

CONTRIBUTING TO SHIFT2RAIL'S NEXT GENERATION OF HIGH CAPABLE AND SAFE TCMS AND BRAKES.

D3.5 – Drive-by-Data Architecture Specification

Due date of deliverable: 31/08/2018

Actual submission date: 14/09/2018

Leader/Responsible of this Deliverable: G. Hans, BTG

Reviewed: Y

Document status		
Revision	Date	Description
1	23/06/2017	Initial version, chapter 1
2	11/08/2017	Added: ch. 2.1, 2.2, 2.3 (partly), 2.4, 2.5, 2.8, 2.9, 3.2.8
3	08/06/2018	Updated with parts already reviewed and with other, lesser innovative parts.
4	22/06/2018	Contributions from CAF and SNCF, Analysis of ETB topologies (former 2.5.3) shifted to new Annex G, Adaptation of Consist Level Quantities (0)
5	13/07/2018	Updated with all contributions received so far
6	23/07/2018	Added ch. 3.2.2
7	31/07/2018	Added contributions from CAF (4.2), Siemens (2.3.1, 3.2.1, 3.3.1) and ASTS (3.5.6, 4.3, 4.4)
8	10/08/2018	Update with respect to comments received from S4R (CTA-T3.5-X-BTD-061-02) and with respect to peer review comments (CTA-T3.5-R-BTD-063-02); update of quantities (Table 5, Table 6)
9	17/08/2018	Added contributions from Siemens (3.2.9, 3.5.3), final quality check Prepared for TMT Review
10/11	11/09/2018	Update after TMT Review / S4R review (comments collection: CTA-T3.5-R-BTD-066-03).
12	14/09/2018	Final version

Project funded from the European Union's Horizon 2020 research and innovation programme

Dissemination Level

PU	Public	
CO	Confidential, restricted under conditions set out in Model Grant Agreement	X

Start date: 01/09/2016

Duration: 25 months

ACKNOWLEDGEMENTS



This project has received funding from the Shift2Rail JU under the European Union's Horizon 2020 research and innovation programme. Grant Agreement no. 730539.

REPORT CONTRIBUTORS

Name	Company	Details of Contribution
Nerea Elorza Daniel Gutierrez	CAF	Sub-chapters: 3.4, 4.2, Annex J Review of all parts
Rainer Mattes	SIEMENS	Sub-chapters: 2.3.1, 3.1.1.3, 3.2.1, 3.2.9, 3.3.1, 3.5.3, 3.5.5.5 Review of all parts
Gernot Hans Thomas Gallenkamp Bernd Brandstetter Benjamin Scherer	BTG	Sub-chapters: 1, 2.1, 2.2, 2.3.2, 2.3.3, 2.4, 2.5, 2.6, 2.7, 2.8, 2.9, 2.10, 3.1.1.1, 3.1.1.2, 3.1.2, 3.1.3, 3.1.4, 3.1.5, 3.2.2, 3.2.3, 3.2.4, 3.2.5, 3.2.6, 3.2.7, 3.2.8, 3.2.10, 3.2.11, 3.3.2, 3.3.3, 3.3.4, 3.3.5, 3.3.6, 3.5.1, 3.5.2, 3.5.4, 3.5.5.1, 3.5.5.2, 3.5.5.3, 3.5.5.4, 3.5.5.6, 3.5.5.7, 3.5.7, 4.1, 5, Annex A, Annex B, Annex C, Annex D, Annex F, Annex G, Annex H, Annex I Review of all parts
Costantino Mariano Fabrizio Cardoni	ASTS	Sub-chapters: 3.5.6, 4.3, 4.4, Annex E Review of all parts
Philippe Laporte Clement Collet	SNCF-M	Sub-chapters: 2.11 Review of all parts
Wolfgang Benner Stefan Tesar	DB	Review of all parts

EXECUTIVE SUMMARY

This report provides the Drive-by-Data architecture specification which has been elaborated within Task 3.5 of the CONNECTA WP3. The Drive-by-Data architecture aims to specify the Next-Generation Train Communication Network (NG-TCN) which is one of the main building blocks of S2R's next generation of TCMS architectures.

The report concludes the work on the definition of the NG-TCN which has been started with requirements collection (deliverable D3.1 [03]) and continued with state-of-the-art analysis (deliverable D3.2 [04]) and RAMS&Security Analysis (deliverable D3.3 [05]). Associated questions related to safety certification are covered in deliverable D3.4 [06]. The work was done in close cooperation with S2R's project SAFE4RAIL WP1 and reflects all the discussions and workshops we had in common with SAFE4RAIL.

In summary, the main achievements of this work are:

- Introduction of a new TRDP traffic class (TSN-PD) for scheduled data traffic based on standard IEEE 802.1Qbv (Time Sensitive Networking TSN). This traffic class is intended to be used for safety critical and latency critical data.
- Time synchronization concept based on IEEE 802.1AS-rev as prerequisite for scheduled traffic.
- Definition of a new network architecture with separated ETB lines and diverse virtual data communication planes (Figure 1) for scheduled data traffic.
- Safe Data Transmission protocol and safety layer definition for the transport of safety critical data up to highest safety integrity levels (SIL4).
- Safe train inauguration concept for train composition discovery with highest safety integrity levels (SIL4).
- Definition of a security architecture and security methods to achieve state-of-the-art cyber security in alignment with actual security standards.

Besides those functional extensions, also improvements with respect to performance (Ethernet links with 10 Gigabit transmission speed) and integration of wireless subnets (e.g. WLAN and WPAN) are considered, preparing the NG-TCN for future IoT applications.

This new NG-TCN architecture allows to replace conventional train lines for train control and provides the capabilities to integrate safety-related sub-systems like the Electronic Distributed Valve (EDV) brake (CONNECTA WP5) and ETCS signalling (X2RAIL project). Due to its ability to transport data of mixed criticality, the same communication infrastructure can be used both for TCMS functions and operator-/customer-oriented services. Furthermore, the possibility to reserve bandwidth for critical data supports the process of incremental certification: non-safety related communication cannot interfere with safety-related communication.

The general objective of removing conventional train lines led to a conflict with the legacy train network architecture defined in IEC61375-2-5. This conflict was resolved with a new network architecture using separated ETB lines, and further analysis of this new architecture revealed also significant improvements with respect to reliability, functional safety and fire safety. A drawback of

this new architecture is its inability to continue communication over powerless consists¹, but the advantages of the new architecture outperform by far this disadvantage.

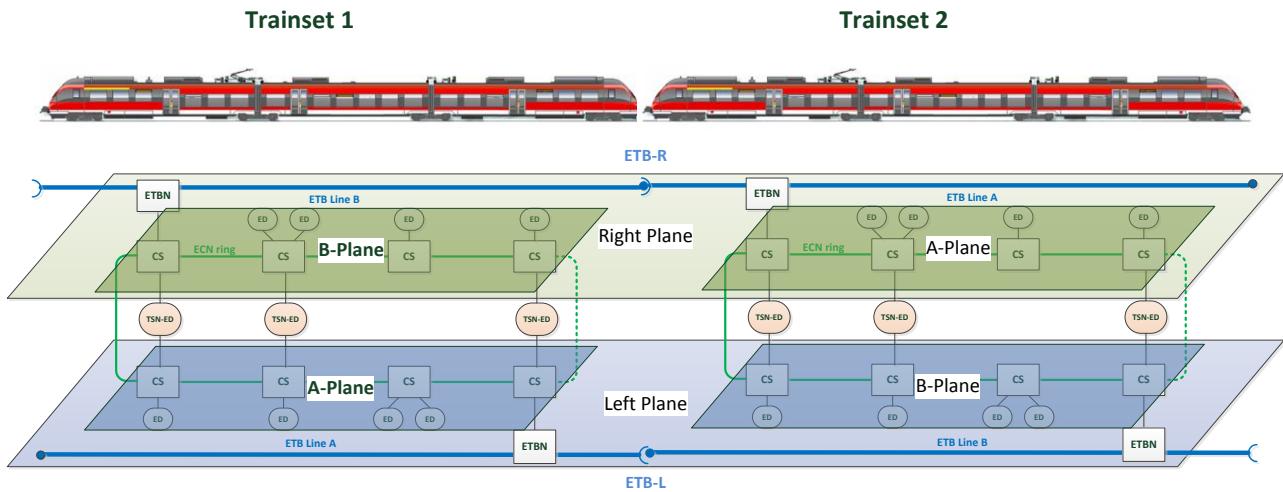


Figure 1: NG-TCN Network with virtual network planes

The achievements of CONNECTA T3.5 help to contribute to S2R's main objectives of cutting life-cycle costs, increasing railway capacity and increasing reliability and punctuality. They also provide the necessary input to launch related standardization activities within IEC TC9 WG43.

¹ Some subsystems like the brake subsystem are required to be active also in this case, which requires a technical solution like for instance a local energy supply.

ABBREVIATIONS AND ACRONYMS

AC	Application Condition
AFDX	Avionics Full Duplex Ethernet
AP	Access Point
ARP	Address Resolution Protocol
ASN.1	Abstract Syntax Notation 1
ATO	Automatic Train Operation
ATP	Automatic Train Protection
AUTOSAR	Automotive Open System Architecture
AV2	ANTIVALENT2
AVB	Audio/Video Broadcasting
BC	Boundary Clock
BCU	Brake Control Unit
BEP	Bit Error Probability
BMCA	Best Master Clock Algorithm
BMS	Bogie Monitoring System
BPDU	Bridge Protocol Data Unit
BSW	Basic Software
CAN	Controller Area Network
CBTC	Communications Based Train Control
CCTV	Closed Circuit Television
CCU	Central/Consist Control Unit
CHAP	Challenge Handshake Authentication Protocol
CO	Consist Orientation
ConsistMC	Consist Master Clock
COS	Customer Oriented Services
CPU	Central Processing Unit

CRC	Cyclic Redundancy Check
CS	Consist Switch
CSM	Crypto Service Manager
CSMA/CD	Carrier Sense Multiple Access / Collision Detection
CTA	CONNECTA project
DA	Destination Address
DCU	Door Control Unit
DHCP	Dynmaic Host Configuration Protocol
DMI	Driver Machine Interface
DNS	Domain Name System
DPDT	Double Pole, Double Throw
DIX	Digital Equipment Corp., Intel Corp. and Xerox Corp.
E2E	End to End
EAP	Extensible Authentication Protocol
ECN	Ethernet Consist Network
ECR	Ethernet Consist network Ring
ECSC	ETB Control Service Client
ECSP	ETB Control Service Provider
ECU	Electronic Control Unit
ED	End Device
ED-S	ED Safe
ED-S.SF	ED-S implementing Signaling Functions.
ED-X	ED-A/ED-B interface
EDV	Electronic Distributed Valve
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
EMU	Electrical Multiple Unit Train
ERTMS	European Railway Traffic Management System

ETB	Ethernet Train Backbone
ETBN	ETB Node
ETBR	ETB Repeater
ETCS	European Train Control System
EVC	European Vital Computer
FCS	Frame Check Sequence
FDF	Function Distribution Framework
FDT	Forwarding Delay Time
FDX	Full Duplex
FFFIS	Form Fit Functional Interface
FIS	Functional Interface Specification
FMEA	Failure Mode and Effect Analysis
FOC	Functional Open Coupling
FT AVG	Fault-tolerant average
GbE	Gigabit Ethernet
GlobalMC	Global Master Clock
gPTP	Generalized Precision Time Protocol
HMI	Human Machine Interface
HSR	High-availability Seamless Redundancy
HST	High Speed Train
HVAC	Heat, Ventilation and Air Conditioning
IANA	Internet Assigned Numbers Authority
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
I/O or IO	Input/Output
IoT	Internet of Things
IP	Internetworking Protocol
IPSec	IP Security

IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISO	International Organization for Standardization
JRU	Juridical Recorder Unit
LACP	Link Aggregation Control Protocol
LAN	Local Area Network
LCC	Life Cycle Cost
LIN	Local Interconnected Network
LLC	Logical Link Control
LRE	Link Redundancy Entity
MAC	Medium Access Control
MC	Master Clock
MC	Multicast
MCG	Mobile Communication Gateway
MCtr	Master Controller
MIB	Management Information Base
MIO	Modular Input/Output
MRC	Media Redundancy Client
MRM	Media Redundancy Manager
MRP	Media Redundancy Protocol
MSTP	Multiple Spanning Tree Protocol
MVB	Multifunction Vehicle Bus
ND	Network Device
NDP	Neighbor Discovery Protocol
NG-TCN	Next/New Generation TCN
NIC	Network Interface Card
NMS	Network Management System
NTP	Network Time Protocol

PRP	Parallel Redundancy Protocol
PTP	Precision Time Protocol
OID	Object Identifier
OOS	Operator Oriented Services
OPC	OLE for Process Control (No longer used)
OPC UA	OPC Unified Architecture
OPEN Alliance SIG	One-Pair Ether-Net Alliance Special Interest Group
OS	Operating System
OSI	Open Systems Interconnection
OTD	Operation Train Directory
PDU	Protocol Data Unit
PCU	Propulsion Control Unit
PDU	Protocol Data Unit
PNAC	Port Based Network Access Control
PoE	Power over Ethernet
PRE	Preamble
PRP	Parallel Redundancy Protocol
RADIUS	Remote Authentication Dial-In User Service
RAMS	Reliability, Availability, Maintainability, Safety
PSE	Power Sourcing Equipment
PTP	Precision Time Protocol
RCT	Redundancy Check Trailer
RF	Radio Frequency
RSTP	Rapid Spanning Tree Protocol
RT	Router
RTE	Runtime Environment
RT-Protocol	Real-Time Protocol
S2R	Shift2Rail

SA	Source address
SAC	Singly Attached Clock
SAN	Singly Attached Node
SC	Slave Clock
SC-32	32Bit CRC-Code with polynomial '1F4ACFB13'
SDSINK	Safe Data Sink
SDSRC	Safe Data Source
SDT	Safe Data Transmission
SDTv2	SDT Version 2
SDTv4	SDT Version 4
SecOC	Secure Onboard Communication
SIL	Safety Integrity Level
SNMP	Simple Network Management Protocol
SOF	Start-of-frame delimiter
StbM	Synchronized Time Base Manager
SPDT	Single Pole, Double Throw
STC	Safe Topography Counter
STM	Specific Transmission Module
STP	Spanning Tree Protocol
SWC	Software Component
TC	Transparent Clock
TCMS	Train Control and Management System
TCN	Train Communication Network
TCP	Transmission Control Protocol
TCXO	Temperature compensated oscillator
TE	Train End
TFFR	Tolerable Function Failure Rate
THR	Tolerable Hazard Rate

TI	Train Inauguration
TLS	Transport Layer Security
TM	TTDB Manager
TND	Train Network Directory
ToS	Type of Service
TRL	Technical Readiness Level
TS	Train Sequence
TRDP	Train Realtime Data Protocol
TSI	Technical Specification for Interoperability
TSN	Time Sensitive Networking
TSN-PD	TSN Process Data
TTDB	Train Topology Database
TTL	Time To Live
UC	Unicast
UDP	User Datagram Protocol
UNISIG	Union Industry of Signalling
UR	Uniform Resource Identifier
UUID	Universally Unique Identifier
VDP	Vital Data Packet
WAP	Wireless Access Point
WLAN	Wireless LAN
WLCN	Wireless Consist Network
WP	Working Package
WPAN	Wireless Personal Area Network
WTCMS	Wireless TCMS
WLED	Wireless End Device
WLTB	Wireless Train Backbone

DEFINITIONS

Conventional	Related to legacy technology (e.g. conventional train lines, conventional data traffic), opposed to the new technologies defined for NG-TCN
TSN Traffic	Scheduled traffic according to IEEE 802.1Qbv

TABLE OF CONTENTS

Acknowledgements.....	2
Report Contributors.....	2
Executive Summary	3
Abbreviations and Acronyms	5
Definitions	12
Table of Contents.....	13
List of Figures	18
List of Tables	22
1 Introduction	25
2 NG-TCN Architecture	28
2.1 General.....	28
2.2 NG-TCN Topology	29
2.2.1 General	29
2.2.2 Network Topology	30
2.3 Network Components.....	32
2.3.1 Classification	32
2.3.2 Functional roles	34
2.3.3 Operational roles	35
2.4 Quantities.....	36
2.5 Train Backbone.....	37
2.5.1 Inter-Consist ETB Interface	37
2.5.2 Consist Internal ETB Topology	37
2.5.3 NG-TCN Train Backbone	38
2.6 Consist Network.....	39
2.7 Connection between train backbone and consist network	40
2.7.1 Network services for train-wide data exchange.....	40
2.7.2 Safety related services	41
2.7.3 ETB/ECN safe train inauguration architecture variants	42
2.7.4 Ethernet Train Backbone Node (ETBN).....	43
2.8 Network interfaces and protocols	44
2.8.1 General	44
2.8.2 Protocol Interfaces	45
2.8.3 List of protocols	45
2.9 Time synchronization	47

2.9.1 General	47
2.9.2 Syntonization vs Synchronization	47
2.9.3 Hardware vs Software implementation	48
2.9.4 Steady state vs. start up and coupling	48
2.9.5 NG-TCN clock domain architecture	48
2.9.6 Clock properties	51
2.10 Security concept.....	51
2.10.1 General	51
2.10.2 System under Consideration (ZCR1).....	52
2.10.3 High Level Cyber Security Risk Assessment (ZCR2).....	54
2.10.4 Security Architecture – Security Zones and Conduits (ZCR3).....	54
2.10.5 Detailed Cyber Security Risk Assessment (ZCR5)	56
2.10.6 Cyber Security Requirements and Counter Measures (ZCR6)	56
2.11 RAMS aspects	56
2.11.1 Reliability.....	57
2.11.2 Availability	59
2.11.3 Maintainability.....	61
2.11.4 Safety	62
3 Communication Layers	64
3.1 Physical layer.....	64
3.1.1 Media (media definition incl. cabling and connectors).....	64
3.1.2 ETB Bypass	71
3.1.3 PoE	71
3.1.4 Sleep mode	72
3.1.5 Security aspects.....	72
3.2 Data Link Layer	72
3.2.1 PDU (Ethernet frame format).....	72
3.2.2 MAC Addressing	74
3.2.3 L2 Switching function.....	75
3.2.4 QoS (Priorities).....	77
3.2.5 Traffic shaping/policing.....	78
3.2.6 Virtual LANs	81
3.2.7 Clock synchronization.....	83
3.2.8 Scheduled traffic (TSN)	89
3.2.9 Redundancy management	98
3.2.10 Train backbone topology discovery	111
3.2.11 Security aspects	126

3.3 Network layer	126
3.3.1 IP addressing	126
3.3.2 IP to MAC address resolution.....	127
3.3.3 IP routing.....	128
3.3.4 ICMP	132
3.3.5 MC group management.....	133
3.3.6 Security aspects	134
3.4 Transport layer.....	134
3.4.1 TCP/UDP	134
3.4.2 UDP/TCP port assignment (Well-known or dedicated ports).....	135
3.4.3 Security aspects	135
3.5 Application Layer.....	135
3.5.1 URI addressing.....	135
3.5.2 Real-time data communication (TSN, TRDP)	137
3.5.3 SIL4 Safe Data Transmission protocol (SDTv4)	139
3.5.4 Safe train inauguration	165
3.5.5 Network application services	182
3.5.6 Network monitoring&diagnosis	202
3.5.7 Security	208
4 NG-TCN Configuration and Set-Up.....	216
4.1 Start-up / shut-down	216
4.2 Network configuration (static)	218
4.2.1 Static data to be configured	219
4.2.2 Requirements and method for network configuration.....	220
4.3 Download	221
4.3.1 Remote configuration download	224
4.3.2 Download of software updates	224
4.3.3 Download of diagnostic information	225
4.4 Service access	226
5 Conclusions	236
5.1 General	236
5.2 KPIs	238
5.3 Open items.....	238
A Annex – Network device capability matrix	240
B Annex – Network performance analysis	242
B.1 General.....	242
B.2 Network performance principles.....	242

B.3	Network Component Characteristics	243
B.4	Estimated expected end-to-end latency in NG-TCN	245
C	Annex – Requirement traceability matrix	247
D	Annex – Input to standardization	257
D.1	Motivation and background	257
D.2	Proposed changes and extensions	257
D.3	Other affected standards	259
E	Annex – Reflection on Signalling subsystem integration.....	260
E.1	Signalling system	260
E.2	Integration of ETCS Signalling components in NG TCN.....	260
E.2.1	ID_60072	265
E.2.2	ID_60074	273
E.2.3	ID_60076	274
E.2.4	ID_60077	278
E.2.5	ID_60079	279
E.2.6	ID_60080	280
E.2.7	ID_60081	280
E.2.8	ID_60083	281
E.2.9	ID_60085	283
E.2.10	ID_60086	285
E.3	Integration of Metro Signalling components in NG-TCN.....	286
E.3.1	ID_60089	286
E.4	Integration of ATO components in NG-TCN	286
E.4.1	ID_60094	286
F	Annex – Proposal for a proof-of-concept test setup	288
G	Annex – Analysis of Consist Internal ETB Topologies	290
G.1	Objective	290
G.2	Use cases	290
G.3	Transmission medium	291
G.4	Inner-consist Architecture Variants	292
G.5	Cost impact	295
G.6	Reliability	297
G.7	Safety	298
G.7.1	Functional safety	298
G.7.2	Fire protection	299
G.7.3	Safety ranking	299
G.8	Functional aspects	299

G.9	Powerless Consist	300
G.10	Conclusions.....	301
H	Annex – Security zones and conduits.....	304
I	Annex – ETB Bypass (for legacy applications)	316
I.1	General.....	316
I.2	Bypass relay circuit.....	317
I.2.1	Bypass relay failure modes (single relay).....	317
I.2.2	Common mode faults.....	318
I.2.3	Physical layer 1000BASE-T versus 100BASE-TX.....	318
I.3	Line redundancy	319
I.4	Relay Control to Optimize Detectability and Availability	320
J	Analysis of single points of failure.....	322
	References	329

