2 multicast. This means that routers must implement boundary clocks to keep network segments synchronized.

NOTE 1 PTP also foresees a UDP multicast and unicast communication, but within a substation, only layer 2 communication provides the sufficient accuracy.

Contrarily to SNTP, each clock in the network calculates the link delay to its neighbours. This is called a “peer-to-peer delay” mechanism. All devices must be PTP-aware.

NOTE 2 PTP foresees also an “end-to-end delay” calculation similar to SNTP but within a substation only “peer to peer” delay calculation can provide the required accuracy.

A clock calculates the link delay λ to the next node by sending a Pdelay_Request, to which the other node responds with a Pdelay_Response containing the time between reception of the Pdelay_Request and the Pdelay_Response. The clock calculates the link delay λ as:

$$\lambda = \frac{(t_4 - t_1) - (t_3 - t_2)}{2}$$

Since the asymmetry of a link is very small (some nanoseconds), the delay can be better estimated than in NTP.

Each bridge holds a transparent clock, which calculates a correction value as the sum of its link delay λ to the clock from which it received the Sync, of any correction κ that came along with the Sync it received and of its own residence delay ρ:

$$\rho = (t_6 - t_5)$$

NOTE 3 Timestamps for computing the residence delay are taken from the node's local clock. Since these accumulated residence delays are used by a slave to adjust the time provided by a master, errors resulting from differences in the rates of the master and the transparent clocks should be negligible. For instance, if the rates of the master and local clocks differ by 0,01 %, the error introduced can reach 0,01 % of the measured residence delay. For a residence delay of 1 ms, the maximum error amounts to 100 ns in each bridge (a 1 ms residence time is a pessimistic case at 100 Mbit/s when PTP does not have the highest priority). This inaccuracy accumulates in a chain of transparent clocks. Therefore, syntonizing the local clocks of transparent and boundary clocks may be necessary to achieve the required accuracy.

The ordinary (slave) clocks receive the Sync and compensate the received reference time by the network delay.

Two methods exist to correct the transmitted time, "one-step" and "two-step" clocks.

14.6.5.3 PTP one-step clock correction

Each transparent clock adds its correction ($\lambda + \rho + \kappa$) to the Sync message's correction field while the frame is being transmitted over the egress port. This method requires a dedicated hardware to timestamp the start of the message, calculate and modify the correction field and the checksum of the outgoing Sync frame and insert it into the message body while parts of the message have already been transmitted. This "on-the-fly" correction can be applied both to cut-through and to store-and-forward bridges (see Figure 68).

14.6.5.4 PTP two-step clock correction

To avoid a dedicated hardware for modifying the Sync message on-the-fly, a two-step clock records the precise time at which it received the Sync, forwards the Sync message with the uncorrected time, and records the precise time at which it sent the Sync. There exist dedicated PHY chips that time-stamp messages within a few ns. Sending the Sync message is not time-critical, it can be done by a CPU.

The two-step transparent clock calculates the correction field as the sum of the ingress Sync correction κ, the residence delay ρ and the (previously measured) peer delay λ and sends a Follow_Up message with a new time correction κ as shown in Figure 69. The same scheme applies to the calculation of the peer delay.

The receiver assumes that Sync and Follow_Up messages are paired; they have the same PTP sequence number.

NOTE PRP and HSR present a special case that is explained in 14.6.6.2, since pairing of Sync, Follow_Up and Announce must be observed.

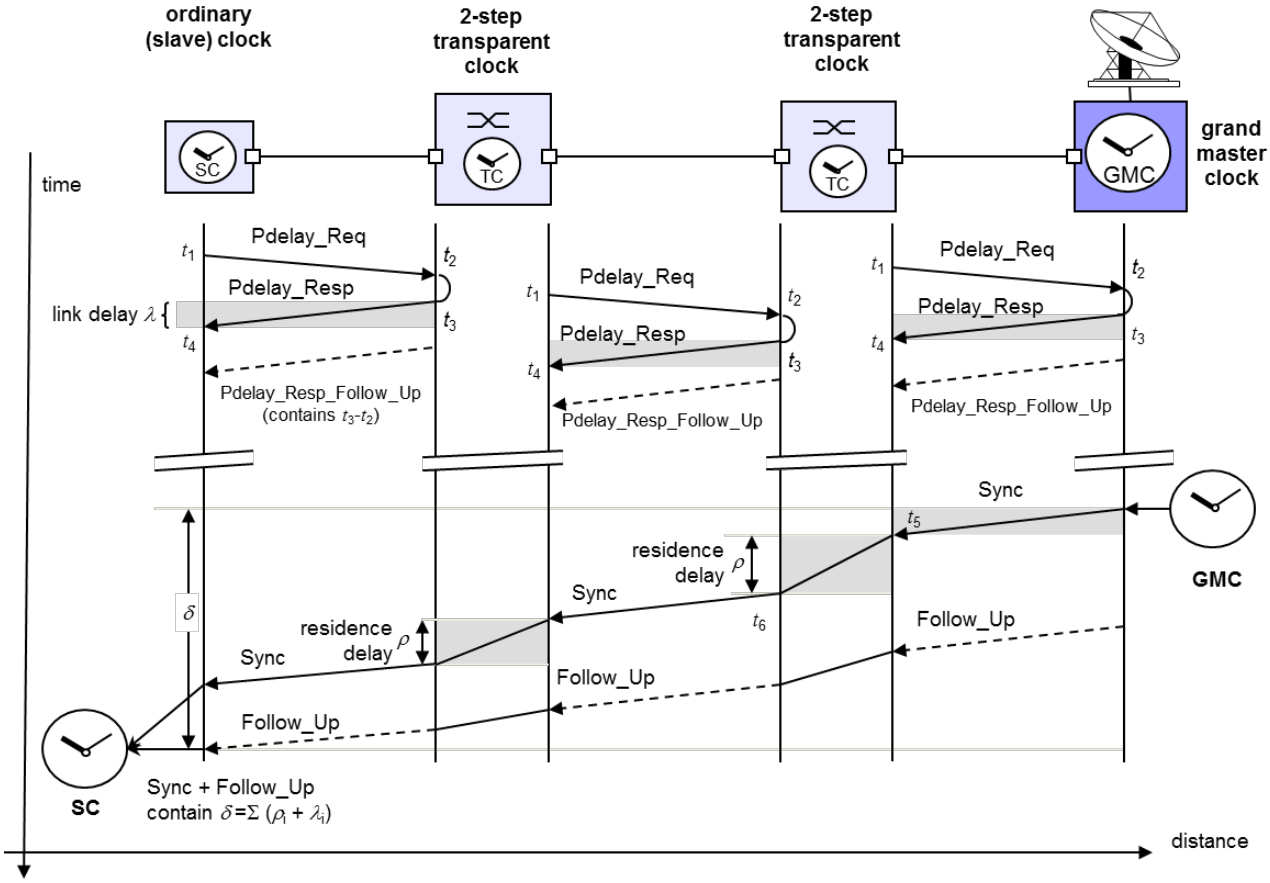


Figure 69 – PTP two-step clock synchronization and delay measurement

The engineer is faced with two synchronization methods, depending on the ability of its devices. Commercial clocks use mainly two-step PTP, few offer one-step clocks. The two systems can be mixed if devices accept both one-step and two-step clocks.

14.6.5.5 PTP BMC algorithm vs. alternate master

Initially, the Best Master Clock (BMC) algorithm elects a master clock among the master-capable clock nodes participating in the network. To this effect, each master clock broadcasts Announce messages which carry their clock quality information. The clock with the best clock quality wins and becomes master, while the other master-capable devices keep on listening for its Announce messages, but do not send their own unless a failure occurs.

When a master clock fails or degrades (loss of satellites in GPS), a back-up master clock takes over. The back-up detects failure or degradation of the master by listening to its Announce messages. A time-out on the Announce messages causes the back-up master clocks (if there are several of them) to compete for the role of master by applying the BMC algorithm.

To speed up election, the alternate master option defined by IEC 61588 is recommended. This option allows alternate masters that are not currently the best master to exchange PTP timing information with slave ports, and for a slave port to acquire knowledge of the characteristics of the transmission path between itself and each alternate master, even if it does not use it currently. This allows a fast switchover to an alternate master with a small phase excursion when the master fails.

To speed up recovery, the preferred back-up master is configured with an Announce time-out shorter than the Announce time-out of other master-capable ordinary clocks (e.g. to 2,0 s).

Such mechanism reduces collisions in case several master clocks try to become masters after a failure of the master in charge.

14.6.5.6 PTP Announce interval and holdover time

In case of loss of the master, a slave clock is required to keep on ticking with a sufficient accuracy during a holdover time (5 s) until the back-up clock takes over. This implies that in addition to synchronization, nodes must syntonize their clocks (tune their frequency).

14.6.5.7 PTP time domains

It is recommended to consider the substation as a single time domain and not to use user-defined time bases.

14.6.5.8 PTP migration path from legacy protocols

PTP slave clocks can be used to provide a 1 PPS signal for legacy equipment, without the need for additional GPS receivers or a separate timing network.

The migration path towards systems with PTP based clock synchronization requires a transitional period when networking devices will have to support both the new PTP protocol in parallel with SNTP or IRIG-B. It will take some time until protection and control IEDs receive PTP slave functionality. Therefore a PTP enabled network could let the bridge act as a boundary clock, PTP slave on one side and SNTP, 1 PPS or IRIG-B master towards the legacy devices. Such a scenario has the advantage of being future-proof as in case of upgrades of IEDs to PTP, no modifications would be required to the bridges in all protection and control cabinets as these are already PTP-enabled.

14.6.6 PTP clock synchronization and IEC 62439-3:2012

14.6.6.1 PTP profile in IEC 62439-3:2012

Annex B of IEC 62439-3:2012 provides a profile of IEC 61588 suitable for industrial automation networks that considers peculiarities of PRP and HSR.

Annex B of IEC 62439-3:2012 aims at reaching an accuracy of 1 μs in a maximum size network consisting of a series of up to 16 transparent clocks.

Each transparent clock uses a local oscillator with a drift of less than 15 μs/s which, once syntonized, is expected to keep an accuracy of 1 μs/s within the holdover time of 5 s.

The master clockAccuracy according to 7.6.2.5 of IEC 61588:2009 is expected to be better than class 0x20 (25 ns) during the holdover time.

The profile of IEC 62439-3:2012 is characterized as follows:

a) all network elements (masters, end nodes, bridges, media converters,...) support transparent clocks;

b) boundary clocks may exist at the outskirts of the grandmaster multicast domain;

c) each transparent clock introduces less than 50 ns of inaccuracy in the correction field of forwarded Sync messages;

d) media converters (e.g. fibre – copper) introduce less than 50 ns of jitter each;

e) cable asymmetry does not exceed 25 ns;

f) only Ethernet layer 2 communication is used (UDP communication is not used);

g) only multicast messages are used (unicast messages are not used);

h) only peer-to-peer delays are calculated (end-to-end path delay computation is not used);

i) both 1-step and 2-step synchronization are allowed (one-step is preferred);

j) best Master Clock algorithm applies to all clocks (including slave clocks);

k) default settings are specified as:

- Announce message period (logSyncInterval=0): once every 1 s,
- Sync messages period (logAnnounceInterval=0): once every 1 s,
- Timeout for Announce messages (announceReceiptTimeout=3): wait 3 s (can be set to 2 s for the preferred redundant master),
- Pdelay_Request period (logMinDelayReqInterval=0): once every 1 s,
- Holdover time: accuracy kept within 1 μs after reference signal loss: at least 5 s,
- Priority1 is 128 for grandmaster-capable devices, 255 for slave-only devices,
- Priority2 is 128 for grandmaster-capable devices, 255 for slave-only devices,
- The grandmaster clockClass is 6 or 7 (when degraded), respectively,
- DomainNumber is 0.

14.6.6.2 PTP clock synchronization on PRP

The PRP redundancy concept foresees that the grandmaster clock is doubly attached to both LANs, either as DANP or through a RedBox.

It is also possible that two different master clocks emerge, one in each LAN. This situation can occur in a degraded situation in which the link to the master fails on one LAN and a back-up master is elected on that LAN. It may also occur when boundary clocks are used.

Ordinary clocks have two ports (this is the only difference with 3.1.22 of IEC 61588:2009) and are also attached to both LANs.

An ordinary clock receives the Sync (and possibly Follow-Up) and Announce messages from each LAN independently. Duplicate Discard does not apply since intermediate transparent clocks (e.g. in bridges) are not aware of the redundancy trailer and could remove the trailer with its sequence number when forwarding the Sync after modification.

As 9.3 of IEC 61588:2009 prescribes, all PRP ordinary clocks implement the BMCA specified in over both ports to select their master. Under normal conditions, they receive the same master over the two channels and accept both PTP Syncs.

Even if PRP-A and PRP-B have extremely different hop counts, the time correction in each LAN ensures that the time stamp is accurate, with just a higher jitter from the LAN with the largest number of hops. The clock control algorithm can weigh the time information differently depending on the magnitude of the time correction.

A slave ordinary clock treats therefore each side as a different clock, but as long as the clocks on both sides have the same grandmaster identity, it combines the received synchronization messages to improve its accuracy. The slave clock may use for this purpose the sequence numbers of the PTP messages. Otherwise, it selects the best quality master.

14.6.6.3 PTP clock synchronization on HSR

When the master clock is an HSR device, each other HSR node normally receives two Sync messages with different delays (and therefore different contents) from opposite sides of the ring. Therefore, on a HSR network, the duplicate discard scheme does not apply to PTP messages. Each direction is treated as a separate clock, nodes utilize both Syncs to synchronize and syntonize their clocks. When two-step clock correction is used, a node aggregates the Sync and Follow-Up from each direction separately.

From a PTP point of view, an HSR node acts both as a transparent clock and as an ordinary clock; this is called a hybrid clock. A transparent clock can introduce a delay of up to 125 μs (even if the transparent clock treats PTP messages with the highest priority) since ongoing transmissions cannot be interrupted. The worst-case time inaccuracy of a transparent clock as given in its data sheet (PICS) or MIB should not exceed 50 ns.

Since a ring can have up to 50 nodes in series, the delay (ring worst-case 6,25 ms) and jitter (ring worst-case 2,5 μs) can become significant. Indeed, phasor measurement units require a time inaccuracy of less than 1,0 μs. Therefore, the timing of the network must be checked at engineering time and, if insufficient for the application, the ring must be split.

It is recommended to locate the redundant masters at opposite diameters of the ring to limit the number of hops.

14.6.6.4 Coupling PRP and HSR clocks

When coupling a PRP network to an HSR ring, the two RedBoxes handle the Sync messages coming from the grand master clock. Therefore, in the case the PRP network operates with two-step clock correction, the RedBoxes translate the two-step clock messages Sync + Follow_Up to a one-step Sync message in the HSR ring. The RedBoxes in the HSR ring should be ideally located at opposite positions in order to limit the number of hops (or transparent clocks) for each node of the ring in the normal case as shown in Figure 70.

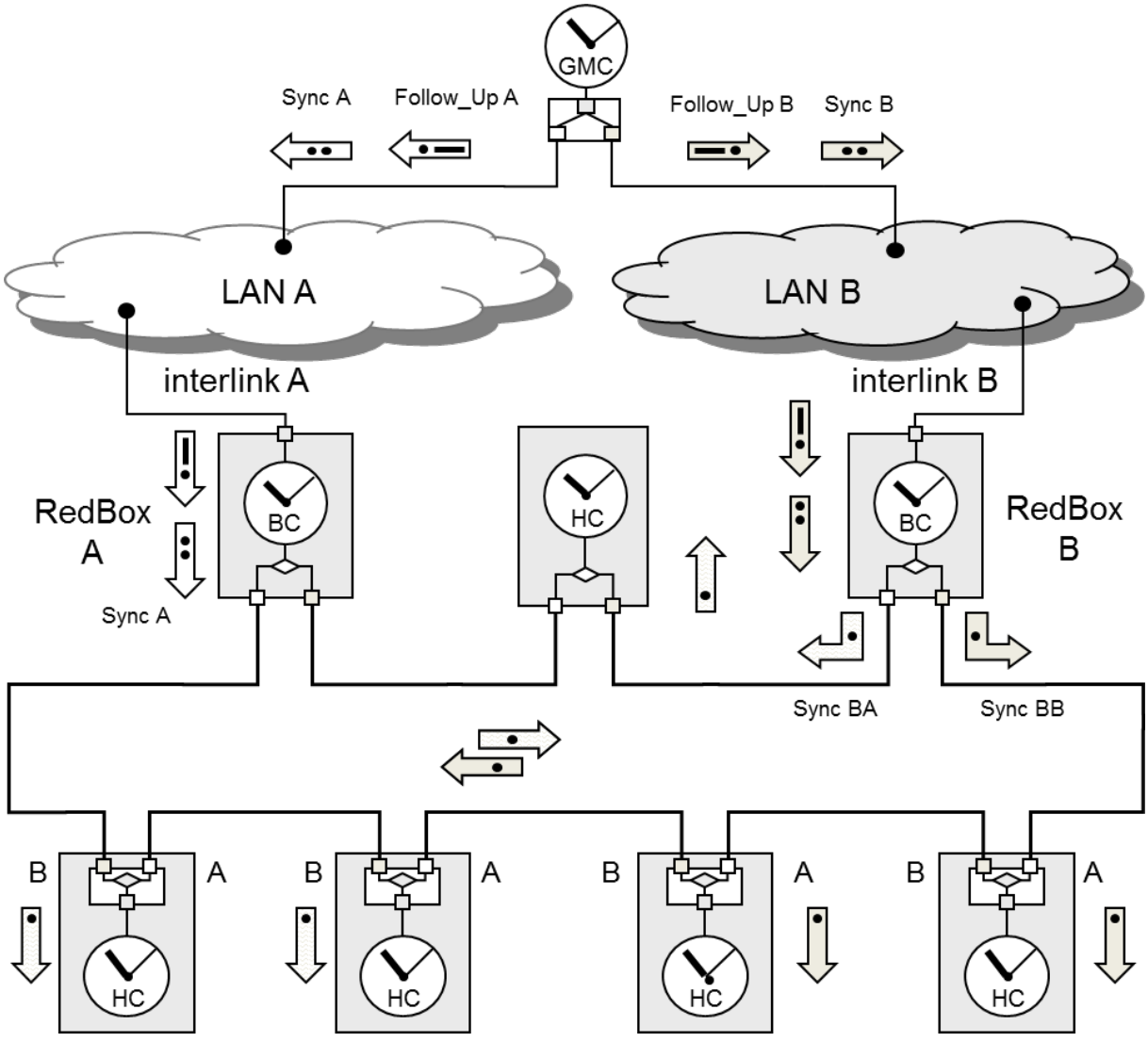


Figure 70 – Clocks in a PRP network coupled by BCs with an HSR ring

The RedBoxes can implement a boundary or a transparent clock.

A boundary clock results in only one clock sending over the HSR ring, the other boundary clock is parked because the Best Master Clock algorithm applies and lets only one clock sending over the ring. The HSR tag must carry a sequence number which, together with the MAC address of the RedBox, identifies the duplicates.

NOTE The two RedBoxes have different MAC and IP addresses for all traffic for which they are source or (sole) destination.

If the RedBoxes implement each a transparent clock, then four Syncs circulate through the ring and the HSR nodes must therefore deal with all four of them. The Syncs sent over the HSR ring receive an own HSR sequence number and the MAC address of the RedBox so they can be removed from the ring. The MAC address of the current master is lost, but can be retrieved through the message contents (sourcePortIdentity).

14.6.7 IEEE C37.238-2011 Power profile

14.6.7.1 IEEE C37.238-2011 Default settings

The IEEE C37.238 architecture and default settings are identical to IEC 62439-3 (14.6.6).

14.6.7.2 IEEE C37.238-2011 MIB

The IEEE C37.238 defines SNMP management objects which correspond to IEC 61588. In addition, it includes objects to manage the grandmaster identity and time inaccuracy during engineering, see 19.3 and 19.6.

14.6.7.3 IEEE C37.238-2011 TLVs

Each master appends two mandatory TLVs (parameters) to its Announce messages, the IEC 61588 compliant TLV ALTERNATE_TIME_OFFSET_INDICATOR mentioned in 14.6.7.3.1 and a power-profile-specific TLV.

14.6.7.3.1 IEEE C37.238-2011 ALTERNATE_TIME_OFFSET_INDICATOR

IEEE C37.238-2011 prescribes that each master appends to its Announce messages the IEC 61588-defined ALTERNATE_TIME_OFFSET_INDICATOR TLV that carries the offset of the clock with respect to UTC. This facilitates the setting of the HMI of the IEDs at the beginning and end of daylight saving time periods.

NOTE IEEE did not yet decide if the offset is with respect to UTC or TAI. A proposal is to assume that a value that is an exact multiple of 1 800 is an offset to UTC, while a value that has a residue from the division by 1 800 is relative to TAI, e.g. 3 600 would be relative to UTC and 3 632 would be relative to TAI.

14.6.7.4 IEEE C37.238-2011 profile-specific TLV

IEEE C37.238-2011 prescribes that each master appends to its Announce messages one C37.238-specific TLV that contains two fields: grandmasterID and timeInaccuracy.

a) The 16-bit grandmasterID field carries in its least-significant octet a short (8-bit) identifier of the current grandmaster that is intended to be copied into the smpSynch field of 19.4.8 of IEC 61850-7-2:2010. Although each Announce message carries a 64-bit grandMasterIdentifier, the smpSynch field only accommodates 8 bits.
In IEC 61850-9-2:2011, smpSynch specifies that the values 5 to 254 identify the grandmasterID.

   The allocation of the grandmasterID to a master clock is an engineering issue.

b) The 64-bit timeInaccuracy field which optionally carries an estimation of the absolute value of the inaccuracy of the local clock, which is divided into two fields:

- the 32-bit grandmasterTimeInaccuracy, a more precise value of the clockAccuracy of the clockQuality field specified in Table 6 of the IEEE Std 1588:2009, expressed in nanoseconds;
- a 32-bit networkTimeInaccuracy, which is configured at the grandmaster and is set to 0 by default. This value may be set to TimeInaccuracy accumulated in the worst network path, expressed in nanoseconds. The field “networkTimeInaccuracy” is provided for experimental purposes, and its use is undefined.

The TLV is shown in Figure 71.

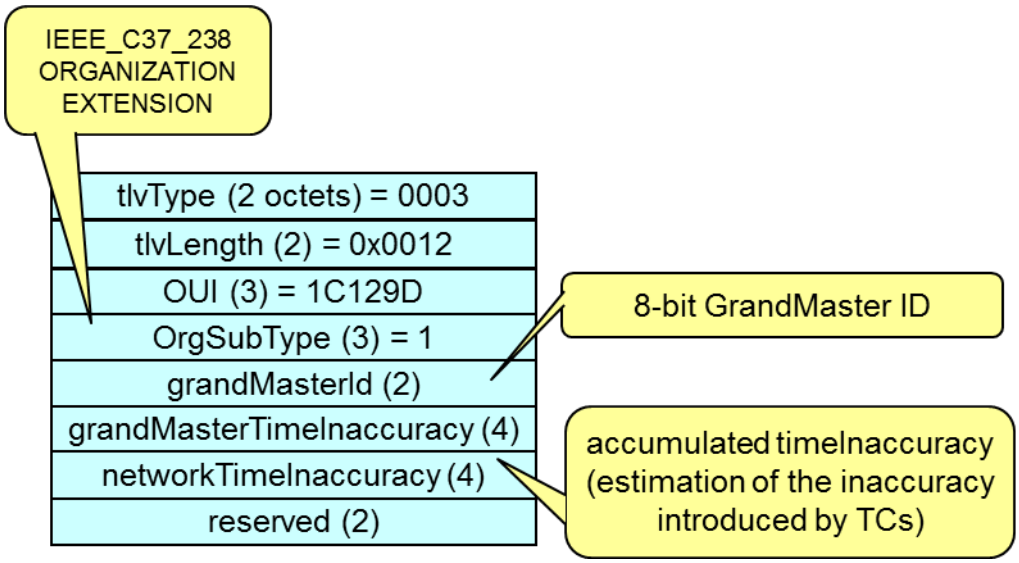


Figure 71 – C37.238-specific TLV

14.7 PTP network engineering

14.7.1 PTP reference clock location

The use of PTP is a trade-off between additional costs of PTP-capable bridges and the number of IEDs in a substation to be synchronized with high precision. A very small number of these IEDs calls for a point to point solution with IRIG–B or 1 PPS, while a larger number justifies a network of PTP-capable switches.

When engineering a network, the first step is to locate the reference clocks so as to minimize the clock inaccuracy. Each transparent clock introduces a time inaccuracy – whose worst-case value LocTimeInacc is specified in its data sheet. On the path from the grandmaster to an IED: the time inaccuracy of the different transparent clocks through which the Sync message transited increases by the value of each transparent clock. This value at a given node is the NetTimeInacc. The worst case value of NetTimeInacc is the sum of the LocTimeInacc of all transparent clocks in the least favourable path from any master to that node.

Figure 72 shows that the Sync message from the GPS time server to IED z crosses 8 transparent clocks in the worst case, which occurs when the RSTP blocks the right port of the first bridge. If every transparent clock introduces a worst-case time inaccuracy of 50 ns, the total worst-case inaccuracy along that path will be 400 ns.

In case the grandmaster clock (e.g. attached to the GPS) fails, a back-up rubidium clock takes over. Figure 72 shows that one more transparent clock must be crossed, and NetTimeInacc for IED z rises to 450 ns.

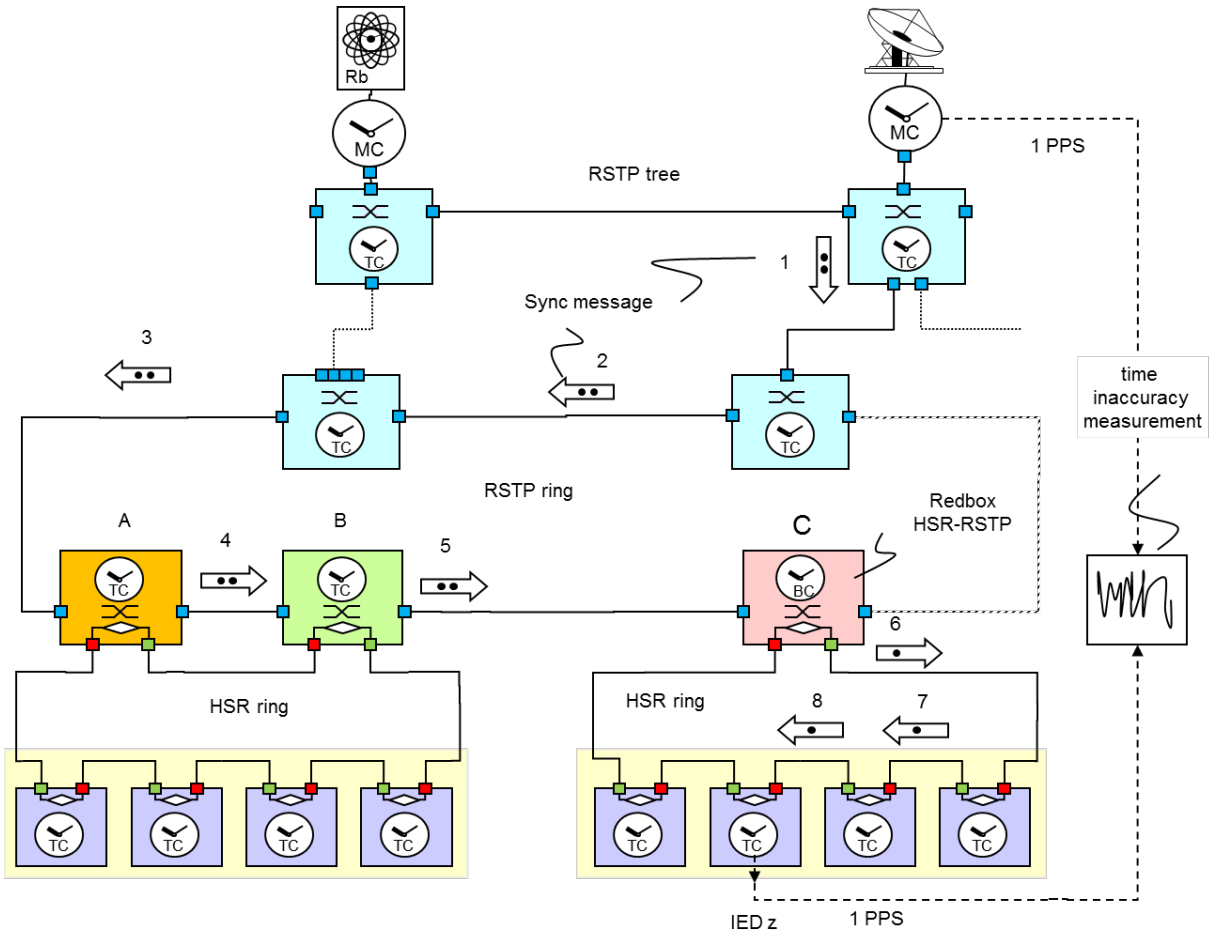
The effective value of NetTimeInacc can be measured for each IED, i.e. by comparing the 1 PPS signal generated by the grandmaster and the 1 PPS signal generated by the ordinary

clock of IED z, as shown in Figure 72. To perform this measurement, it is recommended to generate the 1 PPS signal in all clocks at least for testing.

The maximum clock inaccuracy permitted on an IED is an engineering parameter called EngTimeInacc. This conservative estimate of the inaccuracy considers how accurate an event is time-stamped on a given IED. Therefore, it considers the sum of:

- the network time inaccuracy (which varies from device to device);
- the grandmaster inaccuracy (which varies and is indicated in the Sync messages);
- any inaccuracy introduced by the sensors or the IED itself.

The effective error in time-stamping can be calculated by generating an event on an IED at a given time, e.g. synchronized to the 1 PPS of the reference clock, and comparing it to the value in the time-stamp in the corresponding frame received by the SCADA or a network analyser.



Key

GMC grand-master clock

BMC backup master clock

TC transparent clock

Figure 72 – Hierarchy of clocks

14.7.2 PTP connection of station bus and process bus

While the stricter timing requirements apply to the process bus, the reference clock should be located on the station bus and the process bus devices should be synchronized to it. The device connecting station bus and process bus (Ethernet bridge or IED with bridging functionality) acts as a PTP transparent clock synchronizing the process bus devices.

However, when the reference clock on the station bus becomes unavailable, a device on the process bus, preferably the connecting device, should take over as a grandmaster, both towards the station bus (if it still operates) and towards the process bus. When the station bus resumes operation, the connecting device relinquishes its master role to the reference clock.

It is recommended to locate the redundant clocks so that a common mode of failure is unlikely and so that the worst case number of transparent clocks in the path to an ordinary clock is less or equal to the original grandmaster clock (e.g. at opposed diameters of a ring in a ring topology).

14.7.3 Merging units synchronization

Clock synchronization at the process level depends on the considered application and network architecture and topology. Indeed, in the case of local protection functions such as overcurrent, the relevant data are usually collected by the same merging unit and then no external synchronization is required. If the data are coming from different merging units, e.g. differential protection function, the merging units have to be synchronized. How many merging units are required to perform a given function depends not only on the required availability in case of losses, but also on geographical distance and layout of the substation. The number of synchronized merging units should be minimized, e.g. by using synchronization islands. Such synchronization islands could be either suitable for process bus topologies based on multiple rings or multiple stars as well as multiple point-to-point links. The latter case is more complex, as it would require each physical merging unit to host multiple logical devices "Merging Unit" in order for these to belong to different synchronization islands at the same time.

15 Network security

Refer to IEC 62351.

16 Network management

16.1 Protocols for network management

When choosing network elements, consideration should be given to their ability to provide continuous metrics of their health plus their ability to transport the traffic on their incoming ports.

IEC 61850 MMS traffic only offers a time-out on acknowledged messages to monitor the health of the communication path. More sophisticated methods can be used if a common time clock is available that allows estimating the one-way latencies. However, just checking the overall delay does not distinguish communication failures, bridge overload or application errors, and therefore, network-health tools should be used that rely on the ability of the devices to monitor the condition of their network connections.

Two techniques are available to monitor devices health, SNMP and IEC 61850.

- SNMP is the standard network management protocol for bridging devices, but its implementation is now common for any device. When a device supports SNMP, it is said "manageable". Available information is structured into MIBs which are a type of database used to manage the devices in a communication network. The list of the standard MIBs and the selected content which is supported by a device depends on the vendor's choices. In addition, "private MIBs" are supported by some devices in order to offer vendor-specific detailed information (described by the MIB provided by the device's vendor). MIBs contents are described using the ASN.1 grammar and then can be easily imported into a network management tool. An SNMP MIB has been defined also for PRP and HSR. This requires SCADA level nodes to support SNMP, at least through an OPC server.
- An alternative to the SNMP protocol for network management within substations is the use of the IEC 61850 MMS services in case the network elements implement them. Such

services allow seamless integration of networking devices into Substation Control and Monitoring Systems that lack the SNMP protocol functionality. To this effect, objects have been defined in IEC 61850-7-4:2010 to represent communication properties. Additional modelling is proposed in Clause 19 to extend capabilities in configuring and monitoring the networking feature of devices. This requires bridges to support MMS, although they are not classical IEDs.

This continuous monitoring is now being accepted as a technology to mitigate regulatory-board requirements for placing communication networks out of service for annual maintenance tests.

16.2 Network management tool

Monitoring the status of the network is essential, as soon as the network handles critical distributed functions and redundancy mechanisms are implemented to overcome a first failure.

Then tools which can continuously monitor the real health of the network, and of the network bridging devices, and detect the occurrence of a network failure are of very valuable usage.

More globally, here are the expected benefits in using a Network monitoring tool:

- Confidence that the network is performing as expected.
- Considering that some advanced properties of Ethernet have been used to manage the Ethernet data flow, this tool helps validating that the networking devices are configured properly, and then that the data flow is spread as desired.
- Reduce downtime – Increase productivity.
- Fast and easy visual identification of failures.
- Faster and more accurate understanding of the cause of a problem and how to repair it.
- Traps degradations and intermittent disturbances to predict future failures.
- Breaks the barrier between electrician and IT related skills.

16.3 Network diagnostic tool

The main potential functions of a network diagnostic tool are as follows:

- Retrieve network diagnostic information and check device health.
- Discover and identify any devices connected on the Ethernet network (field devices as well as infrastructure devices).
- Retrieve IEC 61850 network and communication related information from any devices.
- Retrieve MIBs from any manageable devices.
- Learn device capabilities and parameters as soon as there are available remotely through IEC 61850 and/or SNMP.
- Help to validate the correct settings used for managing the data flow such as Multicast Address Filtering settings, VLAN settings.
- Identify any communication links between devices even if logically disabled.
- Compare the discovered topology against the engineered topology defined in the SCD, or against a previously saved topology, i.e. looking for missing devices or links and different parameters.
- In case of network redundancy, check the effective health, i.e. if traffic follows the expected flow. Produce an alarm as soon as the network is changing from the normal flow state.
- Provide to the operator a single synthesis on network health.

- Time-stamp and display alarms on the tool's screen as soon as they occurred (including its source, its label, the time when it occurred, and its status).
- Locate easily on the network map the device or link that generates the alarm.
- Analyse network data flow and identify issues at communication level.
- Analyse network data flow and identify issues at application level (using the application level tags and function naming).

17 Remote connectivity

Engineer access allows performing bulk upgrades, management of configuration files, backup or configuration restoration.

There might be a requirement for remote access so that certain or all IEDs can communicate to/from a control centre, another substation or from any place in the corporate utility network or from outside this network. The inter-substation communication, substation to control centre communication or secure remote access is outside the scope of this document.

NOTE Bulk upgrades require considering throughput and security in the configuration of the communication network.

18 Network testing

18.1 Introduction to testing

Network components are a vital part of the power utility automation since their failure impacts the control functions and even the protection functions. As such, the quality of the network and switches must achieve a similar level as that of the protection relays. IEC 61850-4 defines several stages for ensuring quality, which are repeated in Figure 73.

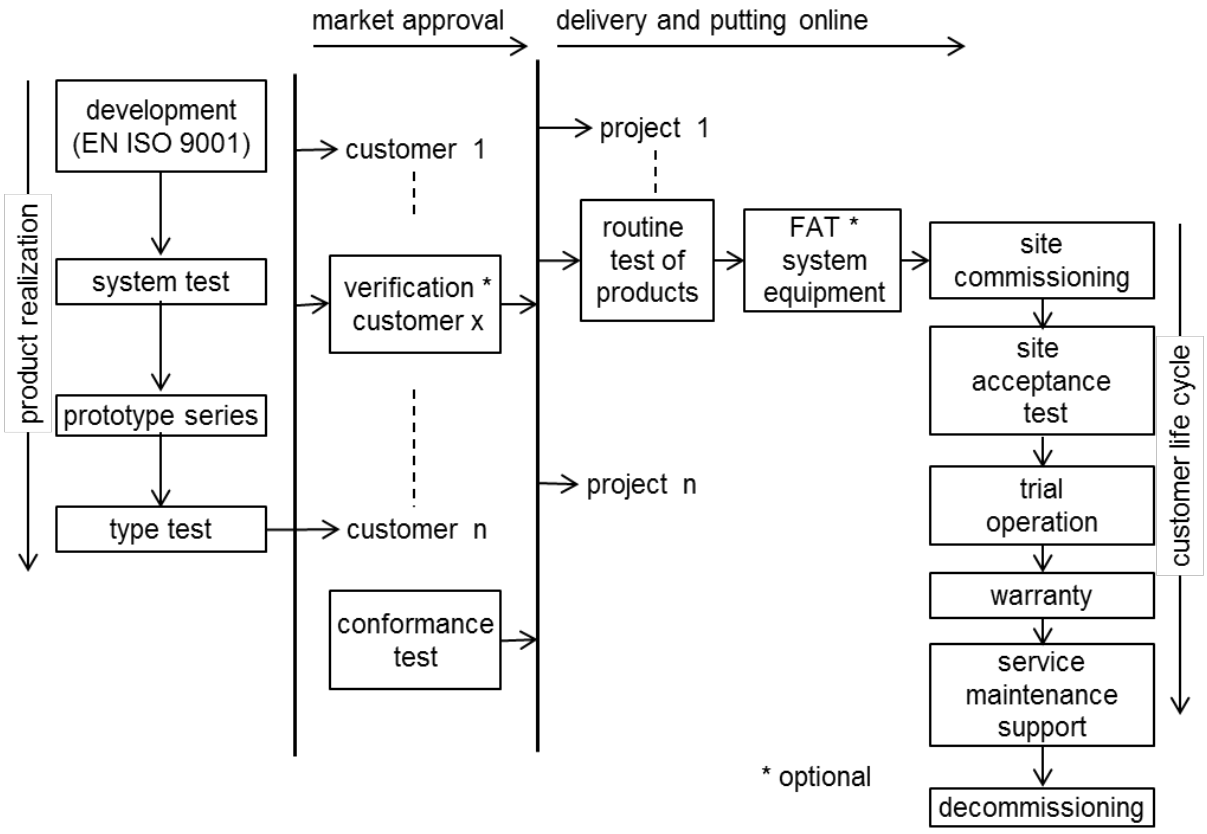


Figure 73 – Quality assurance stages (copied from IEC 61850-4)

In the product development stage, a manufacturer develops the product and executes product release tests.

An independent test lab executes the type testing, which basically ensures that the device type operates up to the specifications and fulfils the mechanical, electromagnetic and environmental requirements of the claimed standards.

During the market approval stage, the system integrator performs a verification test to select a product. This test verifies if the product meets the functional and performance requirements under worst case conditions. The verification test also checks that the different components of the network interoperate correctly for even the largest envisioned systems.

During the project execution stage, the network of a specific power utility project undergoes a factory acceptance and site acceptance testing.

During operation, a part of the tests continues to monitor the network, so as to detect failures and replace quickly the failed devices.

Subclauses 18.2 to 18.4 describe the network testing activities for each stage more in detail.

18.2 Environmental type testing

The type testing of network and other electronic devices checks EMC immunity, EMC emission, environmental and mechanical resilience under the conditions of power utility environments.

The environmental type testing is defined in IEC 61850-3.

18.3 Conformance testing

18.3.1 Protocols subject to conformance testing

The conformance test verifies if network equipment conforms to the claimed standards. This guideline does not define conformance test procedures, since these belong to the claimed standards.

The applicable protocols and conformance test description for a typical Ethernet switch are listed in Table 45.

Table 45 – Standards applicable to network elements

Protocol	Reference	Conformance test
Priority queuing	IEEE 802.1Q-2011	-
Virtual LAN	IEEE 802.1Q-2011	-
Rapid spanning tree protocol (RSTP)	IEEE 802.1D-2004	Clause 8 of IEC 62439-1: 2010 – measure RSTP performance
Simple network management protocol (SNMP)	RFC 3416	-
Simple Network Time protocol (SNTP)	RFC 2030	-
Multiple MAC Registration Protocol (MMRP)	IEEE 802.1Q-2011	-
Multiple VLAN Registration Protocol (MVRP)	IEEE 802.1Q-2011	-
Precision Time synchronization Protocol (PTP) for power applications	IEEE C37.238	ISPCS Plug fest

Protocol	Reference	Conformance test
Parallel redundancy protocol (PRP) (RedBox)	Clause 4 of IEC 62439-3:2012	Clause 4 of IEC 62439-1:2010
High-availability Seamless Redundancy (HSR)	Clause 5 of IEC 62439-3:2012	Clause 4 of IEC 62439-1:2010

18.3.2 Integrator acceptance and verification testing

Integrator acceptance and verification tests verify which products meet the functional and performance requirements for the intended network configuration under worst case conditions.

Such tests are repeated for several products and, based on the test results, the integrator can decide which products to use for its future projects.

To compare the performance of different products, the tests need to be executed multiple times under well-defined and repeatable conditions, so as to gather comparable statistical data like average, minimum and maximum performance.

Since the integrator uses these products in a number of projects, these tests ensure that a set of products is applicable even for the largest and most demanding projects.

18.3.3 Simple verification test set-up

Figure 74 shows a simple test set-up used as a reference in the following tests. It does not replace a full system test, but it is used to specify the necessary steps.

The test set-up is optimized to minimize the number of switches.

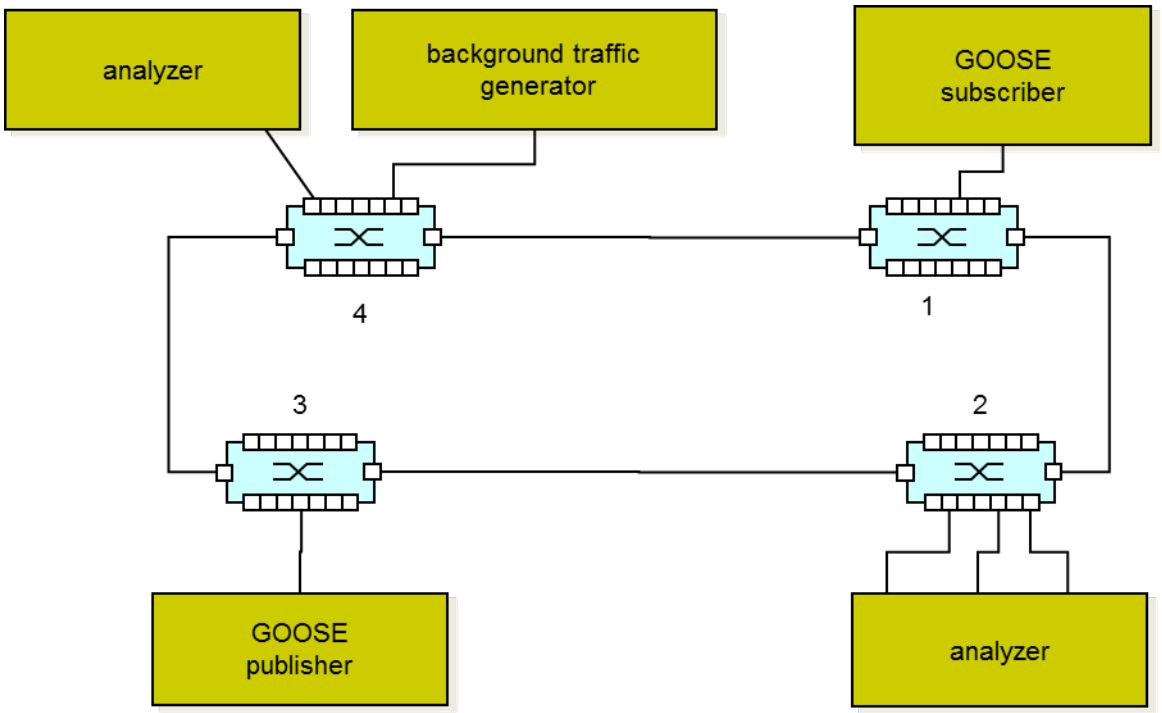


Figure 74 – Test set-up for verification test

The test set-up consists of the following components:

- 4 Ethernet switches (using RSTP) in a ring configured for the test;

- IEC 61850 GOOSE Publisher with 100 Mbit/s port;
- IEC 61850 GOOSE Subscriber with 100 Mbit/s port;
- IEC 61850 Analyser with one or more 100 Mbit/s ports;
- Background traffic generator with 100 Mbit/s port;
- Multiple SV publishers;
- Several devices/switches with HSR or PRP functionality;
- One or two PTP master clocks.

The traffic generator allows generating worst case conditions, consisting of 98 % low priority network load and of 2 % high-priority traffic with large GOOSE messages (see 11.2.3) sent with a period of 1 ms.

An SV message generator can also be used to simulate multiple SV publishers. Each publisher creates a network load of about 4 % consisting of SV messages sent with a period of 250 μs in a 50 Hz system.

To calculate the minimum and maximum test results the test procedure is repeated at least 5 times.

18.3.4 Simple VLAN handling test

This simple VLAN handling test verifies the handling of VLANs using GOOSE messages with different VIDs.

Id	Test procedure	Verdict
VLAN1	Check whether the VLAN tag in the GOOSE message is correct after passing at least two switches.	
VLAN2	Check whether a VLAN tagged message only appears on the corresponding port.	
VLAN3	Check whether a VLAN tagged message with VID=0 is rewritten to the default VID of the corresponding VLAN.	

18.3.5 Simple priority tagging test

This simple priority tagging test verifies that higher priority messages prevail over lower priority messages. In a network with mixed priority packages, no high priority packages should be dropped.

Id	Test procedure	Verdict
Prio1	GOOSE simulator sends 1 000 messages within 1 s with priority=LOW, with no or less than 5 % network traffic.	
Prio2	GOOSE simulator sends 1 000 messages within 1 s with priority=MEDIUM, with no or less than 5 % network traffic.	
Prio3	GOOSE simulator sends 1 000 messages within 1 s with priority=HIGH, with no or less than 5 % network traffic.	
Prio4	GOOSE simulator sends 1 000 messages within 1 s with the priority lower than the 98 % background traffic on a separate VLAN.	
Prio5	GOOSE simulator sends 1 000 messages within 1 s with the priority the same as the 98 % background traffic on a separate VLAN.	
Prio6	GOOSE simulator sends 1 000 messages within 1 s with the priority higher than the 98 % background traffic on a separate VLAN.	
Prio7	GOOSE simulator sends 1 000 messages within 1 s with the priority lower than the 98 % background traffic on the same VLAN.	

Id	Test procedure	Verdict
Prio8	GOOSE simulator sends 1 000 messages within 1 s with the priority the same as the 98 % background traffic on the same VLAN.	
Prio9	GOOSE simulator sends 1 000 messages within 1 s with the priority higher than the 98 % background traffic on the same VLAN.	

18.3.6 Simple multicast handling test

This simple multicast handling test verifies that the specific multicast (SV or GOOSE) messages are received on the configured ports and not received on other ports.

Id	Test procedure	Verdict
Mcg1	Check whether the MC messages are received on the configured ports after disconnecting/reconnecting a backbone cable.	
Mcg2	Check whether the MC messages are not received on the other ports after disconnecting/reconnecting a backbone cable.	
Mcg3	Check that messages with an unknown multicast are received on all ports.	

18.3.7 Simple RSTP recovery test

This test neither replaces the IEEE 802.1D conformance tests nor the guidelines of IEC 62439-1:2010.

This simple RSTP test verifies the recovery of a single communication failure and measures the recovery time as well as the number of packet drops in function of:

- Packet size;
- Network load;
- Connecting / disconnecting the backbone ring.

The measured recovery time is the difference between the timestamp of the last received message before the failure and the timestamp of the first received message after the failure. The packet drop is the difference in sequence number of the last and first received GOOSE message.

Id	Test procedure	Verdict	Measurements (min/max)
Rsp1	Disconnection test with large GOOSE messages and about 98 % network traffic on the backbone.		
Rsp2	Disconnection test with small GOOSE messages and about 98 % network traffic on the backbone.		
Rsp3	Disconnection test with large GOOSE messages with no traffic.		
Rsp4	Disconnection test with small GOOSE messages with no traffic.		
Rsp5	Connection test with large GOOSE messages and about 98 % network traffic on the backbone.		
Rsp6	Connection test with small GOOSE messages and about 98 % network traffic on the backbone.		
Rsp7	Connection test with large GOOSE messages with no traffic.		
Rsp8	Connection test with small GOOSE messages with no traffic.		

NOTE IEC 61850-5 requires a performance class P1 for type 1B messages with a recovery time shorter than 5 ms per switch. Such performance is possible according to IEC 62439-1:2012, Clause 8, except for the loss of the root bridge.

18.3.8 Simple HSR test

This test applies to a switch implementing the HSR protocol, which implies that it operates as a RedBox. Devices are subject to more complete conformance tests based on IEC 62439-3:2012.

This simple HSR test verifies that on connection failure, no packets are dropped or delayed.

Id	Test procedure	Verdict
Hsr1	Check whether HSR mechanism works on a backbone disconnecting a link with multiple SV publishers in a network.	
Hsr2	Check whether HSR mechanism works on a backbone reconnecting the link with multiple SV publishers in a network.	

18.3.9 Simple PRP test

In a PRP LAN, bridges normally operate as IEEE 802.1D elements, so in principle no test is needed. The PRP test is only needed to ensure that the bridges do not remove the PRP trailers. If the bridge is used as a RedBox, it is only connected to two PRP LANs and this test applies.

This simple PRP test verifies that on connection failures, no packets are dropped or delayed.

Id	Test procedure	Verdict
Prp1	Check whether PRP mechanism works on a backbone disconnecting a link with multiple SV publishers in a network.	
Prp2	Check whether PRP mechanism works on a backbone reconnect the link with multiple SV publishers in a network.	

18.3.10 Simple PTP test

This test applies when the switch is aware of the PTP protocol, i.e. operates as a transparent clock. Complete conformance tests are previously necessary.

This simple test verifies PTP performance, master clock switchover and start-up convergence time. To measure the offset compared to 1 PPS special hardware/software is required.

Id	Test procedure	Verdict
Ptp1	Check whether maximum PTP offset and time inaccuracy compared to a reference directly attached are within 50 ns.	
Ptp2	Verify the switchover from one master clock to another and vice versa.	
Ptp3	Check the convergence time at start-up.	

18.4 Factory and site acceptance testing

During the project execution stage, the network of a specific project is subject first to a factory acceptance and then to site acceptance testing.

While the factory acceptance test is typically a partial set-up that only tests parts of the network, the site acceptance test checks the totality. Therefore, the factory acceptance test should also be used to test the procedures used for the site acceptance test.

A first test is to check whether all switches are correctly configured with respect to IP address, port settings, multicast and VLAN filtering and clock settings if applicable. This can

be done using the remote access over SNMP or IEC 61850 objects. This test also checks the connectivity of the switches.

A second test checks the connectivity of all other devices. This can be done simply by pinging the devices with ICMP messages.

The presence of the MMS stack and its function on each device is a further connectivity and configuration check. Tools exist to verify that all IEDs in the SCD are present and correctly configured.

A third test checks if devices send the GOOSE and SV messages specified in the SCD. Tools exist to check consistency of these messages with the SCD.

A fourth test checks if all subscribed devices receive the configured GOOSE and SV. To support this, the subscriber devices should be configured to indicate an error (e.g. by sending an IEC 61850 report) in case GOOSE and/or SV messages are not received or not as expected.

Resiliency test should also be performed by removing cables or switches to check that the traffic keeps on flowing and the error is reported.

A network monitoring tool can be used to verify the expected network load on each port during normal operation.

A network analyser can be used to verify packet drops in case of disconnecting/re-connecting a link.

19 IEC 61850 bridge and port object model[6]

19.1 Purpose

Network management analyses the status of the devices and configures their properties. This is traditionally done with SNMP, which describes the devices as a collection of data objects known as the management information base MIB. SNMP also specifies an access protocol based on UDP. Within an IEC 61850 substation, an access protocol already exists in form of MMS. Management accesses network devices over MMS using the equivalent of a MIB in the form of a collection of Logical Nodes.

Subclause 19.2 describes a model of a multi-port device in form of IEC 61850 objects that corresponds to an SNMP MIB. This model applies to data switches, bridges and also to simple IEDs that support a subset of bridge functions, in particular HSR and PRP devices.

This model does not contain all information that is usually available in the SNMP MIBs, but selects configuration and status variables relevant in the context of utility automation.

Subclause 19.3 defines the model of an IEC 61588 clock in terms of Logical Nodes.

Subclause 19.4 defines the Logical Nodes and Common Data Classes for bridging and clock. This subclause is auto-generated out of the UML model and will be moved to IEC 61850-7-4. Until then, it is to be considered as informal and defined within (Tr)IEC 61850-90-4:2012 namespace.

---

6 The Logical Nodes in Clause 19 will be moved as a normative part into IEC 61850-7-4 in a future revision. Its contents are still experimental. The Logical Nodes and related objects have been copied from an UML-generated model and cannot be changed in this document.

Subclause 19.5 suggests a mapping from the IEC 61850 bridge model to a standardized bridge MIB, where applicable. If no standardized MIB is available, a description of the data objects and attributes allows the bridge manufacturer to map them to its own individual MIB objects.

Subclause 19.6 suggests a mapping from the IEC 61850 model to the IEC 61588 and IEEE C37.238 objects.

NOTE A two-way mapping between IEC 61850 and SNMP has been proposed that can be used for that purpose. Unfortunately, object names are not preserved due to different naming conventions.

19.2 Bridge model

19.2.1 Simple model

A multiport physical device that has a layer 2 bridge functionality according to IEEE 802.1D implements a switching matrix. Bridge functionality is not restricted to dedicated Ethernet switches. For instance, an IED may act as a bridge between station bus and process bus or implement an additional port for connection of a service device. Even a simple IED with HSR redundancy is a small bridge since it forwards frames from port to port.

In a meshed network, a bridge may implement the Rapid Spanning Tree Protocol (RSTP) to keep the data network free of loops and reconfigure it in case of failure. Ethernet switches also perform VLAN and multicast address filtering.

Bridge functions are often extended by the IEEE 802.1AB Link Layer Discovery Protocol that gathers information about adjacent nodes.

These basic bridge functions are modelled as shown in Figure 75.

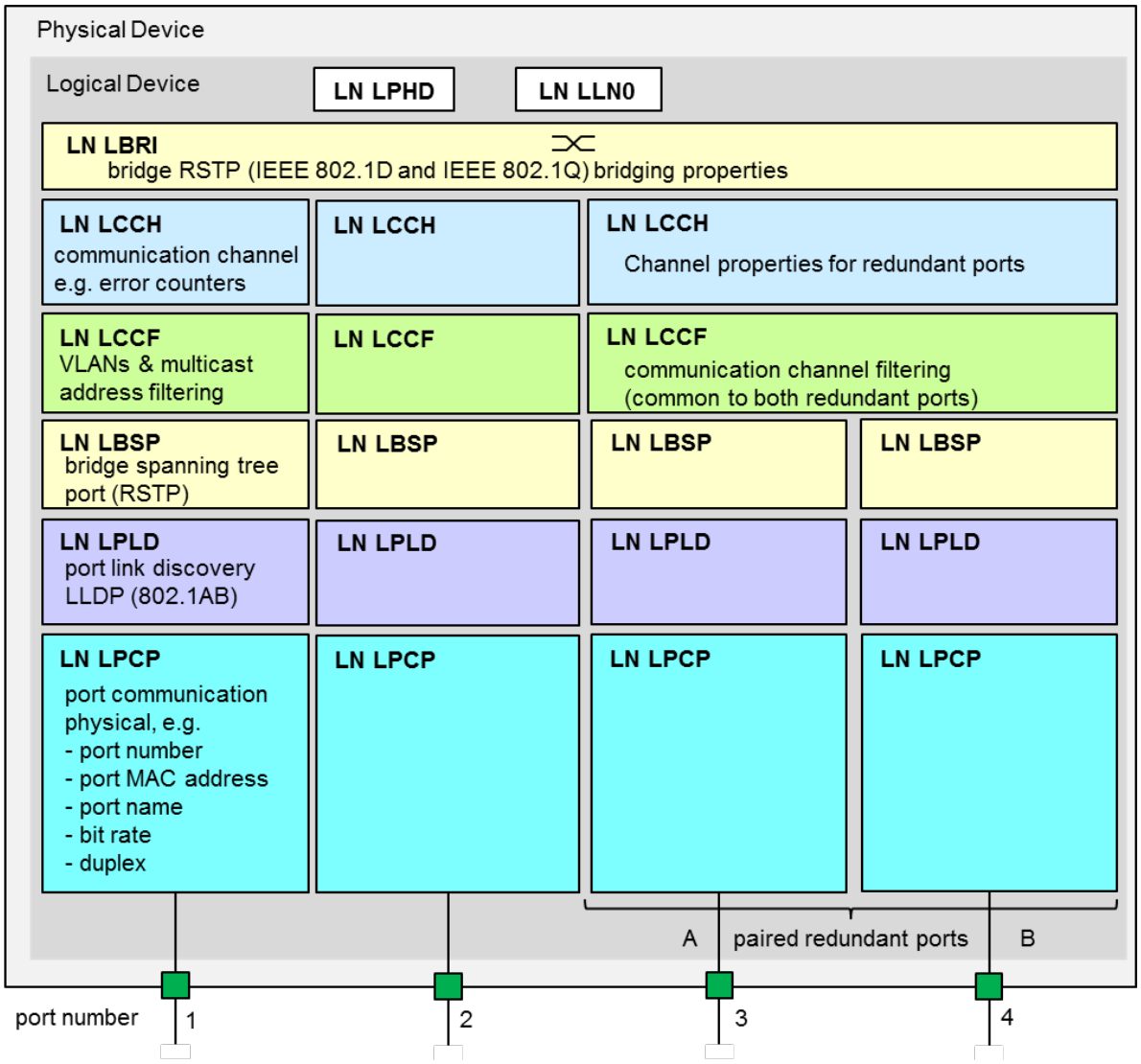


Figure 75 – Multiport device model

The bridge model consists of a collection of Logical Nodes.

- Logical Node LPHD defined in IEC 61850-7-4:2010 represents the physical device properties (e.g. physical health). Since a logical node may only exist within a Logical Device, the LN LPHD is part of a Logical Device. LPHD has been extended to support the bridge functions as defined in 19.4.3.2.2.
- Logical Node LLN0 defined in IEC 61850-7-4:2010 represents the properties (e.g. local/remote operation) of the Logical Device, several of which may exist in a physical device. Typically, a data switch hosts only a single Logical Device.
- Logical Node LBRI (for “Bridge”) defined in 19.4.3.2.3 represents the basic bridge functionality, as of IEEE 802.1D (Bridging and Rapid Spanning Tree Protocol);
- Logical Node LCCF (for “Channel Communication Filtering”) defined in 19.4.3.2.4 represents the VLAN and multicast address filtering if the channel supports IEEE 802.1Q;
- Logical Node LCCH (for “Communication Channel”) defined in IEC 61850-7-4:2010 and extended in 19.4.3.2.5, represents each channel. A channel can consist of one physical port or two paired ports in redundancy. For instance, a simple IED with one redundant channel according to PRP implements one instance of LN LCCH and two instances of LN LPCP.
- Logical Node LPCP (for “Physical Communication Port”) defined in 19.4.3.2.7, is instantiated for each port, and represents the physical properties of a port (e.g. bit rate).

Each port is identified by its port number PortNum (e.g. 3), a port name PortNam (e.g. “J103”) and a port MAC address PortMac (e.g. 00-02-03-AB-04-BC).

- Logical Node LPLD (for “Port Layer Discovery”) defined in 19.4.3.2.8 is instantiated for each port, and represents the properties of the remote device on that link discovered by LLDP (IEEE 802.1AB).
- Logical Node LBSP (for “Port Spanning tree Protocol”) defined in 19.4.3.2.9 is instantiated for each port, and represents the RSTP properties of a port (e.g. RSTP port status: forwarding).

NOTE With exception of LPHD, all system logical nodes (Group L) belonging to the same IED are defined in the same logical device (according to 8.2.1 of IEC 61850-7-1:2011).

An ICD for a bridge contains an LN LLN0, an LN LPHD and an LBRI. It will have as many instances of the LN LPCP as the bridge has physical ports and as many instances of the LN LCCH as the device has logical channels, as the examples in 19.7 show.

19.2.2 Bridge Logical Node linking

The Logical Nodes are linked using references, as shown in Figure 76.

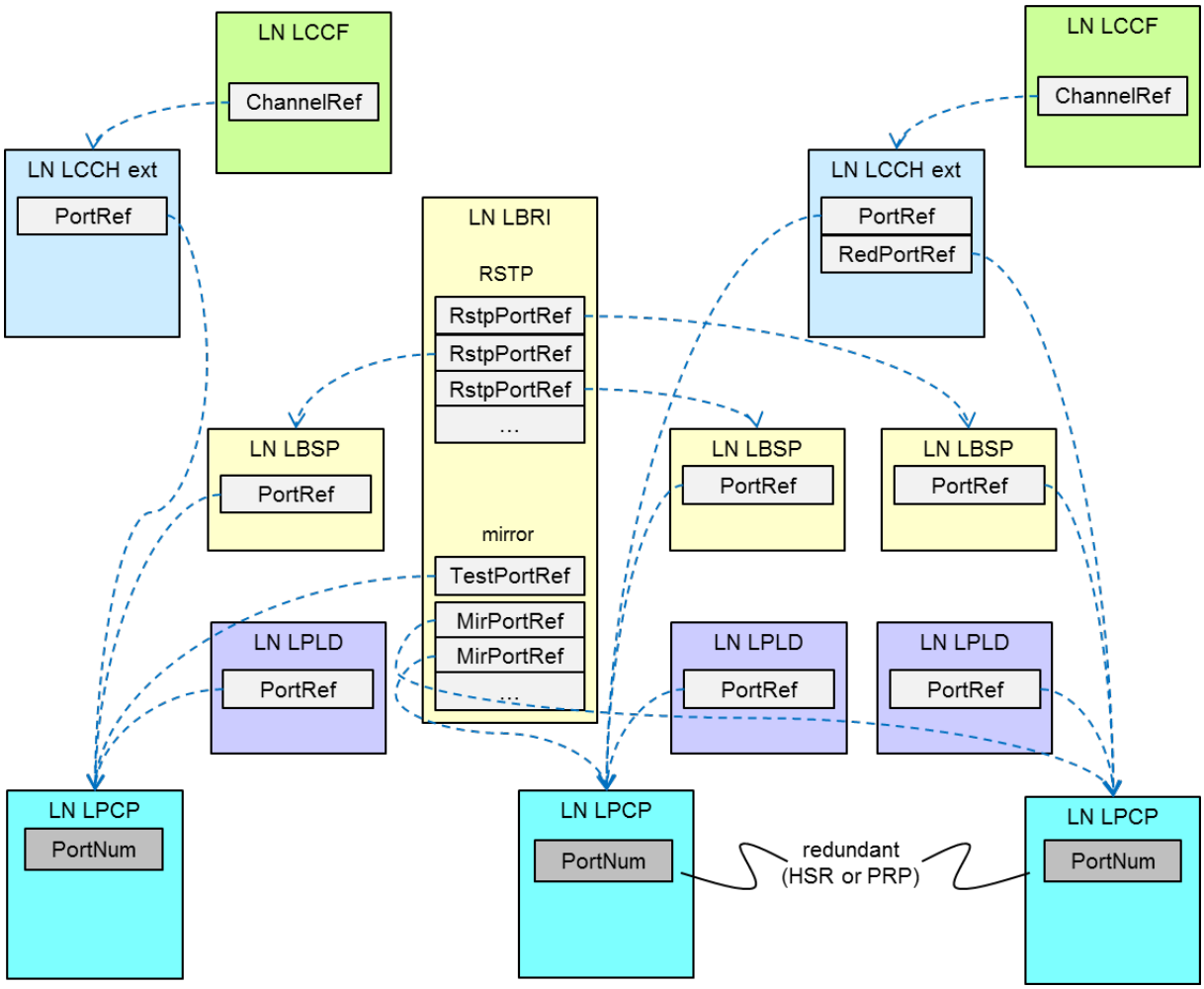


Figure 76 – Linking of bridge objects

19.3 Clock model

19.3.1 IEC 61588 datasets

IEC 61588 represents the clock properties in different datasets:

a) defaultDS: describes the local clock of a device;

b) currentDS: describes the path between a slave clock and the master or grandmaster;

c) parentDS: describes the clock that synchronizes the local clock, either master (boundary clock) or grandmaster;

d) timepropertiesDS: an extension of the parentDS to account for different time scales;

e) portDS: applies to each port of a clock.

These datasets are referenced in the MIB specified in IEEE C37.238 which can be accessed at http://standards.ieee.org/downloads/C37/C37.238-2011/C37.238-2011_MIB-D5-8.mib.
In principle, the MIB objects labelled as “read-only” are statuses, while the MIB objects labelled as “read-write” are settings.

19.3.2 Clock objects

The model of an IEC 61588 compliant clock takes the form of Data Objects and Common Data Classes that correspond to the IEC 61588 datasets mentioned in 19.3.1 and the extensions in the IEEE C37.238 MIB, representing e.g.:

- Roles in which the node can be configured (master-enabled, slave-only);
- Domain number;
- Clock Identity;
- Clock Quality;
- ClockPriority1;
- ClockPriority2;
- Announce interval when clock is master (power of two of 1 s (e.g. 2^4 = 16 s, 2^{-2} = 250 ms);
- Announce time-out in multiples of Announce interval;
- Pdelay_Request interval (power of two of 1 s), per port;
- Sync interval when clock is master (power of two of 1 s);
- Current UTC offset;
- Time Correction: one-step or two-step;
- GrandmasterId;
- OffsetFromMaster;
- TimeInaccuracy.

19.3.3 Simple clock model

A general IEC 61588 clock resides in a multiport device. The structure is similar to that of a bridging device as defined in 19.2, as shown in Figure 77.

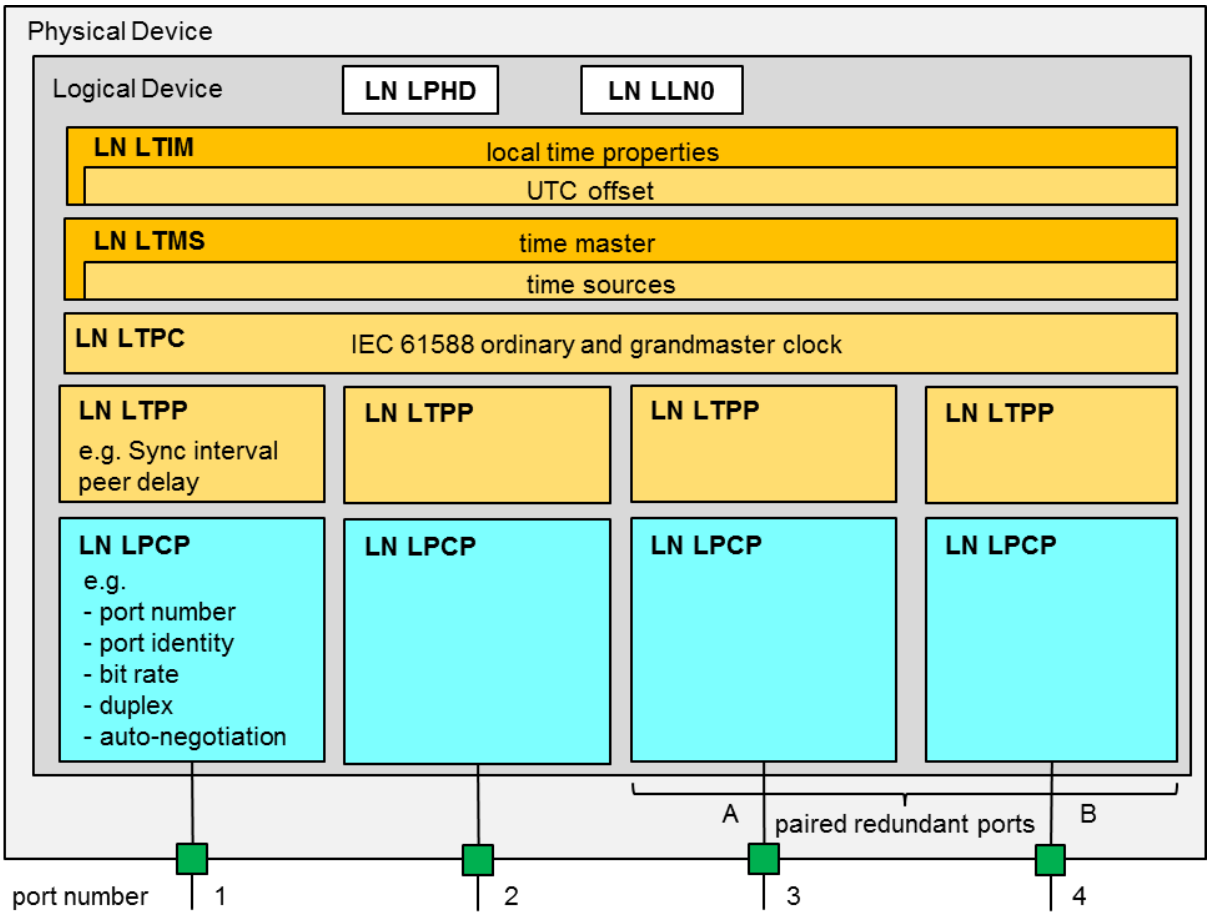


Figure 77 – Clock model

- Logical Node LTIM defined in IEC 61850-7-4:2010 represents the clock available to the applications. The source of that clock is not visible in LN LTIM. LN LTIM extensions in 19.4.3.2.10 allow to represent both the UTC and the TAI time scale.
- The Logical Node LTMS defined in IEC 61850-7-4:2010 represents the clock synchronization source, which may be NTP, IEC 61588, IRIG-B or other. LN LTMS extensions in 19.4.3.2.11 indicate from which clock source the synchronisation is received.
- The Logical Node LTPC defined in 19.4.3.2.12 represents:
  - the IEC 61588 ordinary clock's settings on that node, i.e. the clock that would control the node in absence of external synchronization, which could be the master clock of the time domain if it happens to be the best master clock;
  - the IEC 61588 grandmaster clock's status, which represents the primary time source of the time domain, as seen on that node.

  The LN LTPC has a Data Object indicating from which ports the IEC 61588 synchronization is received.
- The Logical Node LTPP defined in 19.4.3.2.13 represents the IEC 61588 properties of the port, e.g. the measurement of the peer delay. Each port of a pair in redundancy has one clock object, even if redundancy is applied, since IEC 62439-3 prescribes that the duplicate discard does not apply to the IEC 61588 clock synchronization.

NOTE IEC 61588:2009 indicates that an ordinary clock has only one port, but this is only valid when there is no redundancy.

19.3.4 Linking of clock objects

The Logical Nodes are linked using references, as shown in Figure 76.

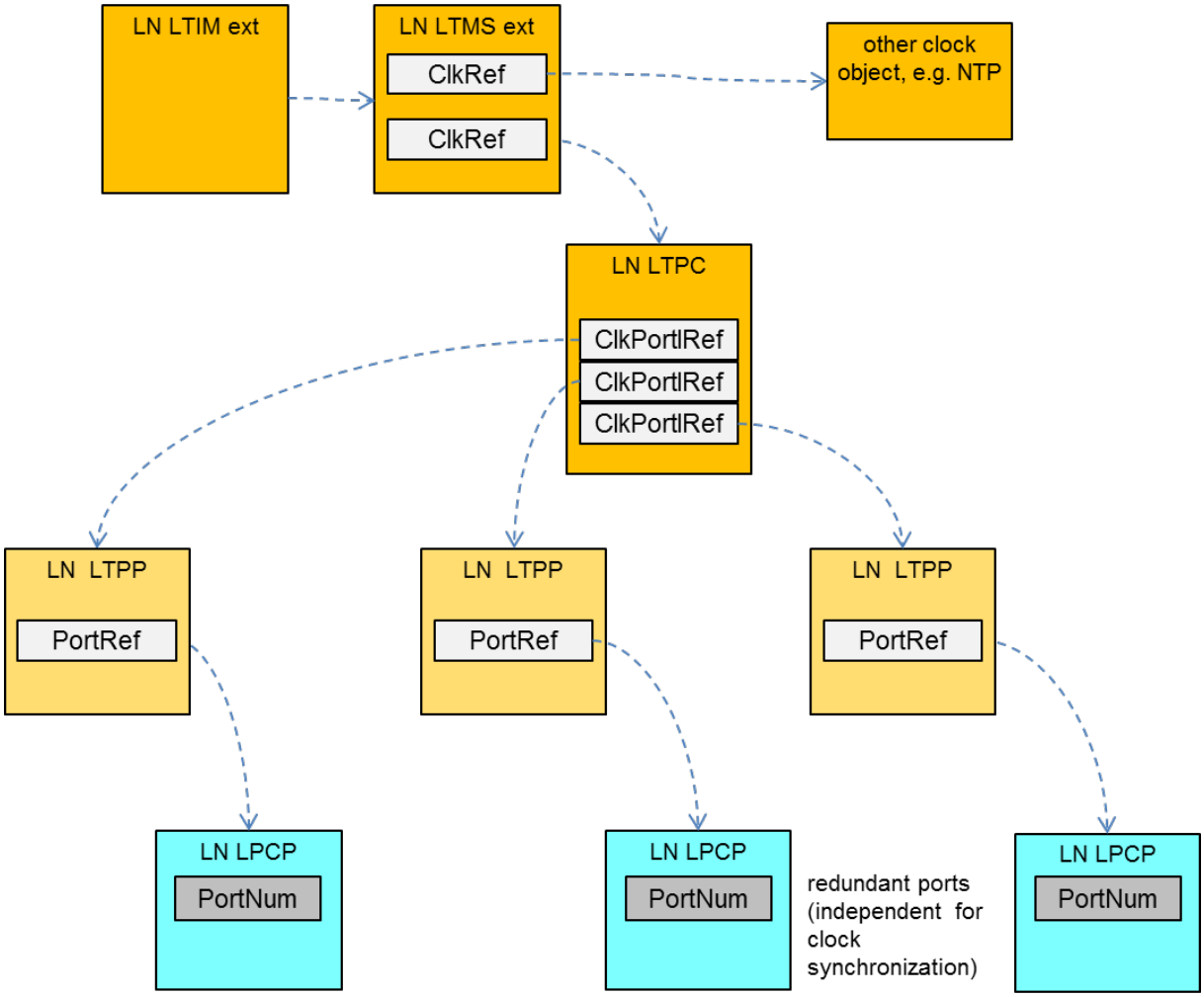


Figure 78 – Linking of clock objects

19.4 Autogenerated IEC 61850 objects

19.4.1 General

NOTE This clause is automatically generated from the model file 'wg10uml02v13-wg18uml02v10c-wg17uml02v10a-jwg25uml02v02c.eap', release WG10UML02v13. Name space definition for this specification is: (Tr)IEC 61850-90-4:2012.

19.4.2 Abbreviated terms used in data object names

Table 46 shows normative terms that are combined to create data object names.

Table 46 – Normative abbreviations for data object names

Term	Description
Addr	Address
Admin	Administrative
Altn	Alternate
Chs	Chassis
Clk	Clock
Desc	Description
Dft	Default
Gm	Grandmaster

Term	Description
Hello	"I am alive" signal of a device
Ldp	Link discovery protocol
Leap	Leap (second)
Mac	MAC address
Mau	Medium access unit
Mir	Mirror
Ngt	Negotiation
Ord	Ordinary
Path	Path
Port	Port
Prio	Priority
Rem	Remote
Rstp	Rapid spanning tree priority
Topo	Topology
Trunk	Trunk
Utc	UTC (Coordinated Universal Time)
Vid	VLAN identification
Vlan	VLAN
Vld	Valid

19.4.3 Logical nodes

19.4.3.1 General

(no doc)

Figure 79 shows class diagram LogicalNodes_90_4.

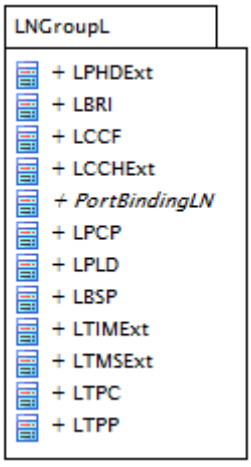


Figure 79 – Class diagram LogicalNodes_90_4::LogicalNodes_90_4

(no doc)

19.4.3.2 System logical nodes LN Group: L

19.4.3.2.1 General

This subclause is a placeholder until the object model is moved to IEC 61850-7-4.

Figure 80 shows class diagram LNGroupLExt.

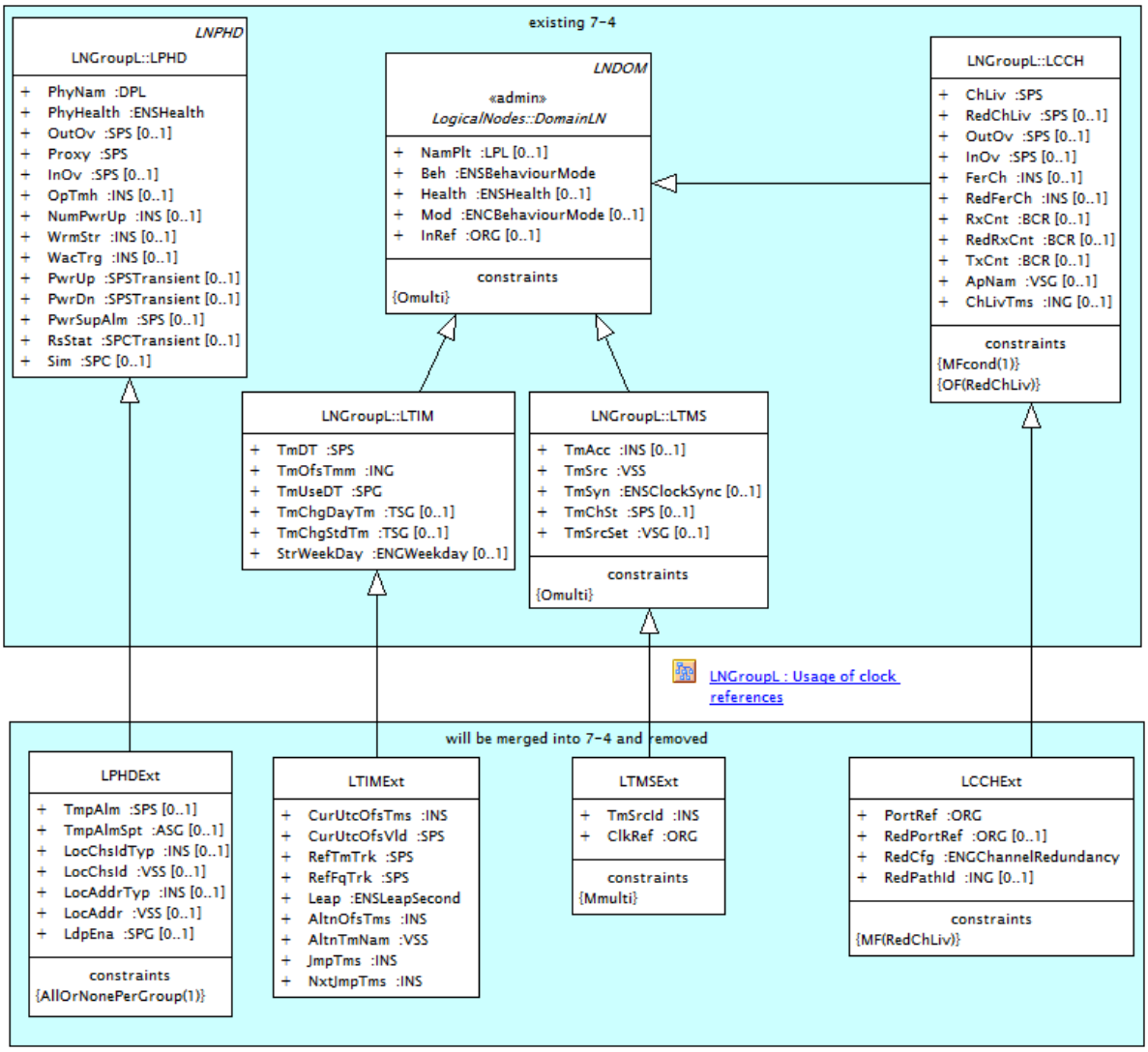


Figure 80 – Class diagram LNGroupL::LNGroupLExt

This diagram shows existing logical nodes (up) and their proposed extensions (down). The extensions have been introduced to support bridge and clock modelling as defined in IEC/TR 61850-90-4.

Figure 81 shows class diagram LNGroupLNew.

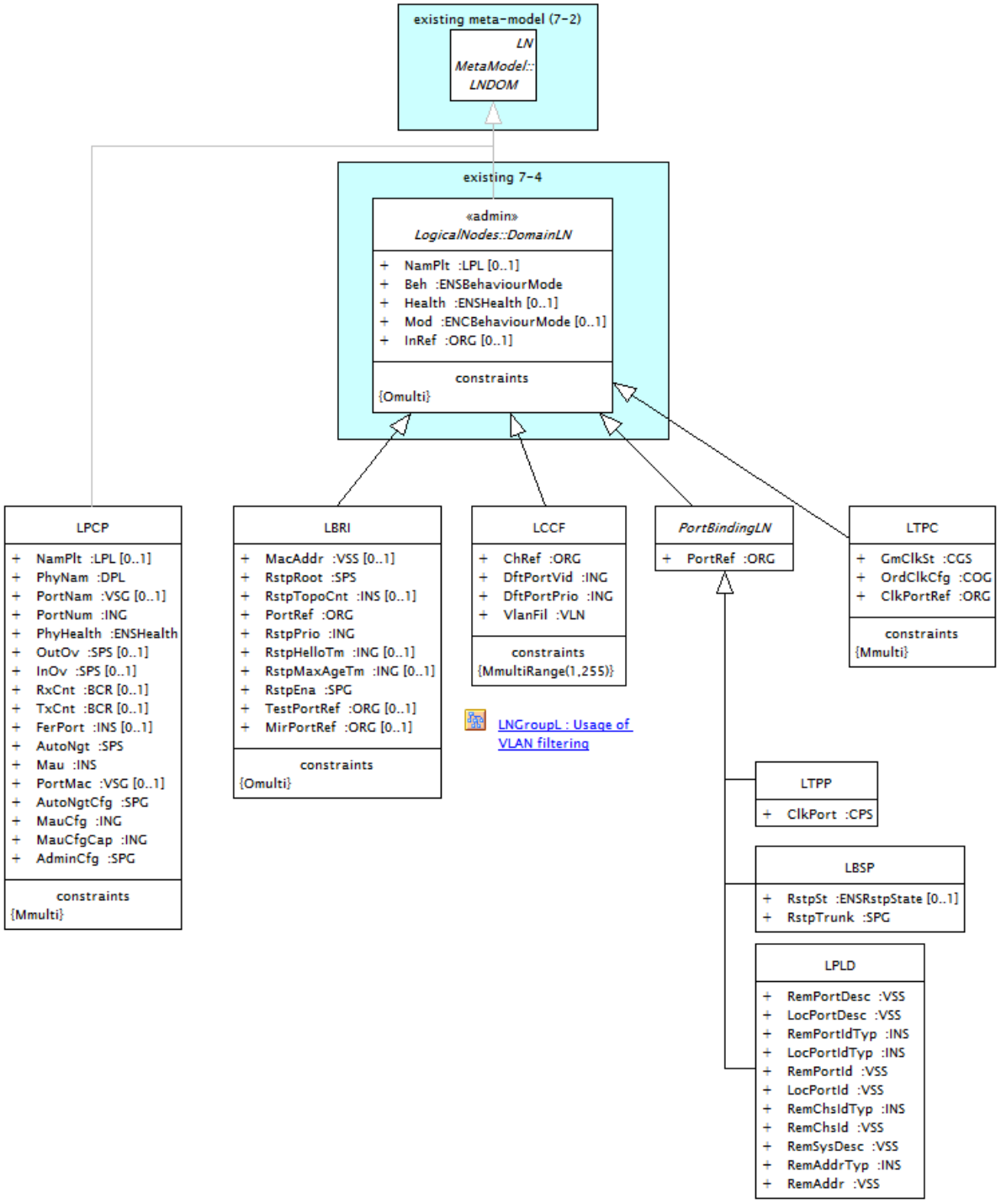


Figure 81 – Class diagram LNGroupL::LNGroupLNew

This diagram shows completely new logical nodes, defined to support bridge and clock modelling as defined in IEC/TR 61850-90-4.

These logical nodes should in the end also move to the group L of IEC 61850-7-4.

19.4.3.2.2 LN: Physical device extension Name: LPHDExt

This logical node contains newly proposed extended data objects to be moved into LPHD, after which this LN shall be removed.

Table 47 shows all data objects of LPHDExt.

Table 47 – Data objects of LNGroupL::LPHDExt

LPHDExt				
Data object name	**Common data class**	**T**	**Explanation**	**M-O-C nds/ds**
Descriptions				
PhyNam	DPL		inherited from: LPHD	M / na
Status information				
TmpAlm	SPS		If true, the temperature exceeded alarm level setting 'TmpAlmSpt'.	O / na
LocChsIdTyp	INS		Type of the local chassis identifier 'LocChsId', according to IEEE 802.1AB.	AllOrNonePerGroup(1) / na
LocChsId	VSS		Local chassis identifier. Interpretation is given through 'LocChsIdTyp', according to IEEE 802.1AB.	AllOrNonePerGroup(1) / na
LocAddrTyp	INS		Type of the local system management address 'LocAddr', according to IEEE 802.1AB.	AllOrNonePerGroup(1) / na
LocAddr	VSS		Local system management address. Interpretation is given through 'LocAddrTyp', according to IEEE 802.1AB.	AllOrNonePerGroup(1) / na
PhyHealth	ENS (HealthKind)		inherited from: LPHD	M / na
OutOv	SPS		inherited from: LPHD	O / na
Proxy	SPS		inherited from: LPHD	M / na
InOv	SPS		inherited from: LPHD	O / na
OpTmh	INS		inherited from: LPHD	O / na
NumPwrUp	INS		inherited from: LPHD	O / na
WrmStr	INS		inherited from: LPHD	O / na
WacTrg	INS		inherited from: LPHD	O / na
PwrUp	SPS	T	inherited from: LPHD	O / na
PwrDn	SPS	T	inherited from: LPHD	O / na
PwrSupAlm	SPS		inherited from: LPHD	O / na
Controls				
RsStat	SPC	T	inherited from: LPHD	O / na
Sim	SPC		inherited from: LPHD	O / na
Settings				
TmpAlmSpt	ASG		Temperature alarm level setting.	O / na
LdpEna	SPG		If true, physical device support for link layer discovery protocol (LLDP) is enabled.	AllOrNonePerGroup(1) / na

19.4.3.2.3 LN: Bridge Name: LBRI

This logical node is used to model bridges. It contains data objects in support of both the IEEE 802.1Q and the IEEE 802.1D, since both are usually associated in a bridging device.

Table 48 shows all data objects of LBRI.

Table 48 – Data objects of LNGroupL::LBRI

LBRI				
Data object name	**Common data class**	**T**	**Explanation**	**M-O-C nds/ds**
Descriptions				
NamPlt	LPL		inherited from: DomainLN	O / na
Status information				
MacAddr	VSS		MAC address of the bridge, as a dash-separated hex number.	O / na
RstpRoot	SPS		If true, this bridge is the root in the spanning tree.	M / na
RstpTopoCnt	INS		Number of topology changes that occurred since last device reset and timestamp of last recorded topology change event based on the local bridge clock.	O / na
Beh	ENS (BehaviourModeKind)		inherited from: DomainLN	M / na
Health	ENS (HealthKind)		inherited from: DomainLN	O / na
Controls				
Mod	ENC (BehaviourModeKind)		inherited from: DomainLN	O / na
Settings				
PortRef	ORG		Reference to RSTP port n (LBSP instance) belonging to this bridge.	M / na
RstpPrio	ING		Bridge priority setting according to IEEE 802.1D.	M / na
RstpHelloTm	ING		RSTP hello time (typically in [s]).	O / na
RstpMaxAgeTm	ING		RSTP maximum age (typically in [s]). May be increased depending on the size of the network.	O / na
RstpEna	SPG		If true, RSTP is enabled.	M / na
TestPortRef	ORG		Reference to test port (LPCP instance).	O / na
MirPortRef	ORG		Reference to mirrored port n (LPCP instance).	Omulti / na
InRef	ORG		inherited from: DomainLN	Omulti / na

19.4.3.2.4 LN: Communication channel filtering Name: LCCF

This logical node is used for VLANs and multicast filtering according to IEEE 802.1Q. When ports are paired for redundancy, the two ports have the same VLAN and multicast settings.

Figure 82 shows custom diagram Usage of VLAN filtering.

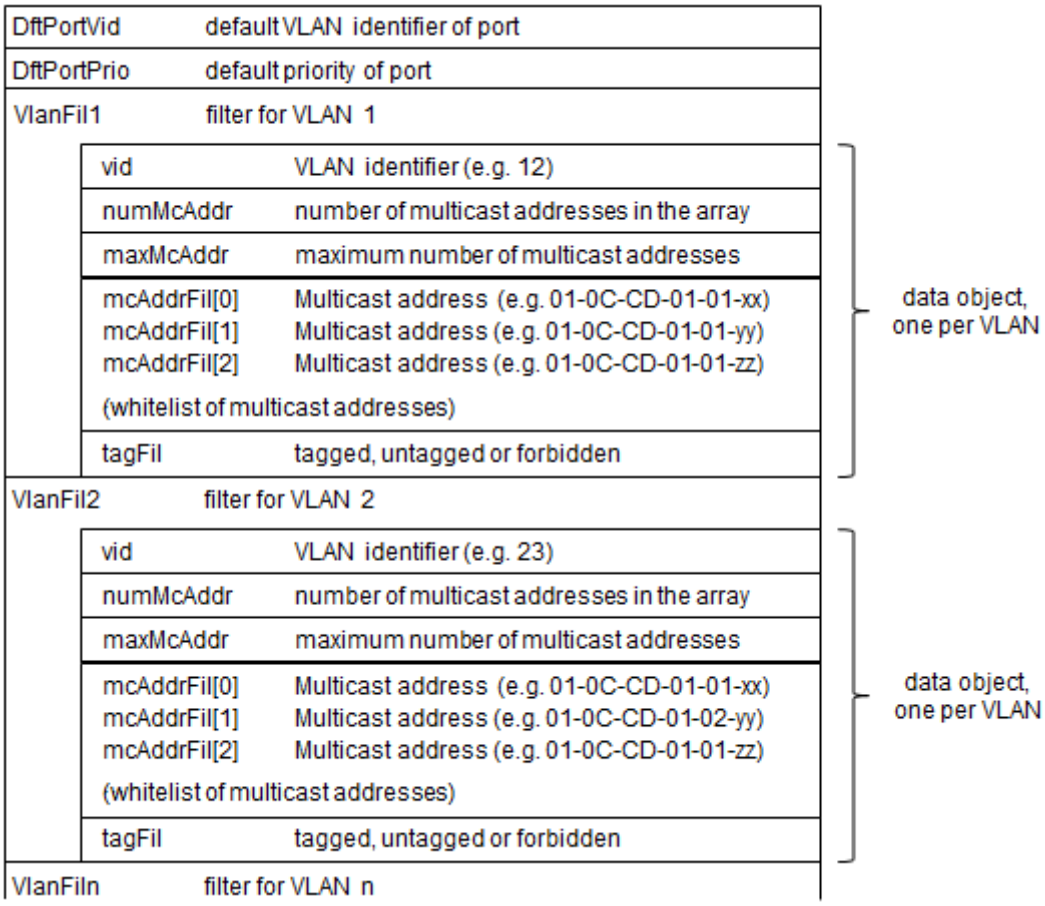


Figure 82 – Usage of VLAN filtering

This diagram illustrates the intended usage of the VLN common data class for multiple VLAN filters, modelled with the data object 'VlanFil'.