LIST OF FIGURES

Figure 1: NG-TCN Network with virtual network planes.....	4
Figure 2: NG-TCN functional domains and interfaces	28
Figure 3: logical Train Network architecture (source [17])	30
Figure 4: Consist network (source [17]).....	30
Figure 5: IEC Compliant Network Topology	31
Figure 6: NG-TCN Topology	32
Figure 7: Consist outer interface	37
Figure 8: Train backbone architecture variants	38
Figure 9: NG-TCN train backbone topology	39
Figure 10: ECN ring topology with dual homing	40
Figure 11: ETB/ECN connection architecture variants	43
Figure 12: ETBN Device	43
Figure 13: NG-TCN ETBN Services (Architecture Variant A)	44
Figure 14: NG-TCN ETBN Services (Architecture Variant C)	44
Figure 15: NG-TCN Protocol Interfaces	45
Figure 16: mixed synchronization domain architecture.....	49
Figure 17: all independent (async) synchronization domain architecture.....	50
Figure 18: one (all sync) synchronization domain architecture	51
Figure 19: NG-TCN Scope Diagram.....	53
Figure 20: Overview of TCMS security zones and conduits	55
Figure 21: Overview of OOS security zones and conduits.....	56
Figure 22: Connections between Reliability, Availability, Maintainability and Safety.....	57
Figure 23: Ethernet 100FDX Physical Interface	65
Figure 24: M12 X-coded.....	67
Figure 25: Standards relating to 10GbE (Source: [49]).....	68
Figure 26: PoE PSE alternative A (from IEEE 802.3)	72
Figure 27: DIX Ethernet Frame	73
Figure 28: IEEE 802.3 Ethernet Frame	73
Figure 29: The Basic IEEE 802.3 MAC Data Frame Format	73
Figure 30: Forwarding process functions (source: [23]).....	75
Figure 31: Token bucket algorithm (illustration).....	79
Figure 32: IEEE1588/IEEE802.1AS two-step timing protocol	84
Figure 33: IEEE1588 one step timing protocol	85
Figure 34: IEEE1588/IEEE802.1AS two-step bridge	85
Figure 35: IEEE1588 peer delay mechanism	86
Figure 36: Error sources in the NG-TCN network.....	87

Figure 37: GlobalMC synchronization startup according to assigned priorities	88
Figure 38: Port control for scheduled traffic (source: IEEE802.1Qbv).....	90
Figure 39: Scheduled flows.....	91
Figure 40: Time Table computation.....	92
Figure 41: A-Plane and B-Plane with redundant devices (ETB Topology D ₁)	93
Figure 42: ECN overlaid with A-Plane and B-Plane.....	93
Figure 43: Link failure in a plane	94
Figure 44: Train-wide TSN Planes	96
Figure 45: TSN over ETB.....	96
Figure 46: Function f _s	98
Figure 47: MRP Ring States (Source: [60])	103
Figure 48: Identical data packets are transmitted simultaneously to both networks (Source: [58])	105
Figure 49: PRP frame format with no VLAN tag (Source: [58]).....	106
Figure 50: Duplicate data packets are transmitted simultaneously in both directions (Source: [58])	107
Figure 51: HSR frame format with no VLAN tag (Source: [58]).....	107
Figure 52: Coupled HSR rings (Source: [58])	108
Figure 53: Frame replication and elimination (Source: [61])	110
Figure 54: Combination of ECN ring and A-Plane / B-Plane.....	114
Figure 55: ETB line redundancy based on link aggregation	115
Figure 56: ETB line redundancy using VLAN reconfiguration	116
Figure 57: ETB line redundancy using VLAN across ECN	117
Figure 58: ETBN setup IEC61375-2-5 or “variant B”	118
Figure 59: Variant D, A-Plane/B-Plane.....	119
Figure 60: ETBN setup Variant D, parallel inauguration	120
Figure 61: ETBN nodes in series (variant B)	121
Figure 62: Consist as a “Black Box”	121
Figure 63: ETBN nodes emulating a serial topology (variant D, centralized inaug.).....	122
Figure 64: Logical connections between ETBNs	122
Figure 65: ETBN B failure scenario	123
Figure 66: Variant D, “centralized” inauguration	124
Figure 67: Variant D, “centralized” inauguration, coupled consists	125
Figure 68: Variant D, “centralized” inauguration, rotation of consist	125
Figure 69: IP Unicast Routing	129
Figure 70: IP Multicast Routing	129
Figure 71: Routing and filtering IP packets.....	131
Figure 72: Dedicated destination ports for UDP/TCP [18]	135

Figure 73: TCN-URI functional addressing scheme (IEC61375-2-3)	136
Figure 74: TSN-PD-PDU.....	138
Figure 75: Safe application and safe communication embedded in ISO/OSI-Reference	141
Figure 76: Communication model SDTv4 used TRDP	142
Figure 77: Communication model SDTv4 used other RT-Format.....	143
Figure 78: SDTv2 Channel valid for SDTv4.....	144
Figure 79: SDTv4 Channel States.....	146
Figure 80: SC-32 Computation.....	148
Figure 81: SC-32 Table.....	149
Figure 82: SDTv4 VDP Variant 1	150
Figure 83: SDTv4 VDP Variant 2	151
Figure 84: CRC1 Computation for VDP Variant 1.....	152
Figure 85: CRC1 and CRC2 Computation for VDP Variant 2	153
Figure 86: CRC1 and CRC2 Computation for VDP Variant 2	154
Figure 87: Redundancy Group (Example with 2 SDSRC)	156
Figure 88: SDSINK state diagram	159
Figure 89: Under-sampling.....	161
Figure 90: Window of expected SSC (example).....	162
Figure 91: Guard time violation (example).....	163
Figure 92: Train directory computation fault tree	166
Figure 93: Services involved in safe train inauguration	167
Figure 94: TTDB computation block diagram (based on IEC61375-2-3)	169
Figure 95: TI Validator block diagram.....	172
Figure 96: Validation train view (example)	173
Figure 97: Independent check with train lines (traditional way).....	178
Figure 98: Independent check with “beacon” telegram.....	178
Figure 99: “Left” and “right” beacon.....	179
Figure 100: BEACON telegram	180
Figure 101: ETB user states	181
Figure 102: DHCP protocol machines.....	184
Figure 103: DHCP session example	185
Figure 104: ETB Control system architecture	188
Figure 105: ETB Control Agent interfaces	189
Figure 106: TTDB Agent interfaces	194
Figure 107: SNMP model.....	196
Figure 108: OID path to the “sysDescr” object	197
Figure 109: TSN Gateway architecture block diagram	200

Figure 110: Multiplexing process.....	201
Figure 111: ETB communication pattern (example)	201
Figure 112: How SNMP Monitoring Works	204
Figure 113: SNMP Details.....	205
Figure 114: Packet Sniffing	206
Figure 115: Illustration of a network-based firewall.....	208
Figure 116: Illustration of a network with host-based firewalls	209
Figure 117: Firewalls in TCMS domain	210
Figure 118: Firewalls in OOS domain.....	210
Figure 119: Symmetric encryption.....	213
Figure 120: Asymmetric encryption	213
Figure 121: PNAC and MACsec overview.....	214
Figure 122: ED start-up state machine.....	217
Figure 123: SNMP set-up for ED, ED-S and ND	222
Figure 124: The three actors of the EAP protocol.....	227
Figure 125: EAP relay mode	227
Figure 126: EAP termination mode	228
Figure 127: Sequence diagram of the 802.1X authentication procedure	229
Figure 128: 802.1X authentication procedure in EAP termination mode.....	231
Figure 129: Train-wide data communication.....	242
Figure 130: Data communication with interfering traffic.....	243
Figure 131: Table 5.1 a as defined in CCS TSI 2016	266
Figure 132: Table 5.1 a as defined in CCS TSI 2016 (cont.)	267
Figure 133: Table A 2.3 as defined in CCS TSI 2016.....	268
Figure 134: Table A 2.3 as defined in CCS TSI 2016 (cont.).....	269
Figure 135: Table A 2.3 as defined in CCS TSI 2016 (cont.).....	270
Figure 136: Table A 2.3 as defined in CCS TSI 2016 (cont.).....	271
Figure 137: Table A 2.3 as defined in CCS TSI 2016 (cont.).....	272
Figure 138: Table A 3 as defined in CCS TSI 2016.....	273
Figure 139 ERTMS/ETCS system and its interfaces	274
Figure 140 Table 1 of train Interface function.....	275
Figure 141 I/O functionality forecast for train interface.	276
Figure 142 Architecture for bus interface regarding Onboard I/O.	277
Figure 143 SDT as referred in Subset 119.....	277
Figure 144 Parallel I/O in the context of NG-TCN.....	278
Figure 145 Possible DMI integration on NG-TCN.....	280
Figure 146 ETCS-JRU interface over NG-TCN.	280

Figure 147 Balise -BTM Antenna-interface.....	281
Figure 148 Down link emission Mask.....	281
Figure 149 “A” Interface	282
Figure 150 Noise for “A” Interface	282
Figure 151 Limit of Noise on “A” Interface	283
Figure 152 Euro loop interface.....	284
Figure 153 Euro Loop Spectrum mask.....	285
Figure 154 Euro radio interface.....	285
Figure 155 ATO integration over NG-TCN	287
Figure 156: CONNECTA-2 Urban Demonstrator.....	288
Figure 157: CONNECTA-2 Regional Demonstrator	289
Figure 158: Topology variant benchmark	301
Figure 159:Bypass Relays, 100BASE-TX, one redundant line shown	316
Figure 160:Bypass Relays, 1000BASE-T , one redundant line shown	317
Figure 161: 3 ETBNs, normal operational mode (100BASE-TX), one redundant line shown.....	318
Figure 162: 3 ETBNs, bypass relay failure (100BASE-TX), one redundant line shown	319
Figure 163: 3 ETBNs, normal operation, redundant line.....	319
Figure 164: 3 ETBNs, failure in middle ETBN	320
Figure 165: Bypass relays 4 groups with 4 relays each.....	320

LIST OF TABLES

Table 1: NG-TCN architecture requirements	29
Table 2: Relevance of the classification for the network components.....	33
Table 3: Functional Roles	34
Table 4: Operational roles.....	35
Table 5: Train Level Quantity	36
Table 6: Consist Level Quantity (preliminary).....	36
Table 7: ECN Topologies – pros and cons	39
Table 8: Network services for train wide communication	41
Table 9: THR of inauguration functions (source: [05]	41
Table 10: List of interface protocols (preliminary)	46
Table 11: Zone and Conduit Requirements (ISO/IEC 62443-3-2 (draft))	52
Table 12: Reliability requirements and information.....	57
Table 13: Availability requirements	59
Table 14: Maintainability requirements.....	61
Table 15: Safety requirements	62
Table 16: Types of Fiber Cables for a LAN (Source: [51])	68

Table 17: 10 Gigabit Ethernet Physical Interfaces (PHY 10GBase-R) for Fiber (Source: [51])	68
Table 18: 10 Gigabit Ethernet Module Form Factors (Optics) (Source: [51])	69
Table 19: 10 Gigabit Operating Ranges Per Type of Fiber and per PHY (Physical Interface) (Source: [51]).....	69
Table 20: 10GbE Copper Cabling Options (Source: [51]).	69
Table 21: Switch port features.....	76
Table 22: Forwarding process profiling	76
Table 23: Recommended priority to traffic class mappings	78
Table 24: Recommended IP TOS to traffic class mappings	78
Table 25: Predefined VLAN for NG-TCN operation (preliminary)	82
Table 26: Frame replication and elimination in IEEE802.1CB	94
Table 27: Flows on ETB.....	97
Table 28: Standardized redundancy protocols	111
Table 29: iptables.....	131
Table 30: TCN-URI elements.....	136
Table 31: TRDPv2 Data Classes	137
Table 32: TSN-PD-PDU	138
Table 33: Deployed measures to Communication errors.....	145
Table 34: Representation of the used polynomials in 32 and 33Bit notation.....	151
Table 35: SDSINK state diagram – triggers.....	159
Table 36: SDSINK state diagram – guards.....	159
Table 37: SDSINK state diagram – operations.....	160
Table 38: ED services involved in safe train inauguration	168
Table 39: TTDB safety critical parameters	170
Table 40: TI Validator entities.....	172
Table 41: Train view for validation (example)	173
Table 42: train direction conditions.....	174
Table 43: Validation train view checking – checks.....	175
Table 44: OTD computation general failure modes	176
Table 45: Used DHCP options	185
Table 46: ETB Control agent/application interface signals	189
Table 47: ETB Control interface signals criticality.....	190
Table 48: ETB Control interface signal failure detection	193
Table 49: PDU types.....	198
Table 50: NG-TCN security events	211
Table 51: ED start-up state machine	217
Table 52: Static configuration for network devices	219

Table 53 - ED SNMP set-up state machine	222
Table 54: Comparing EAP relay and EAP termination	228
Table 55 - Security model of SNMP	232
Table 56 - Cost of SNMP implementations.....	234
Table 57: Open Items	238
Table 58: Network component capability matrix	240
Table 59: Network component characteristics.....	244
Table 60: t_{fw} estimated (Ethernet frame with 1530 octets, 1GbE, LILO, 2.5 ms ETB cycle)	245
Table 61: Scenarios for end-to-end latency estimation.....	245
Table 62: end-to-end latency estimation (unit: μ s).....	246
Table 63: NG-TCN requirements implementation.....	247
Table 64: TCN Standard extensions	257
Table 65: UNISIG Standard extensions	259
Table 66: NG-TCN Signalling function requirements.....	260
Table 67: Use cases	291
Table 68: ETB topology variants characteristics (related to one consist).....	292
Table 69: Cost ranking (copper based ETB, 8-car consist)	296
Table 70: Cost ranking (optical based ETB, 8-car consist)	296
Table 71: Material reliability ranking (copper based ETB, 8-car consist)	298
Table 72: Functional Reliability ranking (copper based ETB, 8-car consist)	298
Table 73: Safety ranking	299
Table 74: ETB topology variants B and D ₁ – Pros and Cons	302
Table 75: ETB Topology variants – characteristics and applications	303
Table 76: Definition of Common Zones	304
Table 77: Definition of Common Conduits	306
Table 78: Definition of TCMS Zone Groups.....	307
Table 79: Definition of TCMS Zones	308
Table 80: Definition of TCMS Conduits	309
Table 81: Definition of OOS Zone Groups.....	312
Table 82: Definition of OOS Zones	312
Table 83: Definition of OOS Conduits	313
Table 84: Relay failure modes.....	317
Table 85: Failure modes and mitigations, Variant B ETB bypass	321
Table 86: Revision of single points of failure analysis	323

1 INTRODUCTION

The CONNECTA project covers different TCMS research topics such as General TCMS Specification (WP1), Wireless TCMS and Train-to-Ground (WP2), Drive-by-Data (WP3), Functional Distribution Architecture (WP4), Brake Control (WP5) and transversal activities such as Virtual Placing on the Market (WP6).

In that context, WP3 work package's concrete goal is to make research on technologies and architectures for a new generation of a train communication system which allows to abstain from conventional² train lines and which shall provide the sole communication platform for all type of applications spanning from mission critical functions until infotainment and CCTV applications.

The goal of this deliverable (D3.5 within WP3) is to provide a specification for a Next Generation Train Communication Network (NG-TCN), which addresses the beforementioned objectives. This specification takes as base the requirements defined in D3.1 and makes use of sophisticated technologies which have been analysed in D3.2. The specification is complemented by the activities executed in T3.3, which aim to analyse the proposed NG-TCN architecture with respect RAMS and Security capabilities.

With respect to the security architecture of the NG-TCN, this specification reuses results of Roll2Rail project's WP2 for the definition of a WTCMS architecture. Many of the concepts and analyses developed for WTCMS are as well valid for a NG-TCN based TCMS, and modifications and adaptations have been done where necessary. Especially the agreement within Roll2Rail's WP2 to use the novel norm IEC 62443 as base for the security concept has been adopted³.

A further aspect to be considered is the relevance of this specification for the future standardization. Starting point is the existing TCN standard (IEC 61375 series), and the ambition is to overcome existing weaknesses by introducing new technologies and by adapting the architecture correspondingly (see D3.2 for a more detailed description of TCN weaknesses). As far as interoperability between train vehicles from different manufacturers is concerned, this new architecture shall then be proposed for an update of the IEC 61375 series.

This specification is subdivided into three major parts. Within the first part (chapter 2), a new network architecture is defined which fits for the newly introduced technologies. Network architecture basically means to define the network topology including a suitable structure of subnets, the related network components and their functionality. But network architecture means also to define overall concepts for time synchronization and security encompassing the whole communication system (the train communication network itself and the connected end devices). Furthermore, the proposed architecture must fulfil the RAMS requirements outlined in D3.1. Therefore RAMS aspects need to

² Throughout this document, the adjective “conventional” is used to classify existing technologies (e.g. conventional train lines, conventional devices or conventional, IEEE802.1Q priority-based data traffic) in contrast to new technologies like TSN-aware data traffic or TSN-aware devices.

³ CLC/TC9X WG26 “Electrical and electronic applications for railway” is currently preparing a technical specification “Railway applications – Cybersecurity”. The security models, the concepts and the risk assessment process described in this technical specification are based or derived from IEC 62443 series standard. This technical specification aims to provide the railway operators, system integrators and product suppliers with guidance and specifications on how cybersecurity will be managed in the context of the EN 50126-1 RAMS lifecycle process.

be analysed. This is done in a qualitative way within this specification, a more detailed quantitative analysis is then done within the complementing D3.3.

The second part of the specification (chapter 3) is devoted to the specification of used techniques and follows the classical approach of the ISO OSI 7 Layer model (ISO/IEC 7498-1), in which the upper layers (session layer, presentation layer, application layer) are all subsumed under one common subchapter “Application Layer”. This part defines the conditions, interfaces and protocols for the exchange of data between all type of end devices connected to a NG-TCN. Common aspects like for instance addressing are covered, but also more specific aspects like train discovery, data relaying with the network, clock synchronization, latency/jitter control and safe data transfer are treated.

The third part (chapter 4) defines some general rules for the configuration and the set-up of a NG-TCN. This is handled in a more abstract way because (static) configuration mostly depends on real implementations which is out of scope of this specification. Nevertheless, it makes sense to define some common principles, to define configuration requirements and also to give hints about the correct configuration of such a sophisticated NG-TCN.

Chapter 5 finally presents the conclusions including a list of items which remain open and need to be closed in subsequent activities.

The document closes with a set of appendices. Annex A provides a network device capability matrix, which maps functionalities to (abstract) network devices. Annex B is devoted to a theoretical analysis of the network performance. With this, compliance to the performance requirements shall be demonstrated. These theoretical values are then later to be verified within CTA-2 which aim to prototype the NG-TCN. Annex C provides the requirement traceability matrix by making references between D3.1 requirements and the related chapters and paragraphs within this document. Annex D intends to make a proposal of which parts of this specification shall be proposed for standardization, e.g. in the IEC 61375 series. Also necessary modifications to existing standards are proposed. Annex E deals with the example of a connected signalling subsystem as it is described in D3.1. The intention is to demonstrate in a common way that the NG-TCN as defined herein fits to the requirements and objectives of the signalling subsystem. Annex F provides a “proof-of-concept” setup proposal (test bench plus test steps) which can then be used in subsequent research projects for verification and validation activities. Annex G contains the analysis of different ETB topology variants in order to identify the most suitable ETB topology for the NG-TCN. Annex H provides a deeper specification of the cyber security zones and conduits which have been defined for the cyber security architecture. Annex I provides a study about an optimal bypass function design, which has been executed prior to the decision to adopt an ETB topology solution without bypass function. Nevertheless it may give valuable information for future applications which still require bypass functionality for legacy ETB topology, e.g. applications using the ETB as defined in IEC61375-2-5. And finally, Annex J resumes the analysis of single points of failures done in T3.3 and checks their coverage by the NG-TCN architecture.

It should be noticed that this document bases on contributions from the different project members and that for this reasons some technical concepts and descriptions are partially repeated in the different sections of this document. To not affect the context they are embedded in, those repetitive parts have not been removed deliberately.

The document has been carefully reviewed by project members and the partners from the collaborative action (SAFE4RAIL). Nevertheless it might still contain errors which may ask for later corrections, e.g. during the course of subsequent projects (e.g. CTA-2).

2 NG-TCN ARCHITECTURE

2.1 GENERAL

One of the objectives of the NG-TCN is to provide one network for connecting the different functional domains TCMS, OOS and COS. An overview over these functional domains with their main characteristics and interfaces is shown in Figure 2 (source: [09]).

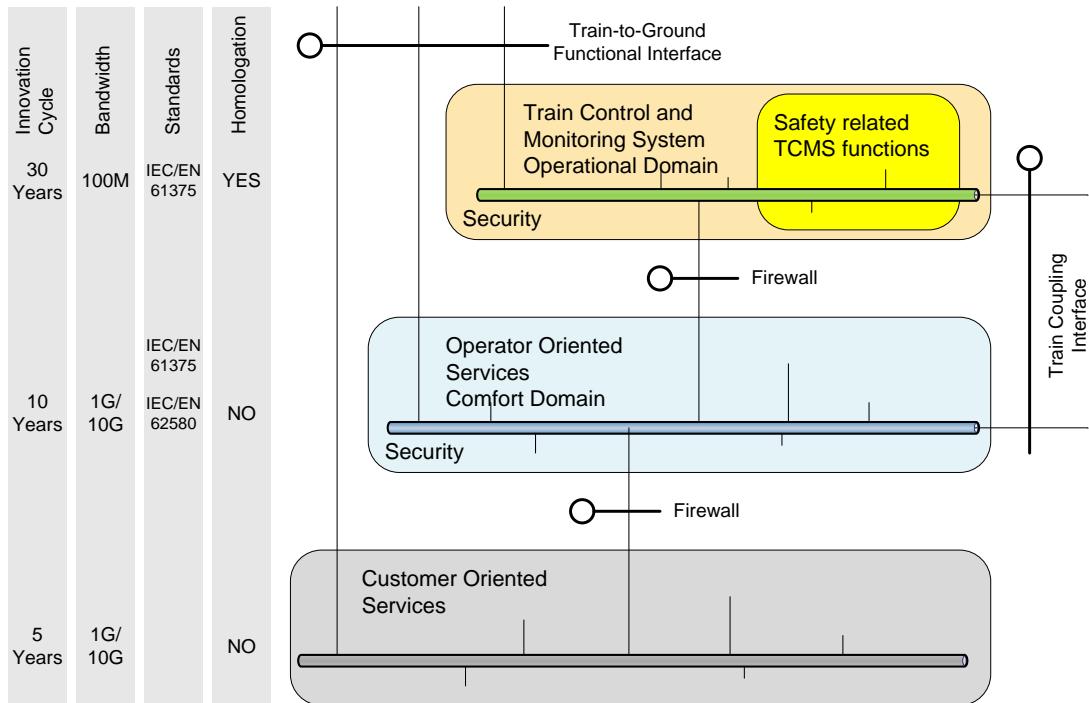


Figure 2: NG-TCN functional domains and interfaces

The general network architecture shall follow the separation in those different functional domains and shall use independent sub-networks (at least logical) for the different domains. The interfaces between the functional domain subnets and to wayside must respect safety and security aspects as it will be outlined later in this document.

More in detail, the TCMS subnet shall be used for

- All functions and devices that require a certification
- All safety related functions

The TCMS subnet shall be insensitive to changes in other subnets, e.g. a change in OOS or COS subnets shall not require a re-certification or re-homologation of the TCMS. This is important because there will be innovation of technologies, functions and devices in the OOS subnet and COS subnet during the lifespan of the train.

Customer devices, e.g. mobile phones or tablets, will be able to connect to the COS subnet. Some web services located in OOS subnet are reachable from the COS subnet. A complete isolation of OOS and COS subnet is not possible if information, e.g. a live stream of a front facing camera generated in OOS, shall be available in customer subnet.

There is no direct connection between the customer network and the TCMS network. All the data from TCMS network to customer network shall go through secured interface to the OOS subnet and further on to the customer network. Only one-directional data flow (TCMS -> OOS -> COS) shall be possible for the data originating in the TCMS subnet.

Train to ground communication is done using the train to ground functional interface. An example of a possible deployment is the location of an MCG in OOS.

2.2 NG-TCN TOPOLOGY

2.2.1 General

The architecture, and as a part of it the topology, of a NG-TCN should ensure that the basic requirements cited in Table 1 (extracted from [03]) are fulfilled.

Table 1: NG-TCN architecture requirements

ID_40019	Intra-consist communication shall not be interrupted during coupling or uncoupling of consists. NOTE: this might contradict the need of train wide clock resynchronization after inauguration	During coupling or uncoupling of consists a train wide communication might not all the time be possible, but the consist internal communication has to keep ongoing. IEC61375-2-5:2015 defines a layer 3 decoupled consist network and train network as a solution of this requirement.
ID_40020	A powerless or defective vehicle or consist shall not interrupt the train wide communication between the consists which are not affected by the power loss/defect.	No single point of failure shall cause a train-wide communication loss. IEC61375-2-5 defines a bypass function as a solution of this requirement.

Those requirements have consequences for the overall network topology. One consequence will be that broadcast domains must be restricted. A defect like a broadcast storm in one consist, e.g. caused by a misbehaving end device or network device, shall neither impair the train wide communication nor the communication within another consist. Similar, but more difficult to detect, are “babbling idiots”, meaning end devices (or network devices) sending apparently correct Ethernet frames, but with a higher frequency than allowed, leading to network overload condition. Of course, there are technical means like broadcast storm protection or bandwidth restriction (frame ingressing policy) which can be applied, but the manifold of failure scenarios is difficult to oversee and hardly manageable. A better way is a clear separation of consist internal communication and train wide communication and therewith limit the spread of faults. This separation can be physical (separated LANs) or logical (one network, logically separated using VLANs). Another major benefit of this separation is that the consist network can be kept static and can be preconfigured, while the train backbone, by nature, is dynamic requiring a dynamic network management (train inauguration). A further reason for a stronger separation is given by security aspects because separated sub-networks can be easily mapped to different security domains, and the interfaces between the subnets can provide protective measures (“defence in the depth”, see 2.10).

With this approach, the logical train network architecture shown in Figure 3 results. It is worth to mention, that this network architecture is in line with IEC61375-1.

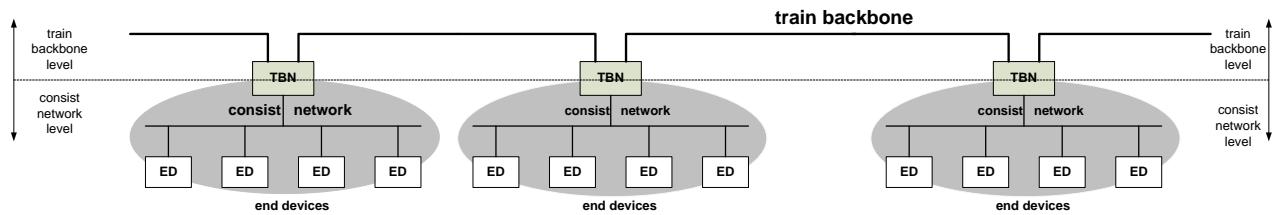


Figure 3: logical Train Network architecture (source [17])

Here we have a train backbone network spanning the whole train and a consist network level covering the consist. Consist network and train backbone are connected by a logical device called “Train Backbone Node” (or “Ethernet Train Backbone Node” ETBN in case of Ethernet). The functionality of this logical device is discussed in 2.7.

A consist can have more than one (logical) consist network as it is shown in Figure 4.

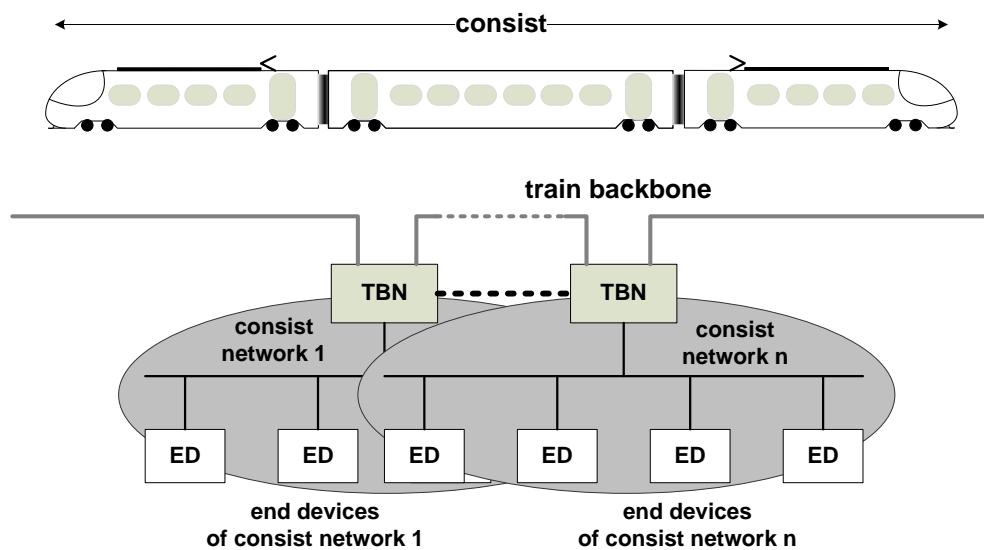


Figure 4: Consist network (source [17])

Multiple consist networks can for instance be used in the different consists of closed trains (see [17]) or to separate different security domains.

2.2.2 Network Topology

Following the general statements made before, a network topology separating train level and consist level can be defined. A first base is the network topology defined in IEC61375-2-5 (ETB) and IEC61375-3-4 (ECN), but these need to be refined and extended to meet the requirements of a NG-TCN. A NG-TCN architecture based on said standards is shown in Figure 5. On ETB level, there are two aggregated ETB lines (A and B) spanning the whole train. On consist level (ECN), an Ethernet ring is spanning the consist, but this could also be another topology like for instance a ladder as defined in IEC61375-3-4 as an option. Besides the cabled ring and the end devices connected to the consist switches, subordinated wireless networks like meshed WLAN or WPAN can be connected. The connection between ECN and ETB is provided by an ETBN, which not only transfers data between the two networks, but is also responsible to establish the dynamic train backbone (train inauguration). Train-to-ground communication is provided by the MCG, which is connected to the ECN.

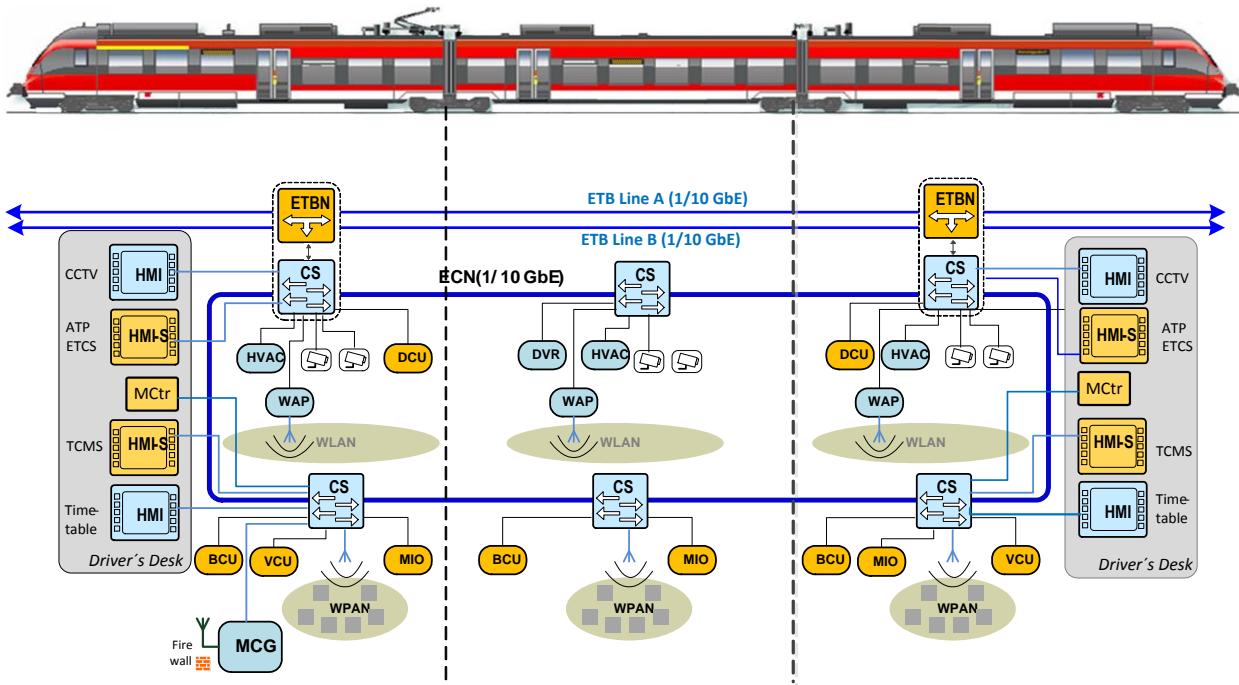


Figure 5: IEC Compliant Network Topology

Another topology, which provides some enhancements compared to the IEC compliant topology, is shown in Figure 6. The difference is that the ETB uses two separated ETB lines A and B related to the sides of the consist (side A and side B as defined in IEC61375-1). As it will be demonstrated in sub-chapter 2.5.2 and Annex G, both topology alternatives have their specific pros and cons, but the new option has advantages with respect to safety and reliability and therefore facilitates the achievement of higher safety integrity levels, which is one of the main objectives of NG-TCN. For this reason, the conclusion inside the CONNECTA WP3 was to choose this new topology as base for the NG-TCN. The IEC compliant network topology stays untouched and can still be used for legacy applications as well as for applications demanding it.

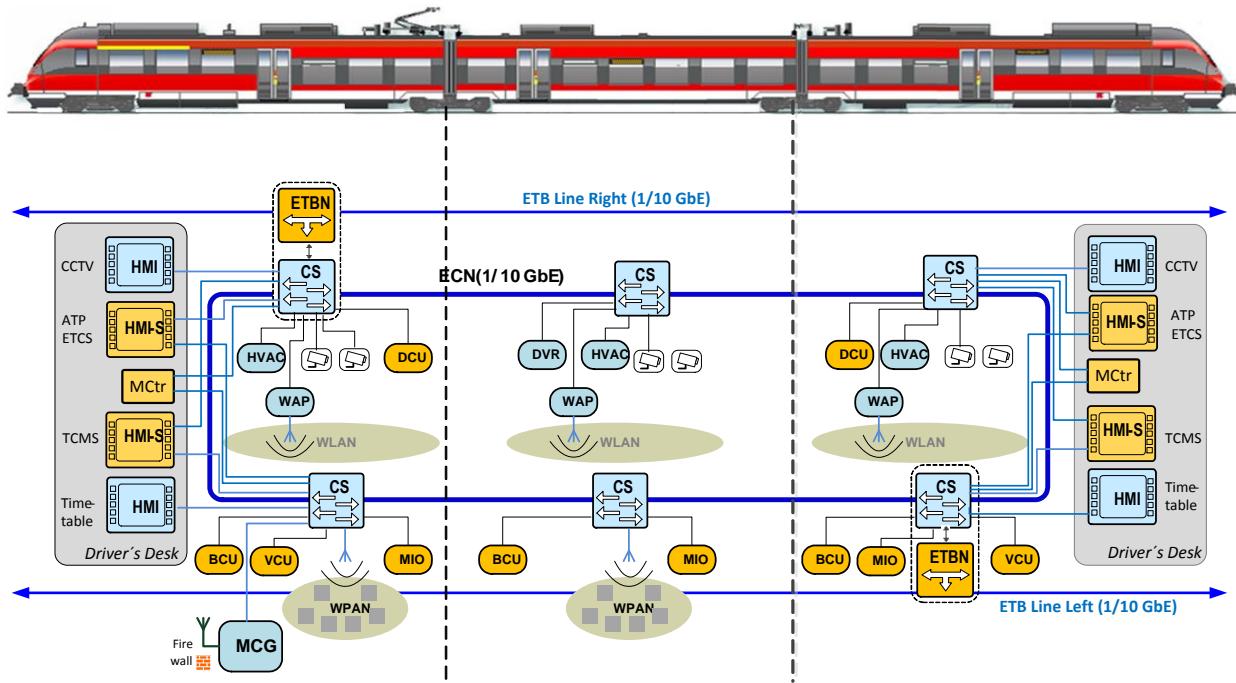


Figure 6: NG-TCN Topology

2.3 NETWORK COMPONENTS

2.3.1 Classification

NOTE: the following description uses references [40] and [41].

In general, network components are divided into 2 categories:

1. “Passive network components” are parts of a network that are involved in the data transmission, but they don’t change or affect the data. Passive network components are for example cables, connectors and plugs.
2. “Active network components”:
 - a. Network devices (e.g. switches, routers)
 - b. ED and ED-S with or without integrated switch functionality

A wired network is basically a combination of various active and passive network components.

The focus of the classification is based on the active network components, especially End Devices (ED and ED-S), but if a 10GbE technology must be used, it must be considered that this also has an influence on the passive network components. (e.g. the use of fibre optic instead of copper-wiring). A classification of the network components used within the NG-TCN architecture is helpful to be able to divide functional and non-functional requirements at component level and provides information which extensions and/or topological connections are mandatory for the respective components.

A classification of the used network components is done regarding the criticality from the highest to the lowest priority:

- a) **SCNC**: “Safety Critical Network Component”: (for example: ED-S)
- b) **TCNC**: “Time Critical Network Component without safety functionality”: (for example: Traction Control Units TCU)
- c) **NTCNC**: “Non-safe and non-time critical network component” (for example: Passenger counting systems in OOS domain)

There is a wide variety of active network components, but the consideration is largely limited to the components that are intended to perform the respective vehicle functions (ED and ED-S). The functional role of different network components itself is described in the following subchapter 2.3.2.

All different types of the classified network components should be connected to the same physical network and operate and exchange data at functional level on the same physical network without mutual interference up to the maximum of allowed network components at consist and train level. (see chapter 0 Quantities)

A SCNC is always also time-critical, therefore the SCNC and the TCNC must be TSN aware, while NTCNC does not expect deterministic traffic.

Both SCNC and TCNC often, but not necessarily, have higher availability requirements. Therefore, the availability of the network on the one hand and the availability of these components on the other hand play a decisive role for the group of these components.

Table 2: Relevance of the classification for the network components

	SCNC	TCNC	NTCNC
Functional domains	Should be restricted to use within TCMS incl. safety critical subsystems	Should be restricted to use within TCMS	The use within TCMS, OOS and COS domains should be possible and not restricted depending on the functionality
Deterministic data transfer	SCNC should be TSN aware or should be connected to a TSN aware switch.	TCNC should be TSN aware or should be connected to a TSN aware switch.	For NTCNC there is no deterministic dataflow expected, so no extension or specific switches are necessary.
Higher Network availability required	SCNC should have an integrated 4 port switch or should be connected to 2 different CS in a virtual ring and support the IEEE802.1CB (Redundancy, Frame Replication and elimination) mechanism.	TCNC should have an integrated 4 port switch or should be connected to 2 different CS in a virtual ring and support the IEEE802.1CB (Redundancy, Frame Replication and elimination) mechanism.	For NTCNC the TSN awareness is in general not required, so the TSN standard IEEE802.1CB could not be used for higher availability. Other mechanisms are possible for example the use of MRP, when the component has at least a 2-port switch integrated.
Higher component availability required	For example, the SCNC should be redundant and the activity (master backup) should be negotiated between the two redundant	The TCNC should be redundant and the activity (master backup) should be negotiated between the two redundant components	In most cases not necessary for the class of network component.

	SCNC	TCNC	NTCNC
	components using an appropriate procedure.	using an appropriate procedure.	
Safety	Safe capable up to SIL x (x depending on the required Safety Function) Support of SDTv4 ⁴	Non-safe Component – no restriction	Non-safe Component – no restriction
Examples of an assignment of end devices to the classification (without claim to completeness)	Safety partition of a VCU, BCU or DCU.	non-safe-partition of VCU or TCU.	PIS, HVAC, IOT-Components

2.3.2 Functional roles

Functional roles are introduced as an abstraction from real physical devices used in the network. In practise, managed devices may have, by static configuration, specific functional roles, transforming them to abstract, logical network devices serving a specific purpose in the network. In principle, the functional roles could all be implemented by different devices, but for practical reasons (cost reduction, limiting number of different devices) they are combined in a few network devices (for instance, an ETB switch device may incorporate functional roles ETBN, CS and ECSP).

Table 3: Functional Roles

Functional role	Description
ETBN	<p>The ETBN connects the ECN with the ETB and manages the ETB. Main functions are:</p> <ul style="list-style-type: none"> • Forwarding Ethernet frames along the ETB (IEEE 802.1Q “bridging”) • Bypass (option only for topology variant B) • IP packet transfer between ETB and ECN • Train inauguration (IEC61375-2-5) • Train Network Directory • ECN Clock master • TSN gateway
ETBR	<p>The ETBR is used as repeater on the ETB. Main functions are:</p> <ul style="list-style-type: none"> • Forwarding Ethernet frames along the ETB deterministically <p>NOTE: The ETBR can be implemented in different ways, e.g. on physical layer or as a 2-port switch. The ETBR should be diagnosable.</p>
CS	Consist Switch, a managed Ethernet switch (IEEE802.1Q bridge) in the ECN. It provides trunk ports for connecting to other CS and end device ports for connecting ED to the ECN.

⁴ SDTv2 as specified in IEC61375-2-3 shall be supported as well but is not in the scope of CONNECTA. Other safety protocols like PROFISAFE or UNISIG may be used on consist level (ECN).

Functional role	Description
ECSP	The ECSP implements NG-TCN network services which are used by connected ED: <ul style="list-style-type: none"> • TTDB Manager Interface (IEC 61375-2-3) • ECSP interface (IEC 61375-2-3) • DNS (TCN-DNS) Server⁵ • DHCP server (Option) • Authentication server (IEEE 802.1X)
RT	IP layer 3 router and firewall for interconnecting ECN subnets (e.g. VLAN subnets).

A proposed mapping of functional roles to network devices is given in A.

2.3.3 Operational roles

An operational role defines the actual role of a device, which is a dynamic property and can change over time, e.g. following a redundancy shift

Table 4: Operational roles

Operational role	Description
CMS	Consist Master. This is the network device with ECSP capability which is acting as TTDB manager and DNS server. If the ECSP is located on the ETBN device, the master ETBN (see 3.2.10) will have this role. In case this device fails, the other ETBN device takes the role over.
CCU	The Consist Computing Unit is a dedicated ED which controls the ETB and provides validated train inauguration information to interested applications and further sub-systems. In addition, it runs train applications. The CCU device is typically redundantly installed, but only one device is allowed to take the active role of a CCU at one time.

⁵ TCN-DNS is specified in IEC 61375-2-3

2.4 QUANTITIES

The quantities of the NG-TCN architecture as specified herein are listed in Table 5 for the train level and in Table 6 for the consist level. These quantities are basically conforming to the requirements defined in [03]. Exceptions to these requirements are mentioned under “comments” and are motivated by the selection of ETB topology variant D₁ as the base for NG-TCN (see 2.5.3). NG-TCN quantities are used for performance, reliability and safety calculations executed in T3.3 and T3.5 of CTA WP3.