Table 49 shows all data objects of LCCF.

Table 49 – Data objects of LNGroupL::LCCF

LCCF				
Data object name	**Common data class**	**T**	**Explanation**	**M-O-C nds/ds**
Descriptions				
NamPlt	LPL		inherited from: DomainLN	O / na
Status information				
Beh	ENS (BehaviourModeKind)		inherited from: DomainLN	M / na
Health	ENS (HealthKind)		inherited from: DomainLN	O / na
Controls				
Mod	ENC (BehaviourModeKind)		inherited from: DomainLN	O / na
Settings				
ChRef	ORG		Reference of the channel (LCCH) to which this filter belongs.	M / na
DftPortVid	ING		Default port's VLAN ID.	M / na
DftPortPrio	ING		Default port's priority.	M / na

LCCF				
Data object name	**Common data class**	**T**	**Explanation**	**M-O-C nds/ds**
VlanFil	VLN		Information for the supported VLAN filter n. There should be at least one VLAN filter corresponding to the default channel VLAN ID even if no VLANs are used.	MmultiRange (1,255) / na
InRef	ORG		inherited from: DomainLN	Omulti / na

19.4.3.2.5 LN: Extension of LCCH Name: LCCHExt

This logical node contains newly proposed extended data objects to be moved into LCCH, after which this LN shall be removed.

Table 50 shows all data objects of LCCHExt.

Table 50 – Data objects of LNGroupL::LCCHExt

LCCHExt				
Data object name	**Common data class**	**T**	**Explanation**	**M-O-C nds/ds**
Descriptions				
NamPlt	LPL		inherited from: DomainLN	O / na
Status information				
ChLiv	SPS		inherited from: LCCH	M / na
RedChLiv	SPS		inherited from: LCCH	MFcond(1) / na
OutOv	SPS		inherited from: LCCH	O / na
InOv	SPS		inherited from: LCCH	O / na
FerCh	INS		inherited from: LCCH	O / na
RedFerCh	INS		inherited from: LCCH	OF(RedChLiv) / na
RxCnt	BCR		inherited from: LCCH	O / na
RedRxCnt	BCR		inherited from: LCCH	OF(RedChLiv) / na
TxCnt	BCR		inherited from: LCCH	O / na
Beh	ENS (BehaviourModeKind)		inherited from: DomainLN	M / na
Health	ENS (HealthKind)		inherited from: DomainLN	O / na
Controls				
Mod	ENC (BehaviourModeKind)		inherited from: DomainLN	O / na
Settings				
PortRef	ORG		Reference to the LPCP port instance (port A if paired).	M / na
RedPortRef	ORG		Reference to the LPCP port instance for redundant port (port B if paired).	MF(RedChLiv) / na
RedCfg	ENG (ChannelRedundancyKind)		Port redundancy protocol.	M / na
RedPathId	ING		Path ID for RedBox or QuadBox functionality (applicable for PRP or HSR protocols).	MF(RedChLiv) / na

LCCHExt				
Data object name	**Common data class**	**T**	**Explanation**	**M-O-C nds/ds**
ApNam	VSG		inherited from: LCCH	O / na
ChLivTms	ING		inherited from: LCCH	O / na
InRef	ORG		inherited from: DomainLN	Omulti / na

19.4.3.2.6 <<abstract>> LN: Communication port binding Name: PortBindingLN

Abstract type, holding attributes common to all of the bindings for communication ports.

Table 51 shows all data objects of PortBindingLN.

Table 51 – Data objects of LNGroupL::PortBindingLN

PortBindingLN				
Data object name	**Common data class**	**T**	**Explanation**	**M-O-C nds/ds**
Descriptions				
NamPlt	LPL		inherited from: DomainLN	O / na
Status information				
Beh	ENS (BehaviourModeKind)		inherited from: DomainLN	M / na
Health	ENS (HealthKind)		inherited from: DomainLN	O / na
Controls				
Mod	ENC (BehaviourModeKind)		inherited from: DomainLN	O / na
Settings				
PortRef	ORG		Reference to the port (LPCP instance) to which this binding applies.	M / na
InRef	ORG		inherited from: DomainLN	Omulti / na

19.4.3.2.7 LN: Physical communication port Name: LPCP

This logical node is used to model communication ports.

Table 52 shows all data objects of LPCP.

Table 52 – Data objects of LNGroupL::LPCP

LPCP				
Data object name	**Common data class**	**T**	**Explanation**	**M-O-C nds/ds**
Descriptions				
NamPlt	LPL		Name plate of the logical node. Note: This data object has been temporarily added because this logical node does not derive from DomainLN (which has NamPlt), but we need the means to specify the data name space (NamPlt.InNs) as long as it is different from IEC 61850-7-4. As soon as this logical node gets incorporated into IEC 61850-7-4, this data object will be removed.	O / na

LPCP				
Data object name	**Common data class**	**T**	**Explanation**	**M-O-C nds/ds**
PhyNam	DPL		Physical device name plate.	M / na
Status information				
PhyHealth	ENS (HealthKind)		Reflects the state of the physical device related hardware and software.	M / na
OutOv	SPS		If true, a buffer overflow has occurred for the output buffer and important annunciations may be lost for the communication. It comes back to false when the buffer has returned to normal operation. A general interrogation is recommended or an integrity scan is started automatically.	O / na
InOv	SPS		If true, a buffer overflow has occurred for the input buffer and important annunciations may be lost for the communication. It comes back to false when the buffer has returned to normal operation. A general interrogation is recommended or an integrity scan is started automatically.	O / na
RxCnt	BCR		Number of messages received since last reset.	O / na
TxCnt	BCR		Number of messages sent since last reset.	O / na
FerPort	INS		Frame error rate on this port, defined as the count of erroneous messages for each 1'000 messages received.	O / na
AutoNgt	SPS		If true, the port is set to auto-negotiation.	M / na
Mau	INS		Medium access unit status.	M / na
Settings				
PortNam	VSG		Label of the terminal on the device.	O / na
PortNum	ING		Number of the terminal on the device.	M / na
PortMac	VSG		MAC address of the port, as a dash-separated hex number.	O / na
AutoNgtCfg	SPG		If true, the port is set to auto-negotiation.	M / na
MauCfg	ING		Currently supported value from 'MauCfgCap'; valid only if 'AutoNegCfg'=false.	M / na
MauCfgCap	ING		Supported medium access unit (MAU) setting n. The value corresponds to the MAU type list bit position in RFC 4836. For example, value 16 corresponds to 100BASE-TX full duplex mode.	Mmulti / na
AdminCfg	SPG		If true, the port is administratively up, otherwise it is down.	M / na

19.4.3.2.8 LN: Port link discovery Name: LPLD

This logical node is used to model layer discovery protocol according to IEEE 802.1AB. Its data objects contain data relevant to the remote port connected to a local port.

Table 53 shows all data objects of LPLD.

Table 53 – Data objects of LNGroupL::LPLD

LPLD				
Data object name	**Common data class**	**T**	**Explanation**	**M-O-C nds/ds**
Descriptions				
NamPlt	LPL		inherited from: DomainLN	O / na

LPLD				
Data object name	**Common data class**	**T**	**Explanation**	**M-O-C nds/ds**
Status information				
RemPortDesc	VSS		Textual description of the remote port, according to IEEE 802.1AB.	M / na
LocPortDesc	VSS		Textual description of the local port, according to IEEE 802.1AB.	M / na
RemPortIdTyp	INS		Type of the remote port identifier 'RemPortId', according to IEEE 802.1AB.	M / na
LocPortIdTyp	INS		Type of the local port identifier 'LocPortId', according to IEEE 802.1AB.	M / na
RemPortId	VSS		Remote port identifier. Interpretation is given through 'RemPortIdTyp', according to IEEE 802.1AB.	M / na
LocPortId	VSS		Local port identifier. Interpretation is given through 'LocPortIdTyp', according to IEEE 802.1AB.	M / na
RemChsIdTyp	INS		Type of the remote port chassis identifier 'RemChsId', according to IEEE 802.1AB.	M / na
RemChsId	VSS		Remote port chassis identifier. Interpretation is given through 'RemChsIdTyp', according to IEEE 802.1AB.	M / na
RemSysDesc	VSS		Textual description of the system name of the remote device, according to IEEE 802.1AB.	M / na
RemAddrTyp	INS		Type of the remote system management address 'RemAddr', according to IEEE 802.1AB.	M / na
RemAddr	VSS		Remote system management address. Interpretation is given through 'RemAddrTyp', according to IEEE 802.1AB.	M / na
Beh	ENS (BehaviourModeKind)		inherited from: DomainLN	M / na
Health	ENS (HealthKind)		inherited from: DomainLN	O / na
Controls				
Mod	ENC (BehaviourModeKind)		inherited from: DomainLN	O / na
Settings				
PortRef	ORG		inherited from: PortBindingLN	M / na
InRef	ORG		inherited from: DomainLN	Omulti / na

19.4.3.2.9 LN: Bridge spanning tree port Name: LBSP

This logical node is used to model rapid bridge spanning tree protocol according to IEEE 802.1D.

Table 54 shows all data objects of LBSP.

Table 54 – Data objects of LNGroupL::LBSP

LBSP				
Data object name	**Common data class**	**T**	**Explanation**	**M-O-C nds/ds**
Descriptions				
NamPlt	LPL		inherited from: DomainLN	O / na
Status information				
RstpSt	ENS (RstpStateKind)		RSTP port state.	O / na
Beh	ENS (BehaviourModeKind)		inherited from: DomainLN	M / na
Health	ENS (HealthKind)		inherited from: DomainLN	O / na
Controls				
Mod	ENC (BehaviourModeKind)		inherited from: DomainLN	O / na
Settings				
RstpTrunk	SPG		If true, the port is set to participate in RSTP (is trunk), otherwise it is edge.	M / na
PortRef	ORG		inherited from: PortBindingLN	M / na
InRef	ORG		inherited from: DomainLN	Omulti / na

19.4.3.2.10 LN: Time management extension Name: LTIMExt

This logical node contains newly proposed extended data objects to be moved into LTIM, after which this LN shall be removed.

Table 55 shows all data objects of LTIMExt.

Table 55 – Data objects of LNGroupL::LTIMExt

LTIMExt				
Data object name	**Common data class**	**T**	**Explanation**	**M-O-C nds/ds**
Descriptions				
NamPlt	LPL		inherited from: DomainLN	O / na
Status information				
CurUtcOfsTms	INS		Current lag behind TAI, according to 8.2.4.2 of IEC 61588:2009.	M / na
CurUtcOfsVld	SPS		If true, 'CurUtcOfsTms' is valid, according to 8.2.4.3 of IEC 61588:2009.	M / na
RefTmTrk	SPS		If true, reference time is traceable, according to 8.2.4.6 of IEC 61588:2009.	M / na
RefFqTrk	SPS		If true, reference frequency is traceable, i.e., can be used for 1PPS, according to 8.2.4.7 of IEC 61588:2009.	M / na
Leap	ENS (LeapSecondKind)		Indicates whether a leap second is introduced, and if yes, whether added or subtracted, according to IEC 61588.	M / na
AltnOfsTms	INS		Alternate time offset (as carried in AlternateTimeOffset), according to 16.3.3.4 of IEC 61588:2009.	M / na
AltnTmNam	VSS		Alternate time name (as carried in AlternateTimeOffset), according to 16.3.3.4 of	M / na

LTIMExt				
Data object name	**Common data class**	**T**	**Explanation**	**M-O-C nds/ds**
			IEC 61588:2009.	
JmpTms	INS		Size of next discontinuity (jumpSeconds), according to 16.3.3.5 of IEC 61588:2009.	M / na
NxtJmpTms	INS		Second portion of transmitter time when next discontinuity will occur (timeOfNextJump), according to 16.3.3.6 of IEC 61588:2009.	M / na
TmDT	SPS		inherited from: LTIM	M / na
Beh	ENS (BehaviourModeKind)		inherited from: DomainLN	M / na
Health	ENS (HealthKind)		inherited from: DomainLN	O / na
Controls				
Mod	ENC (BehaviourModeKind)		inherited from: DomainLN	O / na
Settings				
TmOfsTmm	ING		inherited from: LTIM	M / na
TmUseDT	SPG		inherited from: LTIM	M / na
TmChgDayTm	TSG		inherited from: LTIM	O / na
TmChgStdTm	TSG		inherited from: LTIM	O / na
StrWeekDay	ENG (WeekdayKind)		inherited from: LTIM	O / na
InRef	ORG		inherited from: DomainLN	Omulti / na

19.4.3.2.11 LN: Time master supervision extension Name: LTMSExt

This logical node contains newly proposed extended data objects to be moved into LTMS, after which this LN shall be removed.

Figure 83 shows custom diagram Usage of clock references.

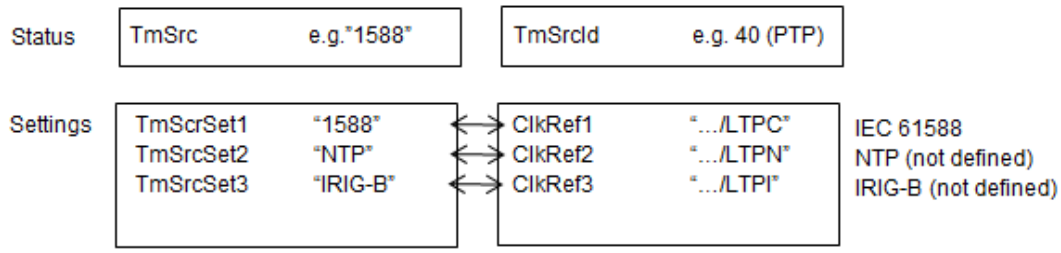


Figure 83 – Usage of clock references

This diagram illustrates usage of data objects 'ClkRef' and 'TmSrcId' and how they fit with data objects 'TmSrcSet' and 'ClkRef'.

Table 56 shows all data objects of LTMSExt.

Table 56 – Data objects of LNGroupL::LTMSExt

LTMSExt				
Data object name	**Common data class**	**T**	**Explanation**	**M-O-C nds/ds**
Descriptions				
NamPlt	LPL		inherited from: DomainLN	O / na
Status information				
TmSrcId	INS		Identity of the time source in 'TmSrc', according to 8.2.4.9 of IEC 61588:2009.	M / na
TmAcc	INS		inherited from: LTMS	O / na
TmSrc	VSS		inherited from: LTMS	M / na
TmSyn	ENS (ClockSyncKind)		inherited from: LTMS	O / na
TmChSt	SPS		inherited from: LTMS	Omulti / na
Beh	ENS (BehaviourModeKind)		inherited from: DomainLN	M / na
Health	ENS (HealthKind)		inherited from: DomainLN	O / na
Controls				
Mod	ENC (BehaviourModeKind)		inherited from: DomainLN	O / na
Settings				
ClkRef	ORG		Reference to clock n (e.g., LTPC instance) providing synchronisation, in order of preference; this corresponds to 'TmSrcSet' n. At present, the only time source having its logical node model is the one specified in IEC 61588.	Mmulti / na
TmSrcSet	VSG		inherited from: LTMS	Omulti / na
InRef	ORG		inherited from: DomainLN	Omulti / na

19.4.3.2.12 LN: PTP clock Name: LTPC

This logical node is used to model clock according to the IEC 61588 precision time protocol, consisting of the ordinary (local) clock configuration (defaultDS) and of the grandmaster (parent) clock status (currentDS, parentDS). The grandmaster attributes are statuses since they represent the remote clock, even if the master clock happens to be the same local clock, in which case the objects have the same value as for the local clock settings.

Table 57 shows all data objects of LTPC.

Table 57 – Data objects of LNGroupL::LTPC

LTPC				
Data object name	**Common data class**	**T**	**Explanation**	**M-O-C nds/ds**
Descriptions				
NamPlt	LPL		inherited from: DomainLN	O / na
Status information				
GmClkSt	CGS		Grandmaster clock status, according to IEEE C37.238.	M / na
Beh	ENS (BehaviourModeKind)		inherited from: DomainLN	M / na
Health	ENS (HealthKind)		inherited from: DomainLN	O / na

LTPC				
Data object name	**Common data class**	**T**	**Explanation**	**M-O-C nds/ds**
Controls				
Mod	ENC (BehaviourModeKind)		inherited from: DomainLN	O / na
Settings				
OrdClkCfg	COG		Ordinary clock configuration, according to IEEE C37.238.	M / na
ClkPortRef	ORG		Reference to the synchronizing port n (LTPP instance).	Mmulti / na
InRef	ORG		inherited from: DomainLN	Omulti / na

19.4.3.2.13 LN: PTP clock port Name: LTPP

This logical node is used to model clock properties of a port, extending the portDS in IEC 61588 by IEEE C37.238 MIB objects.

Table 58 shows all data objects of LTPP.

Table 58 – Data objects of LNGroupL::LTPP

LTPP				
Data object name	**Common data class**	**T**	**Explanation**	**M-O-C nds/ds**
Descriptions				
NamPlt	LPL		inherited from: DomainLN	O / na
Status information				
ClkPort	CPS		Status of the clock port.	M / na
Beh	ENS (BehaviourModeKind)		inherited from: DomainLN	M / na
Health	ENS (HealthKind)		inherited from: DomainLN	O / na
Controls				
Mod	ENC (BehaviourModeKind)		inherited from: DomainLN	O / na
Settings				
PortRef	ORG		inherited from: PortBindingLN	M / na
InRef	ORG		inherited from: DomainLN	Omulti / na

19.4.4 Data semantics

Table 59 shows all attributes defined on classes of LogicalNodes_90_4 package.

Table 59 – Attributes defined on classes of LogicalNodes_90_4 package

Name	Type	(Used in) Description
AdminCfg	SPG	(LPCP) If true, the port is administratively up, otherwise it is down.
AltnOfsTms	INS	(LTIMExt) Alternate time offset (as carried in AlternateTimeOffset), according to IEC 61588, 16.3.3.4.
AltnTmNam	VSS	(LTIMExt) Alternate time name (as carried in AlternateTimeOffset),

Name	Type	(Used in) Description
		according 16.3.3.4 of IEC 61588:2009.
AutoNgt	SPS	(LPCP) If true, the port is set to auto-negotiation.
AutoNgtCfg	SPG	(LPCP) If true, the port is set to auto-negotiation.
ChRef	ORG	(LCCF) Reference of the channel (LCCH) to which this filter belongs.
ClkPort	CPS	(LTPP) Status of the clock port.
ClkPortRef	ORG	(LTPC) Reference to the synchronizing port n (LTPP instance).
ClkRef	ORG	(LTMSExt) Reference to clock n (e.g., LTPC instance) providing synchronisation, in order of preference; this corresponds to 'TmSrcSet' n. At present, the only time source having its logical node model is the one specified in IEC 61588.
CurUtcOfsTms	INS	(LTIMExt) Current lag behind TAI, according to 8.2.4.2 of IEC 61588:2009.
CurUtcOfsVld	SPS	(LTIMExt) If true, 'CurUtcOfsTms' is valid, according to 8.2.4.3 of IEC 61588:2009.
DftPortPrio	ING	(LCCF) Default port's priority.
DftPortVid	ING	(LCCF) Default port's VLAN ID.
FerPort	INS	(LPCP) Frame error rate on this port, defined as the count of erroneous messages for each 1'000 messages received.
GmClkSt	CGS	(LTPC) Grandmaster clock status, according to IEEE C37.238.
InOv	SPS	(LPCP) If true, a buffer overflow has occurred for the input buffer and important annunciations may be lost for the communication. It comes back to false when the buffer has returned to normal operation. A general interrogation is recommended or an integrity scan is started automatically.
JmpTms	INS	(LTIMExt) Size of next discontinuity (jumpSeconds), according to 16.3.3.5 of IEC 61588:2009.
LdpEna	SPG	(LPHDExt) If true, physical device support for link layer discovery protocol (LLDP) is enabled.
Leap	ENS (LeapSecondKind)	(LTIMExt) Indicates whether a leap second is introduced, and if yes, whether added or subtracted, according to IEC 61588.
LocAddr	VSS	(LPHDExt) Local system management address. Interpretation is given through 'LocAddrTyp', according to IEEE 802.1AB.
LocAddrTyp	INS	(LPHDExt) Type of the local system management address 'LocAddr', according to IEEE 802.1AB.
LocChsId	VSS	(LPHDExt) Local chassis identifier. Interpretation is given through 'LocChsIdTyp', according to IEEE 802.1AB.
LocChsIdTyp	INS	(LPHDExt) Type of the local chassis identifier 'LocChsId', according to IEEE 802.1AB.
LocPortDesc	VSS	(LPLD) Textual description of the local port, according to IEEE 802.1AB.
LocPortId	VSS	(LPLD) Local port identifier. Interpretation is given through 'LocPortIdTyp', according to IEEE 802.1AB.
LocPortIdTyp	INS	(LPLD) Type of the local port identifier 'LocPortId', according to IEEE 802.1AB.
MacAddr	VSS	(LBRI) MAC address of the bridge, as a dash-separated hex number.
Mau	INS	(LPCP) Medium access unit status.
MauCfg	ING	(LPCP) Currently supported value from 'MauCfgCap'; valid only if 'AutoNegCfg'=false.
MauCfgCap	ING	(LPCP) Supported medium access unit (MAU) setting n. The value corresponds to the MAU type list bit position in RFC 4836. For example, value 16 corresponds to 100BASE-TX full duplex mode.
MirPortRef	ORG	(LBRI) Reference to mirrored port n (LPCP instance).
NamPlt	LPL	(LPCP) Name plate of the logical node. Note: This data object has been temporarily added because this logical node does not derive from DomainLN (which has NamPlt), but we need the means to specify the data name space (NamPlt.lnNs) as long as it is different from

Name	Type	(Used in) Description
		IEC 61850-7-4. As soon as this logical node gets incorporated into IEC 61850-7-4, this data object will be removed.
NxtJmpTms	INS	(LTIMExt) Second portion of transmitter time when next discontinuity will occur (timeOfNextJump), according to 16.3.3.6 of IEC 61588:2009.
OrdClkCfg	COG	(LTPC) Ordinary clock configuration, according to IEEE C37.238.
OutOv	SPS	(LPCP) If true, a buffer overflow has occurred for the output buffer and important annunciations may be lost for the communication. It comes back to false when the buffer has returned to normal operation. A general interrogation is recommended or an integrity scan is started automatically.
PhyHealth	ENS (HealthKind)	(LPCP) Reflects the state of the physical device related hardware and software.
PhyNam	DPL	(LPCP) Physical device name plate.
PortMac	VSG	(LPCP) MAC address of the port, as a dash-separated hex number.
PortNam	VSG	(LPCP) Label of the terminal on the device.
PortNum	ING	(LPCP) Number of the terminal on the device.
PortRef	ORG	(LCCHExt) Reference to the LPCP port instance (port A if paired). (LBRI) Reference to RSTP port n (LBSP instance) belonging to this bridge. (PortBindingLN) Reference to the port (LPCP instance) to which this binding applies.
RedCfg	ENG (ChannelRedundancyKind)	(LCCHExt) Port redundancy protocol.
RedPathId	ING	(LCCHExt) Path ID for RedBox or QuadBox functionality (applicable for PRP or HSR protocols).
RedPortRef	ORG	(LCCHExt) Reference to the LPCP port instance for redundant port (port B if paired).
RefFqTrk	SPS	(LTIMExt) If true, reference frequency is traceable, i.e., can be used for 1PPS, according to 8.2.4.7 of IEC 61588:2009.
RefTmTrk	SPS	(LTIMExt) If true, reference time is traceable, according to 8.2.4.6 of IEC 61588:2009.
RemAddr	VSS	(LPLD) Remote system management address. Interpretation is given through 'RemAddrTyp', according to IEEE 802.1AB.
RemAddrTyp	INS	(LPLD) Type of the remote system management address 'RemAddr', according to IEEE 802.1AB.
RemChsId	VSS	(LPLD) Remote port chassis identifier. Interpretation is given through 'RemChsIdTyp', according to IEEE 802.1AB.
RemChsIdTyp	INS	(LPLD) Type of the remote port chassis identifier 'RemChsId', according to IEEE 802.1AB.
RemPortDesc	VSS	(LPLD) Textual description of the remote port, according to IEEE 802.1AB.
RemPortId	VSS	(LPLD) Remote port identifier. Interpretation is given through 'RemPortIdTyp', according to IEEE 802.1AB.
RemPortIdTyp	INS	(LPLD) Type of the remote port identifier 'RemPortId', according to IEEE 802.1AB.
RemSysDesc	VSS	(LPLD) Textual description of the system name of the remote device, according to IEEE 802.1AB.
RstpEna	SPG	(LBRI) If true, RSTP is enabled.
RstpHelloTm	ING	(LBRI) RSTP hello time (typically in [s]).
RstpMaxAgeTm	ING	(LBRI) RSTP maximum age (typically in [s]). May be increased depending on the size of the network.
RstpPrio	ING	(LBRI) Bridge priority setting according to IEEE 802.1D.
RstpRoot	SPS	(LBRI) If true, this bridge is the root in the spanning tree.

Name	Type	(Used in) Description
RstpSt	ENS (RstpStateKind)	(LBSP) RSTP port state.
RstpTopoCnt	INS	(LBRI) Number of topology changes that occurred since last device reset and timestamp of last recorded topology change event based on the local bridge clock.
RstpTrunk	SPG	(LBSP) If true, the port is set to participate in RSTP (is trunk), otherwise it is edge.
RxCnt	BCR	(LPCP) Number of messages received since last reset.
TestPortRef	ORG	(LBRI) Reference to test port (LPCP instance).
TmSrcId	INS	(LTMSExt) Identity of the time source in 'TmSrc', according to 8.2.4.9 of IEC 61588:2009.
TmpAlm	SPS	(LPHDExt) If true, the temperature exceeded alarm level setting 'TmpAlmSpt'.
TmpAlmSpt	ASG	(LPHDExt) Temperature alarm level setting.
TxCnt	BCR	(LPCP) Number of messages sent since last reset.
VlanFil	VLN	(LCCF) Information for the supported VLAN filter n. There should be at least one VLAN filter corresponding to the default channel VLAN ID even if no VLANs are used.

19.4.5 Enumerated data attribute types

19.4.5.1 General

Subclause 19.4.5 contains explicit definitions of enumerated types used in IEC/TR 61850-90-4.

19.4.5.2 Channel redundancy (ChannelRedundancyKind enumeration)

Kind of channel redundancy.

Table 60 shows all literals of ChannelRedundancyKind.

Table 60 – Literals of DOEnums_90_4::ChannelRedundancyKind

ChannelRedundancyKind		
literal	**value**	**description**
none	1	No redundant port.
prp	2	Parallel redundancy protocol, with two channels working in parallel.
hsr	3	Parallel redundancy with bridging, i.e., transmitting from one port to another.

19.4.5.3 LeapSecondKind enumeration

Consideration of the leap second.

Table 61 shows all literals of LeapSecondKind.

Table 61 – Literals of DOEnums_90_4::LeapSecondKind

LeapSecondKind		
literal	**value**	**description**
none	1	No leap second.
removeLeapSecond	2	The last minute of the day will have 59 s.
addLeapSecond	3	The last minute of the day will have 61 s.

19.4.5.4 RSTP state (RstpStateKind enumeration)

RSTP states.

Table 62 shows all literals of RstpStateKind.

Table 62 – Literals of DOEnums_90_4::RstpStateKind

RstpStateKind		
literal	**value**	**description**
disabled	1	Port is disabled in STP, discarding in RSTP.
blocking	2	Port is blocking in STP, discarding in RSTP.
listening	3	Port is listening in STP, discarding in RSTP.
learning	4	Port is learning in both STP and RSTP.
forwarding	5	Port is forwarding in both STP and RSTP.
unknown	6	Port is in an unknown state.

19.4.5.5 Package DetailedDiagram

19.4.5.5.1 General

Figure 84 shows class diagram DOEnums_90_4.

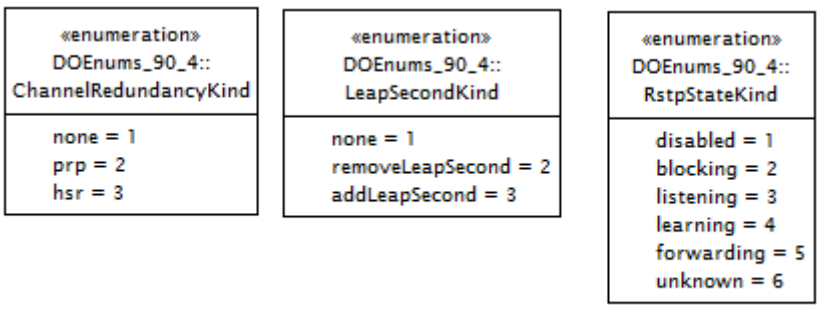


Figure 84 – Class diagram DetailedDiagram::DOEnums_90_4

19.4.6 SCL enumerations

```
<EnumType id="ChannelRedundancyKind">
   <EnumVal ord="1">none</EnumVal>
   <EnumVal ord="2">prp</EnumVal>
   <EnumVal ord="3">hsr</EnumVal>
</EnumType>
<EnumType id="LeapSecondKind">
   <EnumVal ord="1">none</EnumVal>
   <EnumVal ord="2">removeLeapSecond</EnumVal>
   <EnumVal ord="3">addLeapSecond</EnumVal>
</EnumType>
<EnumType id="RstpStateKind">
   <EnumVal ord="1">disabled</EnumVal>
   <EnumVal ord="2">blocking</EnumVal>
   <EnumVal ord="3">listening</EnumVal>
   <EnumVal ord="4">learning</EnumVal>
   <EnumVal ord="5">forwarding</EnumVal>
   <EnumVal ord="6">unknown</EnumVal>
</EnumType>
```

19.4.7 Common data class specifications

19.4.7.1 General

This subclause is a placeholder until the object model is moved to IEC 61850-7-3.

(no doc)

Figure 85 shows class diagram CommonDataClasses_90_4.

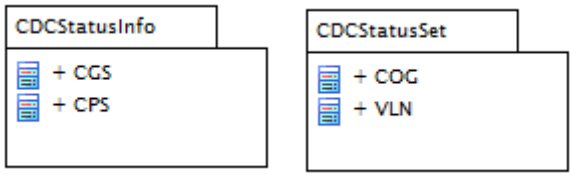


Figure 85 – Class diagram CommonDataClasses_90_4::CommonDataClasses_90_4

(no doc)

19.4.7.2 Common data class specifications for status information

19.4.7.2.1 General

This subclause is a placeholder until the object model is moved to IEC 61850-7-3.

Figure 86 shows class diagram CDCStatusInfo.

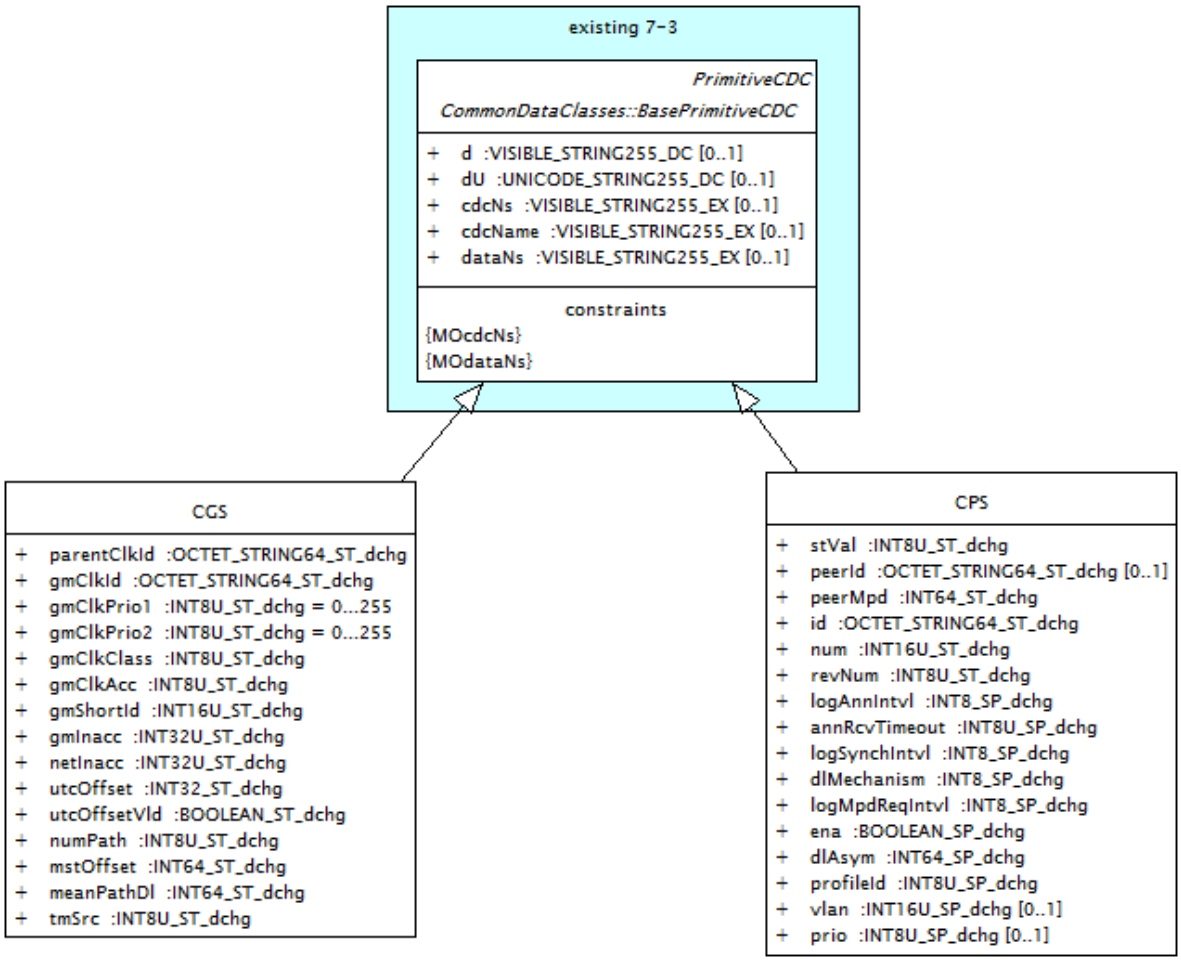


Figure 86 – Class diagram CDCStatusInfo::CDCStatusInfo

(no doc)

19.4.7.2.2 Clock grandmaster status (CGS)

This common data class is used to model grandmaster clock status according to IEC 61588 and IEEE C37.238. It reflects the currentDS, parentDS and timePropertiesDS in IEC 61588.

Table 63 defines the common data class "clock grandmaster status".

Table 63 – Clock grandmaster status common data class definition

CGS					
Data attribute name	**Type**	**FC**	**TrgOp**	**(Value/Value range) Description**	**M/O/C**
status					
parentClkId	OCTET_STRING64	ST	dchg	Master EUI-64 clock identity, according to 8.2.3.2 of IEC 61588:2009.	M
gmClkId	OCTET_STRING64	ST	dchg	Grandmaster EUI-64 clock identity, according to 8.2.3.6 of IEC 61588:2009.	M
gmClkPrio1	INT8U	ST	dchg	(range=[0...255]) Grandmaster clock priority1, according to 8.2.3.8 of IEC 61588:2009.	M
gmClkPrio2	INT8U	ST	dchg	(range=[0...255]) Grandmaster clock	M

CGS					
Data attribute name	**Type**	**FC**	**TrgOp**	**(Value/Value range) Description**	**M/O/C**
				priority2, according to IEC 61588, 8.2.3.9.	
gmClkClass	INT8U	ST	dchg	Grandmaster clock class, according to 8.2.3.7 of IEC 61588:2009.	M
gmClkAcc	INT8U	ST	dchg	Grandmaster clock time accuracy class, according to 8.2.3.7 of IEC 61588:2009.	M
gmShortId	INT16U	ST	dchg	Grandmaster short identifier, according to IEEE C37.238, 5.9.6.	M
gmInacc	INT32U	ST	dchg	Grandmaster time inaccuracy, according to 5.13 of IEEE C37.238:2011.	M
netInacc	INT32U	ST	dchg	Network time inaccuracy, according to 5.13 of IEEE C37.238:2011.	M
utcOffset	INT32	ST	dchg	Offset from UTC time [s], according to 8.2.4.2 of IEC 61588:2009.	M
utcOffsetVld	BOOLEAN	ST	dchg	If true, offset from UTC is valid, according to 8.2.4.2 of IEC 61588:2009.	M
numPath	INT8U	ST	dchg	Number of paths traversed between local clock and grandmaster clock, according to 8.2.2.2 of IEC 61588:2009.	M
mstOffset	INT64	ST	dchg	Offset from master time [ns], derived from 8.2.2.3 of IEC 61588:2009.	M
meanPathDl	INT64	ST	dchg	Mean path delay, derived from 8.2.2.4 of IEC 61588:2009.	M
tmSrc	INT8U	ST	dchg	Time source, according to 8.2.4.9 of IEC 61588:2009.	M
configuration, description and extension					
d	VISIBLE_STRING255	DC		inherited from: BasePrimitiveCDC	O
dU	UNICODE_STRING255	DC		inherited from: BasePrimitiveCDC	O
cdcNs	VISIBLE_STRING255	EX		inherited from: BasePrimitiveCDC	MOcdcNs
cdcName	VISIBLE_STRING255	EX		inherited from: BasePrimitiveCDC	MOcdcNs
dataNs	VISIBLE_STRING255	EX		inherited from: BasePrimitiveCDC	MOdataNs

19.4.7.2.3 Clock port status (CPS)

This common data class is used to model clock port status according to IEC 61588 and IEEE C37.238.

Table 64 defines the common data class "clock port status".

Table 64 – Clock port status common data class definition

CPS					
Data attribute name	**Type**	**FC**	**TrgOp**	**(Value/Value range) Description**	**M/O/C**
status					
stVal	INT8U	ST	dchg	State, according to 8.2.5.3.1 of	M

CPS					
Data attribute name	**Type**	**FC**	**TrgOp**	**(Value/Value range) Description**	**M/O/C**
				IEC 61588:2009.	
peerId	OCTET_STRING64	ST	dchg	EUI-64 identity of the peer port.	O
peerMpd	INT64	ST	dchg	Mean path delay, according to 8.2.5.3.3 of IEC 61588:2009.	M
id	OCTET_STRING64	ST	dchg	Clock port identifier, according to 8.2.5.2.1 of IEC 61588:2009.	M
num	INT16U	ST	dchg	Clock port number, according to 8.2.5.2.1 of IEC 61588:2009.	M
revNum	INT8U	ST	dchg	Revision number, according to 8.2.5.4.6 of IEC 61588:2009.	M
setting					
logAnnIntvl	INT8	SP	dchg	Log announce interval setting, according to 8.2.5.4.1 of IEC 61588:2009.	M
annRcvTimeout	INT8U	SP	dchg	Announce receive timeout setting, according to 8.2.5.4.2 of IEC 61588:2009.	M
logSynchIntvl	INT8	SP	dchg	Log synchronised interval setting, according to 8.2.5.4.3 of IEC 61588:2009.	M
dlMechanism	INT8	SP	dchg	Delay mechanism setting, according to 8.2.5.4.4 of IEC 61588:2009.	M
logMpdReqIntvl	INT8	SP	dchg	Log minimum path delay request interval setting, according to 8.2.5.4.5 of IEC 61588:2009.	M
ena	BOOLEAN	SP	dchg	If true, enabled setting, according to C37.238.	M
dlAsym	INT64	SP	dchg	Delay asymmetry setting, according to C37.238.	M
profileId	INT8U	SP	dchg	Profile identifier, according to C37.238.	M
vlan	INT16U	SP	dchg	IEEE 802.1Q VLAN identifier to use for outgoing PTP messages, according to C37.238. If both 'vlan'=0 and 'prio'=0, PTP messages are not tagged.	O
prio	INT8U	SP	dchg	IEEE 802.1Q priority to use for outgoing PTP messages, according to C37.238. If both 'vlan'=0 and 'prio'=0, PTP messages are not tagged.	O
configuration, description and extension					
d	VISIBLE_STRING255	DC		inherited from: BasePrimitiveCDC	O
dU	UNICODE_STRING255	DC		inherited from: BasePrimitiveCDC	O
cdcNs	VISIBLE_STRING255	EX		inherited from: BasePrimitiveCDC	MOcdcNs
cdcName	VISIBLE_STRING255	EX		inherited from: BasePrimitiveCDC	MOcdcNs
dataNs	VISIBLE_STRING255	EX		inherited from: BasePrimitiveCDC	MOdataNs

19.4.7.3 Common data class specifications for status settings

19.4.7.3.1 General

This subclause is a placeholder until the object model is moved to IEC 61850-7-3.

Figure 87 shows class diagram CDCStatusSet.

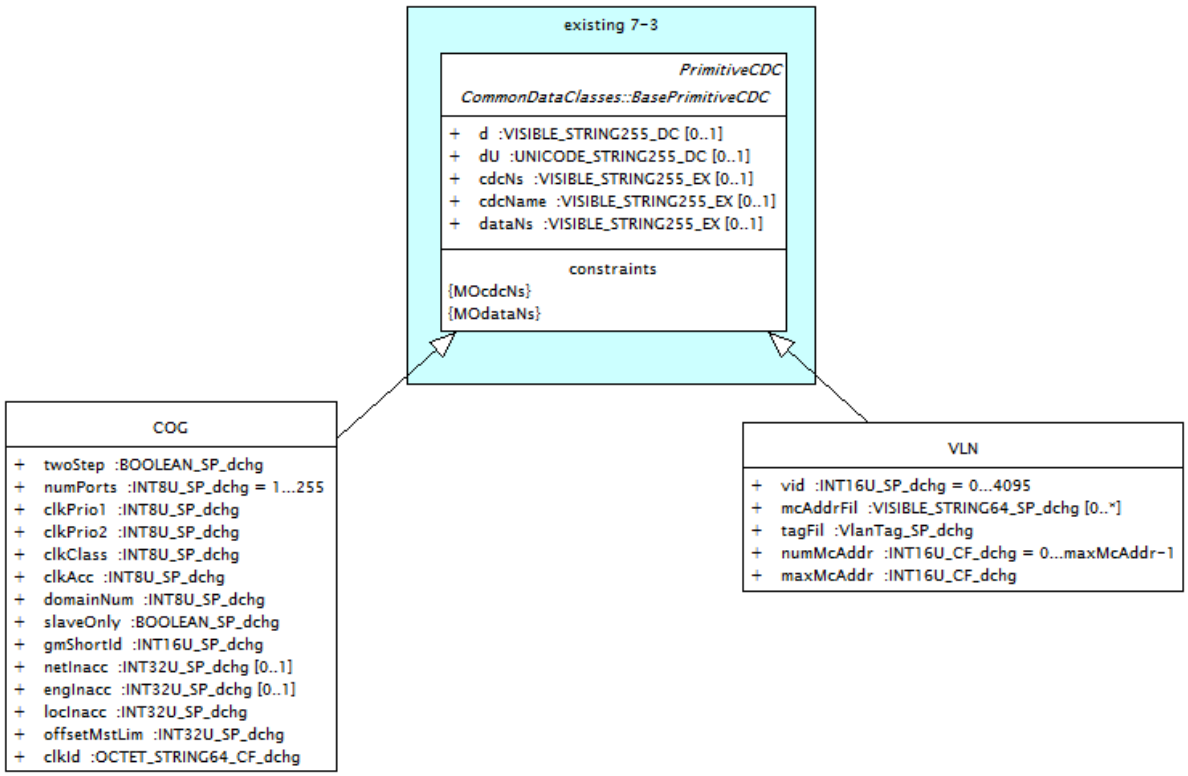


Figure 87 – Class diagram CDCStatusSet::CDCStatusSet

(no doc)

19.4.7.3.2 Clock ordinary settings (COG)

This common data class is used to model ordinary clock configuration according to IEC 61588 and IEEE C37.238. It reflects the defaultDS in IEC 61588.

Table 65 defines the common data class "clock ordinary settings".