Table 5: Train Level Quantity

Train Level	Quantity	Comment
Number of consists per train	1 ... 32	Compliant to IEC61375-2-5 NOTE: NG-TCN defines 2 ETBN per consist
Number of vehicles per train	1 ... 63	Compliant to IEC61375-2-5
Number of ETBN per train	2 ... 64	2 ETBN per consist
Number of ETBN per ETB line	1 ... 32	Compliant to IEC61375-2-5
Number of ETBN and ETBR per ETB line	1 ... 63	Determines the data transmission latency on ETB. Presence of ETBR reduce the maximal number of ETBN per ETB line
Number of ETBR between two ETBN	0 ... 4	
Number of ETB lines ⁶ per train	1 ... 2	Can be operated with one ETB line (no redundancy) or two ETB lines (ETB-L and ETB-R redundancy).
Number of ECN per train	1 ... 32	IEC61375-2-5 allows up to 63

Table 6: Consist Level Quantity (preliminary)

Consist Level	Quantity	Comment
Number of vehicles per consist	1 ... 32	Consists with more than one vehicle restrict the number of consists per train
Number of ETBN per consist	2	
Number of ETBN per ETB line in consist	1	
Number of ECN per consist	1	IEC61375-2-5 allows up to 32. This restriction reflects the design goal to use one physical network for all domains.
Maximal number of CS hops between an ED and the local ETBN	0 ... 32	Determines the transmission latency between an ED and the ETBN in a consist network. 0 = ED directly connected to ETBN
Maximal number of CS hops between two ED connected to same ECN	0 ... 32	Determines the transmission latency between two ED 0 = ED directly connected
Total number of ED and ND per consist	0 ... 2 ¹⁴ -2	As defined in IEC61375-2-5
Number of safe ED per consist	0 ... 512	Important for safety calculations

⁶ A „line“ can be a wire but also a radio channel. In the case of radio channel, the number of relevant channels to reach the NG-TCN goals will be determined by the WP2 of CONNECTA.

Consist Level	Quantity	Comment
Number of CS per consist	0 ... 32	Equals the maximal number of CS per ECN
Number of ED per consist directly connected to the ETB	0 ... 254	Optional feature of IEC61375-2-5. These devices may receive an IP address out of the TB address domain.

2.5 TRAIN BACKBONE

2.5.1 Inter-Consist ETB Interface

One of the objectives of the NG-TCN is to simplify the physical inter-consist interface by reducing the number of conventional train lines⁷ and by using shared media for the transmission of mixed criticality data. The train communication network is classically divided into a consist internal network and a train backbone, the latter one responsible for inter-consist data communication. The minimal, but still reliable, data communication interface between two consists is to provide a duplicated medium (Line A and Line B) between two consists as it is depicted in Figure 7. This interface corresponds to the interface definitions given for instance in the TCN standard series (IEC61375) and in UIC Leaflet 556 [32], and shall also be used as inter-consist interface for the NG-TCN.

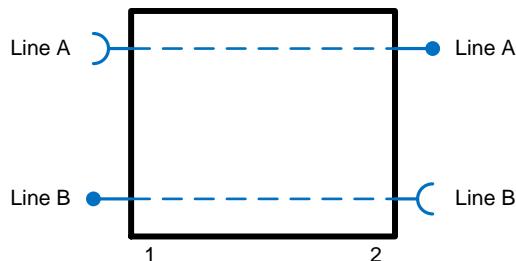


Figure 7: Consist outer interface

This interface definition makes no assumptions about the train backbone topology inside consists itself. However, the consist internal topology has an influence on how data are transmitted over the inter-consist interface.

2.5.2 Consist Internal ETB Topology

Contrary to the inter-consist communication interface, which should be uniquely defined to ensure interoperability between consists of different manufacturers (see 2.5.1), there is some freedom for the network topology inside a consist. Figure 8 shows the different topology variants for the ETB (train backbone topology variants A to E). The consist network itself is simply shown as a cloud because its topology (ring, ladder or star) is not relevant here.

⁷ UIC 558 [33] defines conventional train lines for audio connection to driver, public announcement, lighting control and door release/closing.

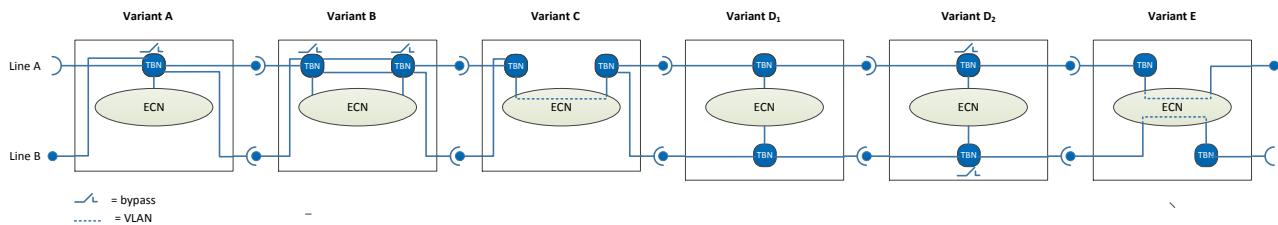


Figure 8: Train backbone architecture variants

Topology variants A and B are those specified in IEC61375-2-5 [19]. This ETB topology was adopted from the topology defined for WTB (IEC61375-2-1 and UIC Leaflet 556), which primarily addressed locomotive hauled passenger trains where each vehicle is a consist and typically contains one train backbone node in case of passenger coaches or two in case of train sets or locomotives.

Topology variant C is a theoretical possibility, but as shown later of no practical use. Topology variants D and E are topologies partly in use as proprietary solutions. Variant D has been split in two sub-variants D₁ and D₂, one without (D₁) and one with bypass function (D₂).

In order to identify the optimal ETB topology for NG-TCN, an analysis of all topology variants has been executed and the results are documented in Annex G. The conclusion of this analysis clearly identifies ETB topology variant D₁ as being the optimal solution for a TSN aware NG-TCN.

2.5.3 NG-TCN Train Backbone

With the conclusions made in G, the proposal is to use ETB topology variant D₁ for the NG-TCN as a network suitable for high integrity and low latency communication. This leads to the overall NG-TCN train backbone architecture shown in Figure 9.

The indicated directions are those defined in IEC61375-1, but to clearly distinguish the two train-wide ETB lines, an extension is made by assigning a side direction (left/right). That means that it is distinguished between a left side ETB-L and a right side ETB-R.

Within consists, the two ETB lines are still assigned to consist sides A (ETB line A) and B (ETB line B) as this is statically defined during consist design. But when consists are coupled, those consist sides are mapped to the corresponding train sides (left/right). This can be seen in Figure 9 where the two consists have different orientations.

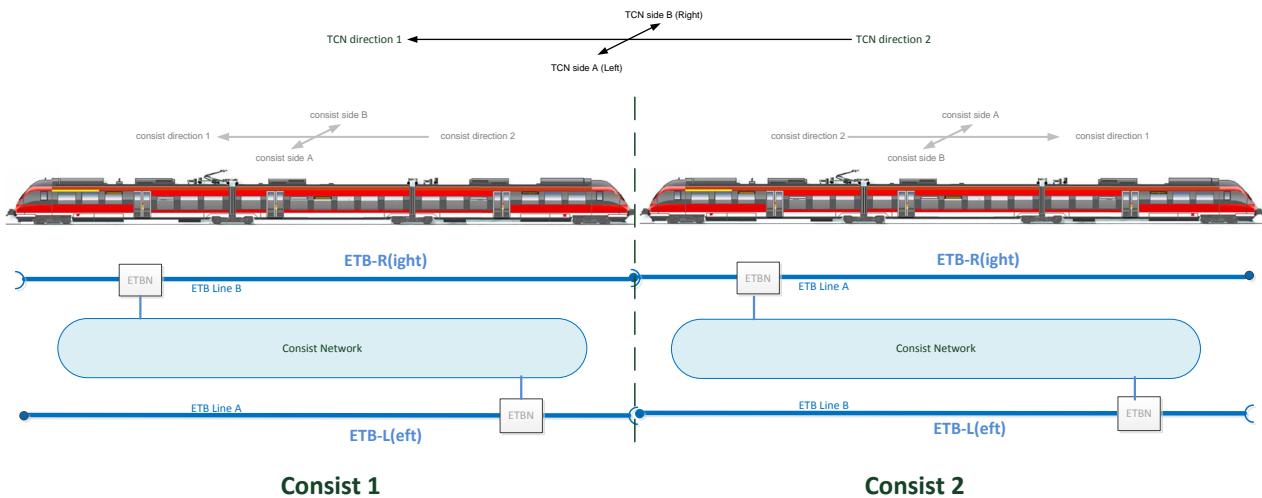


Figure 9: NG-TCN train backbone topology

2.6 CONSIST NETWORK

IEC61375-3-4 defines different possible ECN physical network topologies which are:

- Linear topology
- Linear topology (parallel network) with dual homing
- Ring topology
- Ring topology with dual homing
- Ladder topology with dual homing

Although the standard allows to choose any of those topologies, the definition of the NG-TCN as a high integrity network imposes some constraints. This can best be demonstrated when analysing the different topologies (Table 7):

Table 7: ECN Topologies – pros and cons

Topology	Pros	Cons
Linear topology	Simple and cost efficient	Single point of failure. Link or switch fault segments the network.
Linear topology (parallel network) with dual homing	No single point of failure. Well suited for TSN because a fault does not require a reconfiguration of TSN schedules.	All ED must support dual homing.
Ring topology	No single point of failure. Broadly used and supported. Lowest number of Ethernet links in a network with no single point of failure. Several ring redundancy protocols available (e.g. MRP). Dual homing not required.	Not suitable for TSN, because any ring or link failure causes a reconfiguration of the TSN schedules (see 3.2.8).

Topology	Pros	Cons
Ring topology with dual homing	No single point of failure. Supported by most existing solutions.	Ring or link failure may cause a reconfiguration of the TSN. All ED must support dual homing.
Ladder topology with dual homing	No single point of failure, capable to handle double faults.	Ring or link failure may cause a reconfiguration of the TSN. All ED must support dual homing. Not well supported (requires special redundancy protocols, or in case RSTP is used, is less deterministic).

As can be seen, there is no optimal topology. But what also can be seen is that linear topology (parallel network) with dual homing is the only one with good TSN support, while the ring topology avoids the dual homing for all devices. Hence, a combination of the two would be the optimal solution, and this is possible. As it will be elaborated in 3.2.8 in more detail, the proposal for NG-TCN is to use a physical ring topology superimposed with a logical parallel linear topology (A-Plane/B-Plane).

With this the proposed NG-TCN network topology looks as shown in Figure 10. The ECN ring is built with consist switches, and ED can be connected either with single Ethernet link or with double Ethernet link (dual homing).

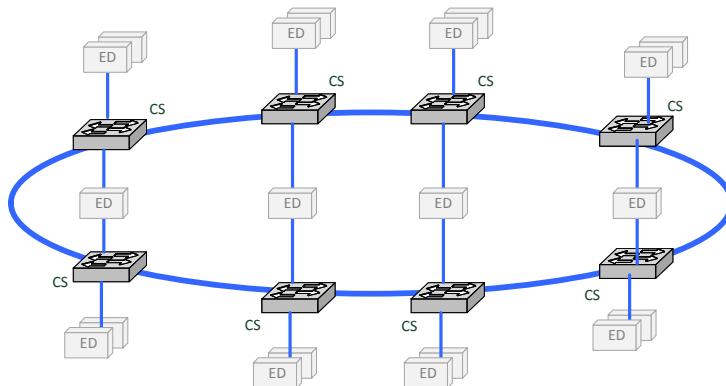


Figure 10: ECN ring topology with dual homing

To avoid a loop which will cause a broadcast storm, the ring must be logically interrupted at some location. This will be the task of the ring redundancy protocol as defined in 3.2.9, by blocking Ethernet ring ports if required.

2.7 CONNECTION BETWEEN TRAIN BACKBONE AND CONSIST NETWORK

This subchapter, dealing with the connection between train backbone and consist network, defines the architectural features which are necessary to enable the (safe) data exchange over ETB between end devices connected to consist networks of different consists.

2.7.1 Network services for train-wide data exchange

For train wide data exchange a set of network services is required which are listed in Table 8. The detailed service description and service specification can be found in the related chapter. Some of

those services are safety related which will be subject of the next sub-chapter. The IEC service indicates to which service defined in IEC61375-2-3/IEC61375-2-5 these functions belong.

Table 8: Network services for train wide communication

Service	Functions	IEC Service	Safety related	Related chapter
ETB Inauguration	<ul style="list-style-type: none"> Discover the ETB topology and generate the train network directory (TND) Inhibit train inauguration on demand Indicate train lengthening/shortening 	ETBN	Yes	3.2.10
Operational Train Inauguration	Compute the TTDB after train composition change or after train leadership change.	ECSP	Yes	3.5.4
TSN Gateway	Transfer TSN packets between ECN and ETB	-	No	3.5.5
Ethernet Switching	Switch Ethernet frames along the ETB	ETBN	No	3.2
Time Sync	Provide Master Clock and Boundary Clock	-	No	2.9
IP Routing	Route IP packets between ETB and ECN (unicast and multicast)	ETBN	No	3.3
DNS Service	Provide ED interface for resolving TCN-URI addresses to IP addresses.	DNS	No	3.5.5
TTDB Info service	Provide ED interface for retrieving TTDB information	TTDB Manager	Yes	3.5.5
ETB Control Service	Provide ED interface for: <ul style="list-style-type: none"> Inform about ETB state Set/reset leading Inhibit Train composition confirmation/correction Sleep control 	ECSP	Yes	3.5.5
ETBN Control Service	Provide ED interface for ETBN control as specified in IEC61375-2-5	ETBN	No	-
TND Info Service	Provide ED interface for retrieving TND information as specified in IEC61375-2-5	ETBN	Yes	-

2.7.2 Safety related services

Train inauguration functions as defined in [03] are analysed in [05] and safety targets are derived for all functions. Table 9 lists all inauguration functions with their derived THR⁸ value.

Table 9: THR of inauguration functions (source: [05])

Function	THR
Determine the number of cars	< 10 ⁻⁸ /h
Determine the sequence of cars	< 10 ⁻⁶ /h
Identify the train end cars	< 10 ⁻⁸ /h
Determine the orientation of cars	< 10 ⁻⁸ /h

⁸ In accordance to EN50126

Because all the safety related network services for train wide communication as listed in Table 8 contribute to those inauguration functions, they must provide the same level of safety integrity as requested for the inauguration functions, which will be SIL4 corresponding to the $THR < 10^{-8}/h$.

2.7.3 ETB/ECN safe train inauguration architecture variants

The THR of the inauguration functions as defined in Table 9 must be apportioned to the network functions which together protect against the hazard. This functional decomposition is part of the system design and depends on the selected architecture. In the case of NG-TCN, three architecture variants for ETB control are possible (Figure 11):

Variant A: Only ETBN service is running on ETBN device, while all other services run on CCU. The ETBN device only supports a lower SIL, therefore a “checker” is needed on CCU which validates the safety critical output of the ETBN device and qualifies it for SIL4.

Pros: checker is simple (needs only to validate the TND)

Cons:

ETB related services distributed to two devices, which requires the specification of a new interface between ETBN and ECSP.

ECSP with its complex state machines must be SIL4 compliant

Variant B: The classical architecture with ETBN device hosting ETBN service, ECSP service and TTDB Manager service. ECSC service resides on the CCU ED.
Disadvantage is that both ETBN device and CCU must support SIL4.

Pros: all ETB related services on one device

Cons: both ETBN device and CCU must support SIL4

Variant C: Like variant B, but with an ETBN device supporting a lower SIL. To comply with the required THR, a “checker” is needed on CCU which validates the safety critical output of the ETBN device and qualifies it for SIL4.

Pros: all ETB related services on one device

Cons: checker must validate the more complex TTDB

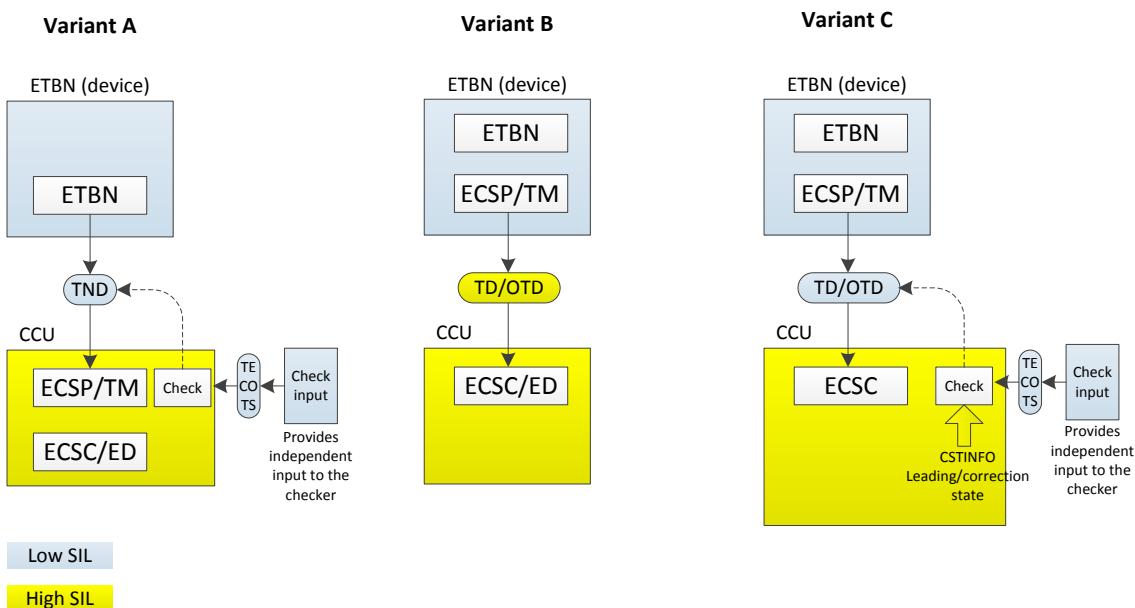


Figure 11: ETB/ECN connection architecture variants

Variant B is ruled out because an ETBN device capable running SIL4 functions is not realistic. The principal feasibility of variant A has already been demonstrated in [05]. Variant C is subject of sub-chapter 3.5.4 about safe train inauguration and is actually the most favored variant.

2.7.4 Ethernet Train Backbone Node (ETBN)

Device design

The ETBN device provides the physical connection between ECN and ETB (Figure 12). For connecting to ETB and ECN, it provides at least three Ethernet ports, two for ETB and one for ECN. Besides this minimal configuration, there might be variants:

- Support of ETB topology variant B, meaning 4 ETB ports instead of 2
- Support of 2 ECN ports, which permit to insert the ETBN in an ECN ring network
- Support of ED ports for connecting EDs directly to the ETB (see IEC61375-2-5)
- Support of ED ports for connecting EDs to the ECN. This solution could be beneficial for simple consists with only a few ED.

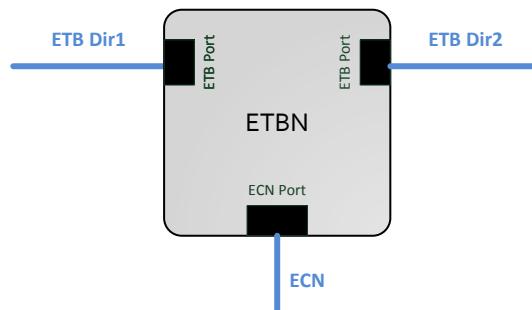


Figure 12: ETBN Device

NG-TCN makes no restrictions concerning the selection of variants.

Functionality

Dependent on the architecture variant presented in 2.7.3, the ETBN device has to support the services defined in Table 8. This is illustrated in Figure 13 (architecture variant A) and Figure 14 (architecture variant C). For the definition of the individual services please refer to the references given in Table 8.

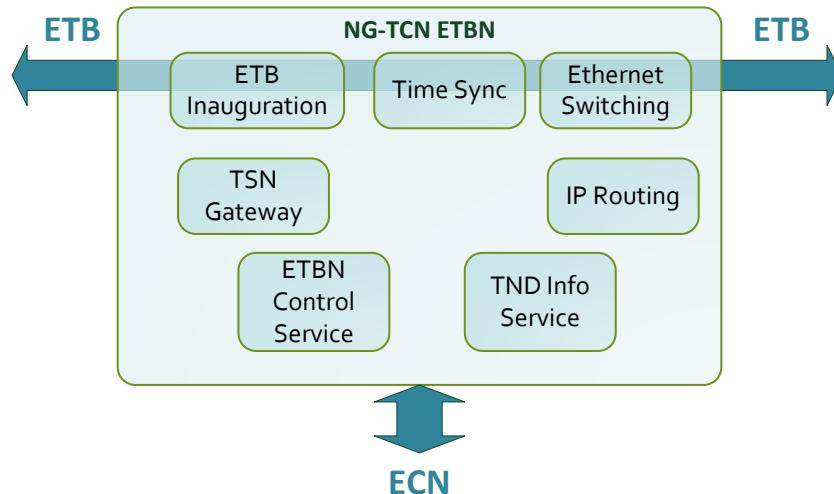


Figure 13: NG-TCN ETBN Services (Architecture Variant A)

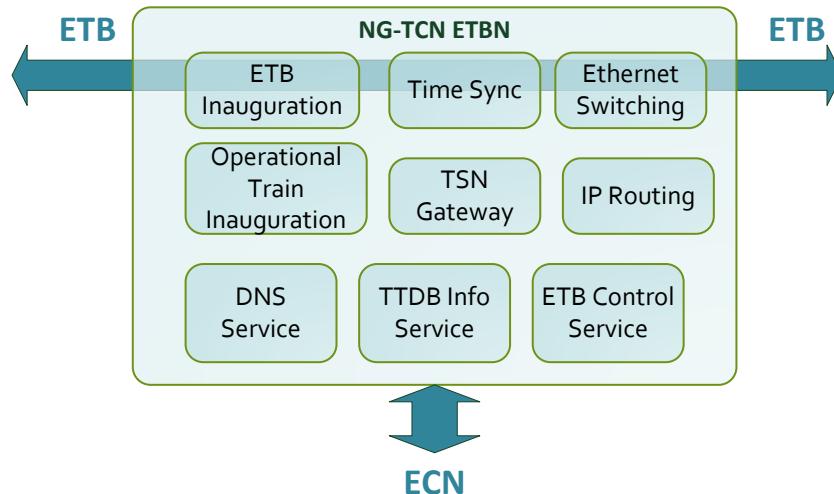


Figure 14: NG-TCN ETBN Services (Architecture Variant C)

2.8 NETWORK INTERFACES AND PROTOCOLS

2.8.1 General

NG-TCN must support a lot communication protocols which all need to be well specified to achieve interoperability between the different network components. Most of the supported protocols are

standard Ethernet or IP based protocols, but there are also some protocols which have been specially developed or are standard protocol based, but with modifications.

2.8.2 Protocol Interfaces

To achieve interoperability, basically five network interfaces are of interest, which are all depicted in Figure 15.

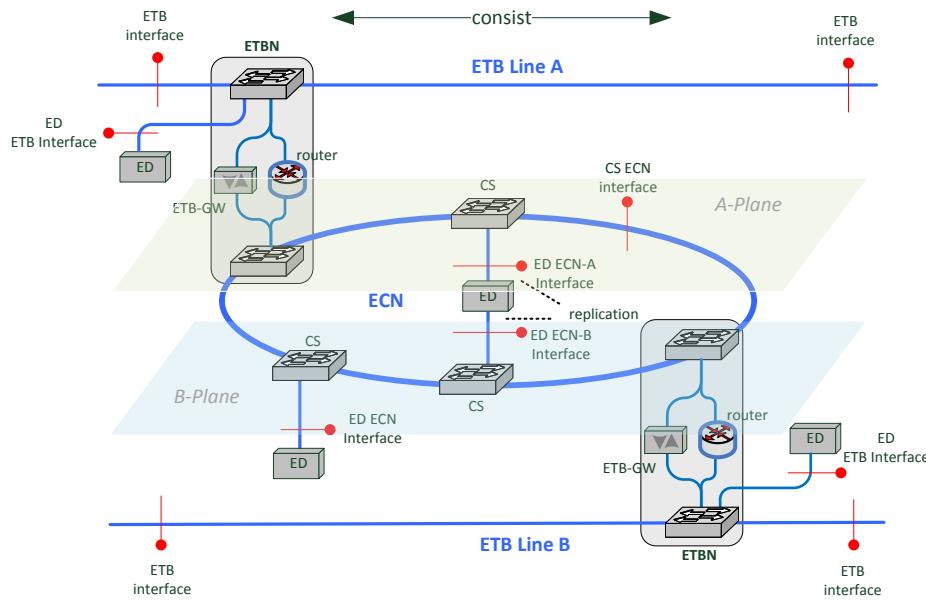


Figure 15: NG-TCN Protocol Interfaces

ETB Interface (ETB)	The interface on ETB line is mainly used for the exchange of train wide application data. It is also used by the ETBN to perform the train inauguration. This interface is specified in IEC61375-2-5 (lower communication layers), IEC61375-2-3 (upper communication layers) and IEC61375-2-4 (application layer), with the extension and modifications of said standards defined within this document.
CS ECN Interface (ECN)	This interface is mainly used for the exchange of train wide and consist internal application data. Train wide data are directed to/from the local ETBN which routes the data to the ETB. The interface is also used for ring management.
ED ETB Interface	This interface is used by ED directly connected to the ETB for data exchange among themselves, see IEC61375-2-5 for details. Not further considered herein.
ED ECN-A/B Interface (ED-X)	Physical Ethernet interface to ECN Plane A or ECN Plane B, see 3.2.8. Both interfaces are used for TSN traffic with replicated frames. For non TSN traffic, either one of the interfaces can be used.
ED ECN Interface (ED)	This interface connects non TSN-aware ED to NG-TCN via managed consist switches. Over this interface, all the services offered by NG-TCN towards EDs are supported.

2.8.3 List of protocols

Table 10 lists all relevant (used) protocols together with their relationship to the ISO OSI Layer they belong to, the affected network interface, their specification and the related chapter within this document.

Table 10: List of interface protocols (preliminary)

Protocol	OSI	Interface				Specification	Chapter	Comment
		ED	ECN	ED-X	ETB			
100BASE-TX	1	x	x	x	x	IEEE 802.3	3.1.1	= 100FDX fast Ethernet
1000BASE-T	1	x	x	x	x	IEEE 802.3	3.1.1	= GbE
ARP	3	x	x	x	x	RFC 826	3.3.2	IPv4 only
DHCP	7	x	x	x		RFC 2131	3.5.5	Option 82 only on ECN ring
DNS	7	x	x	x		RFC 1034, RFC1035 IEC61375-2-3	3.5.5	Adaptations of DNS for dynamic TCN-URI resolution are defined in IEC61375-2-3
EAP	2	x		x		IEEE 802.1X	3.5.7	
EAPOL	2	x		x		IEEE 802.1X	3.5.7	EAP over LAN
ECSP Control	7	x	x	x		IEC61375-2-3	3.5.5	
ETBN Control	7	x	x	x		IEC61375-2-3	3.5.5	
FRER	2	x	x	x		IEEE 802.1CB	3.2.8	
gPTP	2		x	x	x	IEEE802.1AS-rev	3.2.7	
HTTPS	7	x	x	x	x	RFC 2818	–	Secure file transfer selected in IEC61375-2-6
ICMP	4	x	x	x	x	RFC 792	3.3.4	
IGMP	4	x		x		RFC 3376	3.3.5	
Ingress policing	2		x	x	x	IEEE802.1Qci	3.2.5	
IPv4	3	x	x	x	x	RFC 791	3.3.1	
IPv6	3	x	x	x	x	RFC 2460	–	
Link Aggregation	2				(x)	IEEE 802.1AX	–	Only for ETB Topology variant B
LLDP	2	x		x	x	IEEE 802.1AB	–	
MACsec	2	x	x	x	x	IEEE 802.1AE	3.2.11	as an option
NDP	3	x	x	x	x	RFC 4861, RFC 3122	–	IPv6 only
NTP	7	x	x	x		RFC 958	–	
Scheduled traffic	2		x	x	x	IEEE802.1Qbv	3.2.8	
SDTv2	7	x	x	x	x	IEC61375-2-3	3.5.3	SIL2 data transmission protocol
SDTv4	7	x	x	x	x	CTA D3.5	3.5.3	SIL4 data transmission protocol
SNMP	7	x	x	x	x	RFC 1901, RFC 1905, RFC 1906	3.5.5	
Stream reservation	2		x	x	x	IEEE802.1Qcc	–	
SSH	7	x	x	x	x	RFC 4250	3.5.7	
syslog	7	x	x	x		RFC 5424	3.5.7	
TCP	4	x	x	x	x	RFC 793	–	

Protocol	OSI	Interface				Specification	Chapter	Comment
		ED	ECN	ED-X	ETB			
Time synchronization	2		x	x	x	IEEE802.1AS-rev	3.2.7	
TRDP	5/7	x	x	x	x	IEC61375-2-3 CTA D3.5	3.5.2	Extension for scheduled traffic in CTA D3.5
TTDB Manager	7	x	x	x		IEC61375-2-3	3.5.5	
TTDP	3				x	IEC61375-2-5 CTA D3.5	3.2.10	Support of ETB Topology variant D in CTA D3.5
UDP	4	x	x	x	x	RFC 768	–	
VLAN	2	x	x	x	x	IEEE 802.1Q	3.2.6	
VRRP	4		x			RFC 5798	3.2.10	

2.9 TIME SYNCHRONIZATION

2.9.1 General

The clock synchronization between network devices and end devices serves an important role in the overall design of the NG-TCN. It is prerequisite for the “time sensitive” network, in that it allows to assign and reserve time slots for certain classes of real-time traffic to avoid “collisions” (not collisions in the sense of CSMA/CD but queuing of same priority packets). Overall time synchronization serves multiple purposes:

- Use of scheduled traffic (see 3.2.8), which would not be possible without having exact knowledge of time
- Process synchronization. Leads to low and reproducible latency between distributed processes and high-performance operation and optimized resource use
- Exact time stamping for logging. Allows to establish an unambiguous consolidated log over distributed system devices.
- Wall clock time presentation. Present time in human readable time-of-day format. No need for additional legacy time synchronization protocols like NTP.

AVB/TSN uses clock synchronization in accordance to IEEE802.1AS-rev [27] (also known as gPTP), which in turn is based on IEEE1588-2008 (also known as PTP v2). gPTP requires the use of two-step processing with an optional one-step processing mode.

2.9.2 Syntonization vs Synchronization

Syntonization describes a mechanism to tune the clock frequency of a slave clock to the clock frequency of a master clock. After syntonization the clocks have a constant but arbitrary time offset to each other.

Synchronization leads to a state where master and slave clocks are synchronized and their offset is zero. To achieve the synchronization the slave clock is detuned until the time offset reaches zero. Or (for larger offset) the slave clock's time is set to the master time. Just setting the time on a slave

clock may lead to a non-monotonic time but is an approach for fast synchronization. It may be readily done during initial bootup, but it is unwanted during normal operation.

If a clock is used for relative time measurements only (as for example required in a transparent clock) syntonization is sufficient.

2.9.3 Hardware vs Software implementation

High timing accuracy requires hardware support on switches and end devices to implement precise time stamping and precise clocks as source of those time stamps. Devices implementing IEEE 802.1Qbv-2015 scheduled traffic readily support hardware time stamping and hardware clock syntonization. If certain end devices do not need to participate in TSN but still want to join the synchronization they may use a PTP software slave clock implementation using software time stamping and ordinary system clock instead of hardware timestamping.

2.9.4 Steady state vs. start up and coupling

In the steady state, when a basic synchronization is established, the clocks are kept syntonized by slightly tuning the frequency of the slave clocks. The output of fault-tolerant average (FT AVG) can be used as input for tuning the frequency. During start-up the clocks are typically largely out of sync, so that small frequency adjustments are not feasible. Then the clock's time value is tuned.

The same applies for coupling consists. Using that mechanism and with the prerequisite that the clock counters and frequency adjusts are implemented in hardware accuracies of well within 1 μ s can be reached.

Mechanisms how to cope with the initial setting of clocks are not standardized and are application dependent. The synchronization of the clocks on ETB should be established after 1 s after coupling or decoupling. The start-up is less critical and may take some more time. During de-/coupling the time domains on ECN shall not be influenced and shall stay synchronized.

2.9.5 NG-TCN clock domain architecture

The goal of the NG-TCN clock domain architecture is to establish a robust synchronization which is fault tolerant and redundant to increase the system availability. This is reached by introducing multiple clock masters (see 3.2.7) and with different gPTP domains on ETB and in ECNs.

A clock domain encompasses all the consist switches, ETBNs and end devices which are synchronized to the same master clock. All devices connected to one TCMS consist network will be part of a single clock domain. To not disrupt the local operation of a consist network it makes sense to separate clock domains of individual consist networks.

The base of the concept is the presence of multiple potential ETB level master clocks (called global master clock GlobalMC) which are located in the ETBNs. The GlobalMCs of the first and last consist of a train contribute to the establishment of a “synchronization domain” that spans the ETB. As every consist has two ETBNs this results in four GlobalMCs. After those four are synchronized each of them sends its timing information on the ETB on an own gPTP clock domain. A gPTP clock domain is defined as a combination of the communication path over which the time information messages are distributed and the time information they contain. Each ETBN receives information from these four clocks and calculates a fault-tolerant average (FT AVG) of the time and adjusts its own clock accordingly.

Multiple GlobalMCs (2-4) are needed to increase the ability of fault detection and fault distribution mitigation.

By using *two clocks* only, detection potential is limited – clocks can be compared, and it can be detected that something is wrong, but it cannot be determined which clock is failing, so the operation cannot be continued safely.

With *three clocks* in a system, 2 out of 3 voting can be applied and work well in case of simple, consistent and common mode failures, such as when the failure appears the same way at all nodes.

If *four clocks* are used to provide time in a system, mechanisms such as fault-tolerant averaging (FT AVG) can be applied to rule out wrong timing information.

Besides the ETB the ECNs need a common understanding of time also. This leads to different possible synchronization domain architectures that require a different amount of (logical) clocks. These are shown in Figure 16, Figure 17 and Figure 18.

Figure 16 displays an architecture with mixed synchronization domains on ECN- and ETB-level which was presented by Safe4RAIL. The first and last consist holds the GlobalMC_1-4 which can be placed in the ECN. The GlobalMCs span the synchronization domain on both (redundant) ETB lines. Because the used GlobalMCs are located in the ECN the first and last consist must be synchronized to the ETB clock domain.

The other consists shall have their own clock synchronization domain to be independent to changes on ETB for example during coupling or train inauguration. Therefore, they need an own master clock on consist level. Moreover, a redundant master clock is demanded. The clocks which are used in the first and last consist as GlobalMCs can act in the intermediate consists as consist level master clocks (ConsistMC). Each clock will send data over at least 2 gPTP clock domains (in both directions of the ring) for redundancy (the same way as depicted in the last and first ECN), resulting in 4 gPTP clock domains in an ECN.

ED-S will receive the time information from the two clocks. The information of each clock is moreover received redundant. Because of the A-/B-Plane approach the ED-S is connected twice in the ECN. It is in the responsibility of the ED-S to handle that clock information and merge the redundant messages received.

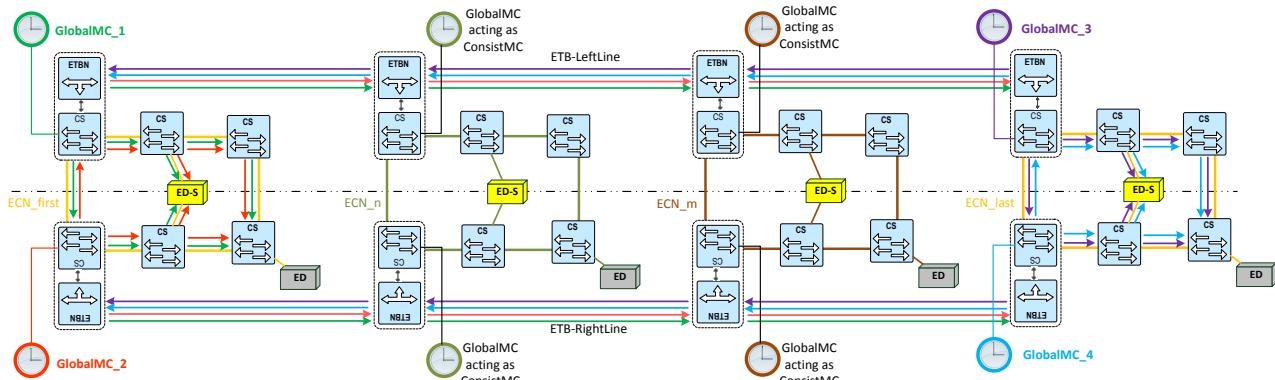


Figure 16: mixed synchronization domain architecture

For simplicity all ETBNs and CS shall be designed the same way and only differ in configuration. But in each ECN only two clocks with a special role (GlobalMC) are needed. And this equals the amount of ETBNs per ECN. This leads to the question why not move the GlobalMCs to the ETBNs and use normal clocks of the CSs as ConsistMCs. With two active master clocks in each ETBN the architecture in Figure 17 is possible. In this variant every ECN domain is independent from the synchronization domain on the ETB lines. The advantage is that a train inauguration can take place without influencing the ECN clock domains directly.

Like in the mixed architecture, time information from a GlobalMC is routed through the ECN to the “opposite” ETB. For example, messages from GlobalMC_2 are routed through the first ECN to the ETB-LeftLine. The synchronization domain stays the same on both (redundant) ETB lines. In this architecture it is recommended that the CS and the ETBN to which the CS is connected to are one device.

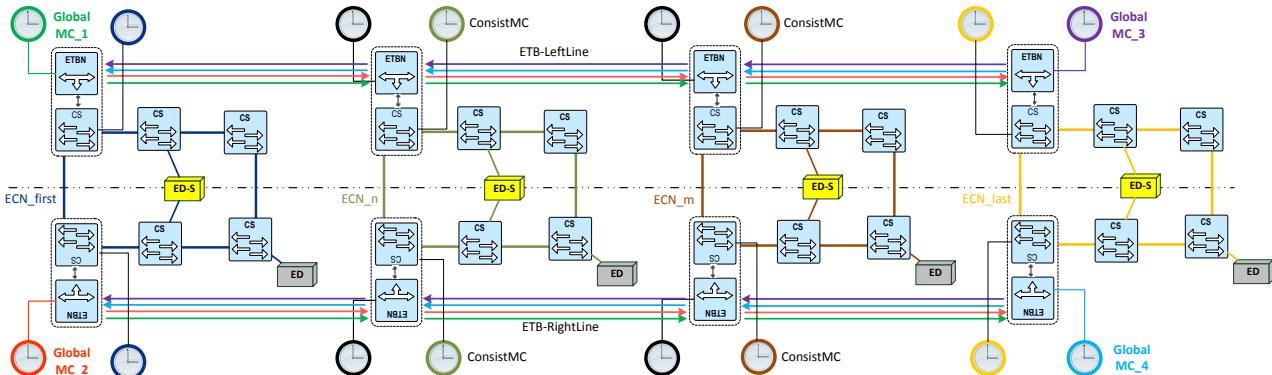


Figure 17: all independent (async) synchronization domain architecture

Another alternative where all ETBNs are designed the same way is depicted in Figure 18. This architecture features only one clock in each ETBN. The intermediate ETBNs act as a boundary clock (BC) and synchronize the ECNs to the clock domain of the ETB. This results in an all synchronized train where only one synchronization domain exists for all ETB-Lines and ECNs. This reduces the number of needed clocks, influences the latency in a possible way and a mapping of the different clock domains is not needed. But the clock domain in every ECN is affected by any resynchronization due to coupling.

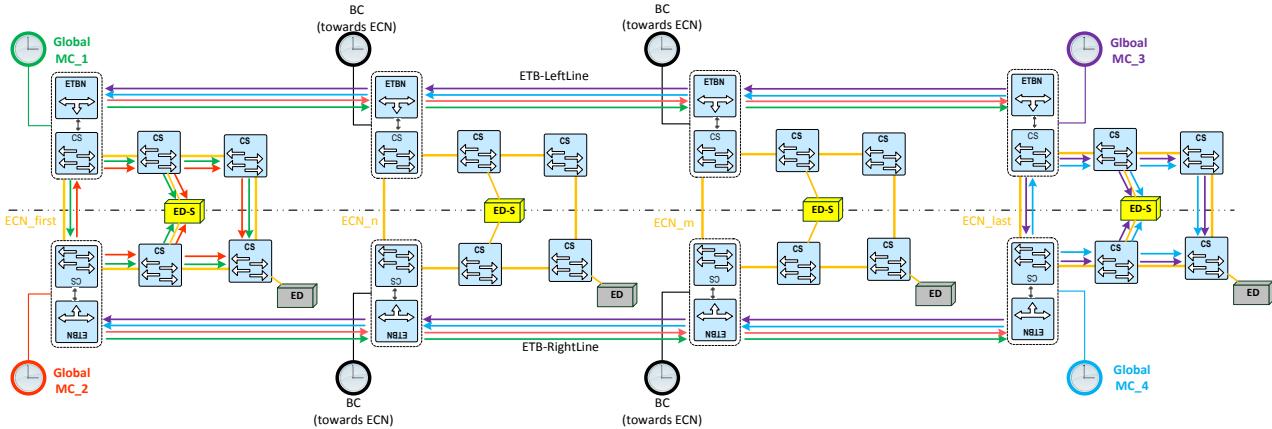


Figure 18: one (all sync) synchronization domain architecture

Currently the favored architecture is the “all independent synchronization domain architecture” because of the independency of the ECNs. This architecture seems to be able to handle synchronization processes during inauguration more easily. It has to be proven in CTA-2 if TSN works in appropriate way with this architecture including the additional needed features like the TSN Gateway.

Moreover, it can be tested if “an all synchronized architecture” brings a higher benefit in regards of timing without introducing problems during the inauguration.

2.9.6 Clock properties

This chapter describes the requirements of the master clocks with special roles (ConsistMC, GlobalMC) and the functions they should feature.

Each ConsistMC or GlobalMC shall:

- identify and mitigate abrupt time changes, jumps (transient) and ramps (permanent)
- optional: identify their own faults and retreat from synchronization on complex fault scenarios (high-integrity clock)
- minimize and avoid chance of injecting synchronization faults into the system and impeding system operation

If an ETBN is not part of the ECN, then a CS must have a clock. The clock source can but doesn't have to be an external one.

A “stratum 3” class TCXO oscillator (short time stability < 1E-9 @10 s) is deemed sufficient and is therefore recommended.

2.10 SECURITY CONCEPT

2.10.1 General

The security concept as defined within this document aims to identify security risks of a NG-TCN, to propose counter measures and to allocate those countermeasures to the components which constitute the NG-TCN (security requirements).

Adopting the approach taken in Roll2Rail for the WTCMS (see [08]), the standard ISA/IEC 62443 will be used as a basis for activities addressing the NG-TCN security. Consequently, the risk assessment proposed for the NG-TCN (System under Consideration – SuC) follows the workflow specified by the novel draft version of ISO/IEC 62443-3-2 [22]. The purpose of the TCMS risk assessment is to derive a justified set of security requirements, i.e. the requirements that express the countermeasures which, when implemented, will reduce the security risk to an acceptable level. The risk matrix and the risk acceptance level are defined specifically for the TCMS cyber security risk assessment in CTA Task 3.3.