Table 65 – Clock ordinary settings common data class definition

COG					
Data attribute name	**Type**	**FC**	**TrgOp**	**(Value/Value range) Description**	**M/O/C**
setting					
twoStep	BOOLEAN	SP	dchg	If true, clock is two-step, according to 8.2.1.2.1 of IEC 61588:2009.	M
numPorts	INT8U	SP	dchg	(range=[1...255]) Number of clock ports on this device, according to 8.2.1.2.3 of IEC 61588:2009, with the exception that the number may be more than 1.	M
clkPrio1	INT8U	SP	dchg	Clock priority1, according to 8.2.1.4.1	M

COG					
Data attribute name	**Type**	**FC**	**TrgOp**	**(Value/Value range) Description**	**M/O/C**
				of IEC 61588:2009.	
clkPrio2	INT8U	SP	dchg	Clock priority2, according to 8.2.1.4.1 of IEC 61588:2009.	M
clkClass	INT8U	SP	dchg	Clock class, according to 8.2.1.3.1.1 of IEC 61588:2009.	M
clkAcc	INT8U	SP	dchg	Clock time accuracy class, according to 8.2.1.3.1.2 of IEC 61588:2009.	M
domainNum	INT8U	SP	dchg	Time domain, according to 8.2.1.4.3 of IEC 61588:2009.	M
slaveOnly	BOOLEAN	SP	dchg	If true, clock cannot become master, according to 8.2.1.4.4 of IEC 61588:2009.	M
gmShortId	INT16U	SP	dchg	Grandmaster short identifier, according to IEEE C37.238.	M
netInacc	INT32U	SP	dchg	Grandmaster network time inaccuracy [ns], according to IEEE C37.238.	O
engInacc	INT32U	SP	dchg	Engineered network time inaccuracy [ns], according to IEEE C37.238.	O
locInacc	INT32U	SP	dchg	Local contribution to network time inaccuracy [ns], according to IEEE C37.238.	M
offsetMstLim	INT32U	SP	dchg	Offset from master limit [ns].	M
configuration, description and extension					
clkId	OCTET_STRING64	CF	dchg	EUI-64 clock identity, in binary format.	M
d	VISIBLE_STRING255	DC		inherited from: BasePrimitiveCDC	O
dU	UNICODE_STRING255	DC		inherited from: BasePrimitiveCDC	O
cdcNs	VISIBLE_STRING255	EX		inherited from: BasePrimitiveCDC	MOcdcNs
cdcName	VISIBLE_STRING255	EX		inherited from: BasePrimitiveCDC	MOcdcNs
dataNs	VISIBLE_STRING255	EX		inherited from: BasePrimitiveCDC	MOdataNs

19.4.7.3.3 VLAN filters (VLN)

This common data class is used to model a collection of multicast addresses associated with a VLAN, including filter for tagging and priority. According to IEEE 802.1Q, a multicast filter belongs to a VLAN even if no VLANs are used (a default channel VLAN ID may be used in this case).

Table 66 defines the common data class "vlan filters".

Table 66 – VLAN filters common data class definition

VLN					
Data attribute name	**Type**	**FC**	**TrgOp**	**(Value/Value range) Description**	**M/O/C**
setting					
vid	INT16U	SP	dchg	(range=[0...4095]) Identifier of the VLAN.	M
mcAddrFil	ARRAY of [0...maxMcAddr-1] of VISIBLE_STRING64	SP	dchg	Array of multicast addresses bound to the VLAN.	O
tagFil	ENUMERATED (VlanTagKind)	SP	dchg	VLAN tagging filter.	M
configuration, description and extension					
numMcAddr	INT16U	CF	dchg	(range=[0...maxMcAddr-1]) Actual size of 'mcAddrFil[]'.	M
maxMcAddr	INT16U	CF	dchg	Maximum supported size for 'mcAddrFil[]'.	M
d	VISIBLE_STRING255	DC		inherited from: BasePrimitiveCDC	O
dU	UNICODE_STRING255	DC		inherited from: BasePrimitiveCDC	O
cdcNs	VISIBLE_STRING255	EX		inherited from: BasePrimitiveCDC	MOcdcNs
cdcName	VISIBLE_STRING255	EX		inherited from: BasePrimitiveCDC	MOcdcNs
dataNs	VISIBLE_STRING255	EX		inherited from: BasePrimitiveCDC	MOdataNs

19.4.8 Enumerated types

19.4.8.1 General

This subclause is a placeholder until the object model is moved to IEC 61850-7-3.

19.4.8.2 VLAN tagging (VlanTagKind enumeration)

Status for VLAN tagging.

Table 67 shows all literals of VlanTagKind.

Table 67 – Literals of DAEnums_90_4::VlanTagKind

VlanTagKind		
literal	**value**	**description**
tagged	0	The port forwards with VLAN tag.
untagged	1	The port removes the VLAN tag and forwards.
forbidden	2	The port does not forward frames with that VLAN ID.

19.4.9 SCL enumerations

This subclause is a placeholder until the object model is moved to IEC 61850-7-3.

```
<EnumType id="VlanTagKind">
   <EnumVal ord="0">tagged</EnumVal>
   <EnumVal ord="1">untagged</EnumVal>
   <EnumVal ord="2">forbidden</EnumVal>
</EnumType>
```

19.5 Mapping of bridge objects to SNMP

19.5.1 Mapping of LLN0 and LPHD attributes to SNMP

Table 68 suggests a mapping from SNMP RFC1213-MIB parameters to the Data Objects of the LLN0 and LPHD.

Table 68 – Mapping of LLN0 and LPHD attributes to SNMP

IEC 61850 Data Attributes	SNMP OID	SNMP Access (read / write)
LLN0.NamPlt.vendor	Vendor specific: Static vendor name.	read
LLN0.NamPlt.swRev	Vendor specific: Bridge software version (firmware & operating system).	read
LLN0.NamPlt.d	1.3.6.1.2.1.1.5: (sysName).	read/write
LPHD.PhyNam.vendor	1.3.6.1.2.1.1.2 (derived): (sysObjectID).	read
LPHD.PhyNam.serNum	Vendor specific: Bridge serial number given by the manufacturer	read
LPHD.PhyNam.model	1.3.6.1.2.1.1.1: (sysDescr).	read
LPHD.PhyNam.location	1.3.6.1.2.1.1.6: (sysLocation).	read/write
LPHD.PhyHealth.stVal	Vendor specific: Bridge status information. Attribute type stVal is Enum (INT8 at MMS level), so a most basic representation is e.g. 1 = good, 2 =warning (redundancy loss), 3 = alarm.	read
LPHD.PwrSupAlm.stVal	Vendor specific: Bridge power supply status information FALSE (0) = all (redundant) power supplies are in good health, TRUE (1) = one of the power supplies is in bad health.	read
LPHD.TmpAlm.stVal	Vendor specific: Bridge Temperature information. Alert if the device temperature is outside the temperature band that the manufacturer defines as safe. The attribute type of stVal is Boolean: FALSE(0) = temperature within safe bounds, TRUE (1) = temperature outside safe bounds	read
NOTE 1 Only the most important mandatory and optional data attributes are mapped here. NOTE 2 When a simple attribute cannot be mapped from SNMP to IEC 61850, a description for the vendor specific data attribute is given. NOTE 3 A “data change” needs to be communicated as a triggered event from the SNMP stack towards the IEC 61850 stack, either by SNMP trap towards the gateway or internally towards the integrated IEC 61850 stack, depending on the use case.		

19.5.2 Mapping of LBRI attributes to SNMP for bridges

Table 69 suggests a mapping from SNMP BRIDGE-MIB parameters to the Data Objects of LBRI.

Table 69 – Mapping of LBRI and LBSP attributes to SNMP for bridges

MMS Data Attributes	SNMP OID	SNMP Access
LBRI.MacAddr.stVal	1.3.6.1.2.1.17.1.1 designated root bridge MAC address	read
LBRI.RstpRoot.stVal	1.3.6.1.2.1.17.2.5 (derived value) designated root bridge. The data attribute stVal is Boolean: TRUE = the Root Bridge MAC equals the Management MAC address of the bridge. FALSE = otherwise	read
LBRI.RstpPrio.stVal	1.3.6.1.2.1.17.2.2 root bridge priority according to IEEE 802.1D	read/write
LBRI.RstpTopoCnt.stVal	1.3.6.1.2.1.17.2.4 Topology change counter	read
LBRI.RstpTopoCnt.t	Vendor specific (see remarks)[7]	read
LBSP.RstpSt.stVal	1.3.6.1.2.1.17.2.15.1.3.x (x=port number) Bridgeport (R)STP state	read

19.5.3 Mapping of LPCP attributes to SNMP for bridges

Table 70 suggests a mapping from SNMP MIB parameters to the Data Objects of LPCP.

Table 70 – Mapping of LPCP attributes to SNMP for bridges

MMS Data Attributes	SNMP OID	SNMP Access
LPCP.FerCh.stVal	1.3.6.1.2.1.2.2.1.20.x(x=port number) Frame error rate (packet error count converted into frame error rate)	read
LPCP.Mau.stVal	1.3.6.1.2.1.26.2.1.1.3.x.1 (x=port number) Bridgeport Duplex value	read
LPCP.RxCnt.actVal	1.3.6.1.2.1.2.2.1.11.x (x=port number) and 1.3.6.1.2.1.2.2.1.12.x (derived value)	read
LPCP.TxCnt.actVal	1.3.6.1.2.1.2.2.1.17.x (x=port number) and 1.3.6.1.2.1.2.2.1.18.x	read
LPCP.AdminCfg.stVal	1.3.6.1.2.1.2.2.1.7.x (x=port number)	read/write

19.5.4 Mapping of LPLD attributes to SNMP for bridges

Table 71 suggests a mapping from SNMP LLDP-MIB parameters to the Data Objects of LPLD.

---

7 In addition to Bridgeport topology change counter and timestamp (LBRI.TopoChgCnt.stVal and LBRI.TopoChgCnt.t: The OID 1.3.6.1.2.1.17.2.3 provides TimeTicks (in hundredths of a second) since the last topology change event. To provide a UTC timestamp, when this DA is accessed, the bridge local time needs to be subtracted by the time span provided via TimeTicks under this OID. The result is the timestamp that is provided through DO LBRI.TopoChgCnt.t.

Table 71 – Mapping of LPLD attributes to SNMP for bridges

MMS Data Attributes	SNMP OID	SNMP Access
LPLD.RemPortDesc.stVal	1.0.8802.1.1.2.1.4.1.1.8.x.y.z (x=lldpRemTimeMark; y=lldpRemLocalPortNum; z=lldpRemIndex) – see LLDP-MIB::lldpRemTable for details	read
LPLD.RemPortIdTyp.stVal	1.0.8802.1.1.2.1.4.1.1.6.x.y.z (x=lldpRemTimeMark; y=lldpRemLocalPortNum; z=lldpRemIndex) – see LLDP-MIB::lldpRemTable for details	read
LPLD.RemPortId.stVal	1.0.8802.1.1.2.1.4.1.1.7.x.y.z (x=lldpRemTimeMark; y=lldpRemLocalPortNum; z=lldpRemIndex) – see LLDP-MIB::lldpRemTable for details	read
LPLD.RemChsIdTyp.stVal	1.0.8802.1.1.2.1.4.1.1.4.x.y.z (x=lldpRemTimeMark; y=lldpRemLocalPortNum; z=lldpRemIndex) – see LLDP-MIB::lldpRemTable for details	read
LPLD.RemChsId.stVal	1.0.8802.1.1.2.1.4.1.1.5.x.y.z (x=lldpRemTimeMark; y=lldpRemLocalPortNum; z=lldpRemIndex) – see LLDP-MIB::lldpRemTable for details	read
LPLD.RemSysDesc.stVal	1.0.8802.1.1.2.1.4.1.1.9.x.y.z (x=lldpRemTimeMark; y=lldpRemLocalPortNum; z=lldpRemIndex) – see LLDP-MIB::lldpRemTable for details	read
LPLD.RemAddrTyp.stVal	1.0.8802.1.1.2.1.4.2.1.1.v.w.x.y.z (v=lldpRemTimeMark; w=lldpRemLocalPortNum; x=lldpRemIndex; y=lldpRemManAddrSubtype; z=lldpRemManAddr) – see LLDP-MIB::lldpRemManAddrTable for details	read
LPLD.RemAddr.stVal	1.0.8802.1.1.2.1.4.2.1.2.v.w.x.y.z (v=lldpRemTimeMark; w=lldpRemLocalPortNum; x=lldpRemIndex; y=lldpRemManAddrSubtype; z=lldpRemManAddr) – see LLDP-MIB::lldpRemManAddrTable for details	read

NOTE Concerning the data attributes that map to LLDP variables: LLDP Remote Systems Data and LLDP Remote Management Address are both tables that contain data received from adjacent nodes. There are as many entries in the table as there are ports in the device. The data mapped from this table into each particular LPLD needs to be aligned with the PortNum of its referenced LPCP i.e. PortNum of the LPCP needs to be the same as the lldpRemLocalPortNum.

19.5.5 Mapping of HSR/PRP link redundancy entity to SNMP

HSR and PRP nodes have two ports and implement a reduced bridge functionality.

While a bridge is usually a self-sufficient device with its own housing, power supply, etc. (though embedded variants exist), HSR/PRP LREs are usually less complex interfaces that are integrated into other devices and their respective management interfaces.

This is reflected in the SNMP MIB specification of HSR/PRP LRE interfaces that is described in IEC 62439-3:2012. The structure of this MIB roughly resembles that of the IETF IF-MIB: Each HSR/PRP LRE in a device is added to the network interface list.

The HSR/PRP ports are mapped according to Table 72.

Table 72 – Mapping of LCCH attributes for SNMP for HSR/PRP LREs

MMS Data Attributes	SNMP OID	SNMP Access (read / write)
LCCH.ChLiv.stVal	1.0.62439.2.1.0.1.0.1.1.10.x (x = LRE number / redundantInterfaceIndex)	read
LCCH.RedChLiv.stVal	1.0.62439.2.1.0.1.0.1.1.11.x (x = LRE number / redundantInterfaceIndex)	read
LCCH.FerCh.stVal	1.0.62439.2.1.1.1.0.1.1.8.x (x = LRE number / redundantInterfaceIndex)	read
LCCH.RedFerCh	1.0.62439.2.1.1.1.0.1.1.9.x (x = LRE number / redundantInterfaceIndex)	read
LCCH.RxCnt.actVal	1.0.62439.2.1.1.1.0.1.1.6.x (x = LRE number / redundantInterfaceIndex)	read
LCCH.RedRxCnt.actVal	1.0.62439.2.1.1.1.0.1.1.7.x (x = LRE number / redundantInterfaceIndex)	read
LCCH.TxCnt.actVal	1.0.62439.2.1.1.1.0.1.1.2.x (x = LRE number / redundantInterfaceIndex)	read
LCCH.RedCfg.stVal	1.0.62439.2.1.0.1.0.1.1.3.x (x = LRE number / redundantInterfaceIndex)	read/write

NOTE The OID of IEC 62439-3 is currently 1.0.62439.2.

19.6 Mapping of clock objects to the C37.238 SNMP MIB

Table 73 shows the correspondence between the clock objects in the IEC 61850 Logical Nodes, in the IEC 61588 datasets and in the IEEE C37.238 MIB.

Table 73 – Mapping of clock objects in IEC 61850, IEC 61588 and IEEE C37.238

Name in IEC 61850	Clause IEC 61588 or C37.238	Name in IEC 61588	Name in IEEE C37.238 MIB
LN LTPC (OCG)	**8.2.1.2**	**defaultDS**	**ieeeC37238defaultDS**
-	8.2.1.2.1	.twoStepFlag	TwoStepFlag
OrdClkCfg.clkId	8.2.1.2.2	.clockIdentity	ClkIdentity
OrdClkCfg.numPorts	8.2.1.2.3	.numberPorts	NumberPorts
OrdClkCfg.clkClass	8.2.1.3.1.1	.clockQuality.clockClass	ClkClass
OrdClkCfg.clkAcc	8.2.1.3.1.2	.clockQuality.clockAccuracy	ClkAccuracy
	8.2.1.3.1.3	.offsetScaledLogVariance	OfsScdLogVar
OrdClkCfg.clkPrio1	8.2.1.4.1	.priority1	Priority1
OrdClkCfg.clkPrio2	8.2.1.4.2	.priority2	Priority2
OrdClkCfg.domainNum	8.2.1.4.3	.domainNumber	DomainNumber
OrdClkCfg.slaveOnly	8.2.1.4.4	.slaveOnly	SlaveOnly
OrdClkCfg.gmShortId	C:5.9.6	-	GMIdentity
OrdClkCfg.netInacc	C:5.12.2	-	NetTimeInacc
OrdClkCfg.engInacc	C:5.12.2	-	EngTimeInacc
OrdClkCfg.locInacc	C:5.13	-	LocTimeInacc
OrdClkCfg.offsetMstLim	C: 5.5.1	-	OfstFrMLimit
	8.2.2	**currentDS**	**ieeeC37238currentDS**
GmClkSt.numPath	8.2.2.2	.stepsRemoved	StepsRemoved
GmClkSt.mstOffset	8.2.2.3	.offsetFromMaster	OfstFrMaster

Name in IEC 61850	Clause IEC 61588 or C37.238	Name in IEC 61588	Name in IEEE C37.238 MIB
GmClkSt.meanPathDl	8.2.2.4	.meanPathDelay	-
	C: 5.13	-	LocTimeInacc
LN LTPG	**8.2.3**	**parentDS**	**ieeeC37238parentDS**
GmClkSt.parentClkId	8.2.3.2	.parentPortIdentity.clockIdentity	ClkIdentity
	8.2.3.2	.parentPortIdentity.portNumber	PortNumber
	8.2.3.3	.parentStats	Stats
	8.2.3.4	.observedParentOffsetScaledLogVariance	ObsOfstScdLVar
	8.2.3.5	.observedParentClockPhaseChangeRate	ObsPhChgRate
GmClkSt.gmClkId	8.2.3.6	.grandmasterIdentity	GMClkIdentity
GmClkSt.gmClkClass	8.2.3.7	.grandmasterClockQuality .clockClass	GMClkClass
GmClkSt.gmClkAcc	8.2.3.7	.grandmasterClockQuality .clockAccuracy	GMClkAccuracy
	8.2.3.7	.grandmasterClockQuality .offsetScaledLogVariance	GMOfstScdLVar
GmClkSt.gmClkPrio1	8.2.3.8	.grandmasterPriority1	GMPriority1
GmClkSt.gmClkPrio2	8.2.3.9	.grandmasterPriority2	GMPriority2
GmClkSt.gmShortId	C: 5.9.6	-	GMIdentity
GmClkSt.gmInacc	C: 5.12.2	-	GMTimeInacc
GmClkSt.netInacc	C: 5.12.2	-	NetTimeInacc
LN LTIM	**8.2.4**	**timePropertiesDS**	**ieeeC37238timePropDS**
CurUtcOfsTms	8.2.4.2	.currentUtcOffset	CurUTCOfst
CurUtcOfsVld	8.2.4.3	.currentUtcOffsetValid	CurUTCOfstVd
Leap	8.2.4.4	.leap59	Leap59
Leap	8.2.4.5	.leap61	Leap61
RefTmTrk	8.2.4.6	.timeTraceable	TmeTraceable
RefFqTrk	8.2.4.7	.frequencyTraceable	FrqTraceable
	8.2.4.8	.ptpTimeScale	PTPTimescale
AltnOfsTms	16.3.3.4	TLV currentOffset	LocalTCurOfs
JmpTms	16.3.3.5	TLV jumpSeconds	LocalTJumpS
NxtJmpTms	16.3.3.6	TLV timeOfNextJump	LocalTNtJump
AltnTmNam	16.3.3.7	TLV displayName	LocalTName
			LeapEvLatest
			UTCOfstNext
			LeapEvExpiry
LN LTMS	**8.2.4**	**timePropertiesDS**	**ieeeC37238PortDS**
TmSrcId	8.2.4.9	.timeSource	TimeSource
LN LTPP	**8.2.5**	**portDS**	**ieeeC37238PortDS**
ClkPort.id	8.2.5.2.1	.portIdentity.clockIdentity	ClkIdentity
ClkPort.num	8.2.5.2.1	.portIdentity.portNumber	PortNumber
	8.2.5.3.1	.portState	PortState
	8.2.5.3.2	.logMinDelayReqInterval	unused
ClkPort.peerMpd	8.2.5.3.3	.peerMeanPathDelay	MPathDly
ClkPort.logAnnIntvl	8.2.5.4.1	.logAnnounceInterval	LogAnnounceInt

Name in IEC 61850	Clause IEC 61588 or C37.238	Name in IEC 61588	Name in IEEE C37.238 MIB
ClkPort.annRcvTimeout	8.2.5.4.2	.announceReceiptTimeout	AnnounceRctTout
ClkPort.logSyncIntvl	8.2.5.4.3	.logSyncInterval	LogSyncInt
ClkPort.dlMechanism	8.2.5.4.4	.delayMech	DelayMech
ClkPort.logMpdReqIntvl	8.2.5.4.5	.logMinPdelayInterval	LogMinPdlyRInt
ClkPort.revNum	8.2.5.4.6	.versionNumer	VersionNumber
ClkPort.ena			PortEnabled
ClkPort.dlAsym			DlyAsymmetry
ClkPort.profileId			ProfileId
			NetProtocol
ClkPort.vlan		-	VlanId
ClkPort.prio		-	Priority
ClkPort.peerId		-	
N.A.	**8.3.2**	**transparentClockDefaultDS**	**ieeeC37238TCDefaultDS**
	8.3.2.2.1	clockIdentity	ClkIdentity
	8.3.2.2.2	numberPorts	NumberPorts
	8.3.2.3.1	delayMech	DelayMech
	8.3.2.3.2	primaryDomain	PriDomain
			Syntonize
	C: 5.9.6	-	CurGMaster
	8.2.1.2.1		TwoStepFlag
		GMIdentity	GMIdentity
		NetProtocol	NetProtocol
		VlanId	VlanId
		Priority	Priority
			GMTimeInacc
			NetTimeInacc
			LocTimeInacc
		transparentClockPortDS	**ieeeC37238TCPortDS**
	8.3.3.2.1	.portIdentity.clockIdentity	PortNumber
	8.3.3.3.1	.logMinPdelayReqInterval	LMinPdlyRInt
	8.3.3.3.2	.faulty	Faulty
	8.3.3.3.3	.peerMeanPathDelay	MeanPDly
			DlyAsymm
			ieeeC37238Events
			ChangeOfMaster
			MasterStepChange
			FaultyState
			PortStateChange
			OfstExceedsLimit
			OtherProfileDetect
			LeapSecAnnounced
			PTPServiceStarted
			PTPServiceStopped

19.7 Machine-readable description of the bridge objects

19.7.1 Method and examples

The UML model and the corresponding Logical Node definition are translated in machine-readable form according to IEC 61850-6:2009.

Three ICD examples follow:

- definition of a bridge type with four ports;
- definition of a node with PTP support;
- definition of a RedBox with HSR.

19.7.2 Four-port bridge

The following code describes the ICD file for a four-port bridge as shown in Figure 88.

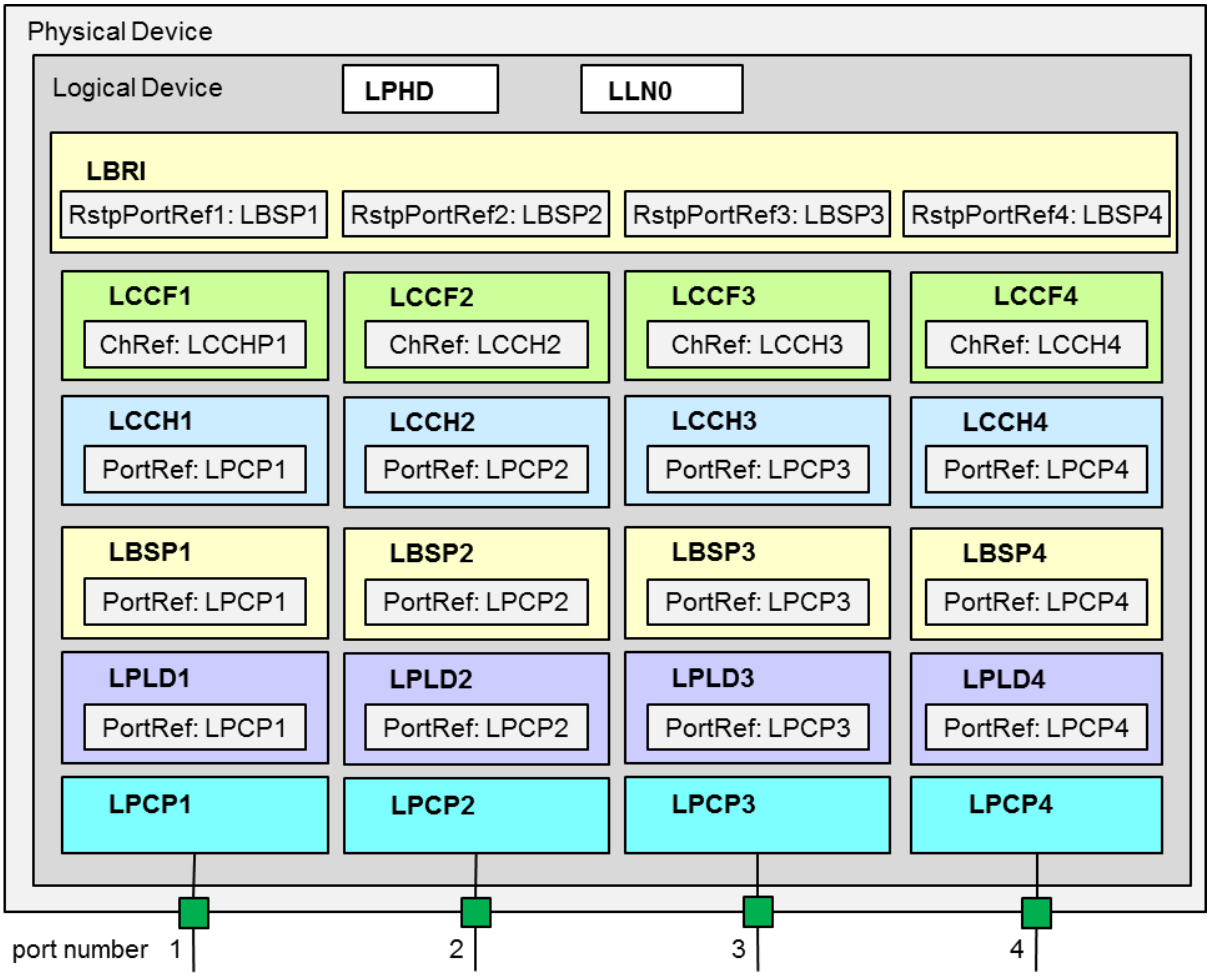


Figure 88 – Four-port bridge

The ICD file specifies a template for the four bridge nodes, consisting of:

- the template of the Logical Device with the four ports;
- the templates for the Logical Node types (e.g. “Switch_LBRI”);
- the templates for the Data Object types (e.g. “Switch_Health_E”);
- the template for the enumeration types (e.g. ChannelRedundancyKind).

```
<?xml version="1.0" encoding="UTF-8"?>
<SCL xmlns="http://www.iec.ch/61850/2003/SCL"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" version="2007" revision="B"
xsi:schemaLocation="http://www.iec.ch/61850/2003/SCL SCL.xsd">
   <Header id="ICD of a bridge with four ports and no PTP support">
      <History>
         <Hitem version="1" revision="A" when="2013.03.20" what="Initial version"
who="HK"/>
      </History>
   </Header>
   <IED name="TEMPLATE">
      <Services nameLength="64">
         <DynAssociation/>
      </Services>
      <AccessPoint name="S1">
         <Server>
            <Authentication/>
            <LDevice inst="LD0">
               <LN0 lnClass="LLN0" inst="" lnType="Switch_LLN0"/>
               <LN lnClass="LPHD" inst="1" lnType="Switch_LPHD"/>
               <LN lnClass="LBRI" inst="1" lnType="Switch_LBRI">
                  <DOI name="PortRef1">
                     <DAI name ="setSrcRef">
                        <Val>@LD0/LBSP1</Val>
                     </DAI>
                  </DOI>
                  <DOI name="PortRef2">
                     <DAI name ="setSrcRef">
                        <Val>@LD0/LBSP2</Val>
                     </DAI>
                  </DOI>
                  <DOI name="PortRef3">
                     <DAI name ="setSrcRef">
                        <Val>@LD0/LBSP3</Val>
                     </DAI>
                  </DOI>
                  <DOI name="PortRef4">
                     <DAI name ="setSrcRef">
                        <Val>@LD0/LBSP4</Val>
                     </DAI>
                  </DOI>
               </LN>
               <LN lnClass="LCCH" inst="1" lnType="Switch_NoRedChannel_LCCH">
                  <DOI name="PortRef">
                     <DAI name ="setSrcRef">
                        <Val>@LD0/LPCP1</Val>
                     </DAI>
                  </DOI>
               </LN>
               <LN lnClass="LCCH" inst="2" lnType="Switch_NoRedChannel_LCCH">
                  <DOI name="PortRef">
                     <DAI name ="setSrcRef">
                        <Val>@LD0/LPCP2</Val>
                     </DAI>
                  </DOI>
               </LN>
                <LN lnClass="LCCH" inst="3" lnType="Switch_NoRedChannel_LCCH">
                  <DOI name="PortRef">
                     <DAI name ="setSrcRef">
                        <Val>@LD0/LPCP3</Val>
                     </DAI>
                  </DOI>
```

```
</LN>
 <LN lnClass="LCCH" inst="4" lnType="Switch_NoRedChannel_LCCH">
    <DOI name="PortRef">
       <DAI name ="setSrcRef">
          <Val>@LD0/LPCP4</Val>
       </DAI>
    </DOI>
</LN>
<LN lnClass="LCCF" inst="1" lnType="Switch_LCCF">
    <DOI name="ChRef">
       <DAI name ="setSrcRef">
          <Val>@LD0/LCCH1</Val>
       </DAI>
    </DOI>
</LN>
<LN lnClass="LCCF" inst="2" lnType="Switch_LCCF">
    <DOI name="ChRef">
       <DAI name ="setSrcRef">
          <Val>@LD0/LCCH2</Val>
       </DAI>
    </DOI>
</LN>
<LN lnClass="LCCF" inst="3" lnType="Switch_LCCF">
    <DOI name="ChRef">
       <DAI name ="setSrcRef">
          <Val>@LD0/LCCH3</Val>
       </DAI>
    </DOI>
</LN>
<LN lnClass="LCCF" inst="4" lnType="Switch_LCCF">
    <DOI name="ChRef">
       <DAI name ="setSrcRef">
          <Val>@LD0/LCCH4</Val>
       </DAI>
    </DOI>
</LN>
<LN lnClass="LBSP" inst="1" lnType="Switch_LBSP">
    <DOI name="PortRef">
       <DAI name ="setSrcRef">
          <Val>@LD0/LPCP1</Val>
       </DAI>
    </DOI>
</LN>
<LN lnClass="LBSP" inst="2" lnType="Switch_LBSP">
    <DOI name="PortRef">
       <DAI name ="setSrcRef">
          <Val>@LD0/LPCP2</Val>
       </DAI>
    </DOI>
</LN>
<LN lnClass="LBSP" inst="3" lnType="Switch_LBSP">
    <DOI name="PortRef">
       <DAI name ="setSrcRef">
          <Val>@LD0/LPCP3</Val>
       </DAI>
    </DOI>
</LN>
<LN lnClass="LBSP" inst="4" lnType="Switch_LBSP">
    <DOI name="PortRef">
       <DAI name ="setSrcRef">
          <Val>@LD0/LPCP4</Val>
       </DAI>
    </DOI>
</LN>
```

```
            <LN lnClass="LPLD" inst="1" lnType="Switch_LPLD">
               <DOI name="PortRef">
                  <DAI name ="setSrcRef">
                     <Val>@LD0/LPCP1</Val>
                  </DAI>
               </DOI>
            </LN>
            <LN lnClass="LPLD" inst="2" lnType="Switch_LPLD">
               <DOI name="PortRef">
                  <DAI name ="setSrcRef">
                     <Val>@LD0/LPCP2</Val>
                  </DAI>
               </DOI>
            </LN>
            <LN lnClass="LPLD" inst="3" lnType="Switch_LPLD">
               <DOI name="PortRef">
                  <DAI name ="setSrcRef">
                     <Val>@LD0/LPCP3</Val>
                  </DAI>
               </DOI>
            </LN>
            <LN lnClass="LPLD" inst="4" lnType="Switch_LPLD">
               <DOI name="PortRef">
                  <DAI name ="setSrcRef">
                     <Val>@LD0/LPCP4</Val>
                  </DAI>
               </DOI>
            </LN>
            <LN lnClass="LPCP" inst="1" lnType="Switch_LPCP">
               <DOI name="PortNum">
                  <DAI name="setVal">
                     <Val>1</Val>
                     </DAI>
               </DOI>
            </LN>
            <LN lnClass="LPCP" inst="2" lnType="Switch_LPCP">
               <DOI name="PortNum">
                  <DAI name="setVal">
                     <Val>2</Val>
                     </DAI>
               </DOI>
            </LN>
            <LN lnClass="LPCP" inst="3" lnType="Switch_LPCP">
               <DOI name="PortNum">
                  <DAI name="setVal">
                     <Val>3</Val>
                  </DAI>
               </DOI>
            </LN>
            <LN lnClass="LPCP" inst="4" lnType="Switch_LPCP">
               <DOI name="PortNum">
                  <DAI name="setVal">
                     <Val>4</Val>
                  </DAI>
               </DOI>
            </LN>
         </LDevice>
      </Server>
   </AccessPoint>
</IED>
<DataTypeTemplates>
   <LNodeType id="Switch_LLN0" lnClass="LLN0">
      <DO name="NamPlt" type="Switch_LPL_LLN0"/>
      <DO name="Beh" type="Switch_Beh_ENS"/>
```

```
        <DO name="Health" type="Switch_Health_ENS"/>
        <DO name="Mod" type="Switch_Mod_ENC"/>
    </LNodeType>
    <LNodeType id="Switch_LPHD" lnClass="LPHD">
        <DO name="PhyNam" type="Switch_DPL"/>
        <DO name="PhyHealth" type="Switch_Health_ENS"/>
        <DO name="Proxy" type="Switch_SPS"/>
        <DO name="LocChsIdTyp" type="Switch_INS_90-4_DS"/>
        <DO name="LocChsId" type="Switch_VSS_90-4_DS"/>
        <DO name="LocAddrTyp" type="Switch_INS_90-4_DS"/>
        <DO name="LocAddr" type="Switch_VSS_90-4_DS"/>
        <DO name="LdpEna" type="Switch_SPG_90-4_DS"/>
    </LNodeType>
    <LNodeType id="Switch_LBRI" lnClass="LBRI">
        <DO name="NamPlt" type="Switch_LPL_90-4"/>
        <DO name="RstpRoot" type="Switch_SPS_90-4"/>
        <DO name="Beh" type="Switch_Beh_ENS_90-4"/>
        <DO name="PortRef1" type="Switch_ORG_90-4"/>
        <DO name="PortRef2" type="Switch_ORG_90-4"/>
        <DO name="PortRef3" type="Switch_ORG_90-4"/>
        <DO name="PortRef4" type="Switch_ORG_90-4"/>
        <DO name="RstpPrio" type="Switch_LBRI_Default_ING_90-4"/>
        <DO name="RstpEna" type="Switch_LBRI_Default_SPG_90-4"/>
    </LNodeType>
    <LNodeType id="Switch_NoRedChannel_LCCH" lnClass="LCCH">
        <DO name="ChLiv" type="Switch_SPS"/>
        <DO name="Beh" type="Switch_Beh_ENS"/>
        <DO name="PortRef" type="Switch_ORG_90-4_DS"/>
        <DO name="RedCfg" type="Switch_RedCfg_None_ENG_90-4_DS"/>
    </LNodeType>
    <LNodeType id="Switch_LCCF" lnClass="LCCF">
        <DO name="NamPlt" type="Switch_LPL_90-4"/>
        <DO name="Beh" type="Switch_Beh_ENS_90-4"/>
        <DO name="ChRef" type="Switch_ORG_90-4"/>
        <DO name="DftPortVid" type="Switch_LCCF_DefaultVid_ING_90-4"/>
        <DO name="DftPortPrio" type="Switch_LCCF_DefaultPrio_ING_90-4"/>
        <DO name="VlanFil1" type="Switch_VLN"/>
    </LNodeType>
    <LNodeType id="Switch_LBSP" lnClass="LBSP">
        <DO name="NamPlt" type="Switch_LPL_90-4"/>
        <DO name="Beh" type="Switch_Beh_ENS_90-4"/>
        <DO name="RstpTrunk" type="Switch_SPG_90-4"/>
        <DO name="PortRef" type="Switch_ORG_90-4"/>
    </LNodeType>
    <LNodeType id="Switch_LPLD" lnClass="LPLD">
        <DO name="NamPlt" type="Switch_LPL_90-4"/>
        <DO name="RemPortDesc" type="Switch_VSS_90-4"/>
        <DO name="LocPortDesc" type="Switch_VSS_90-4"/>
        <DO name="RemPortIdTyp" type="Switch_INS_90-4"/>
        <DO name="LocPortIdTyp" type="Switch_INS_90-4"/>
         <DO name="RemPortId" type="Switch_VSS_90-4"/>
        <DO name="LocPortId" type="Switch_VSS_90-4"/>
        <DO name="RemChsIdTyp" type="Switch_INS_90-4"/>
        <DO name="RemChsId" type="Switch_VSS_90-4"/>
        <DO name="RemSysDesc" type="Switch_VSS_90-4"/>
        <DO name="RemAddrTyp" type="Switch_INS_90-4"/>
        <DO name="RemAddr" type="Switch_VSS_90-4"/>
        <DO name="Beh" type="Switch_Beh_ENS_90-4"/>
        <DO name="PortRef" type="Switch_ORG_90-4"/>
    </LNodeType>
    <LNodeType id="Switch_LPCP" lnClass="LPCP">
        <DO name="NamPlt" type="Switch_LPL_90-4"/>
        <DO name="PhyNam" type="Switch_DPL_90-4"/>
        <DO name="PhyHealth" type="Switch_Health_ENS_90-4"/>
```

```
    <DO name="AutoNgt" type="Switch_SPS_90-4"/>
    <DO name="Mau" type="Switch_INS_90-4"/>
    <DO name="PortNum" type="Switch_ING_90-4"/>
    <DO name="AutoNgtCfg" type="Switch_SPG_90-4"/>
    <DO name="MauCfg" type="Switch_MauCfg_ING_100MFD_90-4"/>
    <DO name="MauCfgCap1" type="Switch_MauCfg_ING_100MHD_90-4"/>
    <DO name="MauCfgCap2" type="Switch_MauCfg_ING_100MFD_90-4"/>
    <DO name="AdminCfg" type="Switch_LPCP_AdminCfg_SPG_90-4"/>
</LNodeType>
<DOType id="Switch_LPL_LLN0" cdc="LPL">
    <DA name="vendor" bType="VisString255" fc="DC"/>
    <DA name="swRev" bType="VisString255" fc="DC"/>
    <DA name="configRev" bType="VisString255" fc="DC"/>
    <DA name="ldNs" bType="VisString255" fc="EX">
       <Val>IEC 61850-7-4:2007</Val>
    </DA>
</DOType>
<DOType id="Switch_LPL_90-4" cdc="LPL">
    <DA name="vendor" bType="VisString255" fc="DC"/>
    <DA name="swRev" bType="VisString255" fc="DC"/>
    <DA name="configRev" bType="VisString255" fc="DC"/>
    <DA name="lnNs" bType="VisString255" fc="EX">
       <Val>(Tr)IEC 61850-90-4:2012</Val>
    </DA>
    <DA name="cdcNs" bType="VisString255" fc="EX">
       <Val>IEC 61850-7-4:2007</Val>
    </DA>
    <DA name="cdcName" bType="VisString255" fc="EX">
       <Val>LPL</Val>
    </DA>
</DOType>
<DOType id="Switch_Beh_ENS" cdc="ENS">
    <DA name="stVal" bType="Enum" type="BehaviourModeKind" fc="ST" dchg="true"/>
    <DA name="q" bType="Quality" fc="ST" qchg="true"/>
    <DA name="t" bType="Timestamp" fc="ST"/>
</DOType>
<DOType id="Switch_Beh_ENS_90-4" cdc="ENS">
    <DA name="stVal" bType="Enum" type="BehaviourModeKind" fc="ST" dchg="true"/>
    <DA name="q" bType="Quality" fc="ST" qchg="true"/>
    <DA name="t" bType="Timestamp" fc="ST"/>
    <DA name="cdcNs" bType="VisString255" fc="EX">
       <Val>IEC 61850-7-4:2007</Val>
    </DA>
    <DA name="cdcName" bType="VisString255" fc="EX">
       <Val>ENS</Val>
    </DA>
</DOType>
<DOType id="Switch_Health_ENS" cdc="ENS">
    <DA name="stVal" bType="Enum" type="HealthKind" fc="ST" dchg="true"/>
    <DA name="q" bType="Quality" fc="ST" qchg="true"/>
    <DA name="t" bType="Timestamp" fc="ST"/>
</DOType>
<DOType id="Switch_Health_ENS_90-4" cdc="ENS">
    <DA name="stVal" bType="Enum" type="HealthKind" fc="ST" dchg="true"/>
    <DA name="q" bType="Quality" fc="ST" qchg="true"/>
    <DA name="t" bType="Timestamp" fc="ST"/>
    <DA name="cdcNs" bType="VisString255" fc="EX">
       <Val>IEC 61850-7-4:2007</Val>
    </DA>
    <DA name="cdcName" bType="VisString255" fc="EX">
       <Val>ENS</Val>
    </DA>
</DOType>
<DOType id="Switch_Mod_ENC" cdc="ENC">
```

```
            <DA name="stVal" bType="Enum" type="BehaviourModeKind" fc="ST" dchg="true"/>
            <DA name="q" bType="Quality" fc="ST" qchg="true"/>
            <DA name="t" bType="Timestamp" fc="ST"/>
            <DA name="ctlModel" bType="Enum" type="CtlModelKind" fc="CF" dchg="true"/>
        </DOType>
        <DOType id="Switch_DPL" cdc="DPL">
            <DA name="vendor" bType="VisString255" fc="DC"/>
        </DOType>
        <DOType id="Switch_DPL_90-4" cdc="DPL">
            <DA name="vendor" bType="VisString255" fc="DC"/>
            <DA name="cdcNs" bType="VisString255" fc="EX">
                <Val>IEC 61850-7-4:2007</Val>
            </DA>
            <DA name="cdcName" bType="VisString255" fc="EX">
                <Val>DPL</Val>
            </DA>
        </DOType>
        <DOType id="Switch_SPS" cdc="SPS">
            <DA name="stVal" bType="BOOLEAN" fc="ST" dchg="true"/>
            <DA name="q" bType="Quality" fc="ST" qchg="true"/>
            <DA name="t" bType="Timestamp" fc="ST"/>
        </DOType>
        <DOType id="Switch_SPS_90-4" cdc="SPS">
            <DA name="stVal" bType="BOOLEAN" fc="ST" dchg="true"/>
            <DA name="q" bType="Quality" fc="ST" qchg="true"/>
            <DA name="t" bType="Timestamp" fc="ST"/>
            <DA name="cdcNs" bType="VisString255" fc="EX">
                <Val>IEC 61850-7-4:2007</Val>
            </DA>
            <DA name="cdcName" bType="VisString255" fc="EX">
                <Val>SPS</Val>
            </DA>
        </DOType>
        <DOType id="Switch_ORG_90-4_DS" cdc="ORG">
            <DA name="setSrcRef" bType="ObjRef" fc="EX"/>
            <DA name="cdcNs" bType="VisString255" fc="EX">
                <Val>IEC 61850-7-4:2007</Val>
            </DA>
            <DA name="cdcName" bType="VisString255" fc="EX">
                <Val>ORG</Val>
            </DA>
            <DA name="dataNs" bType="VisString255" fc="EX">
                <Val>(Tr)IEC 61850-90-4:2012</Val>
            </DA>
        </DOType>
        <DOType id="Switch_ORG_90-4" cdc="ORG">
            <DA name="setSrcRef" bType="ObjRef" fc="EX"/>
            <DA name="cdcNs" bType="VisString255" fc="EX">
                <Val>IEC 61850-7-4:2007</Val>
            </DA>
            <DA name="cdcName" bType="VisString255" fc="EX">
                <Val>ORG</Val>
            </DA>
        </DOType>
        <DOType id="Switch_RedCfg_None_ENG_90-4_DS" cdc="ENG">
            <DA name="setVal" bType="Enum" type="ChannelRedundancyKind" fc="SP"
dchg="true">
                    <Val>1</Val>
            </DA>
            <DA name="cdcNs" bType="VisString255" fc="EX">
                <Val>IEC 61850-7-4:2007</Val>
            </DA>
            <DA name="cdcName" bType="VisString255" fc="EX">
                <Val>ENS</Val>
```

```
    </DA>
    <DA name="dataNs" bType="VisString255" fc="EX">
       <Val>(Tr)IEC 61850-90-4:2012</Val>
    </DA>
</DOType>
<DOType id="Switch_INS_90-4" cdc="INS">
    <DA name="stVal" bType="INT32" fc="ST" dchg="true"/>
    <DA name="q" bType="Quality" fc="ST" qchg="true"/>
    <DA name="t" bType="Timestamp" fc="ST"/>
    <DA name="cdcNs" bType="VisString255" fc="EX">
       <Val>IEC 61850-7-4:2007</Val>
    </DA>
    <DA name="cdcName" bType="VisString255" fc="EX">
       <Val>INS</Val>
    </DA>
</DOType>
<DOType id="Switch_INS_90-4_DS" cdc="INS">
    <DA name="stVal" bType="INT32" fc="ST" dchg="true"/>
    <DA name="q" bType="Quality" fc="ST" qchg="true"/>
    <DA name="t" bType="Timestamp" fc="ST"/>
    <DA name="cdcNs" bType="VisString255" fc="EX">
       <Val>IEC 61850-7-4:2007</Val>
    </DA>
    <DA name="cdcName" bType="VisString255" fc="EX">
       <Val>INS</Val>
    </DA>
    <DA name="dataNs" bType="VisString255" fc="EX">
       <Val>(Tr)IEC 61850-90-4:2012</Val>
    </DA>
</DOType>
<DOType id="Switch_VSS_90-4" cdc="VSS">
    <DA name="stVal" bType="VisString255" fc="ST" dchg="true"/>
    <DA name="q" bType="Quality" fc="ST" qchg="true"/>
    <DA name="t" bType="Timestamp" fc="ST"/>
    <DA name="cdcNs" bType="VisString255" fc="EX">
       <Val>IEC 61850-7-4:2007</Val>
    </DA>
    <DA name="cdcName" bType="VisString255" fc="EX">
       <Val>VSS</Val>
    </DA>
</DOType>
<DOType id="Switch_VSS_90-4_DS" cdc="VSS">
    <DA name="stVal" bType="VisString255" fc="ST" dchg="true"/>
    <DA name="q" bType="Quality" fc="ST" qchg="true"/>
    <DA name="t" bType="Timestamp" fc="ST"/>
    <DA name="cdcNs" bType="VisString255" fc="EX">
       <Val>IEC 61850-7-4:2007</Val>
    </DA>
    <DA name="cdcName" bType="VisString255" fc="EX">
       <Val>VSS</Val>
    </DA>
    <DA name="dataNs" bType="VisString255" fc="EX">
       <Val>(Tr)IEC 61850-90-4:2012</Val>
    </DA>
</DOType>
<DOType id="Switch_SPG_90-4" cdc="SPG">
    <DA name="setVal" bType="BOOLEAN" fc="SP" dchg="true"/>
    <DA name="cdcNs" bType="VisString255" fc="EX">
       <Val>IEC 61850-7-4:2007</Val>
    </DA>
    <DA name="cdcName" bType="VisString255" fc="EX">
       <Val>SPG</Val>
    </DA>
</DOType>
```

```
<DOType id="Switch_SPG_90-4_DS" cdc="SPG">
   <DA name="setVal" bType="BOOLEAN" fc="SP" dchg="true"/>
   <DA name="cdcNs" bType="VisString255" fc="EX">
      <Val>IEC 61850-7-4:2007</Val>
   </DA>
   <DA name="cdcName" bType="VisString255" fc="EX">
      <Val>SPG</Val>
   </DA>
   <DA name="dataNs" bType="VisString255" fc="EX">
      <Val>(Tr)IEC 61850-90-4:2012</Val>
   </DA>
</DOType>
<DOType id="Switch_LBRI_Default_SPG_90-4" cdc="SPG">
   <DA name="setVal" bType="BOOLEAN" fc="SP" dchg="true">
      <Val>true</Val>
   </DA>
   <DA name="cdcNs" bType="VisString255" fc="EX">
      <Val>IEC 61850-7-4:2007</Val>
   </DA>
   <DA name="cdcName" bType="VisString255" fc="EX">
      <Val>SPG</Val>
   </DA>
</DOType>
<DOType id="Switch_LPCP_AdminCfg_SPG_90-4" cdc="SPG">
   <DA name="setVal" bType="BOOLEAN" fc="SP" dchg="true">
      <Val>true</Val>
   </DA>
   <DA name="cdcNs" bType="VisString255" fc="EX">
      <Val>IEC 61850-7-4:2007</Val>
   </DA>
   <DA name="cdcName" bType="VisString255" fc="EX">
      <Val>SPG</Val>
   </DA>
</DOType>
<DOType id="Switch_LBRI_Default_ING_90-4" cdc="ING">
   <DA name="setVal" bType="INT32" fc="SP" dchg="true">
      <Val>0</Val>
   </DA>
   <DA name="cdcNs" bType="VisString255" fc="EX">
      <Val>IEC 61850-7-4:2007</Val>
   </DA>
   <DA name="cdcName" bType="VisString255" fc="EX">
      <Val>ING</Val>
   </DA>
</DOType>
<DOType id="Switch_ING_90-4" cdc="ING">
   <DA name="setVal" bType="INT32" fc="SP" dchg="true"/>
   <DA name="cdcNs" bType="VisString255" fc="EX">
      <Val>IEC 61850-7-4:2007</Val>
   </DA>
   <DA name="cdcName" bType="VisString255" fc="EX">
      <Val>ING</Val>
   </DA>
</DOType>
<DOType id="Switch_MauCfg_ING_100MHD_90-4" cdc="ING">
   <DA name="setVal" bType="INT32" fc="SP" dchg="true">
      <Val>10</Val>
   </DA>
   <DA name="cdcNs" bType="VisString255" fc="EX">
      <Val>IEC 61850-7-4:2007</Val>
   </DA>
   <DA name="cdcName" bType="VisString255" fc="EX">
      <Val>ING</Val>
   </DA>
```

```
</DOType>
<DOType id="Switch_MauCfg_ING_100MFD_90-4" cdc="ING">
   <DA name="setVal" bType="INT32" fc="SP" dchg="true">
      <Val>11</Val>
   </DA>
   <DA name="cdcNs" bType="VisString255" fc="EX">
      <Val>IEC 61850-7-4:2007</Val>
   </DA>
   <DA name="cdcName" bType="VisString255" fc="EX">
      <Val>ING</Val>
   </DA>
</DOType>
<DOType id="Switch_LCCF_DefaultVid_ING_90-4" cdc="ING">
   <DA name="setVal" bType="INT32" fc="SP" dchg="true">
         <Val>1</Val>
   </DA>
   <DA name="cdcNs" bType="VisString255" fc="EX">
      <Val>IEC 61850-7-4:2007</Val>
   </DA>
   <DA name="cdcName" bType="VisString255" fc="EX">
      <Val>ING</Val>
   </DA>
</DOType>
<DOType id="Switch_LCCF_DefaultPrio_ING_90-4" cdc="ING">
   <DA name="setVal" bType="INT32" fc="SP" dchg="true">
         <Val>0</Val>
   </DA>
   <DA name="cdcNs" bType="VisString255" fc="EX">
      <Val>IEC 61850-7-4:2007</Val>
   </DA>
   <DA name="cdcName" bType="VisString255" fc="EX">
      <Val>ING</Val>
   </DA>
</DOType>
<DOType id="Switch_VLN" cdc="VLN">
   <DA name="vid" bType="INT16U" fc="SP" dchg="true">
      <Val>1</Val>
   </DA>
   <DA name="tagFil" bType="Enum" type="VlanTagKind" fc="SP" dchg="true">
      <Val>1</Val>
   </DA>
   <DA name="numMcAddr" bType="INT16U" fc="CF" dchg="true">
      <Val>0</Val>
   </DA>
   <DA name="maxMcAddr" bType="INT16U" fc="CF" dchg="true">
      <Val>255</Val>
   </DA>
</DOType>
<EnumType id="BehaviourModeKind">
   <EnumVal ord="1">on</EnumVal>
   <EnumVal ord="2">blocked</EnumVal>
   <EnumVal ord="3">test</EnumVal>
   <EnumVal ord="4">test/blocked</EnumVal>
   <EnumVal ord="5">off</EnumVal>
</EnumType>
<EnumType id="HealthKind">
   <EnumVal ord="1">Ok</EnumVal>
   <EnumVal ord="2">Warning</EnumVal>
   <EnumVal ord="3">Alarm</EnumVal>
</EnumType>
<EnumType id="CtlModelKind">
   <EnumVal ord="0">status-only</EnumVal>
</EnumType>
<EnumType id="ChannelRedundancyKind">
```

```
            <EnumVal ord="1">none</EnumVal>
            <EnumVal ord="2">prp</EnumVal>
            <EnumVal ord="3">hsr</EnumVal>
        </EnumType>
        <EnumType id="VlanTagKind">
            <EnumVal ord="0">tagged</EnumVal>
            <EnumVal ord="1">untagged</EnumVal>
            <EnumVal ord="2">forbidden</EnumVal>
        </EnumType>
    </DataTypeTemplates>
</SCL>
```

19.7.3 Simple IED with PTP

The following code describes the ICD file for a simple IED with PTP but no LLDP support as shown in Figure 89.

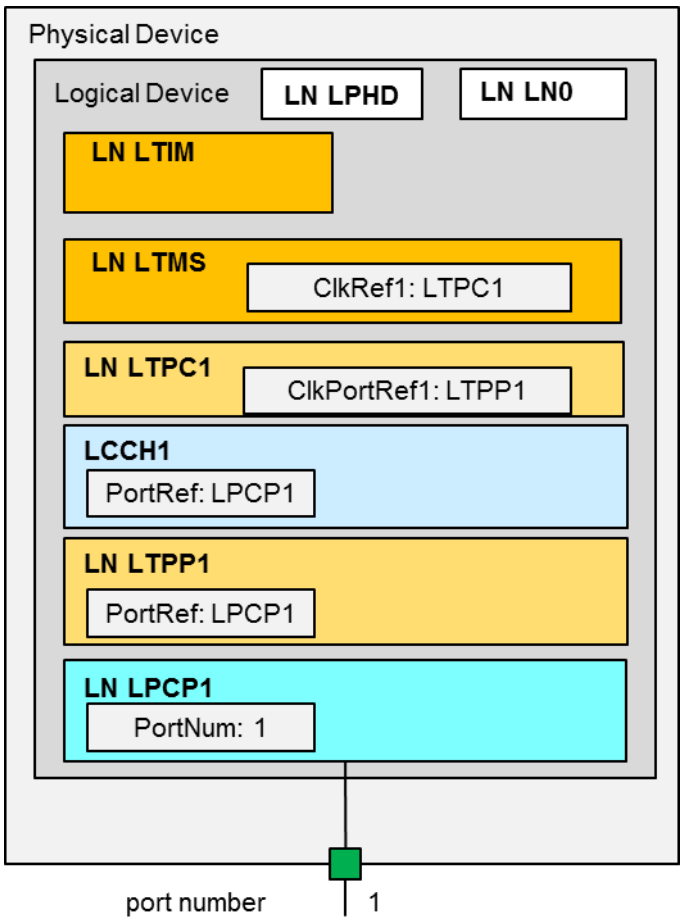


Figure 89 – Simple IED with PTP but no LLDP support

```
<?xml version="1.0" encoding="UTF-8"?>
<SCL xmlns="http://www.iec.ch/61850/2003/SCL"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" version="2007" revision="B"
xsi:schemaLocation="http://www.iec.ch/61850/2003/SCL SCL.xsd">
    <Header id="ICD of an IED with PTP but no LLDP support">
        <History>
            <Hitem version="1" revision="A" when="2013.03.20" what="Initial version"
who="HK"/>
        </History>
    </Header>
    <IED name="TEMPLATE">
        <Services nameLength="64">
            <DynAssociation/>
```

```
    </Services>
    <AccessPoint name="S1">
       <Server>
          <Authentication/>
          <LDevice inst="LD0">
             <LN0 lnClass="LLN0" inst="" lnType="Node_with_PTP_LLN0"/>
             <LN lnClass="LPHD" inst="1" lnType="Node_with_PTP_LPHD"/>
             <LN lnClass="LTIM" inst="1" lnType="Node_with_PTP_LTIM"/>
             <LN lnClass="LTMS" inst="1" lnType="Node_with_PTP_LTMS">
                <DOI name="ClkRef1">
                   <DAI name ="setSrcRef">
                      <Val>@LD0/LTPC1</Val>
                   </DAI>
                </DOI>
             </LN>
             <LN lnClass="LTPC" inst="1" lnType="Node_with_PTP_LTPC">
                <DOI name="ClkPortRef1">
                   <DAI name ="setSrcRef">
                      <Val>@LD0/LTPP1</Val>
                   </DAI>
                </DOI>
             </LN>
             <LN lnClass="LCCH" inst="1" lnType="Node_with_PTP_NoRedChannel_LCCH">
                <DOI name="PortRef">
                   <DAI name ="setSrcRef">
                      <Val>@LD0/LPCP1</Val>
                   </DAI>
                </DOI>
             </LN>
             <LN lnClass="LTPP" inst="1" lnType="Node_with_PTP_LTPP">
                <DOI name="PortRef">
                   <DAI name ="setSrcRef">
                      <Val>@LD0/LPCP1</Val>
                   </DAI>
                </DOI>
             </LN>
             <LN lnClass="LPCP" inst="1" lnType="Node_with_PTP_LPCP">
                <DOI name="PortNum">
                   <DAI name="setVal">
                      <Val>1</Val>
                   </DAI>
                </DOI>
             </LN>
          </LDevice>
       </Server>
    </AccessPoint>
</IED>
<DataTypeTemplates>
    <LNodeType id="Node_with_PTP_LLN0" lnClass="LLN0">
       <DO name="NamPlt" type="Node_with_PTP_LPL_LLN0"/>
       <DO name="Beh" type="Node_with_PTP_Beh_ENS"/>
       <DO name="Health" type="Node_with_PTP_Health_ENS"/>
       <DO name="Mod" type="Node_with_PTP_Mod_ENC"/>
    </LNodeType>
    <LNodeType id="Node_with_PTP_LPHD" lnClass="LPHD">
       <DO name="PhyNam" type="Node_with_PTP_DPL"/>
       <DO name="PhyHealth" type="Node_with_PTP_Health_ENS"/>
       <DO name="Proxy" type="Node_with_PTP_SPS"/>
    </LNodeType>
       <LNodeType id="Node_with_PTP_NoRedChannel_LCCH" lnClass="LCCH">
       <DO name="ChLiv" type="Node_with_PTP_SPS"/>
       <DO name="Beh" type="Node_with_PTP_Beh_ENS"/>
       <DO name="PortRef" type="Node_with_PTP_ORG_90-4_DS"/>
       <DO name="RedCfg" type="Node_with_PTP_RedCfg_None_ENG_90-4_DS"/>
```

```
</LNodeType>
<LNodeType id="Node_with_PTP_LTIM" lnClass="LTIM">
   <DO name="CurUtcOfsTms" type="Node_with_PTP_INS_90-4_DS"/>
   <DO name="CurUtcOfsVld" type="Node_with_PTP_SPS_90-4_DS"/>
   <DO name="RefTmTrk" type="Node_with_PTP_SPS_90-4_DS"/>
   <DO name="RefFqTrk" type="Node_with_PTP_SPS_90-4_DS"/>
   <DO name="Leap" type="Node_with_PTP_LeapSecond_ENS_90-4_DS"/>
    <DO name="AltnOfsTms" type="Node_with_PTP_INS_90-4_DS"/>
   <DO name="AltnTmNam" type="Node_with_PTP_VSS_90-4_DS"/>
   <DO name="JmpTms" type="Node_with_PTP_INS_90-4_DS"/>
   <DO name="NxtJmpTms" type="Node_with_PTP_INS_90-4_DS"/>
    <DO name="TmDT" type="Node_with_PTP_SPS"/>
   <DO name="Beh" type="Node_with_PTP_Beh_ENS"/>
   <DO name="TmOfsTmm" type="Node_with_PTP_ING"/>
   <DO name="TmUseDT" type="Node_with_PTP_SPG"/>
</LNodeType>
<LNodeType id="Node_with_PTP_LTMS" lnClass="LTMS">
   <DO name="TmSrcId" type="Node_with_PTP_INS_90-4_DS"/>
   <DO name="TmSrc" type="Node_with_PTP_VSS"/>
   <DO name="Beh" type="Node_with_PTP_Beh_ENS"/>
   <DO name="ClkRef1" type="Node_with_PTP_ORG_90-4_DS"/>
</LNodeType>
<LNodeType id="Node_with_PTP_LTPC" lnClass="LTPC">
   <DO name="NamPlt" type="Node_with_PTP_LPL_90-4"/>
   <DO name="GmClkSt" type="Node_with_PTP_CGS"/>
   <DO name="Beh" type="Node_with_PTP_Beh_ENS_90-4"/>
   <DO name="OrdClkCfg" type="Node_with_PTP_COG"/>
   <DO name="ClkPortRef1" type="Node_with_PTP_ORG_90-4"/>
</LNodeType>
<LNodeType id="Node_with_PTP_LTPP" lnClass="LTPP">
   <DO name="NamPlt" type="Node_with_PTP_LPL_90-4"/>
   <DO name="ClkPort" type="Node_with_PTP_CPS"/>
   <DO name="Beh" type="Node_with_PTP_Beh_ENS_90-4"/>
   <DO name="PortRef" type="Node_with_PTP_ORG_90-4"/>
</LNodeType>
<LNodeType id="Node_with_PTP_LPCP" lnClass="LPCP">
   <DO name="NamPlt" type="Node_with_PTP_LPL_90-4"/>
   <DO name="PhyNam" type="Node_with_PTP_DPL_90-4"/>
   <DO name="PhyHealth" type="Node_with_PTP_Health_ENS_90-4"/>
   <DO name="AutoNgt" type="Node_with_PTP_SPS_90-4"/>
   <DO name="Mau" type="Node_with_PTP_INS_90-4"/>
   <DO name="PortNum" type="Node_with_PTP_ING_90-4"/>
   <DO name="AutoNgtCfg" type="Node_with_PTP_SPG_90-4"/>
   <DO name="MauCfg" type="Node_with_PTP_MauCfg_ING_100MFD_90-4"/>
   <DO name="MauCfgCap1" type="Node_with_PTP_MauCfg_ING_100MFD_90-4"/>
   <DO name="AdminCfg" type="Node_with_PTP_AdminCfg_SPG_90-4"/>
</LNodeType>
<DOType id="Node_with_PTP_LPL_LLN0" cdc="LPL">
   <DA name="vendor" bType="VisString255" fc="DC"/>
   <DA name="swRev" bType="VisString255" fc="DC"/>
   <DA name="configRev" bType="VisString255" fc="DC"/>
   <DA name="ldNs" bType="VisString255" fc="EX">
      <Val>IEC 61850-7-4:2007</Val>
   </DA>
</DOType>
<DOType id="Node_with_PTP_LPL_90-4" cdc="LPL">
   <DA name="vendor" bType="VisString255" fc="DC"/>
   <DA name="swRev" bType="VisString255" fc="DC"/>
   <DA name="configRev" bType="VisString255" fc="DC"/>
   <DA name="lnNs" bType="VisString255" fc="EX">
      <Val>(Tr)IEC 61850-90-4:2012</Val>
   </DA>
   <DA name="cdcNs" bType="VisString255" fc="EX">
      <Val>IEC 61850-7-4:2007</Val>
```

```
    </DA>
    <DA name="cdcName" bType="VisString255" fc="EX">
       <Val>LPL</Val>
    </DA>
</DOType>
<DOType id="Node_with_PTP_Beh_ENS" cdc="ENS">
    <DA name="stVal" bType="Enum" type="BehaviourModeKind" fc="ST" dchg="true"/>
    <DA name="q" bType="Quality" fc="ST" qchg="true"/>
    <DA name="t" bType="Timestamp" fc="ST"/>
</DOType>
<DOType id="Node_with_PTP_Beh_ENS_90-4" cdc="ENS">
    <DA name="stVal" bType="Enum" type="BehaviourModeKind" fc="ST" dchg="true"/>
    <DA name="q" bType="Quality" fc="ST" qchg="true"/>
    <DA name="t" bType="Timestamp" fc="ST"/>
    <DA name="cdcNs" bType="VisString255" fc="EX">
       <Val>IEC 61850-7-4:2007</Val>
    </DA>
    <DA name="cdcName" bType="VisString255" fc="EX">
       <Val>ENS</Val>
    </DA>
</DOType>
<DOType id="Node_with_PTP_Health_ENS" cdc="ENS">
    <DA name="stVal" bType="Enum" type="HealthKind" fc="ST" dchg="true"/>
    <DA name="q" bType="Quality" fc="ST" qchg="true"/>
    <DA name="t" bType="Timestamp" fc="ST"/>
</DOType>
<DOType id="Node_with_PTP_Health_ENS_90-4" cdc="ENS">
    <DA name="stVal" bType="Enum" type="HealthKind" fc="ST" dchg="true"/>
    <DA name="q" bType="Quality" fc="ST" qchg="true"/>
    <DA name="t" bType="Timestamp" fc="ST"/>
    <DA name="cdcNs" bType="VisString255" fc="EX">
       <Val>IEC 61850-7-4:2007</Val>
    </DA>
    <DA name="cdcName" bType="VisString255" fc="EX">
       <Val>ENS</Val>
    </DA>
</DOType>
<DOType id="Node_with_PTP_Mod_ENC" cdc="ENC">
    <DA name="stVal" bType="Enum" type="BehaviourModeKind" fc="ST" dchg="true"/>
    <DA name="q" bType="Quality" fc="ST" qchg="true"/>
    <DA name="t" bType="Timestamp" fc="ST"/>
    <DA name="ctlModel" bType="Enum" type="CtlModelKind" fc="CF" dchg="true"/>
</DOType>
<DOType id="Node_with_PTP_DPL" cdc="DPL">
    <DA name="vendor" bType="VisString255" fc="DC"/>
</DOType>
<DOType id="Node_with_PTP_DPL_90-4" cdc="DPL">
    <DA name="vendor" bType="VisString255" fc="DC"/>
    <DA name="cdcNs" bType="VisString255" fc="EX">
       <Val>IEC 61850-7-4:2007</Val>
    </DA>
    <DA name="cdcName" bType="VisString255" fc="EX">
       <Val>DPL</Val>
    </DA>
</DOType>
<DOType id="Node_with_PTP_SPS" cdc="SPS">
    <DA name="stVal" bType="BOOLEAN" fc="ST" dchg="true"/>
    <DA name="q" bType="Quality" fc="ST" qchg="true"/>
    <DA name="t" bType="Timestamp" fc="ST"/>
</DOType>
<DOType id="Node_with_PTP_SPS_90-4" cdc="SPS">
    <DA name="stVal" bType="BOOLEAN" fc="ST" dchg="true"/>
    <DA name="q" bType="Quality" fc="ST" qchg="true"/>
    <DA name="t" bType="Timestamp" fc="ST"/>
```

```
            <DA name="cdcNs" bType="VisString255" fc="EX">
               <Val>IEC 61850-7-4:2007</Val>
            </DA>
            <DA name="cdcName" bType="VisString255" fc="EX">
               <Val>SPS</Val>
            </DA>
         </DOType>
         <DOType id="Node_with_PTP_SPS_90-4_DS" cdc="SPS">
            <DA name="stVal" bType="BOOLEAN" fc="ST" dchg="true"/>
            <DA name="q" bType="Quality" fc="ST" qchg="true"/>
            <DA name="t" bType="Timestamp" fc="ST"/>
            <DA name="cdcNs" bType="VisString255" fc="EX">
               <Val>IEC 61850-7-4:2007</Val>
            </DA>
            <DA name="cdcName" bType="VisString255" fc="EX">
               <Val>SPS</Val>
            </DA>
            <DA name="dataNs" bType="VisString255" fc="EX">
               <Val>(Tr)IEC 61850-90-4:2012</Val>
            </DA>
         </DOType>
         <DOType id="Node_with_PTP_ORG_90-4_DS" cdc="ORG">
            <DA name="setSrcRef" bType="ObjRef" fc="EX"/>
            <DA name="cdcNs" bType="VisString255" fc="EX">
               <Val>IEC 61850-7-4:2007</Val>
            </DA>
            <DA name="cdcName" bType="VisString255" fc="EX">
               <Val>ORG</Val>
            </DA>
            <DA name="dataNs" bType="VisString255" fc="EX">
               <Val>(Tr)IEC 61850-90-4:2012</Val>
            </DA>
         </DOType>
         <DOType id="Node_with_PTP_ORG_90-4" cdc="ORG">
            <DA name="setSrcRef" bType="ObjRef" fc="EX"/>
            <DA name="cdcNs" bType="VisString255" fc="EX">
               <Val>IEC 61850-7-4:2007</Val>
            </DA>
            <DA name="cdcName" bType="VisString255" fc="EX">
               <Val>ORG</Val>
            </DA>
         </DOType>
         <DOType id="Node_with_PTP_RedCfg_None_ENG_90-4_DS" cdc="ENG">
            <DA name="setVal" bType="Enum" type="ChannelRedundancyKind" fc="SP"
dchg="true">
                  <Val>1</Val>
            </DA>
            <DA name="cdcNs" bType="VisString255" fc="EX">
               <Val>IEC 61850-7-4:2007</Val>
            </DA>
            <DA name="cdcName" bType="VisString255" fc="EX">
               <Val>ENG</Val>
            </DA>
            <DA name="dataNs" bType="VisString255" fc="EX">
               <Val>(Tr)IEC 61850-90-4:2012</Val>
            </DA>
         </DOType>
         <DOType id="Node_with_PTP_LeapSecond_ENS_90-4_DS" cdc="ENS">
            <DA name="stVal" bType="Enum" type="LeapSecondKind" fc="ST" dchg="true"/>
            <DA name="q" bType="Quality" fc="ST" qchg="true"/>
            <DA name="t" bType="Timestamp" fc="ST"/>
            <DA name="cdcNs" bType="VisString255" fc="EX">
               <Val>IEC 61850-7-4:2007</Val>
            </DA>
```

```
    <DA name="cdcName" bType="VisString255" fc="EX">
       <Val>ENS</Val>
    </DA>
    <DA name="dataNs" bType="VisString255" fc="EX">
       <Val>(Tr)IEC 61850-90-4:2012</Val>
    </DA>
</DOType>
 <DOType id="Node_with_PTP_ING" cdc="ING">
    <DA name="setVal" bType="INT32" fc="SP" dchg="true"/>
</DOType>
  <DOType id="Node_with_PTP_ING_90-4" cdc="ING">
    <DA name="setVal" bType="INT32" fc="SP" dchg="true"/>
    <DA name="cdcNs" bType="VisString255" fc="EX">
       <Val>IEC 61850-7-4:2007</Val>
    </DA>
    <DA name="cdcName" bType="VisString255" fc="EX">
       <Val>ING</Val>
    </DA>
</DOType>
<DOType id="Node_with_PTP_MauCfg_ING_100MFD_90-4" cdc="ING">
    <DA name="setVal" bType="INT32" fc="SP" dchg="true">
       <Val>11</Val>
    </DA>
    <DA name="cdcNs" bType="VisString255" fc="EX">
       <Val>IEC 61850-7-4:2007</Val>
    </DA>
    <DA name="cdcName" bType="VisString255" fc="EX">
       <Val>ING</Val>
    </DA>
</DOType>
<DOType id="Node_with_PTP_INS_90-4" cdc="INS">
    <DA name="stVal" bType="INT32" fc="ST" dchg="true"/>
    <DA name="q" bType="Quality" fc="ST" qchg="true"/>
    <DA name="t" bType="Timestamp" fc="ST"/>
    <DA name="cdcNs" bType="VisString255" fc="EX">
       <Val>IEC 61850-7-4:2007</Val>
    </DA>
    <DA name="cdcName" bType="VisString255" fc="EX">
       <Val>INS</Val>
    </DA>
</DOType>
<DOType id="Node_with_PTP_INS_90-4_DS" cdc="INS">
    <DA name="stVal" bType="INT32" fc="ST" dchg="true"/>
    <DA name="q" bType="Quality" fc="ST" qchg="true"/>
    <DA name="t" bType="Timestamp" fc="ST"/>
    <DA name="cdcNs" bType="VisString255" fc="EX">
       <Val>IEC 61850-7-4:2007</Val>
    </DA>
    <DA name="cdcName" bType="VisString255" fc="EX">
       <Val>INS</Val>
    </DA>
    <DA name="dataNs" bType="VisString255" fc="EX">
       <Val>(Tr)IEC 61850-90-4:2012</Val>
    </DA>
</DOType>
<DOType id="Node_with_PTP_VSS" cdc="VSS">
    <DA name="stVal" bType="VisString255" fc="ST" dchg="true"/>
    <DA name="q" bType="Quality" fc="ST" qchg="true"/>
    <DA name="t" bType="Timestamp" fc="ST"/>
</DOType>
<DOType id="Node_with_PTP_VSS_90-4_DS" cdc="VSS">
    <DA name="stVal" bType="VisString255" fc="ST" dchg="true"/>
    <DA name="q" bType="Quality" fc="ST" qchg="true"/>
    <DA name="t" bType="Timestamp" fc="ST"/>
```

```
        <DA name="cdcNs" bType="VisString255" fc="EX">
          <Val>IEC 61850-7-4:2007</Val>
        </DA>
        <DA name="cdcName" bType="VisString255" fc="EX">
          <Val>VSS</Val>
        </DA>
        <DA name="dataNs" bType="VisString255" fc="EX">
          <Val>(Tr)IEC 61850-90-4:2012</Val>
        </DA>
      </DOType>
      <DOType id="Node_with_PTP_SPG" cdc="SPG">
        <DA name="setVal" bType="BOOLEAN" fc="SP" dchg="true"/>
      </DOType>
      <DOType id="Node_with_PTP_SPG_90-4" cdc="SPG">
        <DA name="setVal" bType="BOOLEAN" fc="SP" dchg="true"/>
        <DA name="cdcNs" bType="VisString255" fc="EX">
          <Val>IEC 61850-7-4:2007</Val>
        </DA>
        <DA name="cdcName" bType="VisString255" fc="EX">
          <Val>SPG</Val>
        </DA>
      </DOType>
      <DOType id="Node_with_PTP_CGS" cdc="CGS">
        <DA name="parentClkId" bType="Octet64" fc="ST" dchg="true"/>
        <DA name="gmClkId" bType="Octet64" fc="ST" dchg="true"/>
        <DA name="gmClkPrio1" bType="INT8U" fc="ST" dchg="true"/>
        <DA name="gmClkPrio2" bType="INT8U" fc="ST" dchg="true"/>
        <DA name="gmClkClass" bType="INT8U" fc="ST" dchg="true"/>
        <DA name="gmClkAcc" bType="INT8U" fc="ST" dchg="true"/>
        <DA name="gmShortId" bType="INT16U" fc="ST" dchg="true"/>
        <DA name="gmInacc" bType="INT32U" fc="ST" dchg="true"/>
        <DA name="netInacc" bType="INT32U" fc="ST" dchg="true"/>
        <DA name="utcOffset" bType="INT32" fc="ST" dchg="true"/>
        <DA name="utcOffsetVld" bType="BOOLEAN" fc="ST" dchg="true"/>
        <DA name="numPath" bType="INT8U" fc="ST" dchg="true"/>
        <DA name="mstOffset" bType="INT64" fc="ST" dchg="true"/>
        <DA name="meanPathDl" bType="INT64" fc="ST" dchg="true"/>
        <DA name="tmSrc" bType="INT8U" fc="ST" dchg="true"/>
      </DOType>
      <DOType id="Node_with_PTP_COG" cdc="COG">
        <DA name="twoStep" bType="BOOLEAN" fc="SP" dchg="true"/>
        <DA name="numPorts" bType="INT8U" fc="SP" dchg="true"/>
        <DA name="clkPrio1" bType="INT8U" fc="SP" dchg="true"/>
        <DA name="clkPrio2" bType="INT8U" fc="SP" dchg="true"/>
        <DA name="clkClass" bType="INT8U" fc="SP" dchg="true"/>
        <DA name="clkAcc" bType="INT8U" fc="SP" dchg="true"/>
        <DA name="domainNum" bType="INT8U" fc="SP" dchg="true"/>
        <DA name="slaveOnly" bType="BOOLEAN" fc="SP" dchg="true"/>
        <DA name="gmShortId" bType="INT16U" fc="SP" dchg="true"/>
        <DA name="netInacc" bType="INT32U" fc="SP" dchg="true"/>
        <DA name="engInacc" bType="INT32U" fc="SP" dchg="true"/>
        <DA name="locInacc" bType="INT32U" fc="SP" dchg="true"/>
        <DA name="offsetMstLim" bType="INT32U" fc="SP" dchg="true"/>
        <DA name="clkId" bType="Octet64" fc="CF" dchg="true"/>
      </DOType>
      <DOType id="Node_with_PTP_CPS" cdc="CPS">
        <DA name="stVal" bType="INT8U" fc="ST" dchg="true"/>
        <DA name="peerMpd" bType="INT64" fc="ST" dchg="true"/>
        <DA name="id" bType="Octet64" fc="ST" dchg="true"/>
        <DA name="num" bType="INT16U" fc="ST" dchg="true"/>
        <DA name="revNum" bType="INT8U" fc="ST" dchg="true"/>
        <DA name="logAnnIntvl" bType="INT8" fc="SP" dchg="true"/>
        <DA name="annRcvTimeout" bType="INT8U" fc="SP" dchg="true"/>
        <DA name="logSynchIntvl" bType="INT8" fc="SP" dchg="true"/>
```

```
            <DA name="dlMechanism" bType="INT8" fc="SP" dchg="true"/>
            <DA name="logMpdReqIntvl" bType="INT8" fc="SP" dchg="true"/>
            <DA name="ena" bType="BOOLEAN" fc="SP" dchg="true"/>
            <DA name="dlAsym" bType="INT64" fc="SP" dchg="true"/>
            <DA name="profileId" bType="INT8U" fc="SP" dchg="true"/>
        </DOType>
        <DOType id="Node_with_PTP_AdminCfg_SPG_90-4" cdc="SPG">
            <DA name="setVal" bType="BOOLEAN" fc="SP" dchg="true">
                <Val>true</Val>
            </DA>
            <DA name="cdcNs" bType="VisString255" fc="EX">
                <Val>IEC 61850-7-4:2007</Val>
            </DA>
            <DA name="cdcName" bType="VisString255" fc="EX">
                <Val>SPG</Val>
            </DA>
        </DOType>
        <EnumType id="BehaviourModeKind">
            <EnumVal ord="1">on</EnumVal>
            <EnumVal ord="2">blocked</EnumVal>
            <EnumVal ord="3">test</EnumVal>
            <EnumVal ord="4">test/blocked</EnumVal>
            <EnumVal ord="5">off</EnumVal>
        </EnumType>
        <EnumType id="HealthKind">
            <EnumVal ord="1">Ok</EnumVal>
            <EnumVal ord="2">Warning</EnumVal>
            <EnumVal ord="3">Alarm</EnumVal>
        </EnumType>
        <EnumType id="CtlModelKind">
            <EnumVal ord="0">status-only</EnumVal>
        </EnumType>
        <EnumType id="ChannelRedundancyKind">
            <EnumVal ord="1">none</EnumVal>
            <EnumVal ord="2">prp</EnumVal>
            <EnumVal ord="3">hsr</EnumVal>
        </EnumType>
        <EnumType id="LeapSecondKind">
            <EnumVal ord="1">none</EnumVal>
            <EnumVal ord="2">removeLeapSecond</EnumVal>
            <EnumVal ord="3">addLeapSecond</EnumVal>
        </EnumType>
    </DataTypeTemplates>
</SCL>
```

19.7.4 RedBox wit HSR

The following code describes the ICD file for a RedBox without RSTP bridging function, as in Figure 90.