The methodology of cyber security risk assessment and security architecture definition is described in [05]. The security architecture bases on the concept of zones and conduits, and the process leading to the security architecture is defined by a set of six zone and conduit requirements:

Table 11: Zone and Conduit Requirements (ISO/IEC 62443-3-2 (draft))

ZCR 1	Identification of the SuC
ZCR 2	Perform a high-level cyber security risk assessment
ZCR 3	Partition of the SuC into zones and conduits
ZCR 4	High-level risk exceeds tolerable risk?
ZCR 5	Perform a detailed cyber security risk assessment
ZCR 6	Document cyber requirements for additional security countermeasures

Identification of the SuC (ZCR1) and zone and conduit partitioning (ZCR3) are clear architecture related tasks and are addressed in this document. The high-level cyber security risk assessment (ZCR2), which is needed for the zone and conduit partitioning, has been done in CTA Task 3.3. The remaining activities ZCR4, ZCR5 and ZCR6 required a deep security analysis of the different zones and conduits and have therefore also been executed in CTA Task 3.3. Solutions for the derived requirements for security countermeasures are then again subject of this document.

2.10.2 System under Consideration (ZCR1)

The System under Consideration is the NG-TCN including the interfaces to end devices, wireless and legacy communication interfaces as shown in following figure.

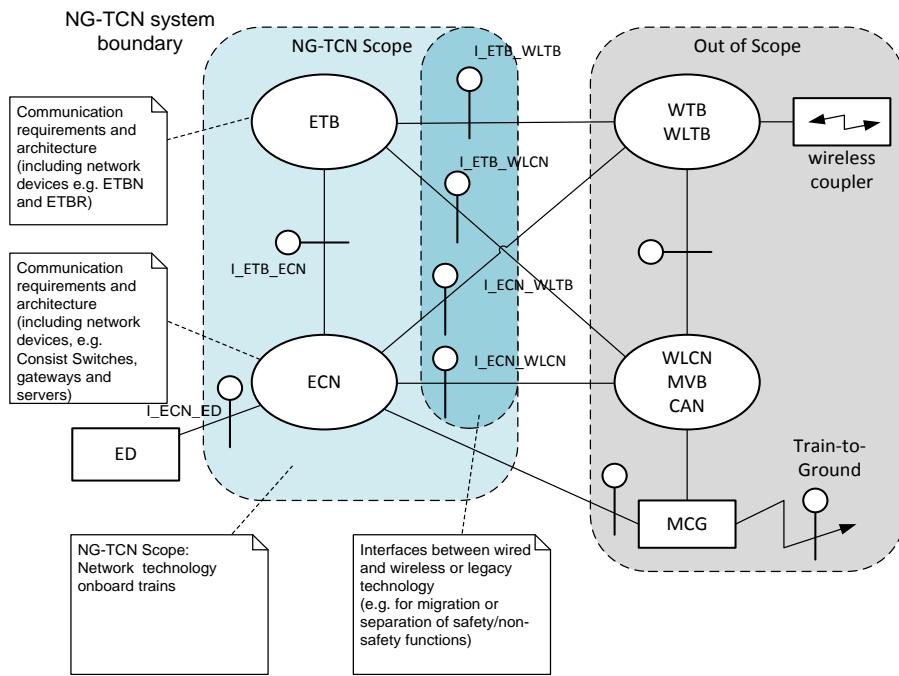


Figure 19: NG-TCN Scope Diagram⁹

The scope of NG-TCN comprises the ETB and ECN with all their assets (hardware and software) and the interface I_ETB_ECN between these networks. In addition, it covers the interface I_ECN_ED to end devices.

Furthermore, interfaces between NG-TCN and wireless networks as defined in [09] are in scope (I_ETB_WLTB, I_ETB_WLCN, I_ECN_WLTB, I_ECN_WLCN). Interfaces to legacy network technologies as defined in IEC 61375 series (WTB, MVB and CAN) are possible and therefore in scope of NG-TCN, but are not further analysed herein, because CTA WP3 is aiming for a pure IP based train onboard network.

A special case is mixing of ETB with WLTB via interface I_WLTB_ETB. Those mixed architectures have been analysed in Roll2Rail WP2 and are for that reason not dealt with in this paper (see [08] and [09]).

Out of scope are:

- the legacy networks, as already defined by IEC61375 series (WTB, MVB and CAN)
- wireless networks as defined in [09]
- wireless couplers (e.g. short-range radio couplers or optical couplers), which may be used to replace conducting contacts by galvanic isolated links to solve the challenge of potential difference between consists; wireless couplers can be viewed as repeaters without network protocol stack.

⁹ The MCG is considered as another ED from this specification point of view. Particularities regarding to the MCG as an ED will be specified in CTA WP2 and as part of IEC61375-2-6 standard.

Note: The MCG uses the same interface I_ECN_ED like other end devices to connect to the wireless consist network. The interface, for the specific services of the MCG, is specified in standard IEC 61375-2-6.

2.10.3 High Level Cyber Security Risk Assessment (ZCR2)

A high level cyber security risk assessment for the whole TCMS system including its functional domains TCMS, OOS and COS has already been executed in Roll2Rail [08]. This analysis considered 3 functionalities, one from each domain, to perform the high-level cyber security risk assessment. These functionalities were: Wi-Fi network for passengers from COS domain, CCTV for video surveillance from OOS domain and External Door Control from TCMS domain.

First it has been evaluated if this analysis can be taken as basis for the NG-TCN security architecture. Due to following reasons, it was decided to create an own analysis:

- The analysis of Roll2Rail is considering a wireless network only.
- The analysis of Roll2Rail is focusing on special devices, but the NG-TCN security architecture shall be more generic.
- The threat landscape used in Roll2Rail was taken from ENISA ETL but in the meantime a railway specific threat landscape has been created by X2Rail-1 WP8.

The high level cyber security risk assessment shows that the likelihood, but especially the impact of threats to the functions of the different functional domains is different. For instance, a man-in-the middle attack in COS may be used to steal passenger data and to misuse it, while the same attack in TCMS might compromise safety leading to catastrophic events. This suggests defining a security architecture which respects those differences.

2.10.4 Security Architecture – Security Zones and Conduits (ZCR3)

For the partitioning of the SuC in Zones and Conduits the ISO/IEC 62443-3-2 [22] gives some general recommendations and guidance, like for instance to base upon the results of the high-level cyber security risk assessment, the criticality of assets, operational function, physical or logical location and required access. For the SuC defined in this document, the Roll2Rail proposal for partitioning, which already bases on the criteria mentioned above, is judged to be an appropriate solution also for NG-TCN. Therefore, the proposed partitioning of the SuC in Zones and Conduits follows the approach taken in Roll2Rail [08] with the following differences:

- The Roll2Rail zones “TCMS”, “TCMS consist”, “OOS”, “OOS consist” and “COS” are no real zones because they are not really matching the criteria for zones as defined in [22]. Hence, they are here only used as a container for zones and conduits belonging to one of the functional domains (“zone groups”).
- The wireless train backbone zone (zone TCMS_WLTB) is replaced by a wired train backbone zone (zone ETB).
- The zone for wireless connected regular TCMS devices (zone TCMS_Const_Regular_Wireless) has been removed because all TCMS devices shall be wire connected for reliability reasons.

Zones using wireless technologies (shaded in light grey) are covered by the work done in Roll2Rail [08] and are not further discussed within this document. Interested readers may consult [08] for a detailed security analysis of the wireless network technology.

The zone and conduits security architecture proposed for NG-TCN distinguished three main security zones, which are related to the three functional domains:

1. TCMS security zones (shown in Figure 20)
2. OOS security zones (shown in Figure 21)
3. COS security zone

Note: The COS security zone is not further considered since securing this zone would be expensive with a very uncertain return on investment. However, the conduit between the COS and OOS domain has been considered.

Definitions of all zones and conduits can be found in H.

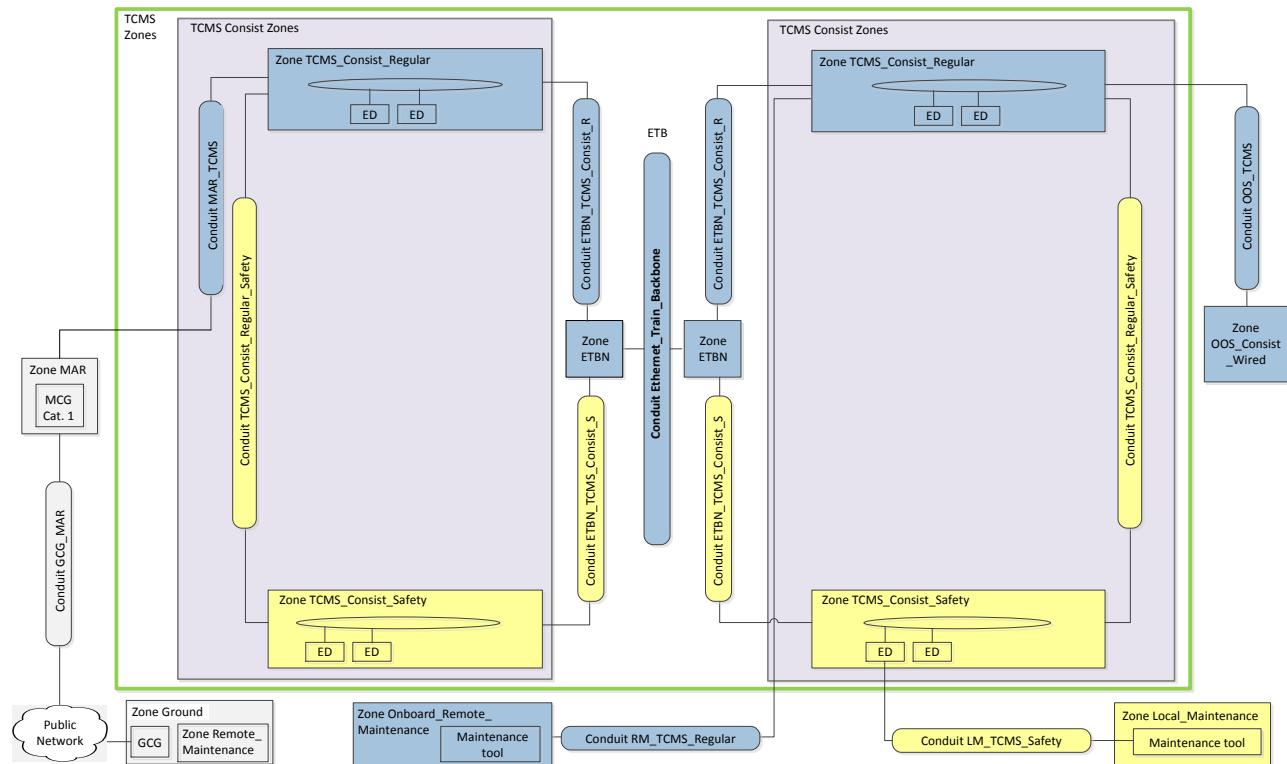


Figure 20: Overview of TCMS security zones and conduits

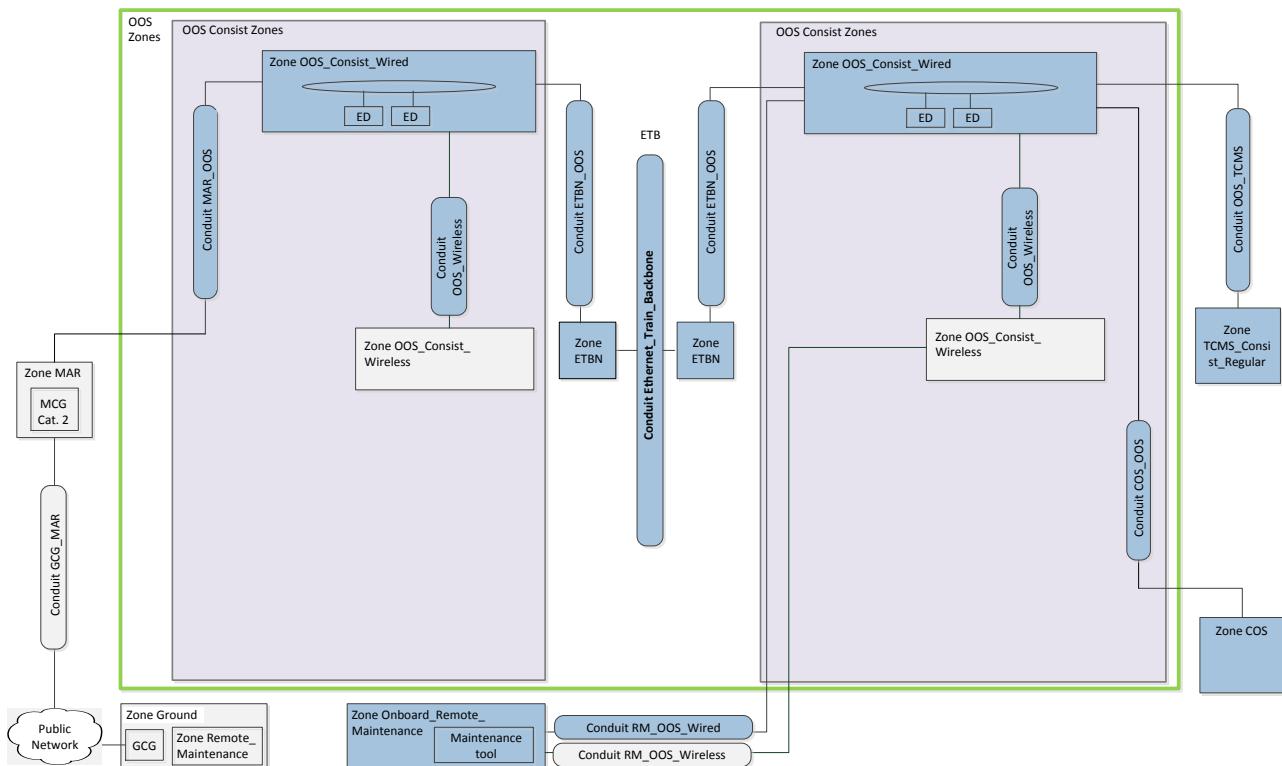


Figure 21: Overview of OOS security zones and conduits

2.10.5 Detailed Cyber Security Risk Assessment (ZCR5)

The detailed cyber security risk assessment has been executed within CTA Task 3.3, see [05].

2.10.6 Cyber Security Requirements and Counter Measures (ZCR6)

Security requirements are derived from the detailed cyber security risk assessment and are subject of CTA Task 3.3, see [05]. Measures which shall counter identified security risks, and which shall satisfy the security requirements, are defined in chapter 3 in relation to the communication layer they belong to.

2.11 RAMS ASPECTS

One aim of the NG-TCN is to support CONNECTA's KPIs (see [02]) which address the main goals of Shift2Rail:

- Decreasing the life cycle cost of railway transports to 50%
- Increasing railway capacity up to 100 %
- Increasing reliability and punctuality up to 50%

These main goals have some important links with the RAMS performances needs for the NG-TCN. The Safety parameter is not explicitly included in Shift2Rail's KPIs, but the European Union Railway Agency regulations don't permit to place in service a rolling stock with a lower safety level than the existing ones. This means that Safety is at least implicitly included in the Shift2Rail goals.

The following paragraphs study some key functions or architecture key points necessary to reach the objectives for RAMS of the NG-TCN as described in chapter 3 of the D3.1 [03]. The RAMS requirements expressed in [03] are compared to the principles used for NG-TCN architecture in order to check whether these requirements are fulfilled or not. For some requirements, a more detailed explanation or justification is given in the relevant sub-chapters.

The widely recognized base of the RAMS studies for the rolling stock is the standard [3] EN 50126-1:2017. Using the definitions of this standard, we can sketch the relationship between Reliability, Availability, Maintainability and Safety in Figure 22.

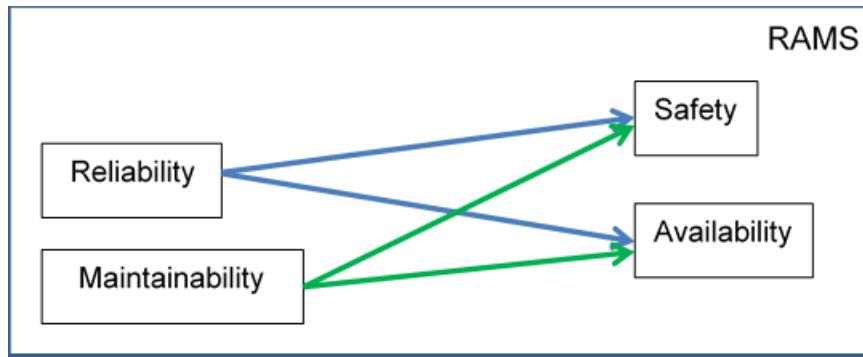


Figure 22: Connections between Reliability, Availability, Maintainability and Safety

NOTE: Testability is also closely linked to Availability, Maintainability and Safety (see standard EN 60706-5:2007 [15]) and has a great influence on it, both during the development of the system and during the lifetime of the train. Nevertheless, due to its typical link to each project, testability is not studied in this deliverable.

2.11.1 Reliability

Reliability requirements and information for the NG-TCN are referenced from ID_20000 to ID_20005 in the document [03] and are summarized in the Table 12 below. The relevant implementation(s) of each requirement is (are) detailed in the column "implementation" of the same table.

Table 12: Reliability requirements and information

ID	Requirement	Remark	Implementation
ID_20000	<i>Reliability of the TCN system is defined as the probability of the system to execute the required function in a correct way when it is working in the environment which it has been designed for.</i>	<i>Information</i>	<i>Not relevant</i>
ID_20001	<i>This probability is measured with the failure rate λ, which is the inverse of the value of the mean time between failures (MTBF): $MTBF = 1/\lambda$</i>	<i>Information</i>	<i>Not relevant</i>

ID	Requirement	Remark	Implementation
ID_20002	The architecture of the NG-TCN shall be designed to reach the required failure rate in a way that the NG-TCN can continue executing its functionality correctly in case of a failure which can lead to a service failure.		Requirement fulfilled mainly by using redundancy to avoid consequences of a single failure. Some complementary mitigations are proposed in the chapter 3.2.2 and the Annex C2 FMECA_analysis of the document [05].
<i>ID_20003</i>	<i>Service failures are considered those failures which could lead to one of the following scenarios: train must be towed, train must be withdrawn immediately, train must be withdrawn at the end of the line, or a significant delay is experienced during service. An error in a safety function may also lead in a service failure.</i>	<i>Information</i>	<i>Not relevant</i>
ID_20004	The maximum failure rate of each function of the NG-TCN shall be: $\lambda \leq 10^{-7}$ failures/hour NOTE: only functions which may cause a service failure as defined in ID_20003 are affected		Using error detection mechanisms and redundancy to ensure the best functional reliability. Nevertheless, this requirement is not reachable without complementary actions. See sub-chapter below.
<i>ID_20005</i>	<i>Failures of the end systems, Human Machine Interface and components which will not be part of the TCMS system are not considered within this value.</i>	<i>Information</i>	<i>Not relevant</i>

We can see in Table 12 that ID_20002 and ID_20004 are requirements for the Reliability of the NG-TCN while the other lines present information to understand these requirements.

NOTE: the failures/hour for ID_20004 shall be interpreted as hours of operation of the NG-TCN.

ID_20002

This requirement makes a direct link between the performance of the NG-TCN and the expected service of the train from an operational point of view.

From a global point of view, the requirement is not purely relying on the performance of the NG-TCN but also on the architecture of the TCMS itself.

As a matter of fact, whatever is the level of performance of the NG-TCN it shall be supported by an optimised distribution of the train functions over the ED and the ED-S. The optimisation of this distribution is a work done by train suppliers by means of proprietary methods during the descending branch of the "V cycle" by instance.

Once this point is decided, the topology of the NG-TCN (ECN and ETB) is able to minimize the impact of a "failure which can lead to a service failure." by application of the following principles:

- Split of train network and consist network
- Using the best topology for ETB to minimize the number of equipment
- Using redundancy to ensure the best functional reliability

ID_20004

The deliverable of task T3.3 [5] (D3.3 – Report on RAMS and Security Analysis) demonstrates in chapter 4.4.2 that the required THR is not reachable by the existing detection mechanism without further and complementary measures. These measures might have some impacts on the SW and HW part of the architecture of the NG-TCN.

Furthermore, the paragraph 3.5 of [5] emphasis that "next steps of the project shall be to mitigate all single point failure modes of the network in order to define a robust network architecture and fulfil the requirement ID_20004", despite the mitigation proposals done in [5]

2.11.2 Availability

Availability requirements for the NG-TCN are referenced as ID_40019 and ID_40020, and as ID_30000 to ID_30014 in the document [2] and are summarized in the Table 13 below. The relevant implementation(s) of each requirement is (are) detailed in the column "implementation" of the same table.

Table 13: Availability requirements

ID	Requirement	Implementation
ID_40019	Intra-consist communication shall not be interrupted during coupling or uncoupling of consists. NOTE: this might contradict the need of train wide clock resynchronization after inauguration.	- Definition of clear functional roles - Two stages topology (ETB & ECN) - Ensure clock synchronisation, but some problems still exist, especially with handling on ED level. This issue is detailed in chapter 2.9.4. - All the architectures considered guarantee the independence between ECN and ETB.
ID_40020	A powerless or defective vehicle or consist shall not interrupt the train wide communication between consists which are not affected by the power loss/defect.	The convenient topologies are defined in sub-chapter 2.5.2 . Most of the topologies (3/4) fulfil this requirement, except ETB topology variant D ₁ which does not tolerate complete powerless consists.
ID_30000	A single point of failure in the network (e.g. wire-break, short cut, device defect) should not lead to a partial or complete communication loss of the entire NG-TCN. EXAMPLE 1: train wide communication shall not be affected by an ETBN being out-of-order EXAMPLE 2: a defective consist switch may only disrupt the communication of end devices directly connected to it, but not the communication between other end devices.	Requirement fulfilled by: Using redundancy to avoid consequences of a single failure. The redundancy is used in many ways: - redundancy of ETB line (relevant to example 2) - redundancy of equipment (e.g. ETBN repeater (relevant to example 1), Ethernet connectors). Some complementary mitigations are proposed in the chapter 3.2.2 and the

ID	Requirement	Implementation
	EXAMPLE 3: a defective WLAN access point may disrupt the communication of wireless end devices associated to it, but not the communication between other end devices.	Annex C2 FMECA_analysis of the document [05]. Those mitigations do not allow to mitigate all the single points of failure.
ID_30001	A single point of failure in one ED or one ED-S should not lead to partial or complete communication loss of the NG-TCN.	This point is covered by the restriction of the broadcast domains. A-Plane and B-Plane usage permits to ensure the requirement for ED-S. Multiple communication paths permit it for the non-safety ED.
ID_30003	Special Environmental constraints should be defined to keep the bit error probability very low (wiring instructions) for a higher availability in general.	Use of multiple devices (e.g. multiple connectors) and appliance of railways state of the art manufacturing rules (e.g. European standard EN 50155 [11], EN 50121-2-3 [12], etc.) ensure to reach this goal.
ID_30004	Network Components only with reported MTBF by the supplier should be used in the network for a quantitatively calculation of the availability.	This requirement shall be a point of attention between the supplier and the customer. This question is tackled by recommending the usage of technology diversity.
ID_30006	An ED-S with main controlling functions of other ED (e.g. IO devices) should be redundant and operate in a "cold-stand by" mode with a maximal switchover time.	This requirement is fulfilled by: - Using the concept of A-Plane and B-Plane, - Using the redundancy of the ED as generally requested in the clause 4.5.4 of [20].
ID_30007	The maximum time for the permitted interruption of a communication over NG-TCN shall be less than 0.1 s (consist network) and 1.0 s for train backbone. NOTE: A possible solution for ECN could be the use of ring topology.	For the ECN: - ECN topology might be optimized to lower the reconfiguration time (e.g. by using ring topology). - For both ECN and ETBN: using TSN is a way to minimize this configuration time (see sub-chapter 3.2.8 in this document).
ID_30011	The network quality should be traceable via standard tools and functions for providing early failure detection.	Following the standards [19] and [20] ensures the existence of ETBN and ECN quality parameters, reachable by standard tools.
ID_30012	In case of a replacement of an ED or ED-S, it should be possible, that the network itself provide the necessary configuration (include addressing) parameter, so that the device replacement without removable media can take place. NOTE: Intention is to reduce mean-time of repairing	The TTDB info is used to fulfil this requirement (see [18]).
ID_30014	The ED or ED-S should have the possibility to be connected to a redundant power supply without interferences to each other.	This requirement is not directly addressed by D3.5. Nevertheless, it is a usual requirement to ensure real redundancy between systems as proposed in this document.

2.11.3 Maintainability

Maintainability requirements and information for the NG-TCN are referenced as ID_40069 and ID_60034 in the document [03] and are summarized in the Table 14 below. The relevant implementation(s) of each requirement is (are) detailed in the column "implementation" of the same table.

Table 14: Maintainability requirements

ID	Requirement	Implementation
ID_40069	<p>It shall be possible to manufacture consists with identical NG-TCN configuration, except for the consist identifier which must be unique for each consist.</p>	Proposing the NG-TCN architecture as a new work for [9] shall insure the fulfilment to this requirement for all the rolling stock that will follow these standards.
ID_60034	<p>ED-S and ED shall implement an alarm to request specific maintenance operations</p> <p>NOTE:</p> <ol style="list-style-type: none"> 1) ED shall provide an alarm-service for internal malfunction of ED. 2) In the context of preventive maintenance, ED-S shall provide an alarm service for internal malfunction of ED-S. 3) ED-S and ED shall provide an alarm-service for internal deviations of their operation limits (for example range temperature). 	<p>Those requirements are not directly addressed by D3.5. It is rather an assumption for safety calculations concerning the safety functions linked to the NG-TCN.</p> <p>For this reason, these are exported constraints to the ED and to the ED-S.</p>

ID_40069

This requirement is a consequence of two different needs, one from the LCC and one for the operation of the train/consist:

- From the LCC: once the configuration (architecture, SW and HW definitions, etc.) is set up the maintainability is eased if the largest possible number of consists can be equipped with this configuration. Thus, by contrast to today, not only the consists themselves but also the software tools (to support complex maintenance) and the working processes for maintenance, which have an important impact on the maintenance costs, will minimize the project dependency. The cost of those tools will also be shared among many projects and also among a high number of stakeholders, what will decrease their cost.
- For the train/consist operation: there shall be only one unique identifier for a given consist, for many reasons. Some of them are:
 - The distinction of each consists in a train made of many consists as all the train commands might not consider in the same way all the consists (e.g. for door selective opening). For that item, the general principles of architecture proposed in this document has proven for many years its efficiency.
 - The distinction of the trains/consists if virtual coupling is developed in the future.

- The requirement for the operators to be able to know the complete configuration of each rolling stock with regard to the European Regulation.

2.11.4 Safety

Safety requirements for the NG-TCN are referenced from ID_30102 to ID_30109 in the document [03] and are summarized in the Table 15 below. The relevant implementation(s) of each requirement is (are) detailed in the column "implementation" of the same table.

Table 15: Safety requirements

ID	Requirement	Implementation
ID_30102	The HW of the ED-S has to fulfil a hazard rate THR of ED-S = 2 10E-11.	This requirement is not directly addressed by D3.5. It is rather an assumption for safety calculations concerning the safety functions linked to the NG-TCN. For this reason, it is an exported constraint to the ED-S.
ID_30103	SW executing safety related functions have to be developed in accordance to EN50128 SIL4.	This requirement is not directly addressed by D3.5. It is rather an assumption for safety calculations concerning the safety functions linked to the NG-TCN. For this reason, it is an exported constraint to safety relevant devices (ED-S or ETBN). Chapter 2.7.3 proposes to mitigate this by using technology diversity.
ID_30104	The relevant safety functions (Software) operating on ED-S has to fulfil the requirements of EN50128 and IEC61508 against random errors. (data corruption in memories, unexpected behaviour of COTS RTOS).	This requirement is not directly addressed by D3.5. It is rather an assumption for safety calculations concerning the safety functions linked to the NG-TCN. For this reason, it is an exported constraint to the ED-S.
ID_30105	A redundant HW-Structure of ED-S should be chosen for error-detection in each of the HW-Channel follow at least 1oo2 failsafe principle.	This requirement is not directly addressed by D3.5. It is rather an assumption for safety calculations concerning the safety functions linked to the NG-TCN. For this reason, it is an exported constraint to the ED-S.
ID_30106	The result of the train inauguration is needed for the detection of addressing errors in case of a safety relevant inter consist communication. Therefore, the train inauguration and the storage of the result needs to be done in a safe manner.	See the chapter 4.4.1 of [5] for a detailed explanation of the consequences of this requirement on the main NG-TCN devices (ETBN and ESC).

ID	Requirement	Implementation
ID_30108	For better Diagnostic Coverage (DC) in the case of an increasing bit error probability it could be useful to read some statistic information (for example CRC-Error) via SNMP. Therefore, the switches should have implemented MIB2 and has to provide them via SNMP.	Following the standard [8], chapter 4.9.2 ensures the fulfilment of this requirement.
ID_30109	Network components which mimic failsafe telegrams are not allowed during failsafe operation.	This requirement is not directly addressed by D3.5. It is rather an assumption for safety calculations concerning the safety functions linked to the NG-TCN. For this reason, it is an exported constraint to the ED and to the ED-S

3 COMMUNICATION LAYERS

3.1 PHYSICAL LAYER

3.1.1 Media (media definition incl. cabling and connectors)

100BASE-TX (100FDX)

100 Mbit Full Duplex Ethernet (100FDX) as specified in [29], clause 25, is defined in IEC61375-2-5 (ETB) and IEC61375-3-4 (ECN) as the standard technology for the Ethernet based TCN. The following paragraphs summarize the technical specification.

100FDX Ethernet Links

An Ethernet link is the connection from port to port between two devices, including both end connectors and intermediate (e.g. inter-vehicle) connectors.

All ND are by default configured for 100FDX.

All Ethernet links have to comply with ISO/IEC 11801 class D channel. Some basic characteristic values are:

Bandwidth: 100 MHz

Impedance 100 Ω

Max. Length 100 m

The achievable length of an Ethernet link is determined by the cable quality and the number and location of intermediate connectors and can in practice be lower than 100m.

100FDX Ethernet ports

Ethernet ports are the physical interface between an ED or an ND and the Ethernet link and connect the Ethernet link with the switching fabric as described in 3.3.2.2. An Ethernet port consists of the parts:

- Mechanical connector.
- Magnetics. Provides common mode voltage rejection and ensures galvanic isolation by a transformer. This can be seen in the example of Figure 23.
- Termination resistor (100 Ω)
- Ethernet-Phy. The Ethernet-Phy is responsible for parameter negotiation (auto-negotiation of transmission speed and half-/full duplex transmission) and for the coding/encoding of the signal.

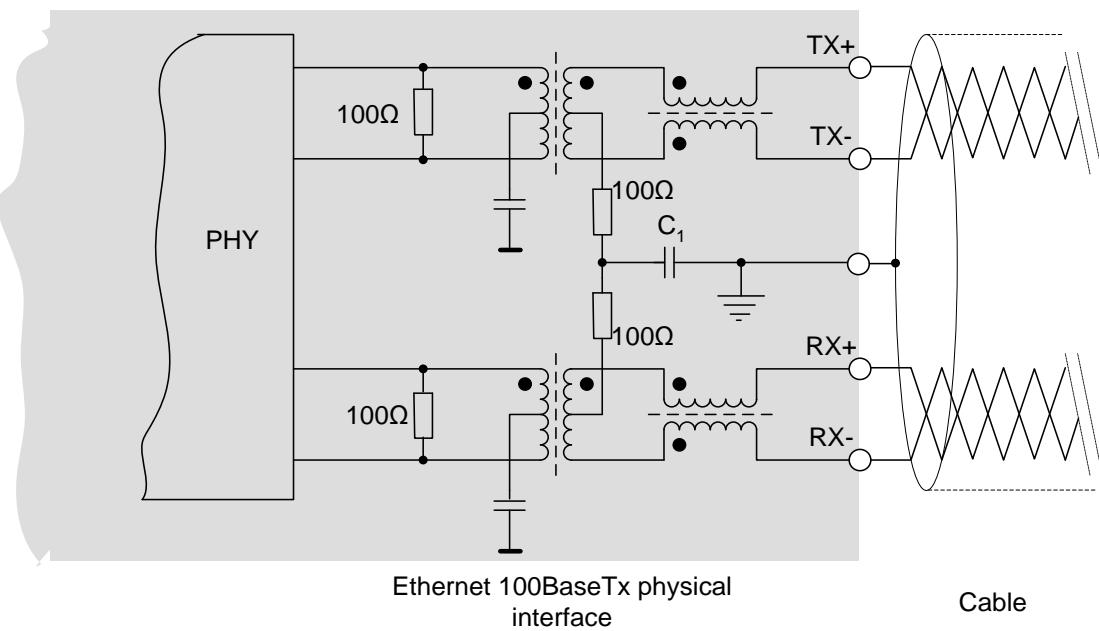


Figure 23: Ethernet 100FDX Physical Interface

Cable and Connector

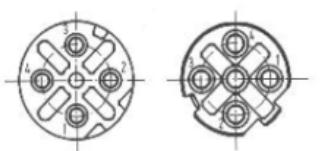
100FDX Connector for active Network Devices - M12 D coded

Active network devices use a 4-lead M12 D-coded circular connector type for connecting to 100FDX cables.

Crimped contacts recommended. Female connector on active network device, male connector on train cable.

Conformance to IEC 61076-2-101, which defines the pin out:

Signal	Function	Cable wire colour	M12 D-coding contact number
TD+	Transmission Data +	Yellow	1
TD-	Transmission Data -	Orange	3
RD+	Receiver Data +	White	2
RD-	Receiver Data -	Blue	4



Female and male connector

100FDX Connector for interior cabling (between walls, cabinets, container, etc.)

Ethernet circular cell arranged in a quartet distribution. Pin out distribution identical to M12:

- TD+: Contact 1, TD-: Contact 3
- RD+: Contact 2, RD-: Contact 4

For cabling railway suitable CAT5e cables in star-quad arrangement are proposed.

1GbE (1000BASE-T)

NG-TCN requires higher transmission rates at least for ETB and for the ECN ring. The following paragraphs summarize the technical specification for 1Gbit Ethernet (1GbE) as it is specified in [29], clause 40.

GbE Link

A GbE Ethernet link is the connection from port to port between two devices, including both end connectors and intermediate (e.g. inter-car) connectors.

GbE Ethernet links have to comply with ISO/IEC 11801 class D channel. Some basic characteristic values are:

Bandwidth: 100 MHz

Impedance 100 Ω

Max. Length 100 m

The achievable length of an Ethernet link is determined by the cable quality and the number and location of intermediate connectors and can in practice be lower than 100m. Laboratory measurements with instrumented railway cables showed that acceptable crosstalk and SNR limits the usable cable length to approximately 80m.

Autonegotiation

Contrary to 100FDX, autonegotiation as defined in IEEE 802.3 is mandatory for GbE. Besides negotiating the transmission speed (10/100/1000 MBit/s) and the transmission mode (half-/full-duplex), GbE requires that one of the transceivers becomes the clock master. Autonegotiation uses, as for 100FDX, four of the 8 cable wires.

GbE port

GbE physical interface looks quite similar to 100FDX physical interface, except that 4 interfaces (wire pairs) are used instead of two. This is mainly because symbol rate (125 MSymbols/s) and frequency spectrum are identical for 100FDX and GbE. However, coding and modulation are distinct to 100FDX.

Cables

Similar as 100FDX, GbE requires at least CAT 5e cables, but with 8 wires instead of 4. Railway suitable cables are available on the market.

In case of a disruption of at least one wire, normally the complete link is off. If one of the wires not used for autonegotiation is interrupted, a degraded operation with 100FDX is still possible.

Connectors

Active network devices use an 8-lead M12 X-coded circular connector type for connecting to GbE cables.

Crimped contacts recommended. Female connector on active network device, male connector on train cable.

Conformance to IEC 61076-2-109, which defines the pin out, see Figure 24.

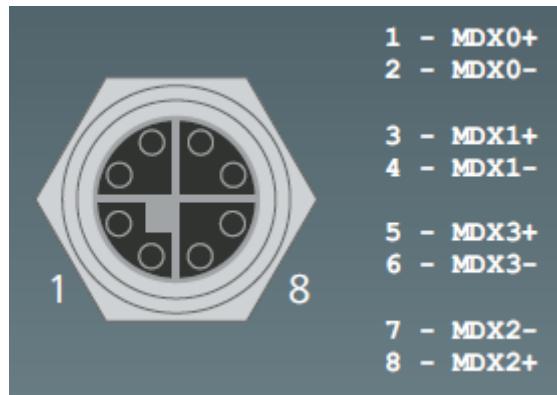


Figure 24: M12 X-coded

NOTE: There is a problem with the pin out defined in IEC 61076-2-109 because the polarity of pins 7/8 is reversed compared to the other pairs. This makes cross-cable wiring error prone. However, most vendors of switch products support this solution. To make it work for crossed cables requires the use of polarity auto-correction, which however is prohibited by IEC 61375-2-5. This issue requires further clarifications.

10GbE

Regarding the requirement ID_40042 (see [03]), NG-TCN shall support transmission rates up to 10 Gigabit Ethernet at least for ETB and for the ECN ring as an option.

Introduction

10 Gigabit Ethernet (10GE, 10GbE, or 10 GigE) is a group of computer networking technologies for transmitting Ethernet frames at a rate of 10 gigabits per second. It was first defined by the IEEE 802.3ae-2002 standard. Unlike previous Ethernet standards, 10 Gigabit Ethernet defines **only full-duplex point-to-point links** which are generally connected by network switches; shared-medium CSMA/CD operation has not been carried over from the previous generations Ethernet standards so half-duplex operation and repeater hubs do not exist in 10GbE.

The 10 Gigabit Ethernet standard encompasses several different physical layer (PHY) standards. A networking device, such as a switch or a network interface controller may have different PHY types through pluggable PHY modules, such as those based on SFP+. Like previous versions of Ethernet, **10GbE can use either copper or fiber cabling**. Maximum distance over **copper cable is 100 meters** but because of its bandwidth requirements, higher-grade cables are required.

Standards

The IEEE802.3 working group has published several standards relating to 10GbE.

Standard	Publication year	Description
802.3ae	2002 ¹⁾	10 Gbit/s Ethernet over fiber for LAN (10GBASE-SR, 10GBASE-LR, 10GBASE-ER, 10GBASE-LX4) and WAN (10GBASE-SW, 10GBASE-LW, 10GBASE-EW)
802.3ak	2004	10GBASE-CX4 10 Gbit/s Ethernet over twin-axial cable
802.3-2005	2005	A revision of base standard incorporating 802.3ae, 802.3ak and errata
802.3an	2006	10GBASE-T 10 Gbit/s Ethernet over copper twisted pair cable
802.3ap	2007	Backplane Ethernet, 1 and 10 Gbit/s over printed circuit boards (10GBASE-KR and 10GBASE-KX4)
802.3aq	2006	10GBASE-LRM 10 Gbit/s Ethernet over multi-mode fiber with enhanced equalization
802.3-2008	2008	A revision of base standard incorporating the 802.3an/ap/aq/as amendments, two corrigenda and errata. Link aggregation moved to 802.1AX.
802.3av	2009	10GBASE-PR 10 Gbit/s Ethernet PHY for EPON
802.3-2015	2015	The latest version of the base standard
802.3bz	2016	2.5 Gigabit and 5 Gigabit Ethernet over Cat-5/Cat-6 twisted pair – 2.5GBASE-T and 5GBASE-T

Figure 25: Standards relating to 10GbE (Source: [49])

10 Gigabit Ethernet and Fiber

There are three important considerations for any fiber cable deployment:

- The type of fiber cable (for example single-mode)
- The type of 10 Gigabit Ethernet physical interface (for example 10GBase-SR)
- The type of optics module form factor (for example XFP)

The following tables summarize the standard fiber cables, physical interfaces, and form factors applicable to 10 Gigabit Ethernet:

Table 16: Types of Fiber Cables for a LAN (Source: [51])

Multi-Mode MMF	62.5/125µm (OM1 grade) fiber	Previous industry standard
	50/125µm (OM2 grade) fiber	Previous industry standard
	50/125µm (OM3 grade) fiber	Current industry standard (new installations)
Single-Mode SMF	9/125µm fiber	Current industry standard

Table 17: 10 Gigabit Ethernet Physical Interfaces (PHY 10GBase-R) for Fiber (Source: [51])

Multi-Mode MMF	10GBase-LX4	Maximum range of 300m (980ft)	Previous industry standard
	10GBase-SR	“Short Range” up to 300m (980ft)	Current industry standard
	10GBase-LRM	“Long Reach Multimode” up to 260m (850ft)	Current industry standard
Single-Mode SMF	10GBase-LX4	Maximum range of 10km (6.2mi)	Previous industry standard
	10GBase-LR	“Long Reach” up to 10km (6.2mi)	Current industry standard
	10GBase-ER	“Extended Reach” up to 40km (25mi)	Current industry standard

Table 18: 10 Gigabit Ethernet Module Form Factors (Optics) (Source: [51])

XENPACK	Large form factor	Previous industry standard
X2 (XPACK)	Smaller form factor than XENPACK	Previous industry standard
XFP	Smaller form factor than X2	Current industry standard
SFP+	Smallest form factor	Current industry standard

Table 19: 10 Gigabit Operating Ranges Per Type of Fiber and per PHY (Physical Interface) (Source: [51])

	Multi-Mode MMF			Single-Mode SMF
10 GE PHY	62.5/125µm OM1	50/125µm OM2	50/125µm OM3	9/125µm
10GBase-LX4	300m (980ft)	240m (790ft)	240m (790ft)	10km (6.2mi)
10GBase-SR	33m (108ft)	33m (108ft)	300m (980ft)	-
10GBase-LRM	220m (720ft)	220m (720ft)	260m (720ft)	-
10GBase-LR	33m (108ft)	33m (108ft)	33m (108ft)	10km (6.2mi)
10GBase-ER	-	-	-	40km (25mi)

Form factor options are interoperable as long as the 10 Gigabit Ethernet physical interface type is the same on both ends of the fiber link. For example, it is possible to deploy a fiber link with one 10GBase-SR XFP optics on the left, and one 10GBase-SR SFP+ optics on the right. However, one 10GBase-SR SFP+ optics cannot connect to one 10GBase-LRM SFP+ optics at the other end of the link.

10 Gigabit Ethernet and Copper

As switching standards mature and copper cabling standards catch up, the use of copper cabling for 10GbE is becoming more common.

Currently, there are three different copper cabling technologies for 10 Gigabit Ethernet, each with different price and performance capabilities.