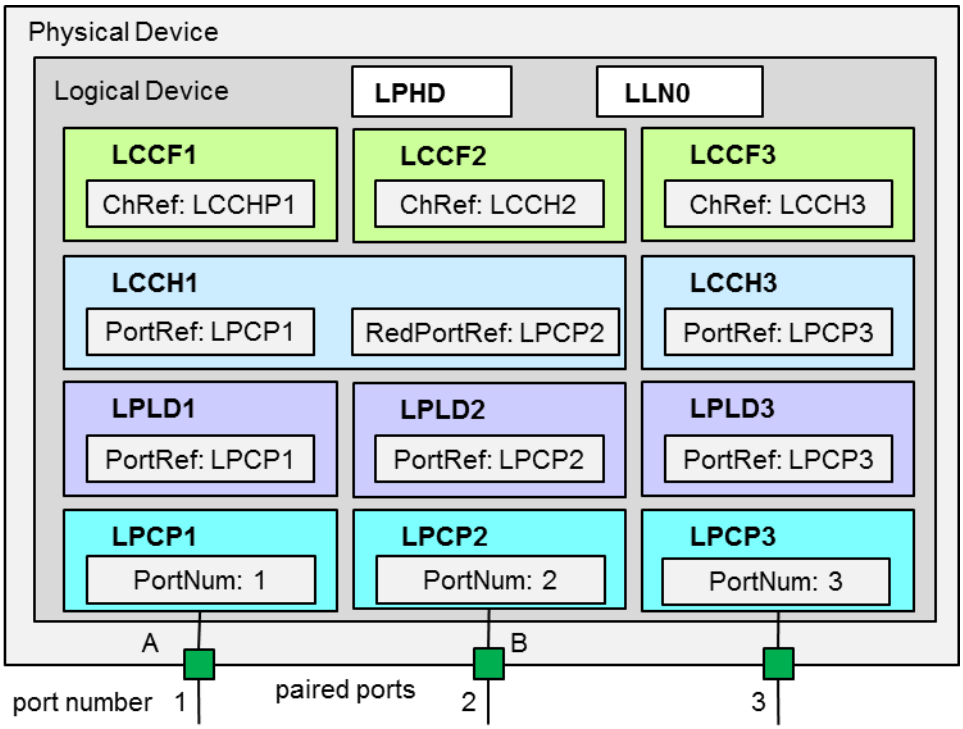


Figure 90 – RedBox with LLDP but no PTP

```
<?xml version="1.0" encoding="UTF-8"?>
<SCL xmlns="http://www.iec.ch/61850/2003/SCL"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" version="2007" revision="B"
xsi:schemaLocation="http://www.iec.ch/61850/2003/SCL SCL.xsd">
   <Header id="ICD of a HSR Redbox with LLDP but no PTP support">
      <History>
         <Hitem version="1" revision="A" when="2013.03.20" what="Initial version"
who="HK"/>
      </History>
   </Header>
   <IED name="TEMPLATE">
      <Services nameLength="64">
         <DynAssociation/>
      </Services>
      <AccessPoint name="S1">
         <Server>
            <Authentication/>
            <LDevice inst="LD0">
               <LN0 lnClass="LLN0" inst="" lnType="Redbox_LLN0"/>
               <LN lnClass="LPHD" inst="1" lnType="Redbox_LPHD"/>
               <LN lnClass="LCCH" inst="1" lnType="Redbox_RedChannel_LCCH">
                  <DOI name="PortRef">
                     <DAI name ="setSrcRef">
                        <Val>@LD0/LPCP1</Val>
                     </DAI>
                  </DOI>
                  <DOI name="RedPortRef">
                     <DAI name ="setSrcRef">
                        <Val>@LD0/LPCP2</Val>
                     </DAI>
                  </DOI>
               </LN>
               <LN lnClass="LCCH" inst="2" lnType="Redbox_NoRedChannel_LCCH">
                  <DOI name="PortRef">
                     <DAI name ="setSrcRef">
                        <Val>@LD0/LPCP3</Val>
```

```
                </DAI>
            </DOI>
        </LN>
        <LN lnClass="LPLD" inst="1" lnType="Redbox_LPLD">
            <DOI name="PortRef">
                <DAI name ="setSrcRef">
                    <Val>@LD0/LPCP1</Val>
                </DAI>
            </DOI>
        </LN>
        <LN lnClass="LPLD" inst="2" lnType="Redbox_LPLD">
            <DOI name="PortRef">
                <DAI name ="setSrcRef">
                    <Val>@LD0/LPCP2</Val>
                </DAI>
            </DOI>
        </LN>
        <LN lnClass="LPLD" inst="3" lnType="Redbox_LPLD">
            <DOI name="PortRef">
                <DAI name ="setSrcRef">
                    <Val>@LD0/LPCP3</Val>
                </DAI>
            </DOI>
        </LN>
        <LN lnClass="LPCP" inst="1" lnType="Redbox_LPCP">
            <DOI name="PortNum">
                <DAI name="setVal">
                    <Val>1</Val>
                </DAI>
            </DOI>
        </LN>
        <LN lnClass="LPCP" inst="2" lnType="Redbox_LPCP">
            <DOI name="PortNum">
                <DAI name="setVal">
                    <Val>2</Val>
                </DAI>
            </DOI>
        </LN>
        <LN lnClass="LPCP" inst="3" lnType="Redbox_LPCP">
            <DOI name="PortNum">
                <DAI name="setVal">
                    <Val>3</Val>
                </DAI>
            </DOI>
        </LN>
    </LDevice>
  </Server>
 </AccessPoint>
</IED>
<DataTypeTemplates>
 <LNodeType id="Redbox_LLN0" lnClass="LLN0">
    <DO name="NamPlt" type="Redbox_LPL_LLN0"/>
    <DO name="Beh" type="Redbox_Beh_ENS"/>
    <DO name="Health" type="Redbox_Health_ENS"/>
    <DO name="Mod" type="Redbox_Mod_ENC"/>
 </LNodeType>
 <LNodeType id="Redbox_LPHD" lnClass="LPHD">
    <DO name="PhyNam" type="Redbox_DPL"/>
    <DO name="PhyHealth" type="Redbox_Health_ENS"/>
    <DO name="Proxy" type="Redbox_SPS"/>
    <DO name="LocChsIdTyp" type="Redbox_INS_90-4_DS"/>
    <DO name="LocChsId" type="Redbox_VSS_90-4_DS"/>
    <DO name="LocAddrTyp" type="Redbox_INS_90-4_DS"/>
    <DO name="LocAddr" type="Redbox_VSS_90-4_DS"/>
```

```
        <DO name="LdpEna" type="Redbox_SPG_90-4_DS"/>
    </LNodeType>
    <LNodeType id="Redbox_RedChannel_LCCH" lnClass="LCCH">
        <DO name="ChLiv" type="Redbox_SPS"/>
        <DO name="RedChLiv" type="Redbox_SPS"/>
        <DO name="Beh" type="Redbox_Beh_ENS"/>
        <DO name="PortRef" type="Redbox_ORG_90-4_DS"/>
        <DO name="RedPortRef" type="Redbox_ORG_90-4_DS"/>
        <DO name="RedCfg" type="Redbox_RedCfg_HSR_ENG_90-4_DS"/>
        <DO name="RedPathId" type="Redbox_ING_90-4_DS"/>
    </LNodeType>
    <LNodeType id="Redbox_NoRedChannel_LCCH" lnClass="LCCH">
        <DO name="ChLiv" type="Redbox_SPS"/>
        <DO name="Beh" type="Redbox_Beh_ENS"/>
        <DO name="PortRef" type="Redbox_ORG_90-4_DS"/>
        <DO name="RedCfg" type="Redbox_RedCfg_None_ENG_90-4_DS"/>
    </LNodeType>
    <LNodeType id="Redbox_LPLD" lnClass="LPLD">
        <DO name="NamPlt" type="Redbox_LPL_90-4"/>
        <DO name="RemPortDesc" type="Redbox_VSS_90-4"/>
        <DO name="LocPortDesc" type="Redbox_VSS_90-4"/>
        <DO name="RemPortIdTyp" type="Redbox_INS_90-4"/>
        <DO name="LocPortIdTyp" type="Redbox_INS_90-4"/>
        <DO name="RemPortId" type="Redbox_VSS_90-4"/>
        <DO name="LocPortId" type="Redbox_VSS_90-4"/>
        <DO name="RemChsIdTyp" type="Redbox_INS_90-4"/>
        <DO name="RemChsId" type="Redbox_VSS_90-4"/>
        <DO name="RemSysDesc" type="Redbox_VSS_90-4"/>
        <DO name="RemAddrTyp" type="Redbox_INS_90-4"/>
        <DO name="RemAddr" type="Redbox_VSS_90-4"/>
        <DO name="Beh" type="Redbox_Beh_ENS_90-4"/>
        <DO name="PortRef" type="Redbox_ORG_90-4"/>
    </LNodeType>
    <LNodeType id="Redbox_LPCP" lnClass="LPCP">
        <DO name="NamPlt" type="Redbox_LPL_90-4"/>
        <DO name="PhyNam" type="Redbox_DPL_90-4"/>
        <DO name="PhyHealth" type="Redbox_Health_ENS_90-4"/>
        <DO name="AutoNgt" type="Redbox_SPS_90-4"/>
        <DO name="Mau" type="Redbox_INS_90-4"/>
        <DO name="PortNum" type="Redbox_ING_90-4"/>
        <DO name="AutoNgtCfg" type="Redbox_SPG_90-4"/>
        <DO name="MauCfg" type="Redbox_MauCfg_ING_100MFD_90-4"/>
        <DO name="MauCfgCap1" type="Redbox_MauCfg_ING_100MFD_90-4"/>
        <DO name="AdminCfg" type="Redbox_AdminCfg_SPG_90-4"/>
    </LNodeType>
    <DOType id="Redbox_LPL_LLN0" cdc="LPL">
        <DA name="vendor" bType="VisString255" fc="DC"/>
        <DA name="swRev" bType="VisString255" fc="DC"/>
        <DA name="configRev" bType="VisString255" fc="DC"/>
        <DA name="ldNs" bType="VisString255" fc="EX">
            <Val>IEC 61850-7-4:2007</Val>
        </DA>
    </DOType>
    <DOType id="Redbox_LPL_90-4" cdc="LPL">
        <DA name="vendor" bType="VisString255" fc="DC"/>
        <DA name="swRev" bType="VisString255" fc="DC"/>
        <DA name="configRev" bType="VisString255" fc="DC"/>
        <DA name="lnNs" bType="VisString255" fc="EX">
            <Val>(Tr)IEC 61850-90-4:2012</Val>
        </DA>
        <DA name="cdcNs" bType="VisString255" fc="EX">
            <Val>IEC 61850-7-4:2007</Val>
        </DA>
        <DA name="cdcName" bType="VisString255" fc="EX">
```

```
      <Val>LPL</Val>
   </DA>
</DOType>
<DOType id="Redbox_Beh_ENS" cdc="ENS">
   <DA name="stVal" bType="Enum" type="BehaviourModeKind" fc="ST" dchg="true"/>
   <DA name="q" bType="Quality" fc="ST" qchg="true"/>
   <DA name="t" bType="Timestamp" fc="ST"/>
</DOType>
<DOType id="Redbox_Beh_ENS_90-4" cdc="ENS">
   <DA name="stVal" bType="Enum" type="BehaviourModeKind" fc="ST" dchg="true"/>
   <DA name="q" bType="Quality" fc="ST" qchg="true"/>
   <DA name="t" bType="Timestamp" fc="ST"/>
   <DA name="cdcNs" bType="VisString255" fc="EX">
      <Val>IEC 61850-7-4:2007</Val>
   </DA>
   <DA name="cdcName" bType="VisString255" fc="EX">
      <Val>ENS</Val>
   </DA>
</DOType>
<DOType id="Redbox_Health_ENS" cdc="ENS">
   <DA name="stVal" bType="Enum" type="HealthKind" fc="ST" dchg="true"/>
   <DA name="q" bType="Quality" fc="ST" qchg="true"/>
   <DA name="t" bType="Timestamp" fc="ST"/>
</DOType>
<DOType id="Redbox_Health_ENS_90-4" cdc="ENS">
   <DA name="stVal" bType="Enum" type="HealthKind" fc="ST" dchg="true"/>
   <DA name="q" bType="Quality" fc="ST" qchg="true"/>
   <DA name="t" bType="Timestamp" fc="ST"/>
   <DA name="cdcNs" bType="VisString255" fc="EX">
      <Val>IEC 61850-7-4:2007</Val>
   </DA>
   <DA name="cdcName" bType="VisString255" fc="EX">
      <Val>ENS</Val>
   </DA>
</DOType>
<DOType id="Redbox_Mod_ENC" cdc="ENC">
   <DA name="stVal" bType="Enum" type="BehaviourModeKind" fc="ST" dchg="true"/>
   <DA name="q" bType="Quality" fc="ST" qchg="true"/>
   <DA name="t" bType="Timestamp" fc="ST"/>
   <DA name="ctlModel" bType="Enum" type="CtlModelKind" fc="CF" dchg="true"/>
</DOType>
<DOType id="Redbox_DPL" cdc="DPL">
   <DA name="vendor" bType="VisString255" fc="DC"/>
</DOType>
<DOType id="Redbox_DPL_90-4" cdc="DPL">
   <DA name="vendor" bType="VisString255" fc="DC"/>
   <DA name="cdcNs" bType="VisString255" fc="EX">
      <Val>IEC 61850-7-4:2007</Val>
   </DA>
   <DA name="cdcName" bType="VisString255" fc="EX">
      <Val>DPL</Val>
   </DA>
</DOType>
<DOType id="Redbox_SPS" cdc="SPS">
   <DA name="stVal" bType="BOOLEAN" fc="ST" dchg="true"/>
   <DA name="q" bType="Quality" fc="ST" qchg="true"/>
   <DA name="t" bType="Timestamp" fc="ST"/>
</DOType>
<DOType id="Redbox_SPS_90-4" cdc="SPS">
   <DA name="stVal" bType="BOOLEAN" fc="ST" dchg="true"/>
   <DA name="q" bType="Quality" fc="ST" qchg="true"/>
   <DA name="t" bType="Timestamp" fc="ST"/>
   <DA name="cdcNs" bType="VisString255" fc="EX">
      <Val>IEC 61850-7-4:2007</Val>
```

```
            </DA>
            <DA name="cdcName" bType="VisString255" fc="EX">
               <Val>SPS</Val>
            </DA>
         </DOType>
         <DOType id="Redbox_ORG_90-4_DS" cdc="ORG">
            <DA name="setSrcRef" bType="ObjRef" fc="EX"/>
            <DA name="cdcNs" bType="VisString255" fc="EX">
               <Val>IEC 61850-7-4:2007</Val>
            </DA>
            <DA name="cdcName" bType="VisString255" fc="EX">
               <Val>ORG</Val>
            </DA>
            <DA name="dataNs" bType="VisString255" fc="EX">
               <Val>(Tr)IEC 61850-90-4:2012</Val>
            </DA>
         </DOType>
         <DOType id="Redbox_ORG_90-4" cdc="ORG">
            <DA name="setSrcRef" bType="ObjRef" fc="EX"/>
            <DA name="cdcNs" bType="VisString255" fc="EX">
               <Val>IEC 61850-7-4:2007</Val>
            </DA>
            <DA name="cdcName" bType="VisString255" fc="EX">
               <Val>ORG</Val>
            </DA>
         </DOType>
         <DOType id="Redbox_RedCfg_None_ENG_90-4_DS" cdc="ENG">
            <DA name="setVal" bType="Enum" type="ChannelRedundancyKind" fc="SP"
dchg="true">
                  <Val>1</Val>
            </DA>
            <DA name="cdcNs" bType="VisString255" fc="EX">
               <Val>IEC 61850-7-4:2007</Val>
            </DA>
            <DA name="cdcName" bType="VisString255" fc="EX">
               <Val>ENS</Val>
            </DA>
            <DA name="dataNs" bType="VisString255" fc="EX">
               <Val>(Tr)IEC 61850-90-4:2012</Val>
            </DA>
         </DOType>
         <DOType id="Redbox_RedCfg_HSR_ENG_90-4_DS" cdc="ENG">
            <DA name="setVal" bType="Enum" type="ChannelRedundancyKind" fc="SP"
dchg="true">
                  <Val>3</Val>
            </DA>
            <DA name="cdcNs" bType="VisString255" fc="EX">
               <Val>IEC 61850-7-4:2007</Val>
            </DA>
            <DA name="cdcName" bType="VisString255" fc="EX">
               <Val>ENS</Val>
            </DA>
            <DA name="dataNs" bType="VisString255" fc="EX">
               <Val>(Tr)IEC 61850-90-4:2012</Val>
            </DA>
         </DOType>
         <DOType id="Redbox_ING_90-4_DS" cdc="ING">
            <DA name="setVal" bType="INT32" fc="SP" dchg="true"/>
            <DA name="cdcNs" bType="VisString255" fc="EX">
               <Val>IEC 61850-7-4:2007</Val>
            </DA>
            <DA name="cdcName" bType="VisString255" fc="EX">
               <Val>ING</Val>
            </DA>
```

```
    <DA name="dataNs" bType="VisString255" fc="EX">
       <Val>(Tr)IEC 61850-90-4:2012</Val>
    </DA>
</DOType>
   <DOType id="Redbox_ING_90-4" cdc="ING">
    <DA name="setVal" bType="INT32" fc="SP" dchg="true"/>
    <DA name="cdcNs" bType="VisString255" fc="EX">
       <Val>IEC 61850-7-4:2007</Val>
    </DA>
    <DA name="cdcName" bType="VisString255" fc="EX">
       <Val>ING</Val>
    </DA>
</DOType>
<DOType id="Redbox_INS_90-4" cdc="INS">
    <DA name="stVal" bType="INT32" fc="ST" dchg="true"/>
    <DA name="q" bType="Quality" fc="ST" qchg="true"/>
    <DA name="t" bType="Timestamp" fc="ST"/>
    <DA name="cdcNs" bType="VisString255" fc="EX">
       <Val>IEC 61850-7-4:2007</Val>
    </DA>
    <DA name="cdcName" bType="VisString255" fc="EX">
       <Val>INS</Val>
    </DA>
</DOType>
<DOType id="Redbox_MauCfg_ING_100MFD_90-4" cdc="ING">
    <DA name="setVal" bType="INT32" fc="SP" dchg="true">
       <Val>11</Val>
    </DA>
    <DA name="cdcNs" bType="VisString255" fc="EX">
       <Val>IEC 61850-7-4:2007</Val>
    </DA>
    <DA name="cdcName" bType="VisString255" fc="EX">
       <Val>ING</Val>
    </DA>
</DOType>
<DOType id="Redbox_INS_90-4_DS" cdc="INS">
    <DA name="stVal" bType="INT32" fc="ST" dchg="true"/>
    <DA name="q" bType="Quality" fc="ST" qchg="true"/>
    <DA name="t" bType="Timestamp" fc="ST"/>
    <DA name="cdcNs" bType="VisString255" fc="EX">
       <Val>IEC 61850-7-4:2007</Val>
    </DA>
    <DA name="cdcName" bType="VisString255" fc="EX">
       <Val>INS</Val>
    </DA>
    <DA name="dataNs" bType="VisString255" fc="EX">
       <Val>(Tr)IEC 61850-90-4:2012</Val>
    </DA>
</DOType>
<DOType id="Redbox_VSS_90-4" cdc="VSS">
    <DA name="stVal" bType="VisString255" fc="ST" dchg="true"/>
    <DA name="q" bType="Quality" fc="ST" qchg="true"/>
    <DA name="t" bType="Timestamp" fc="ST"/>
    <DA name="cdcNs" bType="VisString255" fc="EX">
       <Val>IEC 61850-7-4:2007</Val>
    </DA>
    <DA name="cdcName" bType="VisString255" fc="EX">
       <Val>VSS</Val>
    </DA>
</DOType>
<DOType id="Redbox_VSS_90-4_DS" cdc="VSS">
    <DA name="stVal" bType="VisString255" fc="ST" dchg="true"/>
    <DA name="q" bType="Quality" fc="ST" qchg="true"/>
    <DA name="t" bType="Timestamp" fc="ST"/>
```

```
            <DA name="cdcNs" bType="VisString255" fc="EX">
               <Val>IEC 61850-7-4:2007</Val>
            </DA>
            <DA name="cdcName" bType="VisString255" fc="EX">
               <Val>VSS</Val>
            </DA>
            <DA name="dataNs" bType="VisString255" fc="EX">
               <Val>(Tr)IEC 61850-90-4:2012</Val>
            </DA>
         </DOType>
         <DOType id="Redbox_SPG_90-4" cdc="SPG">
            <DA name="setVal" bType="BOOLEAN" fc="SP" dchg="true"/>
            <DA name="cdcNs" bType="VisString255" fc="EX">
               <Val>IEC 61850-7-4:2007</Val>
            </DA>
            <DA name="cdcName" bType="VisString255" fc="EX">
               <Val>SPG</Val>
            </DA>
         </DOType>
         <DOType id="Redbox_SPG_90-4_DS" cdc="SPG">
            <DA name="setVal" bType="BOOLEAN" fc="SP" dchg="true"/>
            <DA name="cdcNs" bType="VisString255" fc="EX">
               <Val>IEC 61850-7-4:2007</Val>
            </DA>
            <DA name="cdcName" bType="VisString255" fc="EX">
               <Val>SPG</Val>
            </DA>
            <DA name="dataNs" bType="VisString255" fc="EX">
               <Val>(Tr)IEC 61850-90-4:2012</Val>
            </DA>
         </DOType>
         <DOType id="Redbox_AdminCfg_SPG_90-4" cdc="SPG">
            <DA name="setVal" bType="BOOLEAN" fc="SP" dchg="true">
               <Val>true</Val>
            </DA>
            <DA name="cdcNs" bType="VisString255" fc="EX">
               <Val>IEC 61850-7-4:2007</Val>
            </DA>
            <DA name="cdcName" bType="VisString255" fc="EX">
               <Val>SPG</Val>
            </DA>
         </DOType>
         <EnumType id="BehaviourModeKind">
            <EnumVal ord="1">on</EnumVal>
            <EnumVal ord="2">blocked</EnumVal>
            <EnumVal ord="3">test</EnumVal>
            <EnumVal ord="4">test/blocked</EnumVal>
            <EnumVal ord="5">off</EnumVal>
         </EnumType>
         <EnumType id="HealthKind">
            <EnumVal ord="1">Ok</EnumVal>
            <EnumVal ord="2">Warning</EnumVal>
            <EnumVal ord="3">Alarm</EnumVal>
         </EnumType>
         <EnumType id="CtlModelKind">
            <EnumVal ord="0">status-only</EnumVal>
         </EnumType>
         <EnumType id="ChannelRedundancyKind">
            <EnumVal ord="1">none</EnumVal>
            <EnumVal ord="2">prp</EnumVal>
            <EnumVal ord="3">hsr</EnumVal>
         </EnumType>
      </DataTypeTemplates>
</SCL>
```

Annex A
(informative)

Case study – Process bus configuration for busbar protection system

A.1 General

A.1.1 Process bus for busbar protection

Process bus for a busbar protection system is designed in accordance with the data traffic. The key parameters are the data bandwidth required and the data transmission delay time within the process bus which are calculated for a particular substation arrangement.

This is especially the case for large substations, because the individual merging units serving each of the substation bays send their measured values over the process bus to the busbar protection system and there are many nodes generating heavy traffic on the bus.

The following case studies consider the data traffic and the transmission delay time, both of which affect the configuration of the process bus and performance of the busbar protection system. Potential solutions for the configuration of the process bus are shown as a result of the case studies.

A.1.2 Preconditions for case studies

Preconditions for the case studies consider the parameters:

- HSR, multicast and IEC 61850-9-2 LE are applied.
- Sampling rate: 80 samples per cycle.
- One ring process bus is deployed for each protection zone, especially:
  - one ring for each line bay for line protection;
  - one ring for each transformer for transformer protection;
  - one station wide ring for busbar protection.
- Two QuadBoxes (QB) are applied to bridge between two HSR rings in order to improve redundancy, as recommended in IEC 62439-3.
- Each merging unit (MU) transmits one sampled data frame which is 180 octets (Ix4, Vx4) of data for a busbar protection.
- Data traffic for one data frame: 7 Mbit/s (180 octets, 80 samples per period, 60 Hz).
- Latency: one hop.
- 100 Mbit/s, store-and-forward, 180 octets data: 30 μs.
- 1 Gbit/s, store-and-forward, 180 octets data: 3 μs.
- 100 Mbit/s, cut-through, 180 octets data: 20 μs.
- 1 Gbit/s, cut-through, 180 octets data: 2 μs.
- Data within the ring that is not used by the busbar protection is not considered.

The example of process bus configuration is based upon the preconditions shown in Figure A.1.

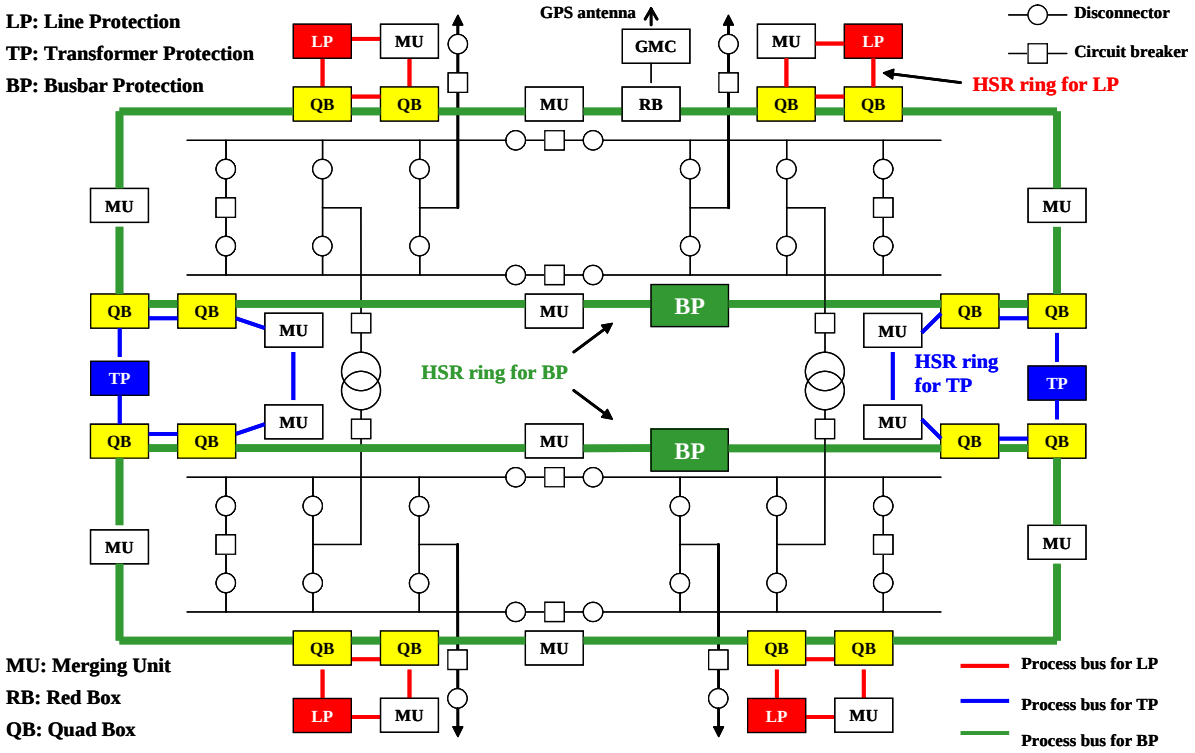


Figure A.1 – Preconditions for the process bus configuration example

A.1.3 Case studies

The case studies consider two large scale model substations:

- Case 1: 56 bays (46 feeders, 4 transformers, 2 bus couplers and 4 bus sections)
- Case 2: 100 bays (92 feeders, 4 transformers, 2 bus couplers and 2 bus sections)

The parameters for Case 1 and Case 2 are:

- Transmission speed: {100 Mbit/s, 1 Gbit/s}
- Data forwarding method in IED: {store-and-forward, cut-through}

For these eight cases, Table A.1 shows the data traffic and expected data transmission delay for the process bus serving the busbar protection system for each case.

Table A.1 – Summary of expected latencies

Case	Number of bays	Transmission speed Mbit/s	Data forwarding method	Data traffic Mbit/s	Transmission delay (average, ms)	Transmission delay (max, ms)
1.a	56	100	Store-and-forward	784	1,6	3,2
1.b	56	1 000	Store-and-forward	784	0,2	0,3
1.c	56	100	Cut-through	784	1,1	2,1
1.d	56	1 000	Cut-through	784	0,1	0,2
2.a	100	100	Store-and-forward	1 400	3,0	5,9
2.b	100	1 000	Store-and-forward	1 400	0,3	0,6
2.c	100	100	Cut-through	1 400	2,0	3,9

Case	Number of bays	Transmission speed Mbit/s	Data forwarding method	Data traffic Mbit/s	Transmission delay (average, ms)	Transmission delay (max, ms)
2.d	100	1 000	Cut-through	1 400	0,2	0,4

The data traffic of the sampled data for the busbar protection system is 784 Mbit/s and 1 400 Mbit/s for the 56 bays and 100 bays substations respectively. This data traffic is large and affects the LAN load and communication processing for all IEDs.

The data transmission delay time is also relatively large and is not negligible from a protection performance perspective. Consequently, this affects the performance of the busbar protection.

According to the results of the case studies, a process bus configuration for a busbar protection system based upon preconditions cannot be realized for a large scale substation from a performance perspective and hence it is necessary to consider alternative solutions for process bus configuration and performance.

A.1.4 Calculation scheme for case 1-a

The calculations are given for Case 1-a as an example for all others in Table A.1.

Number of nodes in the ring = (Number of QB) + (Number of MU) + (Number of busbar relays)

= (46 Feeders × 2 + 4 Transformers × 2) + (2 Bus couplers + 4 Bus sections) + (1 Busbar relay)

= 107

Data traffic = (Number of bays) × (Data traffic per bay) × 2 (see Note)

= 56 bays × 7 Mbit/s × 2

= 784 Mbit/s

NOTE The overall data traffic is doubled because each data frame is sent in both directions in the HSR ring.

Average data transmission delay time

= (Latency of one hop) × (Number of nodes in ring) / 2

= 30 μs × 107 / 2

= 1,6 ms

Maximum data transmission delay time in the event that one of the communication paths fails

= (Latency of one hop) × (Number of nodes in ring)

= 30 μs × 107

= 3,2 ms

A.1.5 Potential solutions

Potential solutions are:

- reduced amount of data;
- increased transmission speed;
- traffic control;
- partitioning the network.

A.2 Reducing the amount of data

A.2.1 Reduction of sampling rate

Reducing the amount of data by reducing the sampling rate is a very effective solution. At the moment 80 samples per cycle is the standard sampling rate for protection, however, lower sampling rates are possible when this does not affect protection performance. It is also possible to pack more than one ASDU into one SV frame, reducing the overhead. In addition, frames can be shortened by reducing the size of the elements, especially in the header. PIs that measure one phase only cause a larger overhead since they transmit one value per frame instead of three or seven.

A.2.2 Higher transmission speed

At least 1 Gbit/s transmission speed is required according to the results of the case studies. In the future, 10 Gbit/s or much higher transmission speeds are expected which enable future improvements in performance.

A.2.3 Traffic control

There are some traffic control techniques that are available at present such as VLAN filtering. These techniques are also considered as one of the potential solutions.

A.2.4 Dividing the network

Physically dividing the network of the busbar protection system process bus is one of the solutions that can be used to reduce data traffic. However, division philosophy should be based upon protection zones, performance and reliability.

A.2.5 Conclusions

The case studies are shown with respect to data traffic and data transmission delay time, both of which affect the process bus configuration, for a HSR based process bus related to a busbar protection system for the case of a large scale substation. Furthermore, potential solutions are proposed to reduce data traffic and improve performance, such as reducing the amount of data, increasing the transmission speed, traffic control and dividing the network. It is recommended that the design of the process bus configuration for the busbar protection system is undertaken in consideration of the results obtained from these case studies and the potential solutions presented, especially for large scale substations.

Annex B
(informative)

Case study – Simple Topologies (Transener/Transba, Argentina)

B.1 Transba architecture and topology – 132 kV substations

Transba operates the 132 kV Buenos Aires Province power network. Most of its substations are 132/33/13,2 kV. At 132 kV voltage level, line protection is implemented by a “distance protection” as a main protection and an “overcurrent protection” as a backup protection, or a differential protection as main and a distance protection as backup, depending on the type of line to be protected.

Figure B.1 shows the first deployment of the SAS architecture, in which Transba still used an RTU as a Station Unit and separated IEDs with protection and control functions. In this first implementation, two automation systems have been used in parallel, namely the legacy RTU using DNP 3.0 and the new IEC 61850-compliant SAS that acquires the control information.

The topology is based on a single fibre optical ring that connects all the managed switches at station level and bay level. At bay level, there are two switches connected with the protection IEDs in a star topology by copper cables.

At station level, there is only one “main” switch, to which the gateway and the Substation Local Operation Console are connected. The gateway is labelled as “Station Unit” (SU).

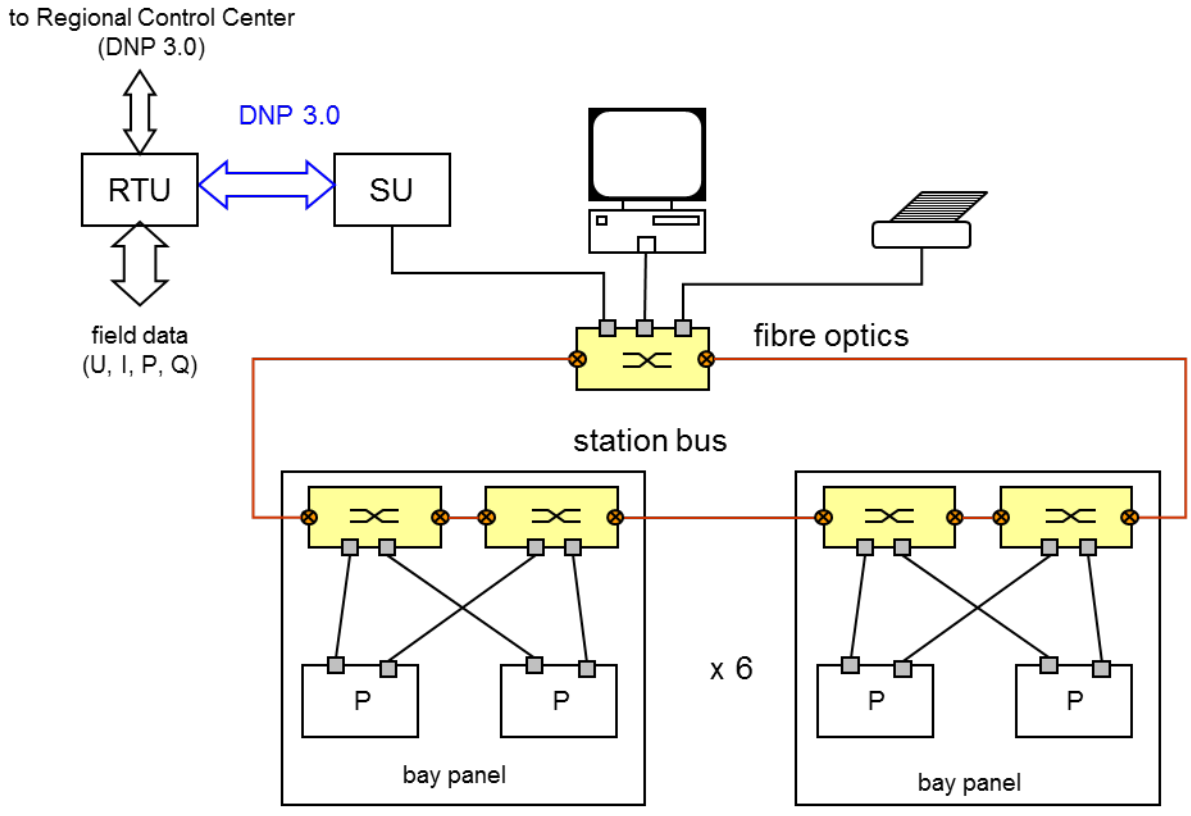


Figure B.1 – First Ethernet-based Transba substation automation network

The new SAS implementations are fully IEC 61850 compliant, so all communications on the LAN are done by IEC 61850. The RTU has been replaced by a Station Unit with gateway functions to be able to communicate with the Control Centre using a DNP 3.0 protocol.

The topology adopted for the SAS, as shown in Figure B.2, is based on several rings corresponding to different voltage levels. Each ring has its own switches, bay units and IEDs to allow control and protection functions to be physically separated in different devices. In the near future, the objective is to use only IEDs with control and protection functions in the same device. The measurements are done by meters connected to the LAN.

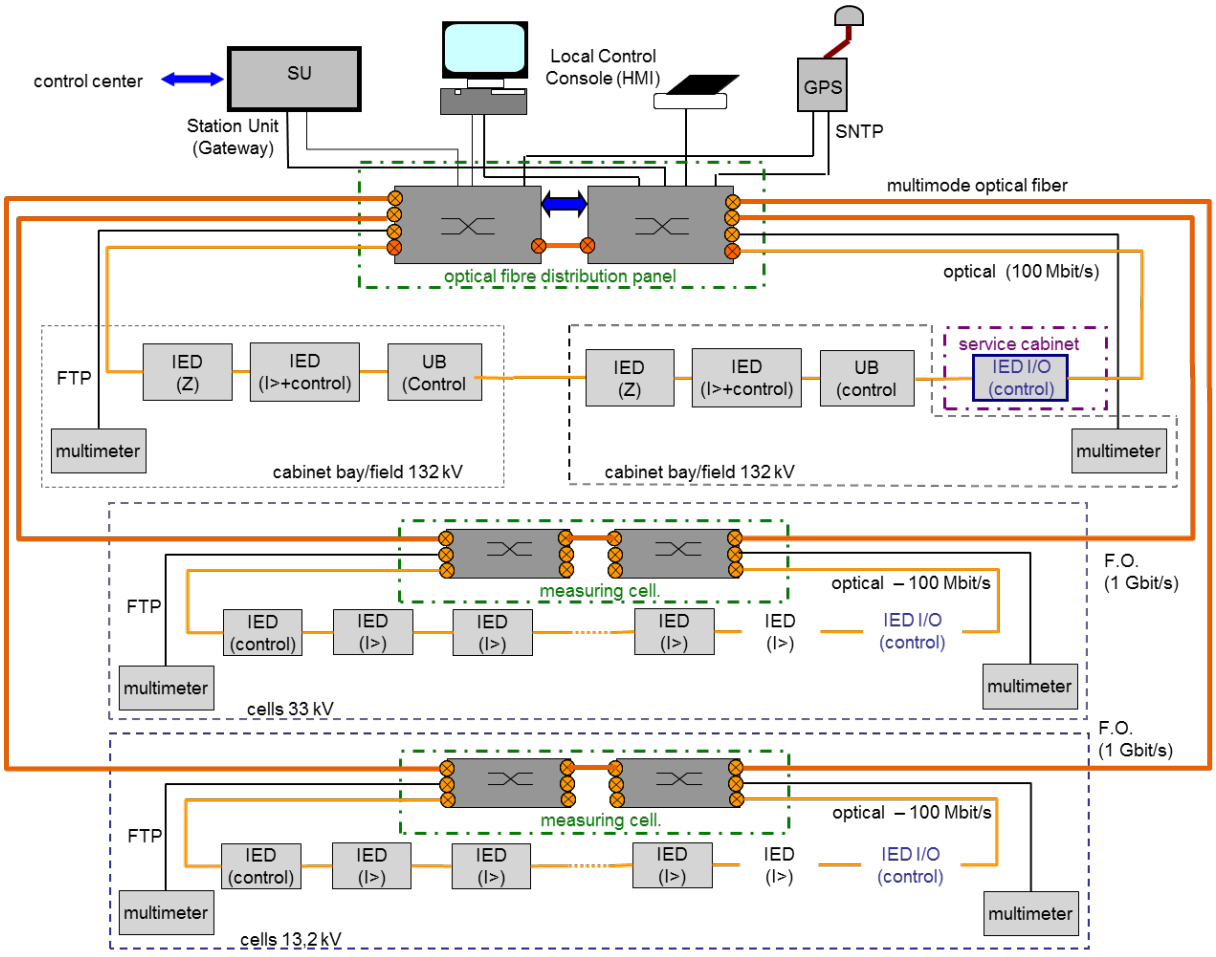


Figure B.2 – Transba SAS architecture

B.2 Transener architecture and topology – 500 kV substations

Transener operates Argentina's 500 kV power network. The architecture and topology shown in Figure B.3 was the first deployment of an Ethernet LAN architecture in a 500 kV substation, even if it was not complying with IEC 61850. It is an example of mixing different technologies.

The architecture was still based on RTUs. The protocol used was DNP 3.0 over TCP/IP. The network connects IEDs, SCADA servers, and serial servers (RS 485/Ethernet) with the Gateway. The network also provides "peer-to-peer" communication between the IEDs (protection relays) of the kiosk.

All switches deployed in the different kiosks are connected in a ring topology by 1 Gbit/s, 50/125 multimode fibres, for bandwidth and attenuation reasons.

In each kiosk, two modular managed switches are deployed, each one with an Ethernet port for each IED (Protection relay) belonging to the primary protection system and secondary protection system. In this way in the kiosk, the topology is a double star.

Several VLANs are deployed. One VLAN is exclusively for protections IEDs, and the control IEDs is connected to another VLAN.

The IEDs (protection relay) have physically redundant ports, with a "hot-stand-by" functionality, i.e. that they have a unique IP address and the ports are operable one at a time, as a "primary" and as a "secondary" port.

The network can overcome the failure of any single component, in particular a switch, an IED port (protection relay), or the IED-switch connection, without loss of functionality. Redundancy grade 1 is achieved.

The time synchronization is done through two GPS via SNTP.

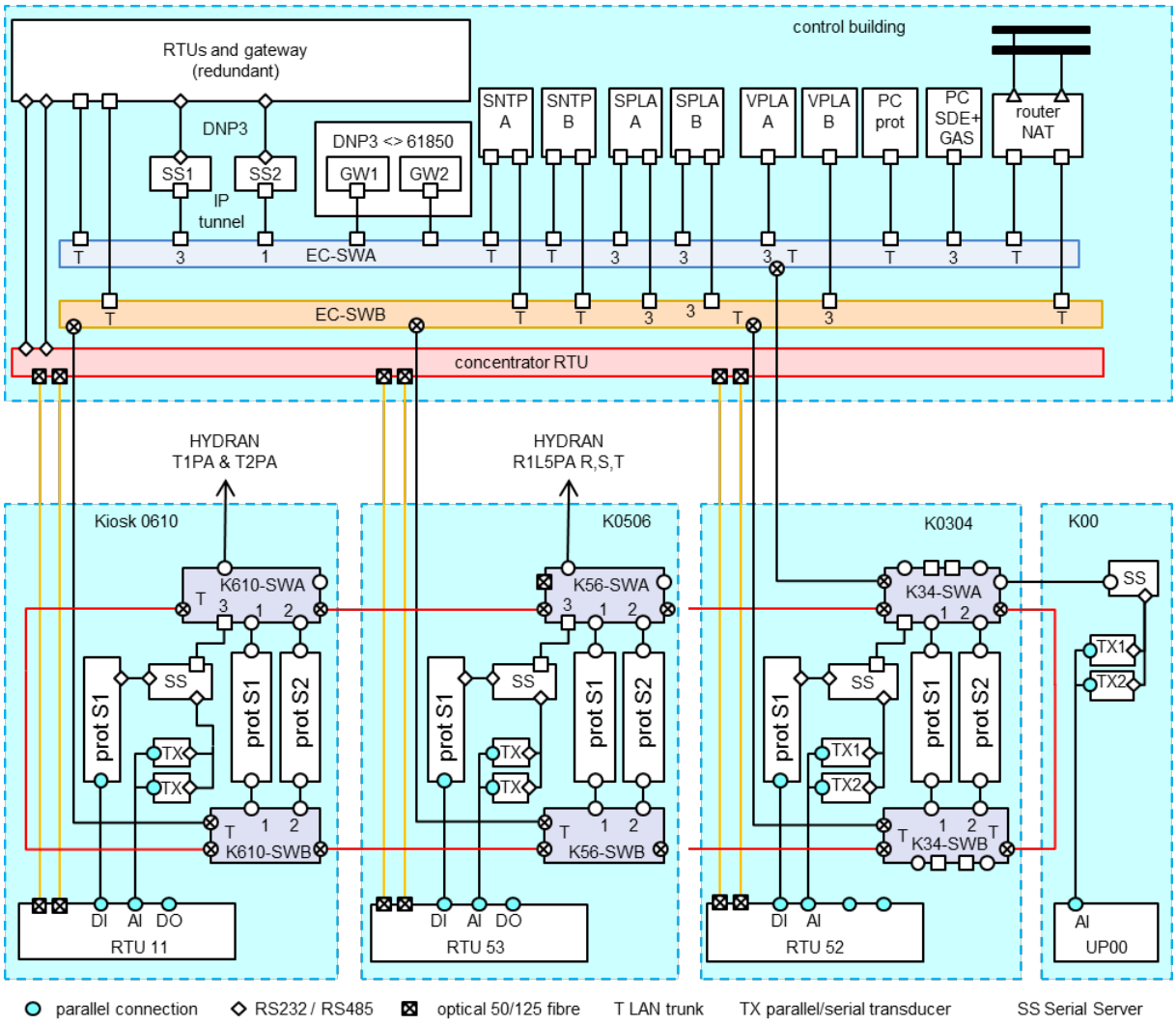


Figure B.3 – Transener substation automation network

B.3 Transener SAS architectures – Esperanza

Figure B.4 shows the first SAS architecture deployed at 500 kV level in a 500/220/132 kV substation. The architectural criteria have also been changed in 500 kV, adopting a full IEC 61850 SAS architecture.

The topology adopted is also based on multiple rings as can be seen in Figure B.3. Depending on the IED port's functionalities the rings will be composed by one or more IEDs. In the topology of Figure B.4, the rings consist of several IEDs, each acting as a bridge between its ports.

Different IEDs are used for protection and for control.

The measurements are acquired with 0,2 class meters due to a requirement regarding the class of the measurements given by the National Control Centre (COC – CAMMESA).

B.4 Transener SAS architectures – El Morejón

Figure B.5 shows a different type of architecture in a 500/220/33 kV substation based on a topology in which the multiple rings support only one IED. The rings are implemented by two different switches like the topology shown in Figure 81.

Figure B.6 shows more in detail the topology of a 500 kV and Figure B.7 the 33 kV kiosks. The 220 kV kiosk is similar in topology as the 500 kV one.

The new architecture that will be adopted for the 500 kV substations will have a similar topology but the IEDs will combine protection and control functions instead of having separate IEDs for the protection functions and control functions. Nevertheless, the IEDs will be duplicated to have a greater availability.

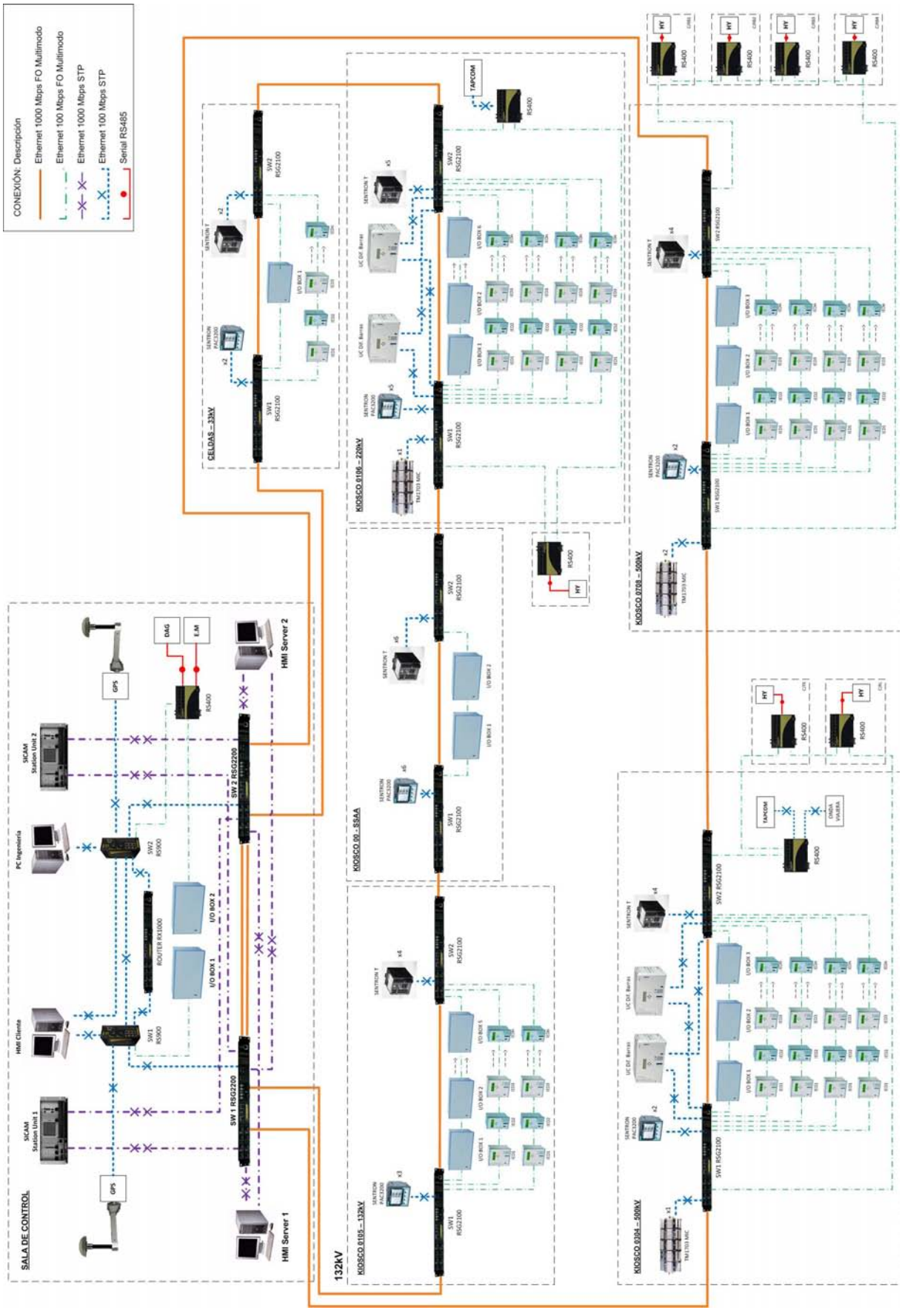


Figure B.4 – Transener SAS architecture – ET Esperanza

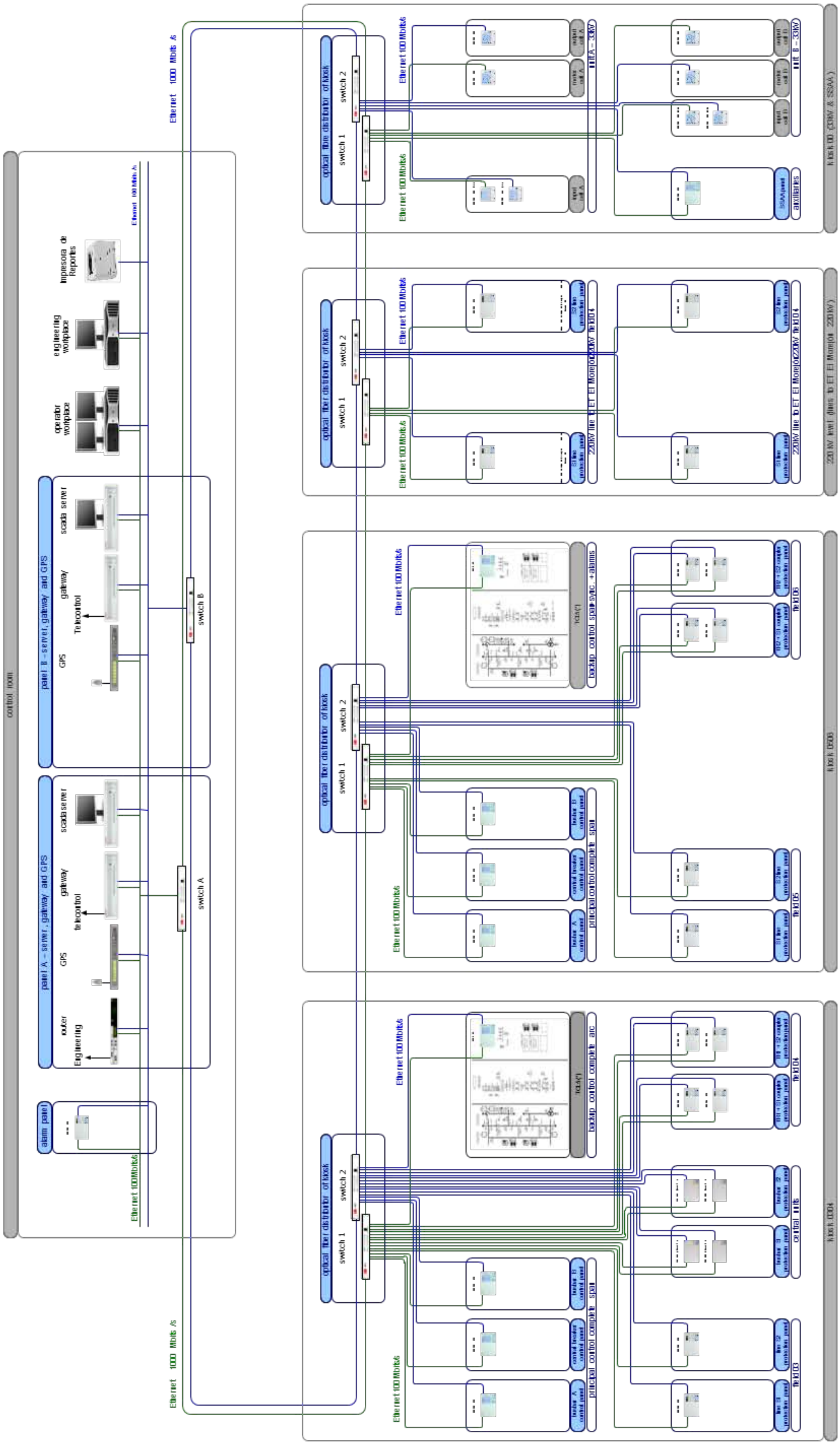


Figure B.5 – Transener 500 kV architecture – El Morejón

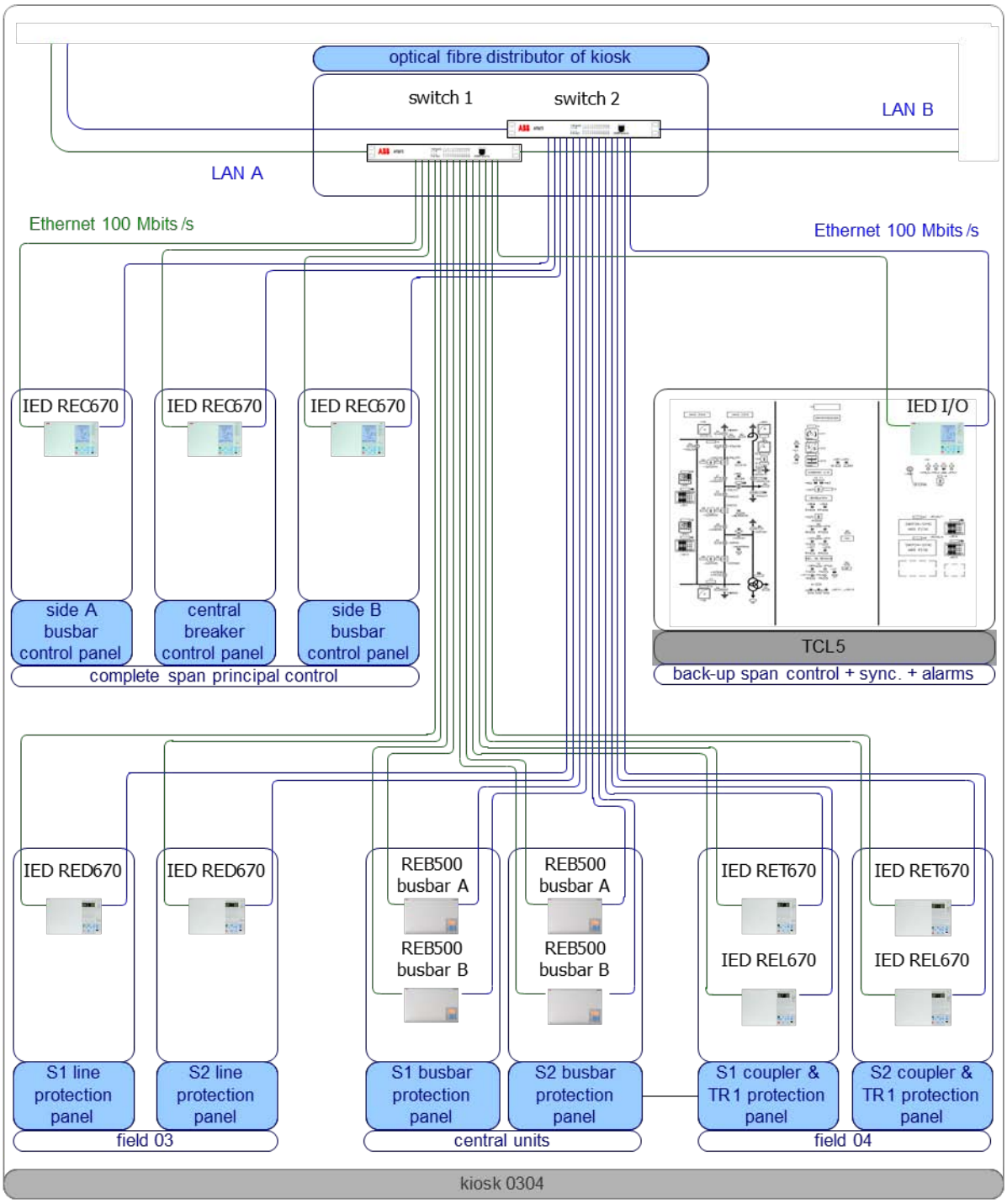


Figure B.6 – 500 kV kiosk topology

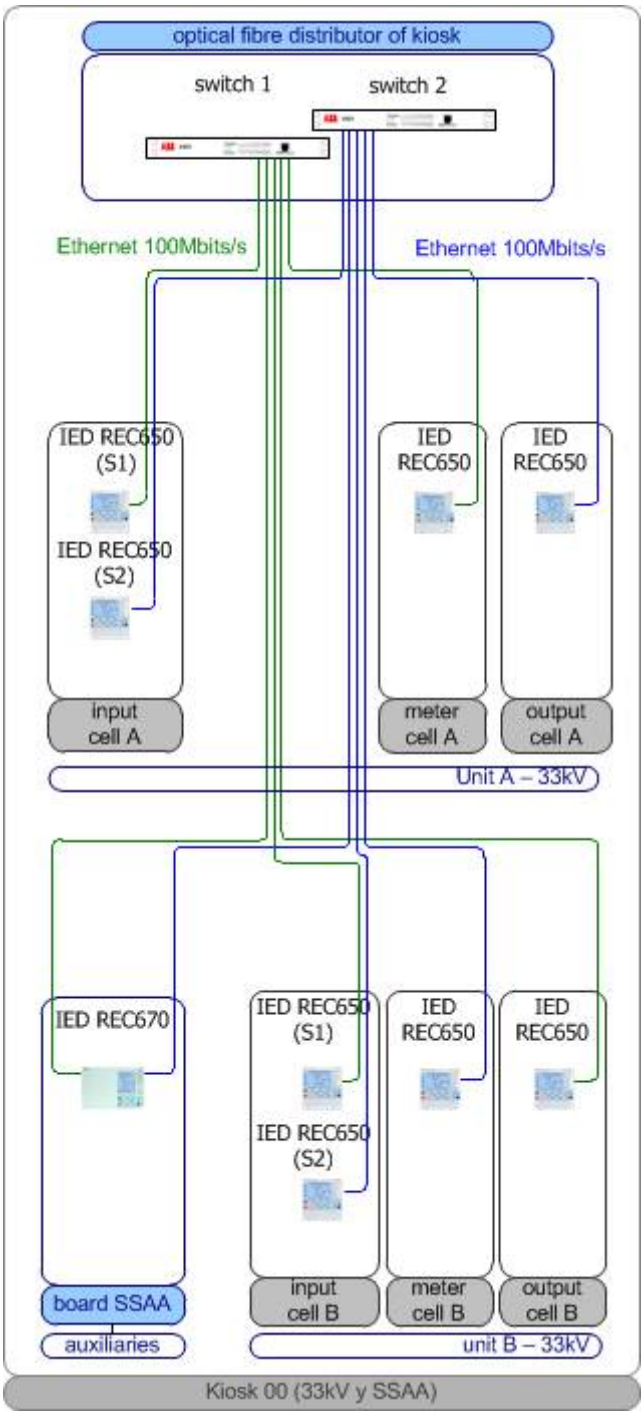


Figure B.7 – 33 kV kiosk topology

Annex C
(informative)

Case study – An IEC 61850 station bus (Powerlink, Australia)

C.1 Normative aspects

This engineering example of a data network for a typical IEC 61850 substation application captures typical requirements and explains implementation decisions, which in some cases deviate from these engineering guidelines.

The present tense is used also to express a design requirement, to distinguish it from a normative requirement (“shall”) or a normative recommendation (“should”).

C.2 Substation layout and topologies

C.2.1 Reference substation: 275 kV / 132 kV

The reference substation consists of a high-voltage part (275 kV) in 1 ½ CB configuration and a medium voltage part (132 kV) with a folded bus topology (see Figure C.1).

The control and protection devices are attached to each circuit breaker. To protect these assets, the control and protection function is executed by two redundant IEDs, X (Main 1) and Y (Main 2). It is critical that the redundant protections are not down at the same time. This must be ensured by a design without single point of failure and a short repair time supported by extensive supervision.

Communication allows the exchange of signals between the different voltage levels in the busbar and transformer protection. The legacy solution used hardwiring for these signals. A solution based on the IEC 61850 standard will replace it, with the option to utilize proprietary communication protocols in justified cases.

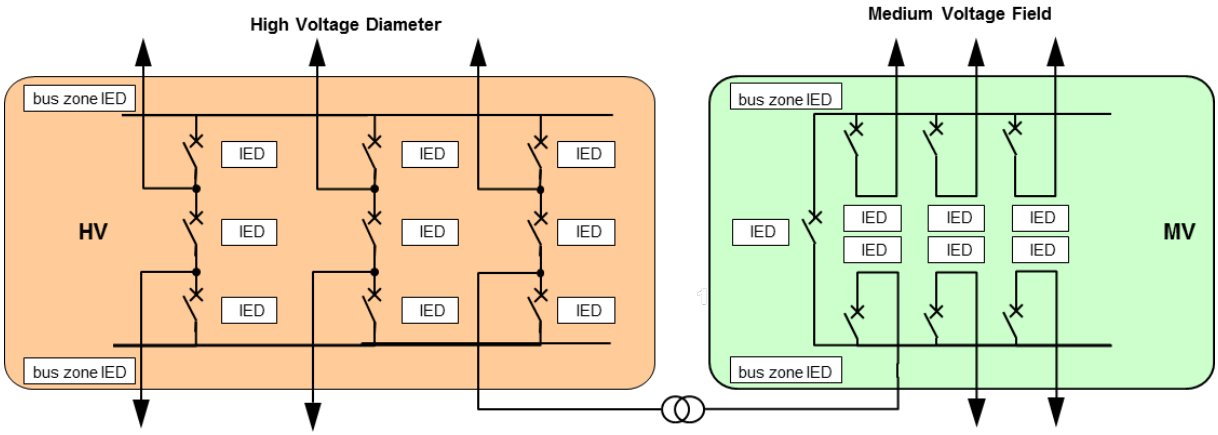


Figure C.1 – Example HV and LV single line diagram and IEDs

C.2.2 Substation sizes

The following site categories have been identified for this engineering, as shown in Table C.1 and Table C.2.

Table C.1 – Site categories HV

HV substation size	Diameter	Bay IED	Common IED	Total IED
Small	5	15	5	20
Medium	10	30	5	35
Large	15	45	5	50

Table C.2 – Site categories MV

MV substation size	Bay IED	Common IED	Total IED
Small	5	5	10
Medium	15	5	20
Large	30	5	35

C.2.3 Physical site layout considerations

Different physical site topologies from green field sites to brown field sites and sites with one building or multiple buildings are considered.

The network topology is constrained by the physical layout of the site and the conducting equipment arrangement.

The number of connections between buildings is kept to a minimum and host connections within a building are consolidated.

C.2.4 Panel layout for a bay

A modular approach is used for panel layout within the substation buildings (see Figure C.2).

The typical building has a number of panels arranged as per the electrical layout, i.e. three adjacent panels for each HV diameter and one panel per breaker for LV.

The network equipment layout and installation location consider the physical layout of the building. Equipment is placed so as to minimize cabling, simplify maintenance and increase modularity.

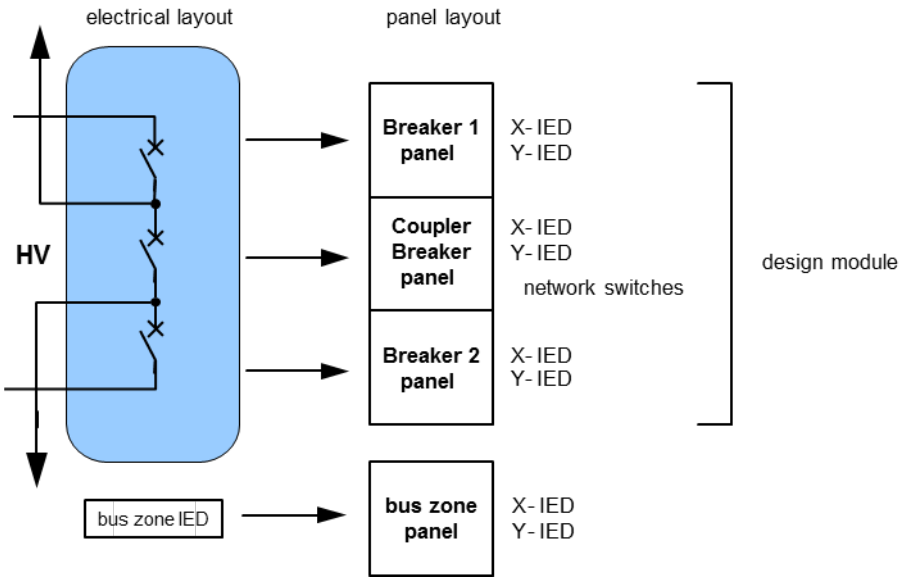


Figure C.2 – HV bay and cabinet module

C.2.5 HV building modules

In a HV building module, the network bridges are located in the coupler panel and all the IEDs in this diameter are wired to these network bridges. For common IEDs, it is proposed to wire these back to the distribution station bridge for the voltage level. These distribution station bridges are located in the Main Building panel (not shown).

Building modules are classified in Table C.3.

Table C.3 – Building modules

Class	Buildings	Panels per building	IEDs per panel	Modules
A	1	30	1X and 1Y	1 HV or LV Main building
B	2	30	1X and 1Y	1 HV and 1 LV Main building
C	4	30	1X and 1Y	1 HV and 1 LV Main building plus 1 HV and LV satellite building

Key design parameters are:

- Up to 4 buildings per site;
- 24 panels per building – 2Y and 1X per panel;
- Match layout of network with diameter for non-redundant network;
- About 8 diameters per building;
- Per diameter about 4 LAN connections for X protection;
- Per diameter about 3 LAN connections for Y protection;
- Per diameter about 3 LAN connections for Y bay control;
- Isolate LV from HV LANs (L2 or L3).

C.3 Requirements put on the network

C.3.1 Requirement classes

The requirements on the network concern:

- connectivity;
- redundancy;
- performance.

C.3.2 Connectivity requirements

C.3.2.1 Support station bus functionality

The network supports IEC 61850 station bus over Ethernet (GOOSE, MMS). The detailed requirements are taken from IEC 61850-5 and IEC 61850-8-1.

C.3.2.2 Support protection functionality

The station bus carries GOOSE messages with Fast Trip signals for protection. A failure of the station bus must not prevent the protection from operating.

C.3.2.3 Support power systems control and monitoring functionality

The station bus carries GOOSE messages for control and monitoring. The loss of the station bus prevents the transmission of interlocking signals, which impacts availability, but not safety. Redundancy is added if necessary to let availability meet the contractual value.

C.3.2.4 Support SCADA / gateway / HMI functionality

The station bus carries MMS messages to let the SCADA / gateway / HMI access the IEDs. Loss of that function is an availability issue.

The Remote SCADA / HMI do not need to be on the station bus and, for security purposes, should not be directly attached to the station bus, but possible through an OPC server.

C.3.2.5 Support engineering access functionality

Engineering access is either provided via the SCADA / gateway / HMI or via existing Operations WAN connection.

Engineering access is required to:

- access the IEDs utilizing standard tools (or open tools in the future);
- access the IEDs utilizing propriety tools;
- capture network traffic on the station bus as far as this is possible in a switched Ethernet.

C.3.3 Redundancy requirements

C.3.3.1 Basic requirement

The loss of a single component of the network (link, switch) cannot result in the loss of control or visibility of more than one item of plant.

Failure of one bridge affects no more than one bay.

NOTE These requirements imply a redundant network for control and monitoring functions. In this case, two LANs A and B in parallel can be used (PRP solution) or the IEDs can be arranged in a bi-directional ring using the HSR protocol.

C.3.3.2 X and Y protection independency requirement

The fail-independence of X and Y protection are ensured by connecting them to different bridges connected themselves independently to the SCADA / HMI.

The station bus is split into multiple networks separated at layer 2. X and Y protection are carried over separate station bus networks, so the failure or recovery time of one of these networks does not affect protection functions.

NOTE A separation at layer 2 and not 3 ensures that GOOSE messages can be exchanged between X and Y.

C.3.4 Quality of Service requirements

C.3.4.1 Quality of Service for fast trip messages (GOOSE Type 1A)

Fast trip messages (GOOSE Type 1A) exhibit a latency of less than 0,6 ms measured from network interface to network interface.

NOTE IEC 61850-5 specifies an application to application delay of 3 ms including the application processing.

C.3.4.2 Quality of Service for MMS

When carrying command information, a delay of some 100 ms is tolerated.

C.3.4.3 QoS and jitter

QoS is utilized to minimize jitter for the higher priority traffic. This is achieved by the higher priority traffic being put into the high priority queue, therefore minimizing its wait times while transiting the network.

C.3.5 Components (hardware and software)

The network design considers the following components:

- IEDs;
- bridges;
- routers;
- firewalls;
- EMS (local HMI);
- EMS (Central).

C.4 Equipment Selection

C.4.1 Criteria

C.4.1.1 Single vendor vs. Multivendor

A single vendor is preferred for the station bus bay functions module. Otherwise, mixing products of different vendors is allowed.

C.4.1.2 Use of vendor-specific features

Vendor specific features that provide advantages in areas of network recovery, security, operations and maintenance are considered.

C.4.2 Physical links

The physical connection between IEDs and bridges is 100 Mbit/s full duplex.

The physical connection between the bridges can be 100 Mbit/s or 1 Gbit/s, depending on the model of bridge and available interfaces. There is little need for 1 Gbit/s but where there is no financial disadvantage, the connection is preferably 1 Gbit/s.

The connections between the bridges are preferably fibre due to electrical isolation requirements.

The physical medium within the building is adapted to the electrical isolation. For isolation below 1 kV, copper links (100Tx) are adequate as per IEC 61000-4-5 for surge voltage (4 kV) for IEC 61000-4-4 fast transients (burst)). For isolation at higher voltage levels, fibre optics are used.

Physical wiring between buildings is multimode optical fibre OM3 (50 micron).

The optical connector type on networking equipment is preferably of the LC type.

NOTE 1 Connector type is not critical as patch cables are used between the equipment and the fibre optical patch panel; these patch cables can have whatever connector is required.

Physical media converters are avoided.

NOTE 2 Most IED manufacturers mainly provide fibre connections, therefore penalizing copper cabling due to the necessary physical media converters which introduce points of failure and require maintenance.

C.4.3 Node connections

End nodes can connect in a number of ways; the methods discussed here are:

- singly attached end nodes;
- doubly attached end nodes.

Nodes are doubly attached in redundant networks and singly attached in the non-redundant networks. Where a node is only available with a single Ethernet port and it needs to be connected to a redundant network, then a RedBox is used to doubly attach the device.

C.4.4 Core router firewall

This device provides routing functions and firewalling functions for the SAS. IDS functions could also be enabled in this device. All access between VLANs is via this device and only known and approved traffic is permitted.

C.4.5 Core bridge

This is an extension to the core router providing the quantity of interfaces required to interface both internally and externally to the SAS. At the same time, it can perform a bridge function.

C.5 Data network topologies

C.5.1 Separate and common data network

The substation automation data network can be either implemented as:

- separate, a self-contained network separate from the Operational WAN;
- common or incorporated with the Operations WAN, utilizing common core and security for both Substation Automation and Operational networks.

An example for these two topologies is shown in Figure C.3.

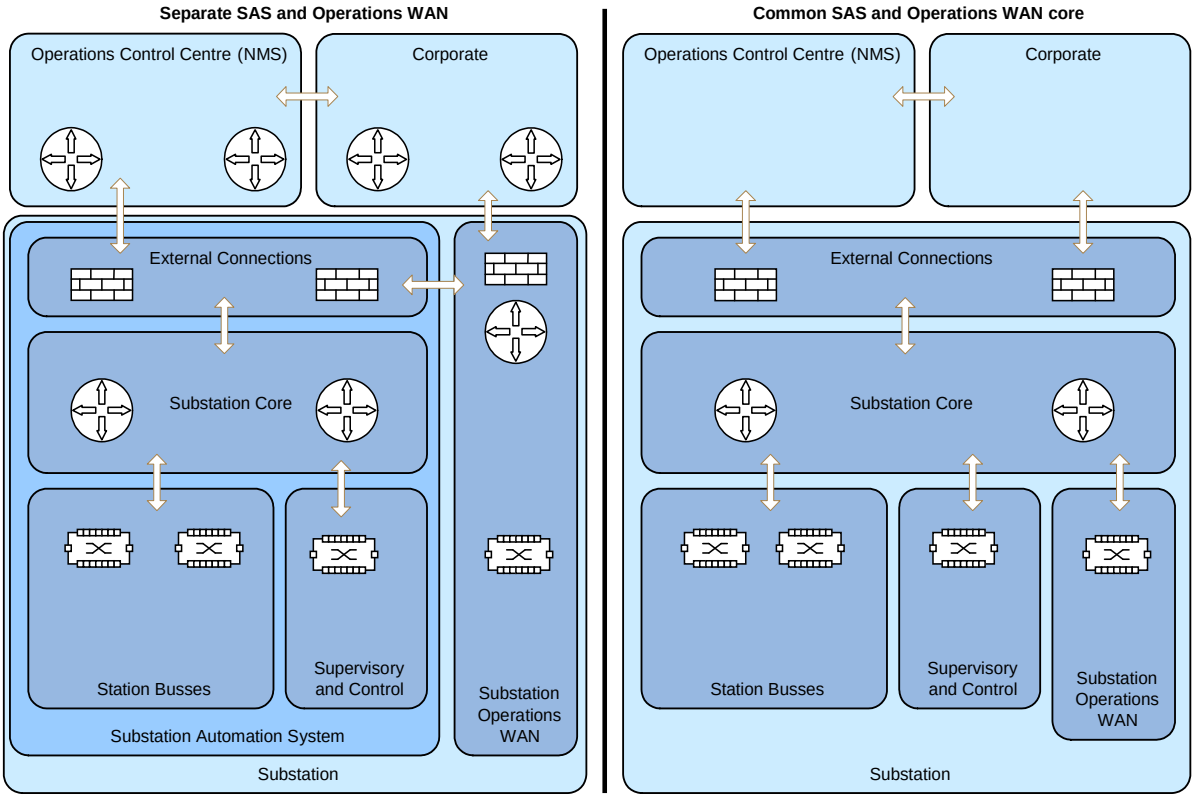


Figure C.3 – Data network areas

While the first option uses a single substation core for all functions in the substation, the second keeps the substation automation system separated from the operational network in the substation.

The common model requires correctly skilled staff, network virtualization, good practices and change control. When this is not provided, it is recommended to keep the Substation Automation network and the Operational network physically separated.

In either of these options, there are four distinct areas of the data network:

- station bus (Bay functions);
- station bus (SCADA Gateway / HMI station-wide functions);
- Core;
- External Connections.

These are further expanded in Figure C.4, showing the whole substation architecture with separate Operational Network from the Substation Automation Network. Traffic flows are depicted in Figure C.5 and further expanded in Figure C.6.

This modular approach allows for each area to be designed individually, taking into account the requirements for connecting modules.

Through analysing the substation structures, the network design is broken down into the modules shown in Table C.4.

Table C.4 – Network modules

Network module	Purpose and function
station bus (Bay Functions)	Provide layer 2 connectivity between Bay IEDs for the delivery of GOOSE, Provide connectivity between Bay IEDs via MMS and other ancillary protocols for the SCADA Operational and Engineering access.
station bus (Station Functions) or Substation Level Platform (SCADA GATEWAY / HMI)	Provide connectivity for Station function.
Core	Provide routing between other modules. Provide basic security between modules.
External Connections	Provide secure interconnects between other networks such as Operations WAN for Engineering/Operational access and EMS for SCADA.

Subclauses C.5.2 to C.5.11 detail each of these modules.

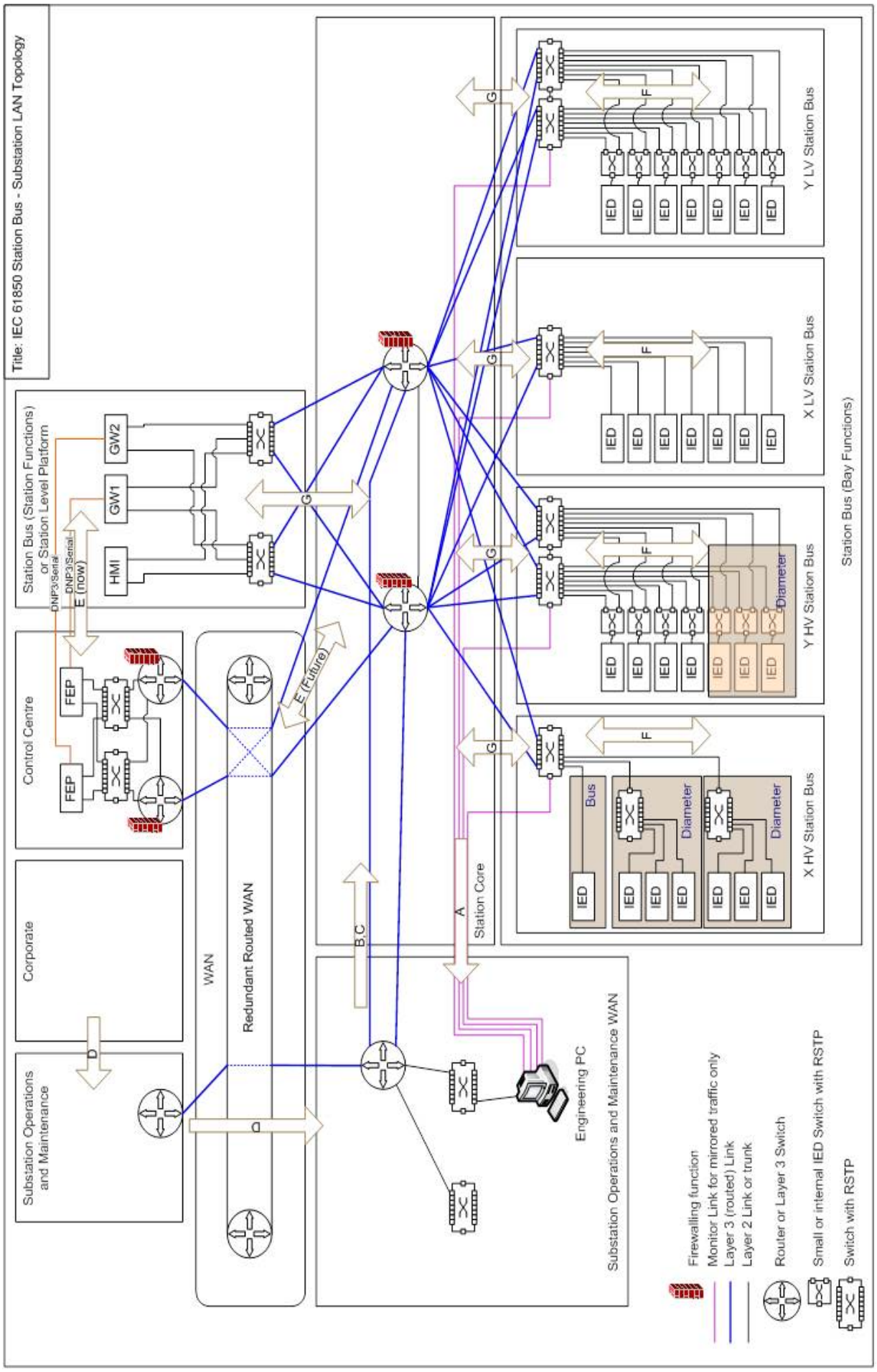


Figure C.4 – Substation LAN topology

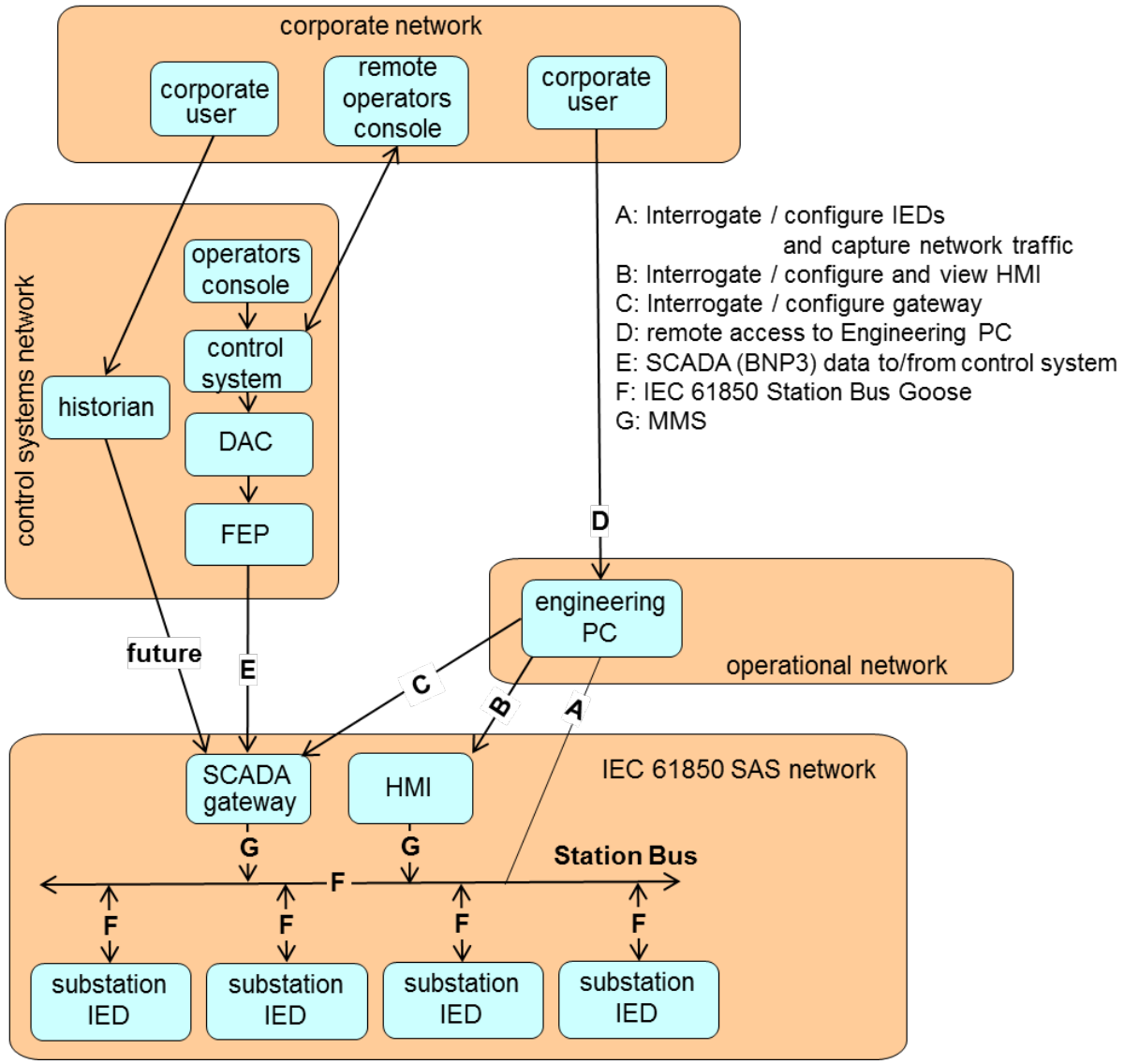


Figure C.5 – SAS Gen1 High level traffic flows

C.5.2 Station bus (station functions) or SCADA gateway / HMI

This network module provides means to connect the SCADA Gateway, HMI and optionally the Engineering PC. Connection of the SCADA Gateway and HMI is straight forward. These are provided via a VLAN with redundant gateway protocols utilized for gateway redundancy; the most likely choice for this is VRRP (Virtual Router Redundancy Protocol). The physical hosts are dual-connected to redundant bridges.

Physical connections for the SCADA Gateway / HMI are provided via dedicated network bridges if the port count is large or most likely via the core network bridges.

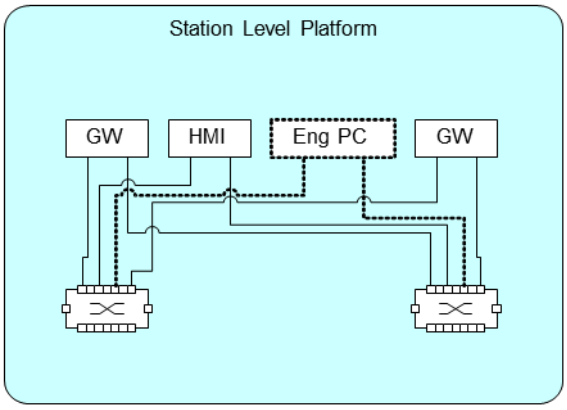


Figure C.6 – SCADA & gateway connection

C.5.3 Station core

The station core (see Figure C.7) provides a routing and firewalling function for policy enforcement. No unknown traffic is permitted to pass through this module. It is expected that this module consists of redundant routers that provide stateful firewalling functions. Intrusion detection is an advantage in this module, but it is unlikely that any blocking outside of traffic permitted by the firewalling is required.

The station core also provides connectivity between all modules in the SAS; therefore, it requires enough network ports to connect these other modules. It is recommended to make this module with a redundant pair of router/firewalls and network bridges for increased port count for connection to other modules. This is commonly called a 'router on a stick' configuration.

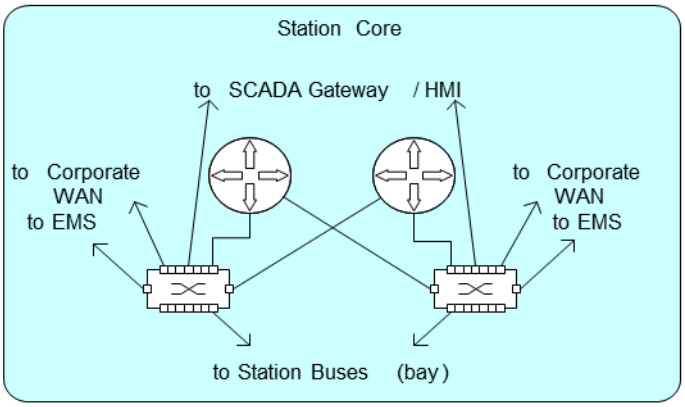


Figure C.7 – Station Core

A routing protocol should be utilized within the Core module to maintain adjacencies between the core routers.

C.5.4 Transformer protection over the network

There are two options for providing transformer protection:

- hardwired between the concerned IEDs utilizing existing inputs and outputs;
- a data link over the data network between the concerned IEDs.

To provide transformer protection over the network would require a domain to be spanned between voltage levels in both the X and Y station buses, this domain would not span between X and Y. This domain could be either connected logically via the Core module or by dedicated Ethernet cables between the bridges associated with the transformer being protected. The likely option is direct connections between the associated bridges.

C.5.5 Automated voltage regulation (AVR)

SCADA Gateway that controls AVR sends GOOSE messages directly to the IEDs executing station bus Bay Functions module. This could be achieved by creating a domain that extends from the station bus Station Function module to the station bus Bay Functions module. This would then allow the SCADA Gateway to converse with MMS to the IEDs via the core router/firewall with appropriate policy enforcement on one domain and also converse with GOOSE directly to the IEDs for AVR.

The major risk in this approach is the multi-homing of the SCADA Gateway between the SCADA GATEWAY / HMI module and the station bus Bay module. Multi-homing is not recommended since traffic can bypass security policy enforcement provided by the core module.

C.5.6 External connections

External Connections are secure connections to systems outside of the SAS. The systems considered in this design are the substation operational functions or SCADA over IP connections. These outside systems are considered as untrusted from a security point of view and appropriate security controls are implemented to these systems. These connections are off the core module, utilizing stringent security techniques.

A routing protocol should be used between the SAS and areas not within the SAS, such as Operations and SCADA over IP. For lack of a better alternative, VRRF and static routes provide redundancy.

C.5.7 Segmentation requirements

The proposed network has been broken down into a number of areas called modules. Each of these modules is a network of LANs or VLANs. Routing and firewalling separate each of these modules.

Figure C.8 shows the domains of the substation, without implying a particular physical layout or the redundancy scheme.

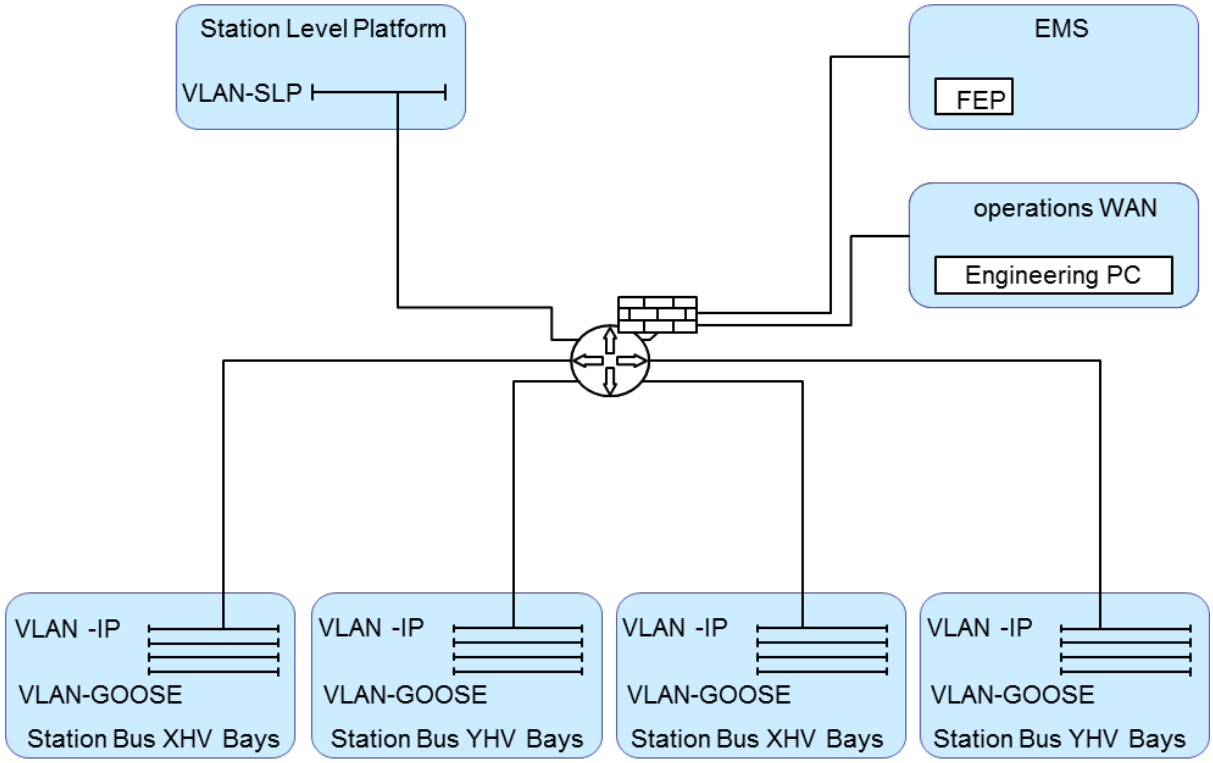


Figure C.8 – Overall VLANs

C.5.8 Station bus and bay domains

The number of domains varies based on the method of defining their use. Traditionally, the purpose of VLANs is to separate traffic and reduce broadcast domains. The approaches that could be used for this purpose are:

- one domain for all traffic where no traffic congestion is expected; or
- one domain for each voltage level and one cross-domain for transformer protection, as shown in Figure C.9;
- one domain per diameter, as shown in Figure C.10.

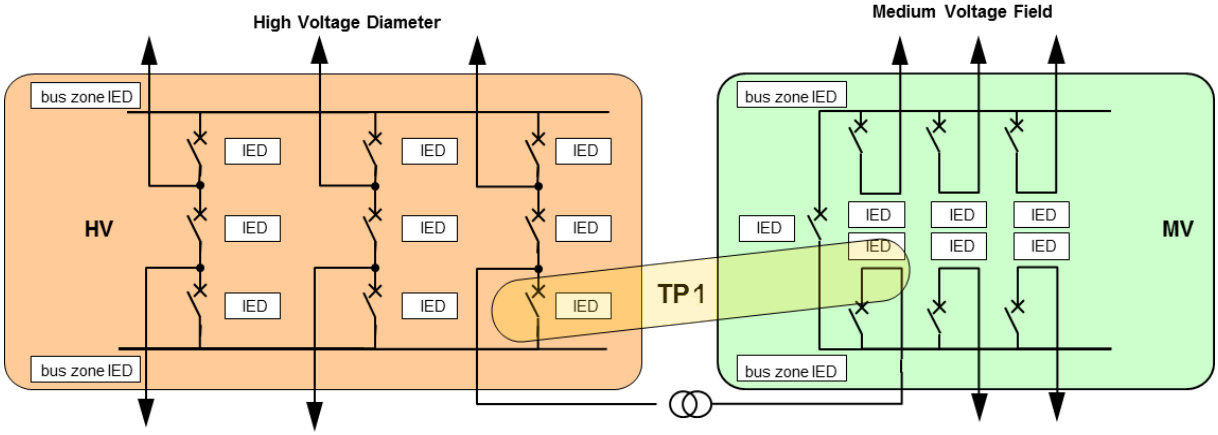


Figure C.9 – Three domains

An assignment of the domains according to Figure C.9 is shown in Table C.5.

Table C.5 – Domain assignment for three domains

Area name	Domain name	Description	Priority	Multicast address
HV	HVS	HV Station Wide		01-0C-CD-01-00-00
TP	TP1_GOOSE	Transformer Protection 1 (optional)		01-0C-CD-01-00-01
LV	LVS	LV Station Wide		01-0C-CD-01-00-02

When the traffic increases more, it is advantageous to assign one domain per diameter, as Figure C.10 shows.

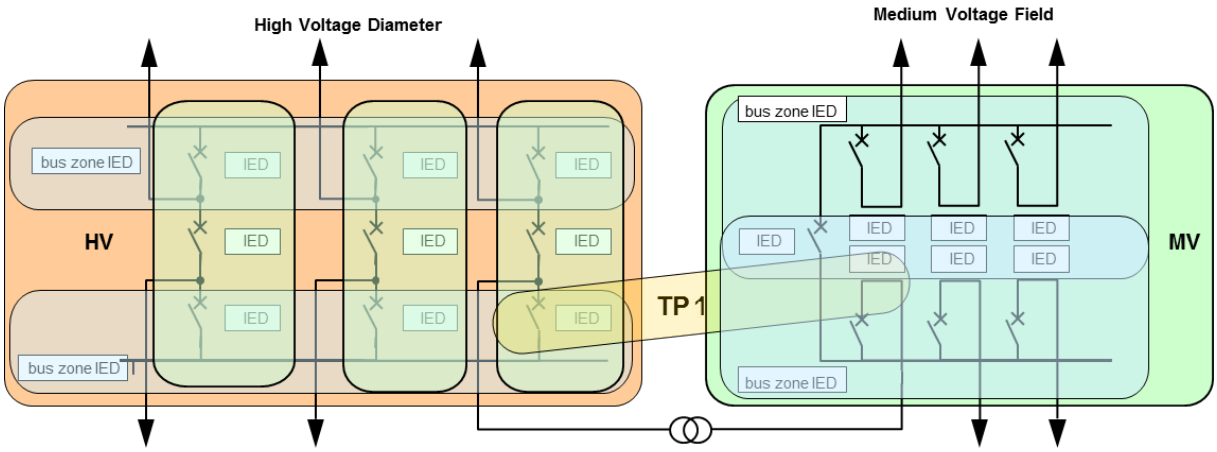


Figure C.10 – One domain per diameter, bus zone and transformer protection

A breakdown of the domains according to Figure C.10 is shown in Table C.6.

Table C.6 – Domain assignment for one domain per diameter

Area name	Domain name	Description	Priority	Multicast address
HV	HVS_GOOSE	HV Station Wide GOOSE		01-0C-CD-01-00-00
D	HVD1_GOOSE	HV Diameter 1 GOOSE		01-0C-CD-01-00-01
D	HVD2_GOOSE	HV Diameter 2 GOOSE		01-0C-CD-01-00-02
D	HVD3_GOOSE	HV Diameter 3 GOOSE		01-0C-CD-01-00-03
BZ	HVBZ1_GOOSE	HV Bus Zone 1 GOOSE		01-0C-CD-01-00-04
BZ	HVBZ2_GOOSE	HV Bus Zone 2 GOOSE		01-0C-CD-01-00-05
TP	TP1_GOOSE	Transformer Protection 1 (optional)		01-0C-CD-01-00-06
LV	LVS_GOOSE	LV Station Wide GOOSE		01-0C-CD-01-00-07
BZ	LVBZ1_GOOSE	LV Bus Zone 1 GOOSE		01-0C-CD-01-00-08
BZ	LVBZ2_GOOSE	LV Bus Zone 2 GOOSE		01-0C-CD-01-00-08

C.5.9 Multicast filtering

Multicast filtering requires a set of access lists on bridge backplanes and/or interfaces to permit only certain multicast frames.

C.5.10 Use of VLANs

Non-IEC 61850 traffic that is not intended for every IED should be placed on different VLANs. Operational WAN should also have an own VLAN.

C.5.11 IP addressing

See 8.1.

C.6 Estimation of the traffic flow

C.6.1 Types of traffic

The three main traffic flows are:

- High Voltage – Intra-diameter;
- Whole of voltage level;
- Inter-voltage level.

Subclause 11.2 of IEC 61850-5:2013 defines message types and performance criteria, a summary of which appears in Table 37 with a mapping to the related interfaces, approximate bandwidth requirements and priority:

C.6.2 GOOSE

For HV, the network traffic on the X or Y network is approximately as follows:

- 15 diameters is worst-case (the most complex substation has 11 diameters).
- Each diameter is made up of 3 bay IEDs per each side X and Y.
- Each side X and Y has 2 Bus IEDs and a few others, with a maximum of 5 per side.
- Therefore the worst case is 50 IEDs per side.
- One IED in steady state sends approximately 300 octets every 500 ms.
- 50 IEDs in steady state have a base network load of 234 kbit/s.
- During a major substation event, all IEDs transmit an additional 5 × 300 octets within 1 s. This loads the network with 50 IEDs transmitting 1 500 octets for 1 s; 50 × 1 500 = 75 000 octets in 1 s which is 586 kbit/s.

So the peak load for the HV station bus is approximately 234 kbit/s {base load} + 586 kbit/s {burst load} = 820 kbit/s.

C.6.3 MMS traffic estimate

For HV, the network traffic on network X or network Y is estimated as follows:

- The largest known substation has 11 diameters, so 15 diameters is worst case.
- Each diameter is made up of 3 bay IEDs per each side X and Y.
- Each side X and Y has 2 × Bus IEDs and a few others, so assume 5.
- The worst case maximum is therefore 50 IED per side.
- An IED in normal state sends approximately 300 octets every 500 ms.

C.6.4 Other services

ICMP – 5 pings/s to all IEDs. 5 × 64 octets/s × (50 {IEDs} + 52 {bridges}) = 255 kbit/s.

SNTP – assuming 100 octets per minute to all IEDs and bridges = 1,33 kbit/s.

SNMP – assuming 3 000 octets every 30 s to 52 bridges = 41 kbit/s.

FTP Services – file transfer: low priority background service in the low priority queue that is allowed to burst to full bandwidth but traffic is dropped if any other services need it.

C.7 Latencies

Table C.7 is a summary of the expected latencies not including queuing latency for each solution with all networks in a non-failed state:

Table C.7 – Summary of expected latencies

Bridge hops	Original		Solution 1		Solution 2	
	Hops	Latency	Hops	Latency	Hops	Latency
HV Diameter	1	32 µs	1	32 µs	3	96 µs
HV Bus	2	64 µs	3	96 µs	3	96 µs
LV Bus	1	32 µs	1 to 3	32 µs to 96 µs	3	96 µs

C.8 Conclusion

Table C.8 shows the expected traffic, which is small enough so that in fact no multicast filtering is needed at all in a 100 Mbit/s network.

Table C.8 – Traffic types and estimated network load

Traffic	Bandwidth required kbit/s
GOOSE – Base	234
GOOSE – Peak	586
MMS – Base	500
MMS – Peak	1 500
Other – ICMP	255
Other – SNTP	1,33
Other – SNMP	41
Other – ASCI	NA
Total	3 117

Annex D
(informative)

Case study – Station bus with VLANs (Trans-Africa, South Africa)

D.1 General

D.1.1 Normative aspects

This engineering of the data network in this IEC 61850 substation captures particular requirements and shows how non-IEC 61850 traffic is being considered with the help of VLANs. Design decisions in Annex D differ in some respects from the engineering guidelines.

The present tense is used also to express a design requirement, to distinguish it from a normative requirement (“shall”, “may”) or a normative recommendation (“should”).

D.1.2 Background

The case study considers four new substations in the southern part of the African continent. The substations provide electrical supply to the new mines being built in the area. The substations are named Substation-A, Substation-B, Substation-C and Substation-D.

D.1.3 Electrical network overview

The substations are laid out linearly with the main EHV feed at Substation-A.

Substation-A is a 220/132/33 kV substation with the following equipment requirements:

- 1 × 220 kV 18-bay bus zone scheme.
- 1 × 132 kV 18-bay bus zone scheme.
- 1 × 132 kV feeder (4-terminals at Substation-A, Substation-C, Substation-B and Substation-D).
- 2 × 220/132 kV 120 MVA transformers.
- 2 × 132/33 kV 60 MVA transformers.
- 1 × 220 kV feeder.
- 1 × 220 kV bus coupler.
- 1 × 132 kV bus coupler.
- 2 × 33 kV feeders.
- 1 × 33 kV bus coupler.

Substation-C is a 132 kV/11 kV substation with the following equipment requirements:

- 1 × 132 kV feeder (4-terminals at Substation-A, Substation-C, Substation-B and Substation-D).
- 1 × 132/11 kV 10 MVA transformer.

Substation-B is a 132 kV/11 kV substation with the following equipment requirements:

- 1 × 132 kV feeder (4-terminals at Substation-A, Substation-C, Substation-B and Substation-D).
- 1 × 132/11 kV 10 MVA transformer.

Substation-D is a 132 kV/11 kV substation about 55 km from Substation-A with the following equipment requirements:

- 1 × 132 kV 6-bay bus zone.
- 1 × 132 kV feeder (4-terminals at Substation-A, Substation-C, Substation-B and Substation-D).
- 2 × 132/11 kV 40 MVA transformers.
- 2 × 11 kV feeders.
- 1 × 11 kV bus coupler.

D.1.4 Substation communication overview

Communications from Substation-A to Substation-C, Substation-B and Substation-D is achieved by means of an OPGW single mode fibre optic cable. The 24-fibre cable allows for sufficient fibre cores for teleprotection and other communication to the substations. Of the remaining fibres, the substation automation network uses four fibres at each substation.

D.1.5 Design and project objectives

This project aims for installing a cost-effective and reliable substation automation network using current technology and in-line with industry best practice.

The objectives of this design are as follows.

- Describe the detailed design of the network with appropriate technical drawings of cabinet layouts and the network topology of all equipment and systems proposed under this scope of work.
- Describe the configuration of the network equipment providing the communications infrastructure for the substation automation network as described in the detailed design to ensure the best possible performance and the highest possible resilience to component or system failures.
- Provide real-time network information to operators and automation engineers which can be integrated into the HMI systems.
- Provide a centralized Network Management System (NMS) for the management of the automation network. The NMS is also required to provide configuration management for the network device configurations and the firmware for each network device.
- Provide secure remote and corporate access to the substation automation network for system engineers and specialists.

D.2 Conceptual design

D.2.1 Substation automation networks

The fundamental design criteria for the implementation of the substation automation networks are high availability, high reliability and maintainability.

High availability is achieved by means of a redundant device and cabling design where this is practically achievable.

High reliability is achieved by product selection based on industrial networking principles and guidelines. The product selection should meet certain minimum build-quality and design-quality criteria.

Maintainability is achieved through a suitable network monitoring and configuration management.

D.2.2 Design parameters

The network is built with rugged industrial Ethernet technology compliant to all or most of the following typical requirements:

Rated for reliable operation in harsh electrical environments:

- IEC 61850-3 and IEEE 1613 (Electric power substations).
- IEC 61000-6-2 and IEC 61800-3 (Industrial environments).
- NEMA TS 2 (Traffic control equipment).

Rated for error free operation in high EMI environments:

- IEEE 1613 Class 2 error free performance under EMI stress for fibre-based networking devices.
- Fibre optic ports should support both short and long haul fibre.

Rated for operation over a wide temperature range:

- –40 °C to 85 °C (+185 °F).
- Passive cooling – no fans.
- CSA/UL 60950 safety approved to +85 °C (+185 °F).

Rated for high availability:

- Integrated single or dual redundant power supplies.
- Wide input range: 24 V=, 48 V=, (88 V= to 300 V= or 85 V~ to 264 V~).
- Dual power supplies should be powered independently, from different input supplies.

Rated for industrial installations:

- Galvanized steel enclosure for durability and impact protection.
- Heavy duty steel DIN rail mount or 19” rack mount.
- Industrial terminal blocks for power and I/O connections.

D.2.3 Network topology and redundancy

The design topology of the automation network upgrade is based on a switched Ethernet design using a hierarchical approach. The topology is based on a redundant backbone with redundant cabling between the backbone switches and the bay level/edge switches (see Figure D.1). This dual-star topology provides a flexible upgrade path and installation simplicity.

The dual backbone design offers strong resilience and low failover time. The standard Rapid Spanning Tree Protocol (RSTP) is used for redundancy management.

The bay level switches are not redundant as this does not offer any benefit considering that many of the IEDs do not provide for redundant network connections. Figure D.2 gives more details.

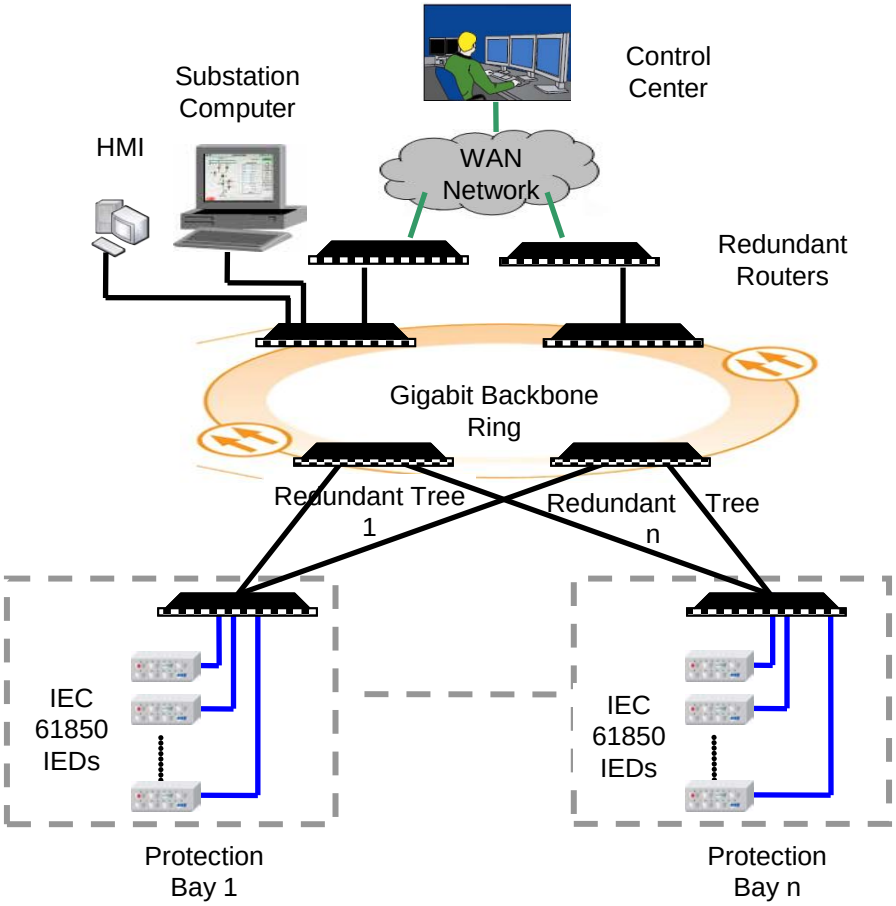


Figure D.1 – Conceptual topology of substation LAN network with redundancy

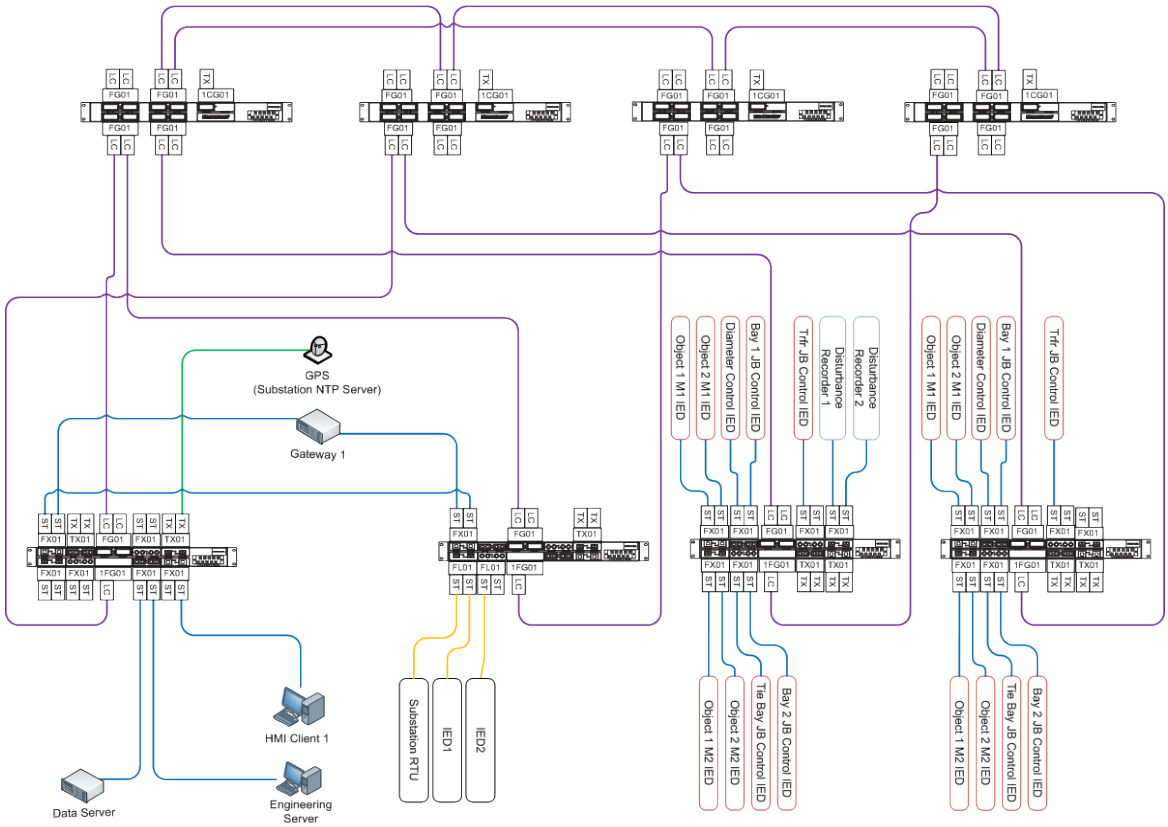


Figure D.2 – Detailed topology of substation LAN with redundancy

D.2.4 Interface standards

D.2.4.1 Fibre cabling

Network cabling uses 12-fibre 50/125 μm multimode fibre-optic cable (100BASE-FX) for connections to edge devices and connections use LC-type connectors on the switch side and the appropriate connector on the edge device side (typically ST connectors). Fibre cable connections between switches use 50/125 μm multimode fibre-optic cable (1000BASE-SX) with LC-type connectors.

Where connections are made to fibre cables between panels, a patch lead with an LC connector on both ends connect the switch port to a mid-coupler in a fibre patch panel. The multimode fibre cable between the panels uses LC connectors at both ends and terminates at mid-couplers in patch panels.

All cabling is identified as per the appropriate labelling standard.

D.2.4.2 Network connections

Lower-tier switches and the IEDs are connected by multimode fibre optic cables using LC connectors on the “switch” end. As most IEDs use ST connectors, LC-ST patch cable are used if the appropriate (LC) connector is not available on the IED end.

The use of copper cable for Ethernet connections is discouraged and is limited to inter-links between switches and devices contained within the gateway panel and in such cases it uses Category 6 (Cat6) Shielded Twisted Pair cables. Other copper cabling is only used for temporary engineering access. Copper patch leads are terminated as per TIA/EIA 568A.

D.2.4.3 Patch panel implementations

For termination of fibre-optic cables between panels, an intermediate patch panel is used at both ends. The cables are terminated with LC connectors and the patch panel/mid-coupler are LC/LC. Fibre patch leads carry LC connectors on both ends.

Fibre-optic fly-leads or patch leads are not used between panels or panel suites even if they are located within the same building. The only exception is when the patch lead is used to connect equipment located in different panels within the same panel suite and provided that the patch lead is suitably “ruggedized” and is run in the bus-wiring conduits.

Fibre-optic cable splicing is executed by suitably qualified personnel and a record of all splices is kept in the Utility documentation.

D.2.4.4 LAN switch port speed and duplex configuration

To minimise potential problems with device connectivity, the following speed and duplex settings are recommended.

D.2.4.5 VLAN numbering

This network is configured with 9 port-based VLANs (and possibly more), as summarized in Table D.1.

Table D.1 – VLAN numbering and allocation

VLAN ID	Usage
100	Dedicated management – reserved for the management interface of the network switches and substation router(s).
101	Substation Automation – devices that are included in this range are Protection IEDs, Substation Data Gateway(s), Station RTU(s), GPS receivers with embedded NTP servers, Tele-protection devices, Human Machine Interfaces (HMIs), Bay Level Controllers and Terminal Servers.
102	IP Telephony – IP Telephones and VoIP gateways.
103	IP Cameras – IP cameras and Digital Video Recorders.
104	Security and Access Control systems.
105	SCADA – this VLAN will be used for IP-based real-time communications to the control centres.
106	Future IEC 61850 process bus communications – devices in this range would include intelligent switchgear and merging units.
200..205	One or more VLANs for WAN links.
110	Engineering which includes devices such as Disturbance Recorders, Engineering Workstations, Engineering Laptops, Test Sets, Condition-based Monitoring systems, Terminal servers, Authentication servers and Travelling Wave fault locators.

D.2.4.6 MAC address allocation

Tagged frames containing VLAN IDs as used by GOOSE messages use VIDs = 2 to 50 with VID = 3 used for intra-bay GOOSE messages.

GOOSE multicast MAC addresses is of the form 01-0C-CD-01-ab-cd,
where the range for “ab” is 00 to 01 and “cd” is 00 to FF.
“ab” is the feeder number, “c” is the relay number and “d” is the GOOSE number.

D.2.5 Inter-VLAN routing

In a network designed with VLANs, different IP subnets need to be allocated to each VLAN. Routing between VLANs is only possible where a VLAN-aware router is installed in the network environment.

Configuring the router's virtual interfaces associates an IP address with a virtual LAN interface identified by its VID. Once all these virtual interfaces are defined, routing becomes possible as the router is "connected" to all the relevant virtual LANs. The Substation Automation Network Security Standard recommends using Access Control Lists (ACLs) between interfaces.

D.2.6 Network quality of service policies

Quality of Service (QoS) is required to ensure appropriate marking and treatment of Substation Automation traffic and normal data across the network. QoS is implemented in tagged Ethernet frames to provide prioritisation of traffic on a switched Ethernet network as defined in IEEE 802.1Q. QoS is also implemented in the IP header (see D.2.9) which is designed to give end-to-end prioritisation of traffic that travels over multiple LAN and WAN links.

The network has been designed to provide 1 000 Mbit/s throughput between the core (backbones) and the bay switches although an effective 100 Mbit/s is achievable end-to-end. QoS prevents oversubscription of backhaul links and prioritise real-time traffic. This is achieved by means of Ethernet prioritisation as per IEEE 802.1Q.

Mapping of priority to CoS (Class of Service) is the mechanism whereby the three priority bits in the Ethernet frame as per IEEE 802.1Q are mapped to the broader categories of Critical, High, Medium and Normal. A fair-weighted queuing philosophy allows lower priority frames to be transmitted in a ratio of 8:4:2:1 thereby allowing fair access to all traffic priorities without negatively impacting the higher priority frames. Table D.2 shows an example ot prioritization.

Table D.2 – Prioritization selection for various applications

Priority	QoS	Typical application
7*	Critical	Network management (applied to management VLAN).
6	High	GOOSE messages used for tripping and inter-tripping.
5	Medium	GOOSE messages used for interlocking merging units.
4	Medium	GOOSE messaging used for other purpose than tripping or interlocking.
3	Medium	Substation Automation (applied to Substation Automation VLAN).
2	Normal	Engineering (applied to Engineering VLAN).
1	Normal	Quality of Supply metering.
0	Normal	Security systems, meters, IP cameras.
*7 is highest priority, 0 is lowest priority.		

NOTE Although 8 priorities are used, only three categories of different priorities are effectively needed.

D.2.7 IP Traffic prioritization and differentiated services (DiffServ)

This solution leverages the new IETF definition of the IPv4 Type of Service (ToS) octet in the IP header by utilizing the Differentiated Services Code Point (DSCP) field to classify packets into any of the 64 possible classes. The packet classification determines the router's treatment of the packet as per IETF-defined Per-Hop Behaviours (PHBs) including Assured Forwarding (AF) and Expedited Forwarding (EF). Traffic that is characterized as EF receives the lowest latency, jitter and assured bandwidth services which are suitable for applications such as Voice over IP (VoIP). AF allows carving out the bandwidth between multiple classes in a network according to the desired policies.

QoS policies allow critical applications to receive the appropriate portion of resources, while ensuring that other applications are not neglected. By classifying the application traffic into premium, gold, silver and other classes, a baseline methodology is set to provide end-to-end

QoS. DiffServ enables this classification by utilizing the DSCP field. Using DiffServ, a properly designed network can deliver assured bandwidth, low latency, low jitter and packet loss for voice while simultaneously ensuring slices of available bandwidth to other classes.

Table D.3 shows a mapping of applications to service levels as an example.

Table D.3 – Mapping of applications to service levels

Application	Service
SCADA/Automation	Gold
Management	Silver
Undefined	Bronze
Data	Best Effort

D.2.8 Packet classification

Packets entering a DiffServ domain or region (collection of DiffServ routers) can be classified in a variety of ways – including layer 4 protocol and port numbers, IP precedence, and layer 2 information (such as Ethernet 802.1Q bits). Once these packets are classified, they can be processed, conditioned and marked.

D.2.9 Packet marking

The IPv4 Type of Service (ToS) octet has been redefined from the 3-bit IP-precedence (see Figure D.3) to a 6-bit DSCP field (see Figure D.4). Packets can be marked with an arbitrary DSCP value or predefined standard values, corresponding to the appropriate AF, EF or user defined class (see Table D.4). For example, EF is designated by the codepoint "101110". The codepoint for best-effort traffic is set to "000000".

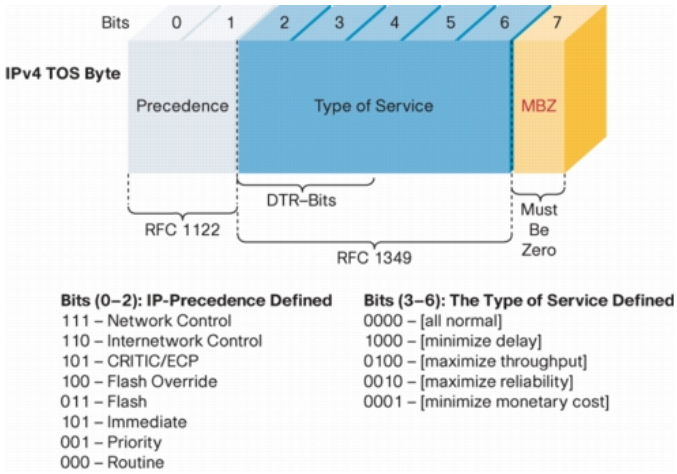


Figure D.3 – Original IPv4 Type of Service (ToS) octet

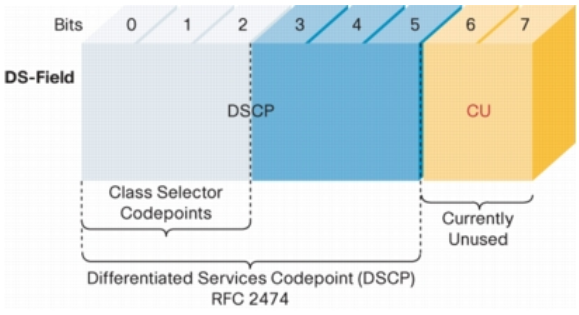


Figure D.4 – Differentiated Services (DiffServ) codepoint field

Table D.4 – List of DiffServ codepoint field values

Name	Dec	TOS	Binary
AF11	10	40	001010
AF12	12	48	001100
AF13	14	56	001110
AF21	18	72	010010
AF22	20	80	010100
AF23	22	88	010110
AF31	26	104	011010
AF32	28	112	011100
AF33	30	120	011110
AF41	34	136	100010
AF42	36	144	100100
AF43	38	152	100110
CS1	8	32	001000
CS2	16	64	010000
CS3	24	96	011000
CS4	32	128	100000
CS5	40	160	101000
CS6	48	192	110000
CS7	56	224	111000
EF	46	184	101110
default	0	0	000000
AF=Assured forwarding			
EF=Expedited forwarding			
CS=Class Selector			

The DSCP mappings shown in Table D.5 are typical of Voice over IP (VoIP) telephony systems. Additional mappings would need to be defined as applications are implemented.

Table D.5 – Example of DSCP to class of service mapping

DSCP	CoS
40	6
46	6

D.2.10 Network IP addressing and device allocations

The IP Addressing Allocation for the Substation Automation Networks is based on the Utility's IP address-plan document applied to a substation based on the previous VLAN allocations.

IP addressing for substation automation devices uses the 10.0.0.0/8 (8 bit network mask) private IP address range.

A substation would be allocated a /21 subnet of the 10.0.0.0/8 IP range. Table D.6 shows an example of the IP address ranges allocation for a Substation A with a range of 10.0.16.0/21.

Table D.6 – Example of DSCP mappings

IP Address / range	Usage
10.0.16.0/25	Management VLAN for network device addressing.
10.0.16.128/25	Engineering services.
10.0.17.0/27	(Future) IP-based SCADA devices.
10.0.17.32/27	Access Control and Security systems.
10.0.17.64/26	Unallocated.
10.0.17.128/25	Unallocated.
10.0.18.0/23	Substation Automation Devices.
10.0.20.0/25	IP telephony.
10.0.20.128/25	IP Cameras.
10.0.21.0/24	Unallocated.
10.0.22.0/23	Future process bus devices.

Graphically, this IP address map is represented in Table D.7.

Table D.7 – Typical substation IP Address map (IP range: 10.0.16.0/21)

<table>
<tr><td colspan="3">10.0.16.0/25 – Network devices – Management
(VLAN 1016)</td><td>10.0.16.128/25 – Engineering
(VLAN 1003)</td></tr>
<tr><td>10.0.17.0/27
SCADA
(VLAN 104)</td><td>10.0.17.32/27
Security
(VLAN 2004)</td><td>10.0.17.64/26
Unallocated</td><td>10.0.17.128/25
Unallocated</td></tr>
<tr><td colspan="4">10.0.18.0/23
substation automation devices
(VLAN 1018)</td></tr>
<tr><td colspan="3">10.0.20.0/25 – IP telephony (VLAN 1001)</td><td>10.0.20.128/25 – IP cameras (VLAN 1002)</td></tr>
<tr><td colspan="4">10.0.18.0/24 – – unallocated</td></tr>
<tr><td colspan="4">10.0.22.0/23
process bus devices
(VLAN 1022)</td></tr>
</table>

D.2.11 IP Address management

IP address management is handled by the Control Applications section.

D.2.12 Network coupling

The automation network is never directly coupled to the corporate/business networks.

A dedicated router with firewall capabilities connects the substation automation network with the business network. This permits remote access from within the Utility business network or via VPN connection to suitably authorised personnel. The firewall keeps access control lists managing traffic flows in a secure manner.

D.2.13 Routing requirements and WAN Interfacing

The Wide-Area Network routing standard is OSPF (Open Shortest Path First) Version 2 as described in RFC 2328. Dynamic routing is considered essential to managing an enterprise-wide routing environment as it minimizes the administrative burden of managing routing tables and provides for dynamic path fail-over in cases of link-loss or other routing metrics as configured.

D.2.14 Network time synchronization

The substations are in the time zone with an offset of +1 h from GMT/UTC.

D.2.15 Network time protocol (NTP)

The Network Time Protocol (NTP) is used for time synchronization of devices that support this protocol. Devices that do not support NTP use direct time synchronization via IRIG signalling from the GPS receiver.

The primary NTP server is the GPS receiver if this one has an embedded NTP server. The Stratum 0 device (GPS receiver) synchronizes the router which in turn becomes alternative NTP time source for synchronizing devices within each VLAN.

In cases where the GPS receiver does not support NTP, the GPS synchronizes via IRIG-B the gateway which becomes the network NTP time source. Devices in such a network are configured to point to the gateway for NTP.

D.2.16 Device management philosophy

D.2.16.1 Management

SNMP collects information and alarms related to environmental, security and performance.

The managed switches support the Simple Network Management Protocol (SNMP) Version 2c as a minimum. SNMP traps are sent to the substation gateway for processing and re-transmission to the control centres.

All switches are enabled to detect a failure in a single channel on a communications circuit connecting to another switch or an end device. Twisted pair cables and fibre-optic cables typically employ distinct transmit and receive channels. The switch can detect a complete device disconnection as well as a single channel failure.

D.2.16.2 Network management system

The management of the Substation Automation Networks from a centralized point is considered essential. An enterprise-grade Network Management System (NMS) platform monitors, configures and maintains the network. The NMS perform a centralised SNMP monitoring service that can monitor services on servers and other devices with an SNMP agent. The NMS can send e-mails and/or SMS notifications.

The Network Management System provides:

- a mechanism to manage all the switch configurations and firmware images;
- centralized management and monitoring of network and networked devices to achieve the highest possible desired level of network availability and performance;
- a scalable system architecture;
- events, alarms and notifications – display network visibility details to enable proactive corrective actions and improved capacity utilization;
- pre-packaged reports for availability metrics and performance metrics as well as providing the tools to create user-defined reports;
- automated network discovery;
- support for SNMP v2c as a minimum.

D.2.16.3 SNMP management and monitoring

The integration of event, alarm and monitoring data for devices that are ancillary to the automation system (i.e. IEDs, etc.) into the SCADA monitoring system is important to operational staff. The devices that provide the network infrastructure, power infrastructure, etc. that can provide data via SNMP are visible in the relevant displays, alarm lists and event lists in the SCADA system from the following devices:

- Environment monitoring equipment;
- Managed Industrial Ethernet Switches;
- Routers;
- Uninterruptible Power Supplies (UPS);
- Linux and Windows-based PCs and Servers;
- Unmanaged device availability (confirmed by means of device “pings”).

SNMP is also used as a core system status metric. The information to be extracted is as follows:

- Real data download throughput of each of the backhaul trunks;
- Real data upload throughput of each of the backhaul trunks;
- Uptime status of all of the edge switch hardware;
- Packet statistics for each of the switch ports;
- Packet loss for each of the switch ports.

Table D.8 lists the SNMP MIBs employed when communicating with a device.

Table D.8 – SNMP MIBs applicable to substation devices

Role	Device	SNMP
client	Gateway	Linux and WinXP MIBs
server	Engineering Server	Linux and WinXP MIBs
client	HMI	Linux and WinXP MIBs
router	Router type 1	Vendor specific MIBs
switch	Backbone Switches	Vendor specific MIBs
switch	Lower-tier Switches	Vendor specific MIBs

The SNMP server at the very least supports SNMP v2c. Other features that are of value include:

- Device Auto Discovery (including managed and unmanaged devices).
- Management Information Base (MIB) Import – Provide the facility to import device specific MIB files to allow convenient mapping from MIB addresses to OPC tag names. MIBs would typically be required to access data specific to a device, e.g. the status of a redundant power supply.
- Calculate metrics such as bandwidth utilization and network error rate statistics from raw SNMP data.
- SNMP Traps Support – Many SNMP-manageable devices can be configured to send unsolicited data to network management software systems such as SNMP servers. This reduces the need for the management systems to continuously poll the devices.

D.3 Detailed design: solution specifications for substation-A

D.3.1 General

The following specification provides the specific details of this solution to allow the equipment to be configured, installed and commissioned in line with Utility's and Tran-Africa Projects standards, guidelines and templates.

D.3.2 Physical environment

D.3.2.1 Power supply

All IEDs and networking equipment at Substation-A is supplied by dual 110 V DC supplies.

The Main 1 and Main 2 110 V DC systems provide approximately 8 h of battery backup in case of AC supply failure.

D.3.2.2 Equipment housing

All backbone infrastructure equipment and cabling are rack mounted in the Gateway cabinet.

The cabinets sit level on their stabilising feet and not resting on the casters.

Cable management within the cabinet is provided by horizontal and vertical cable management. To help support cabling vertically in the rack, Velcro loop ties are installed (via cage nut and bolt) at regular intervals in the front "cable space" on both sides of the rack.

Grounding Earth points are provided for the cabinet and equipment housed in the cabinet via a grounding busbar installed at the rear of the rack.

The layout of equipment, cabling and cable management in the cabinet for each area conforms to the drawings provided.

D.3.2.3 Cooling

All the active equipment is cooled via air conditioning units in the substation building.

The active equipment installed in the communications cabinets produces approximately 1 400 W of heat.

D.3.2.4 Environment monitoring

Air temperature and humidity are monitored via sensors.

D.3.2.5 Cabling

Structured cabling throughout the network within control rooms and substations use Shielded Cat6 using solid conductors. Fly leads are Shielded Cat6 using stranded conductors.

Patch lead colours comply with TIA/EIA 568A.

Fibre optic cabling in the substation is multimode cable. Connections between switches use LC-type connectors and connections to end devices use ST-type or LC-type connectors.

All cabling is identified as per the following labelling standard:

[Substation]-[Building]-[Rack]-[Patch Panel]-[Port#]

Substation: Substation-A

Building ID: Control Room

Rack ID: <GW, S01, S02, 5A>

Patch Panel: <A, B, C, etc. from top to bottom of rack>

Port #: <identified in sequence 1,2,3,4 etc.>

EXAMPLE

Sub-A-CR-2A-B-21 → Control Room – Rack 2A – Patch Panel B – Port 21

D.3.2.6 Device naming

Table D.9 outlines an example of the equipment names and management IP addresses. Device names are compliant with the relevant Utility standard.

Table D.9 – Example of device naming

Device type	Hostname	Location
UPS – SUA3000XLI	e.g. aa-bb-ups01	e.g. Carbon Control Room
PDU – AP7952	e.g. aa-bb-pdu01	e.g. Carbon Control Room

D.3.2.7 Interface addressing and allocation

Table D.10 lists as an example the fields recorded for interface addressing.

Table D.10 – Example of interface addressing and allocation

Hostname	Interface	IP Address	Mask	Gateway
aa-bb-ups01	E0	10.81.150.254	255.255.255.0	10.250.1.1
aa-bb-pdu01	E0	10.81.150.253	255.255.255.0	10.250.1.1

D.3.2.8 NTP

Substation-A is in the time zone of an offset of +1 h from GMT/UTC.

Daylight savings is observed in the country starting on the first Sunday in September and ending the first Sunday in April. Daylight Savings Time (DST) adds +1 h to the reference time.

Devices in Substation-A's Substation Automation network are configured to point to {sub-a-sas-ts01} [10.81.1.1] for NTP.

D.3.2.9 SNMP assignment

SNMP is used as a core system status metric.

The required data to extract are as follows:

- real data download throughput of each of the backhaul trunks;
- real data upload throughput of each of the backhaul trunks;
- uptime status of all of the edge switch hardware;
- packet statistics on each of the switch ports;
- packet loss of each of the switch ports;
- etc.

Table D.11 lists the access methods to the devices.

Table D.11 – Example of device access and SNMP assignment

Role	Device	Ping	Http	SNMP
client	Gateway 1	y	-	WinXP MIBS
client	Gateway 2	y	-	WinXP MIBS
client	HMI 1	y	-	WinXP MIBS
client	HMI 2	y	-	WinXP MIBS
router	Router 1	y	y	Vendor MIBS
switch	Backbone Switches	y	y	Vendor MIBS
switch	Field Switches	y	y	Vendor MIBS

D.3.3 Local area network

D.3.3.1 Overview

The core LAN connectivity for the substation automation network is provided by four backbone switches located in the Gateway panel in the Substation control room.

Redundant switches and Ethernet links are a core design factor of the network.

Bay level or edge switches include the following:

- 2 × UTP ports for engineering access;
- 2 × multimode fibre ports with LC connectors for uplink connections to the backbone switches;
- sufficient multimode fibre ports with ST or LC connectors for IED connectivity;
- plus 25 % spare port capacity.

The field switches provide 100 Mbit/s network connectivity back to the core.

The LAN is configured with VLANs to separate and identify different traffic/device types. QoS is used to mark and prioritise automation traffic (e.g. GOOSE messages) over normal data traffic.

Other switch requirements include:

- Backbone Switches, duplicated for redundancy;
- Edge/field Switches, not duplicated for redundancy although fibre connections back to the backbone switches are;
- IGMP Snooping (V2 as a minimum);
- Rapid Spanning Tree, except on end user ports;
- DHCP Spoof guard;
- MAC flood protection (2 MAC addresses per user port);
- Storm Control (basic).

D.3.3.2 Hardware table

All network equipment deployed in the substation automation network is listed in the hardware table. Table D.12 is a template that records the equipment part number, the equipment order code (if different from the part number), the description of the equipment, the quantity and the location of the equipment.

Table D.12 – Example of hardware identification

Part No	Description	Qty	Bay Detail
RSG2200-R-RM-HIP-HIP-FG01-FG01-FG01-FG01-1CG01	Backbone Switch 1	1	Gateway

D.3.3.3 Power supplies

Each switch is powered by dual 110 V DC supplies. Each switch has a dedicated, appropriately rated 300 V DC miniature circuit breaker for the M1 supply and a separate miniature circuit breaker for the M2 supply.

D.3.3.4 Device naming

A device name table ensures that all devices are allocated a unique device name. These names are the same as on network drawings to unambiguously identify devices. Table D.13 gives an example of a device names table.

Table D.13 – Example of device name table

Device type	Hostname	Location
Ethernet Bridge Type 1	sub-a-sas-bsw01	Substation-A SAS Backbone Switch 1
Ethernet Bridge Type 1	sub-a -sas-s01-sw01	Substation-A SAS Scheme 1 Bay Switch 1
Ethernet Bridge Type 2	sub-a-sas-rio1-sw01	Substation-A SAS Remote I/O Unit for Mine Switch 1
HMI Type 1	sub-a-sas-hmi01	Substation-A SAS HMI 1
Gateway Type 1	sub-a -sas-gw01	Substation-A SAS Gateway 1
Time Server 1	sub-a-sas-ts01	Substation-A SAS Time Server 1
Engineering Workstation	sub-a-sas-ews01	Substation-A Engineering Workstation 1
Router Type 1	sub-a-sas-rx01	Substation-A SAS Router 1
IED Type 1	sub-a-sas-s01-ied1	Substation-A SAS Scheme 1 IED 1
IO Type 1	sub-a-sas-s03-io1	Substation-A SAS Scheme 3 I/O Unit 1
BCU Type 1	sub-a-sas-s04-bcu1	Substation-A SAS Scheme 4 BCU 1
……	……	……

D.3.3.5 Firmware and software versions

All firmware and software version numbers are recorded by equipment type and version number. Table D.14 shows an example.

Table D.14 – Example of firmware and software table

Device role	Device type	Version
Backbone Switches	RSG2200	v3.7.1
Bay Level Switches	RSG2100	v3.7.1
Router	RX1100:- ROX	v1.14.1

D.3.3.6 Interface addressing and allocation

Network equipment configuration details are recorded in a table, each device is identified by the hostname and information related to IP addressing, subnet masks and the VLAN ID associated with the VLAN to which the equipment is connected. Table D.15 shows an example for the bridge “sub-a-sas-bsw01”.

Table D.15 – Example of interface addressing and allocation

Hostname	Interface	IP address	Mask
sub-a-sas-bsw01	VLAN 10 (Management Interface)	10.81.150.1	255.255.255.0
sub-a-sas-bsw02	VLAN 10 (Management Interface)	10.81.150.100	255.255.255.0
sub-a-sas-s01-sw01	VLAN 10 (Management Interface)	10.81.150.101	255.255.255.0
sub-a-sas-s02-sw01	VLAN 10 (Management Interface)	10.81.150.102	255.255.255.0
sub-a-sas-s03-sw01	VLAN 10 (Management Interface)	10.81.150.103	255.255.255.0
…	VLAN 10 (Management Interface)	10.81.150.104	255.255.255.0
sub-a-sas-s(m)-sw(n)	VLAN 10 (Management Interface)	10.81.150.105	255.255.255.0
sub-a-sas-s01-io1	VLAN 1722 (SAS Interface)	172.17.2.2	255.255.255.0
sub-a-sas-s01-io2	VLAN 1722 (SAS Interface)	172.17.2.3	255.255.255.0
sub-a-sas-ts01	VLAN 1722 (SAS Interface)	172.17.2.4	255.255.255.0
sub-a-sas-s01-ied01	VLAN 1722 (SAS Interface)	172.17.2.10	255.255.255.0
…	…	…	…

Network switch details are listed in a separate table for each switch. The table lists the interface module type, the slot number occupied by the interface module, the port number, the device attached to the port, the interface name on the attached device as well as the port description which is configured in the switch port configuration. Table D.16 shows an example of interface allocation for Ethernet bridge “sub-a-sas-bsw01”.

Table D.16 – Example of network switch details

Module	Slot	Port	Device	Device interface	Port description
FX07	1	1	sub-b-sas-s01-sw01	Port 2	Link-to-sub-b-sas-s01-sw01
FX07	1	3	sub-a-sas-rio1-sw02	Port 9	Link-to- sub-a-sas-rio1-sw02
FX02	2	2	sub-a-sas-s01-sw01	Port 1	Link-to- sub-a-sas-s01-sw01
…….	…….	…….	…….	…….	…….

D.3.3.7 VLAN definitions and IP addressing

The substation IP address map is documented and displayed on the network overview drawings. The VLAN ID, the name of the VLAN as configured on the switches, the VLAN description and the IP address range corresponding to the VLAN ID are documented as shown in Table D.17.

Table D.17 – Example of VLAN definitions

VLAN ID	VLAN name	Description	IP Network	Gateway
1	Default	SHUTDOWN	SHUTDOWN	SHUTDOWN
10	Man_Vlan	Substation-A Substation Automation Network Switch Management VLAN	10.81.150.0 / 24	10.81.150.1
1722	sub-a_Vlan	Substation Automation VLAN at Substation-A	172.17.2.0 / 24	172.17.2.1

D.3.3.8 IP Routing

The information related to inter-VLAN routing and the WAN routing is specified in a table as shown in Table D.18. This configuration applies to the substation router and details the router's hostname, the routing protocol in use for the portion of the routing table described, and the routing entries associated with the portion of the routing table described.

Table D.18 – Example of IP routing

Device	Routing protocols	Route entries
aa-bb-bsw01	OSPF	
aa-bb-bsw01	Connected	VLAN 10, 1722

Dynamic OSFPv2 routing protocol is used at the router.

D.3.3.9 QoS

Enable QoS to ensure appropriate marking and treatment of Substation Automation traffic and normal data across the network.

The network has been designed to give a minimum throughput of 100 Mbit/s between the core and an end device. QoS prevents oversubscription of backhaul links and prioritises real-time traffic. Table D.19 shows the mapping.

Table D.19 – Example of QoS mapping

Device/Port	Service	QOS
Automation	Gold	8
N/A	Silver	7
Management	Bronze	6
Data	Best Effort	1
* 8 is highest priority, 1 is lowest priority.		

D.3.3.10 DHCP

DHCP is used on the network for IP address allocation for VPN clients and for engineering access. The DHCP server is the router. All devices are allocated static IP addresses.

D.3.3.11 Trunk and link aggregation

Link aggregation bundles according to IEEE 802.3 are configured across multiple switch ports which have an identical configuration (e.g. the same VLAN information and the same trunk information).

Each bundle is configured as “desirable” at one end, and as “auto” at the other. The end closest to the core is configured as “desirable”. If the link is horizontal (e.g. the link between two area core switches) then the 'a' side switch should be set to “desirable”.

The group number is a unique number on the switch. For a point to point link with a single VLAN, the group number is configured to be the same as the VLAN of the link. If the link is a trunk, then the VLAN ID of the native VLAN is used. Where the same set of trunked VLANs are configured on multiple bundles on the same switch, then once the native VLAN has been used, all the other VLANs are used in order.

Link Aggregation Control Protocol (LACP) standardises the direction of the LACP negotiation, so that the bundles are all configured consistently on each switch. When trouble shooting, any anomaly is easier to detect and correct without the need for logging on to both ends of every link.

Care must be taken that if the group number already exists on the switch, the original ports and the new ports do not end up in the same group. Table D.20 shows how the table is structured.

Table D.20 – Example of trunk and link aggregation table (void)

Device	Interfaces	Channel number	Device	Interfaces	Channel number
Not required for this site at this stage					

D.3.3.12 LAN Switch Port Speed and Duplex Configuration

The port speed and configuration is recorded as shown in Table D.21.

Table D.21 – LAN switch port speed and duplex configuration

HMIs, Gateways, Time Servers and Engineering Workstations	
Connection	Speed [Mbit/s] / Duplex
All devices fixed	100 / Full
Trunks	
Connection	Speed / Duplex
Trunk connections	100 / Full
IEDs, BCUs, IO Devices	
Connection	Speed / Duplex
All devices fixed	100 / Full
Backbone Interlinks	
Connection	Speed / Duplex
All devices fixed	1 000 / half
Engineering PCs	
Connection	Speed / Duplex
All devices auto negotiate	auto / auto

D.3.3.13 LAN Switch port security Settings

The implementation of multiple security layers is considered good practice when implementing substation automation networks. The settings in Table D.22 are recommended.

Table D.22 – LAN switch port security settings

HMIs, Gateways, Time Servers and Engineering Workstations	
Security Setting	Option
No security setting configured on all switch ports which connect to HMIs, Gateways, Time Servers and the Engineering Workstation	MAC Address filtering
Trunks	
Security Setting	Option
No security setting configured on trunk ports.	None
IEDs, BCUs, IO Devices	
Connection	Option
No security setting configured on all switch ports which connect to IEDs, BCUs and IO devices	MAC Address filtering
Backbone Interlinks	
Connection	Option
No security setting configured on all backbone interlink switch ports	None
Engineering PCs	
Connection	Option
802.1x security configured on all Engineering PC connection ports	Authentication is via the RADIUS server with the corporate Active Directory as backend.

D.3.3.14 Rapid Spanning Tree

The topology of the Substation-A Automation network has been designed so that all bay level switches have a physical loop to two backbone switches. The network is designed to rely on a consistent spanning tree topology to ensure network resilience to port, cable or switch failure. Spanning tree is also required as a precaution against incorrect patching and future changes and should be configured in the following way.

For point to point links, the backbone switch is the root bridge.

All root bridges have their priority set to 8192, and secondary root bridges set to 16384 by using the appropriate configuration parameter.

To reduce delays in workstation, IED and Gateway, the port is configured as an edge port on all end-node switch ports. All other switch ports, including those not yet in use, are not configured as edge ports.

When a switch port is enabled, it goes through the normal spanning tree process of listening/learning/forwarding. For switch ports that are connected to known end stations, this process is superfluous, and only delays the forwarding of packets to and from the end station.

Setting a port as an edge port allows a port to avoid the listening and learning process so that it moves directly to the forwarding state. When using this setting on a link between switches, care must be taken to avoid creating spanning tree loops.

D.3.3.15 Network Security Enhancements

D.3.3.15.1 DHCP Snooping

DHCP Snooping prevents a rogue DHCP server from issuing IP addresses to clients. Specific interfaces are configured to allow DHCP servers. All other interfaces are configured to deny all DHCP offer messages. Table D.23 shows the corresponding table.

Table D.23 – Example of DHCP snooping

Device	Ports	DHCP server
sub-a-sas-bsw01	7	Router 1
sub-a-sas-bsw04	7	Router 1

D.3.3.15.2 Storm Control

Storm Control restricts the number of broadcast and/or multicast packets which could inundate a network and degrade its overall performance. Table D.24 shows an example of settings in a bridge.

Table D.24 – Example of storm control table

Device	Ports	Multicast flood level	Broadcast flood level
sub-a-sas-bsw01	1 – 19	8 000	2 000
sub-a-sas-bsw02	1 – 19	8 000	2 000
sub-a-sas-bsw03	1 – 19	8 000	2 000
sub-a-sas-bsw04	1 – 19	8 000	2 000

Storm Control is enabled on all compatible switches as per the provider's requirements.

D.3.3.16 Link Layer Discovery Protocol (LLDP)

The Link Layer Discovery Protocol (LLDP) is a vendor-neutral layer-2 network protocol which allows connected equipment to share information about other directly connected equipment such as the operating system version and IP address.

LLDP is configured on all links between network equipment and disabled on all connections to IEDs, HMIs, time servers, BCUs and Engineering ports.

D.3.3.17 Authentication

Authentication via ssh CLI and https interfaces are configured per switch with the predefined user and password.

Bibliography

[1] IEC 60044-8:2002, *Instrument transformers – Part 8: Electronic current transformers*

[2] IEC 61508-1, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*

[3] IEC 61850-10, *Communication networks and systems for power utility automation – Part 10: Conformance testing*

[4] IEC 61850-90-2, *Communication Networks and Systems in Substations – Part 90-2: Using IEC 61850 for the communication between substations and control centres*[8]

[5] IEC 61850-90-12, *Communication Networks and Systems in Substations – Part 90-12: Wire Area Network engineering guidelines*[9]

[6] IEC 61869-9, *Instrument Transformer – Part 9: Digital interface for instrument transformers*[10]

[7] IEC 61918:2010, *Industrial communication networks – Installation of communication networks in industrial premises*

[8] ISO/IEC 7498-1:1994, *Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model*

[9] IEEE 610.7-1995 – *IEEE Standard Glossary of Computer Networking Terminology*

[10] IEEE PSRC H12 Report R10, *Report on Configuration of Ethernet Networking Devices Used for P&CI in Electrical Substations,* 2001 December 11

[11] EPRI, *System & Network Management*, (J. Hughes, Kay Clinard, Christoph Brunner, Marco Janssen, John T. (Jack) Robinson)

[12] EPRI Report, "*System and Network Management of Utility Automation Systems,"* Joseph Hughes

[13] Australian Transmission Utilities, *SAS – Architecture Review and Recommendation*

[14] Powerlink, IEC 61850 – *SAS Gen1 Station Bus Network Topology Design Review and Recommendations,* Scott Williamson, 2010 May 14

[15] UCA 61850-9-2, *Implementation Guideline for Digital Interface to Instrument Transformers Using IEC 61850-9-2,* UCA International Users Group, Raleigh, NC, USA

[16] CIGRE Technical Brochure D2.23, *The use of Ethernet Technology in the Power Utility Environment,* Paris, 2011

[17] CISCO-Rockwell, *Ethernet-to-the-Factory 1.2 Design and Implementation Guide*

[18] RFC 959 IETF, File Transfer Protocol

[19] RFC 1034 / RFC 1035, IETF, Domain Name Server

[20] RFC 1918 IETF, Adress Allocation for Private Internet, 1996

---

8 Under consideration.

9 Under consideration.

10 Under consideration.

[21] RFC 2131, IETF, Dynamic Host Configuration Protocol

[22] RuggedCom, *Fibre-optical guideline*

[23] IRIG Standard 200-04 – IRIG Serial Time Code Formats – September 2004, Timing Committee, Telecommunications and Timing Group, Range Commanders Council, US Army White Sands Missile Range, NM

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

Tel: + 41 22 919 02 11
Fax: + 41 22 919 03 00
info@iec.ch
www.iec.ch