Table 20: 10GbE Copper Cabling Options (Source: [51])

Media	Copper cable	Range (max)	Average latency	
CX4	Twin-ax copper	15m (49ft)	0.1 µs	IEEE 802.3ak-2004
SFP+Direct Attach	Twin-ax copper SFP+CU	10m (33ft)	0.1 µs	MSA SFF-8431 housing
10GBase-T	Twisted pair CAT6 RJ45	30m (98ft)—50m (164ft)	>1.5 µs	IEEE 802.3an-2006
	Twisted pair CAT6a RJ45	100m (98ft)	>1 µs	
	Twister pair CAT7 GG45	100m (98ft)	>1 µs	

10GBase-CX4, published in 2004, was the first 10 Gigabit Ethernet copper standard. CX4 was relatively economical and allowed for very low latency. Its disadvantage was a too-large form factor for high density port counts in aggregation switches.

SFP+ is the latest standard for optical transceivers. 10 Gb SFP+Cu Direct Attach Cables (DAC) connect directly into an SFP+ housing. This new copper solution has become the connectivity of

choice for servers and storage devices in a rack because of its low latency, small form factor, and reasonable cost.

10GBase-T or IEEE 802.3an-2006 was released in 2006 to run 10 Gigabit Ethernet over CAT6a and CAT7 copper cabling up to 100 meters.

Selection of an appropriate 10 Gigabit physical media for NG-TCN:

When selecting an appropriate 10 Gigabit physical media to construct 10GbE network, two broad categories of copper and optical fiber will be considered as a result. In this subclause these two options for 10 Gigabit Ethernet: 10GBASE-T copper network vs 10G SFP+ fiber network will be explored and compare their main features to provide an overall understanding.

10GBASE-T Copper Network Option

10GBASE-T is the standard technology that enables 10 Gigabit Ethernet operations over balanced twisted-pair copper cabling system, including Category 6A unshielded and shielded cabling. It is the technology that provides end users with cost-effective media to achieve 10Gbps data rates. 10GBASE-T offers relatively great flexibility in network design due to its 100-meter reach capability. 10GBASE-T copper equipment includes 10G core Gigabit Ethernet switch, access switch with 10G uplinks, and 10G network interface cards for servers and storage devices. In order to build a 10GBASE-T copper network, there are generally two cabling solutions: 10Gb copper switch with Cat6 cable or 10GbE SFP+ switch with 10GBASE-T SFP+ transceiver.

10G SFP+ Fiber Network Option

Apart from copper network option, SFP+ modules and the matching fiber cables are needed to connect 10GbE switch over 100m to achieve 10G Ethernet operation. SFP+ direct attach cable (DAC) is a fixed assembly that is purchased at a given length. SFP+ DAC provides high performance in 10Gb Ethernet network applications by using an enhanced SFP+ connector to send 10Gbps data through a pair of transmitter and receiver over a thin twinax cable or fiber optic cable. It is a low-cost alternative to traditional fiber and twisted-pair copper cabling in data center deployments.

10GBASE-T Copper vs 10G SFP+ Fiber Comparison

1. Power Consumption and Latency:

10GBASE-T components today require anywhere from 1.5 to 4 watts per port depending on the distance of the cable. While SFP+ interface that has been widely applied for 10 Gigabit ToR (Top of the Rack) switches requires approximately 1 watt per port regardless of the distance. In addition, 10G SFP+ offers better latency with typically about 0.3 microseconds per link. 10GBASE-T latency is about 2.6 microseconds per link due to more complex encoding schemes within the equipment. When comparing 10GBASE-T technology with the alternative SFP+ technology, it is obvious that SFP+ is the more appropriate technology to ensure optimal performance with lowest power consumption and latency in data center. (latency is described without the TSN awareness)

2. Cost and Interoperability

With Cat6 cables becoming less expensive than fiber cables and SFP+ 10G copper cable, the cost of 10GBASE-T copper technology has been declined in the past years. In the meanwhile, it maximizes the utilization of existing copper structured cabling, so it will save much capital

expenditure as well. What is more, 10GBASE-T is given the advantages of being an interoperable and standards-based technology that uses the familiar RJ45 connector. For onboard application the existing X-coded M12-connector and CAT6 cable solutions which are already used today for 1000BASE-T can be readily taken for 10GBASE-T. Therefore, it can provide backwards compatibility with legacy networks. However, SFP+ fiber solution is limited with little or no backwards compatibility.

3. Conclusion:

For the use of 10 GbE within NG-TCN both technologies were possible, and a good choice could be to use of 10 GBASE-T within the ECN and SFP+ Fiber within ETB.

ETB: new technology could be chosen, no need of interoperability.

ECN: backward compatible with existing networks and network devices.

WLAN

WLAN (IEEE802.11) is essential for connecting stationary or mobile devices wirelessly to ECN. For this reason, it is foreseen to connect WLAN APs to the ECN and to connect WLED to the network within the scope of the CONNECTA-2 project (see F).

WPAN

WPAN (IEEE802.15) is a collection of emerging wireless technologies especially designed for IoT applications (see [04]). This by itself is a huge research field and therefore not in scope of CONNECTA. However, the architecture of NG-TCN is prepared to connect, similar to WLAN APs, WPAN APs to the ECN for connecting typical IoT devices like for instance smart sensors wirelessly.

3.1.2 ETB Bypass

The ETB bypass function required was required for some of the ETB topology variants described in 2.5.2, but with the decision taken in CONNECTA WP3 to adopt ETB Topology variant D₁, a bypass function is no longer needed.

Before that decision was taken, some research on the optimization of the bypass function implementation was performed, which is now summarized in I.

3.1.3 PoE

PoE is optionally supported by CS network devices. PoE is used to supply power to connected ED. The CS devices implementing PoE shall be compliant to IEEE 802.3 (output power at PSE: 15.4 W). Optionally they may support the extended power range specified in IEEE 802.3at (output power at PSE: 25.5 W).

Figure 26 shows the connection between PSE (located in the CS), and the PoE-PD (located in the powered ED). The alternative A of PoE IEEE 802.3 Clause 33 is applied because only two pairs of cable wires are used (Tx/Rx).

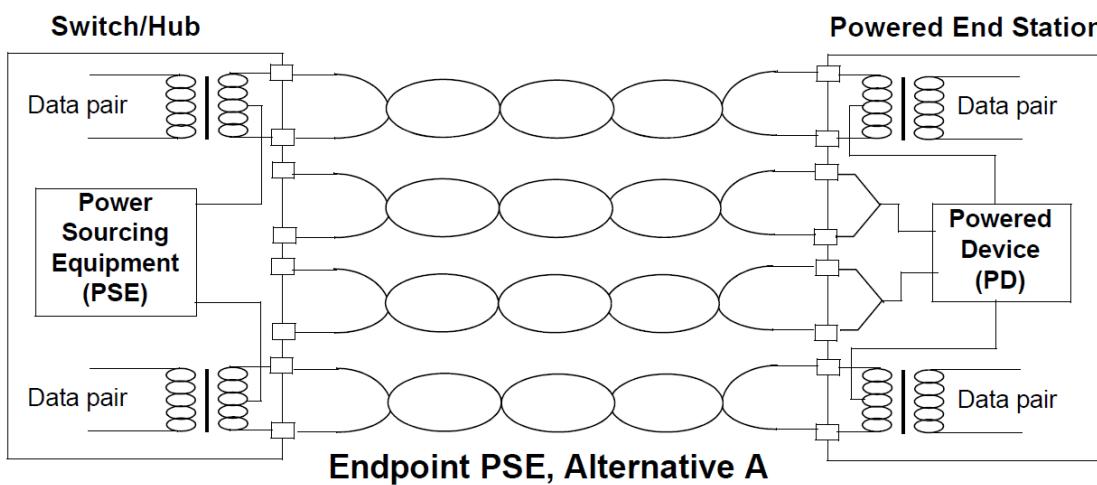


Figure 26: PoE PSE alternative A (from IEEE 802.3)

3.1.4 Sleep mode

Sleep mode is defined in IEC61375-2-3 as an option. The use case behind is the possibility to put a complete train to a low power mode and to ‘awake’ the train from one location by a manual action (like switching-on lighting in one coach) or remote via the MCG. Functionally, it is comparable to the “Wake On LAN” technology introduced by AMD in the 1990ties for computer networks. Sleep mode can be activated on user request or automatically, e.g. when local power source (e.g. battery) is running low.

For NG-TCN the sleep mode concept as defined in IEC61375-2-3 can be kept without modification.

3.1.5 Security aspects

Security of the physical layer shall primarily be provided by physical means. Network cables and especially connectors shall not be openly accessible but secured in locked cabinets. Cabinets shall be equipped with sensors to monitor (violent) opening. Unused switch ports shall be disabled to prevent from unforeseen connections.

3.2 DATA LINK LAYER

3.2.1 PDU (Ethernet frame format)

NOTE: The following description is based on references [36], [37], [38] and [39].

Brief history of Ethernet

The original Ethernet was developed as an experimental coaxial cable network in the 1970s by Xerox Corporation to operate with a data rate of 3 Mbps using a carrier sense multiple access collision detect (CSMA/CD) protocol for LANs with sporadic but occasionally heavy traffic requirements. Success with that project attracted early attention and led to the 1980 joint development of the 10-Mbps Ethernet Version 1.0 specification by the three-company consortium: Digital Equipment Corporation, Intel Corporation, and Xerox Corporation. For that reason, the frame format which was developed is often called DIX-format or later the Ethernet II-Format.

The original IEEE 802.3 standard was based on, and was very similar to, the Ethernet Version 1.0 specification. The draft standard was approved by the 802.3 working group in 1983 and was

subsequently published as an official standard in 1985 (ANSI/IEEE Std. 802.3-1985). Since then, several supplements to the standard have been defined to take advantage of improvements in the technologies and to support additional network media and higher data rate capabilities, plus several new optional network access control features. Throughout the rest of this chapter, the terms Ethernet and 802.3 will refer exclusively to network implementations compatible with the IEEE 802.3 standard. What is important here is that since DIX and IEEE802.3 frames are identical in terms of the number of bits and length of fields, both frames can coexist on the same network but may not be able to communicate to one another.

Preamble	Destination Address	Source Address	Type	Data			Cyclical Redundancy Check
8 bytes	6 bytes	6 bytes	2 bytes	Up to 1500 bytes			4 bytes

Figure 27: DIX Ethernet Frame

Preamble	Start Frame Delimiter	Destination Address	Source Address	Length	LLC	Data	Pad	Frame Check Sequence
7 bytes	1 byte	6 bytes	6 bytes	2 bytes		Up to 1500 bytes		4 bytes

Figure 28: IEEE 802.3 Ethernet Frame

The Basic Ethernet Frame Format

Since the IEEE802.3 standard is relevant for further developments of and for the use of network components in the NG-TCN environment, only this standard is described in more detail below. The IEEE 802.3 standard defines a basic data frame format that is required for all MAC implementations, plus several additional optional formats that are used to extend the protocol's basic capability. The basic data frame format contains the seven fields shown in Figure 29:

IEEE 802.3 Frame									
56 bits	8 bits	48 bits	48 bits			16 bits	368 to 12000 bits (46 to 1500 bytes)	32 bits	
Preamble	SFD	Individual/ Group Address Bit	Globally/ Locally Administered Address Bit	Destination Address	Source Address	Length	LLC/Data	Frame Check Sequence	

Figure 29: The Basic IEEE 802.3 MAC Data Frame Format

- **Preamble (PRE) — Consists of 7 bytes.**

The PRE is an alternating pattern of ones and zeros that tells receiving stations that a frame is coming, and that provides a means to synchronize the frame-reception portions of receiving physical layers with the incoming bit stream.

- **Start-of-frame delimiter (SOF) — Consists of 1 byte.**

The SOF is an alternating pattern of ones and zeros, ending with two consecutive 1-bits indicating that the next bit is the left-most bit in the left-most byte of the destination address.

- **Destination address (DA) — Consists of 6 bytes.**

The DA field identifies which station(s) should receive the frame. The left-most bit in the DA field indicates whether the address is an individual address (indicated by a 0) or a group address (indicated by a 1). The second bit from the left indicates whether the DA is globally administered (indicated by a 0) or locally administered (indicated by a 1). The remaining 46 bits are a uniquely assigned value that identifies a single station, a defined group of stations, or all stations on the network.

- **Source addresses (SA) — Consists of 6 bytes.**

The SA field identifies the sending station. The SA is always an individual address and the left-most bit in the SA field is always 0.

- **Length/Type — Consists of 2 bytes.**

This field indicates either the number of MAC-client data bytes that are contained in the data field of the frame, or the frame type ID if the frame is assembled using an optional format. If the Length/Type field value is less than or equal to 1500, the number of LLC bytes in the Data field is equal to the Length/Type field value. If the Length/Type field value is greater than 1536, the frame is an optional type frame, and the Length/Type field value identifies the particular type of frame being sent or received.

- **Data**

Is a sequence of n bytes of any value, where n is less than or equal to 1500. If the length of the Data field is less than 46, the Data field must be extended by adding a filler (a pad) sufficient to bring the Data field length to 46 bytes.

- **Frame check sequence (FCS) — Consists of 4 bytes.**

This sequence contains a 32-bit cyclic redundancy check (CRC) value, which is created by the sending MAC and is recalculated by the receiving MAC to check for damaged frames. The FCS is generated over the DA, SA, Length/Type, and Data fields.

3.2.2 MAC Addressing

TSN according to IEEE802.1Q defines common QoS services for different layer 2 technologies. The following discussion assumes that wired Ethernet according to IEEE802.3 is used for network layers 1 (physical layer) and 2 (data link layer). To that end the standard IEEE802.3 layer 2 frame format applies and is used utilizing the optional VLAN tag.

In context of TSN data is managed as “stream” with the source identified by a “stream ID”. The stream is destined to a “stream destination address” and able to be received by one or more end devices.

TSN stream ID

The TSN stream ID is mainly used for the management of FRER (see 3.2.9). The TSN stream ID is a 64-bit unique identifier formed by the unique 48-bit MAC address of the source device's Ethernet interface and a 16-bit extension to allow multiple streams per source device. The device uses its unique interface MAC address as MAC source address exactly as it would do ordinarily.

Stream destination address (stream forwarding)

The stream destination address is constructed by a locally managed multicast MAC address (48-bit, range to be defined) combined to a 12-bit VLAN ID (the 3 VLAN priority bits define the TSN traffic class). That is the device puts the locally managed multicast MAC address as MAC destination address. The frame is forwarded to end device(s) in the system by the intermediate switches based on the MAC destination address and the VLAN priority.

The use of a locally managed multicast MAC address as destination addresses requires all involved switches in the network to adjust their forwarding databases accordingly. Either by static compile time configuration or a run-time protocol.

3.2.3 L2 Switching function

General

Switching Ethernet frames through the ECN and along the ETB is in the responsibility of network devices with ETBN, ETBR and CS functional roles, but also, with restricted functionality, in the responsibility of ED. The process of switching (or ‘forwarding’) is generally defined in [23], but because this standard defines many options, a profiling will be necessary. The different process steps involved in the switching process are sketched in Figure 30, which describes the processing of Ethernet frames ingressing a specific switch port. In the following sections, all the different process steps will be discussed and profiled.

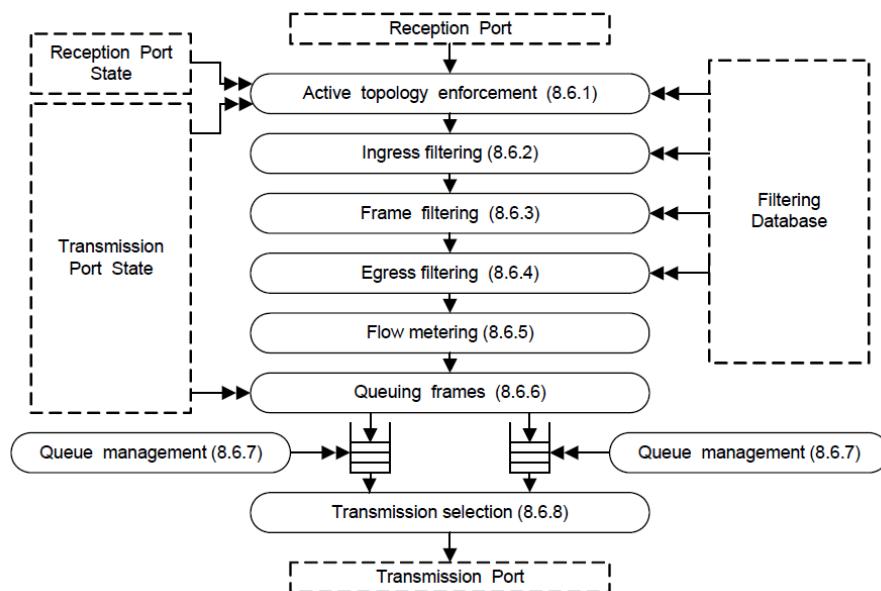


Figure 30: Forwarding process functions (source: [23])

Reception port

Reception ports are all CS ED ports, the CS ring ports, the CS ETBN port, the ETBN/ETBR ETB ports and the ETBN/ETBR ECN ports. There might also be device internal ports, dependent on the design.

All ports shall support the features listed in Table 21.

Table 21: Switch port features

Feature	CS ED port	CS ring port	CS ETBN port	ETBN/ETBR ETB port	ETBN/ETBR ECN port
Transmission rate	100FDX GbE (opt)	GbE 10GbE (opt)	GbE	GbE 10GbE (opt)	GbE
Autonegotiation	Yes	Yes	Yes	Yes	Yes
Autocrossing	Yes	—	—	—	—
Connector (copper media)	M12 (D-coded) M12 (X-coded)				
Connector (fiber media)	—	—	—	—	—
Port authentication (IEEE 802.1X)	yes	optional	optional	optional	optional
Adding, recognizing, interpreting, and removing VLAN tags as defined in [23].	yes	yes	yes	yes	yes

Forwarding process

The forwarding process defines how an Ethernet frame received on a port is further processed. The forwarding process is defined in [23] sub-clause 8.6. Table 22 lists the different steps of the forwarding process and their profiling for NG-TCN.

Table 22: Forwarding process profiling

Forwarding process step	Explanation	Profile
Active topology enforcement	Prevent data loops and unwanted learning of source MAC addresses.	Shall be supported
Ingress filtering	A frame received on a Port that is not in the member set associated with the frame's VID shall be discarded if ingress filtering is enabled.	Shall be supported
Frame filtering	Take filtering decisions, i.e., reduces the set of potential transmission Ports for each received frame	Shall be supported
Egress filtering	Any Port that is not in the member set for the frame's VID is removed from the set of potential egress Ports	Shall be supported
Flow metering	Apply flow classification and metering to frames that are received on a Port and have one or more potential transmission ports.	Policing of TSN data traffic shall be supported as defined in [24] and [25]. See 3.2.5 for more details.
Queuing frames	The Forwarding Process shall queue each received frame to each of the potential transmission Ports	8 traffic classes (corresponding to 8 queues per port) shall be supported.
Queue management	Defines the rules about removal of queued frames from the queue.	Shall be supported

Transmission selection	For each Port, frames are selected for transmission based on the traffic classes that the Port supports, and the operation of the transmission selection algorithms supported by the corresponding queues on that Port.	Strict priority transmission selection algorithm shall be supported. Credit-based shaper transmission selection algorithm may be supported Scheduled traffic shall be supported.
------------------------	---	--

Transmission Port

See 'Reception Port'.

3.2.4 QoS (Priorities)

For the different traffic classes supported by NG-TCN related to priorities are defined, which rule the forwarding order in Ethernet switches. Each traffic class is assigned to one switch queue, and a queued Ethernet frame is transmitted if it is eligible for egressing and the queue got clearance for transmission.

A frame is eligible for egressing if it is first in queue and if there is no other eligible frame in one of the higher-priority queues. The queue gets clearance for transmission if allowed so by TSN schedule (see 3.2.8).

The traffic class an Ethernet frame belongs to is determined by the priority assigned during switch ingress. For NG-TCN eight priority levels are defined (0 ... 7). This priority assignment is ruled by (in priority order):

1. If the frame (tagged or untagged) is ingressing on a port which shall grant best effort only (e.g. for connecting service PC, comfort devices, cyber-security untrustable devices), a statically defined port priority 0 (best effort) shall be assigned.
2. If the frame is ingressing untagged, a priority related to information in the IP header (DSCP/ToS field) shall be assigned as defined in Table 24.
3. If the frame is ingressing tagged with IEEE 802.1p priority information, this priority shall be assigned according to Table 23.

Table 23: Recommended priority to traffic class mappings

Explicit priority (IEEE 802.1p)	Traffic class (assigned priority)	Description	Remarks
0	1	Conventional Best Effort	
1	0	Conventional Background	See IEEE802.1Q table 8-4.
2	2	Conventional TRDP Message Data, Video, Audio	
3	3	Conventional TRDP Process Data	
4	4	TSN Traffic	
5	5	TSN Traffic	
6	6	TSN Traffic	
7	7	High priority management data (e.g. PTP Sync messages)	

Table 24: Recommended IP TOS to traffic class mappings

IP TOS field	Traffic Class
0x00...0x3f	0
0x40...0x7f	1
0x80...0xbf	2
0xc0...0xff	3

For TSN traffic 3 traffic classes are reserved, which can be used for critical process, video or audio data.

Four priority levels are reserved for conventional data traffic, which is in line with the IEC61375 standard. As the higher priorities are reserved for TSN traffic (except priority 7 which only has a minor impact) that consumes a predefined maximum bandwidth, conventional data traffic will only experience a communication medium with a reduced bandwidth. The consequence is that also for conventional data traffic QoS can be preserved, and legacy applications are not affected by the additional TSN traffic.

3.2.5 Traffic shaping/policing

Traditionally, traffic shaping defines the ability of a sender to limit the transmission rate of egressing Ethernet frames. Traffic policing on the other hand defines the ability of a receiver to supervise the rate of ingressing Ethernet frames and to limit it when a defined threshold is exceeded.

Rate control is traditionally done with a token bucket algorithm, whose basic concept is described first. The credit-based shaper defined in IEEE802.1Q uses this algorithm to control the transmission rate of egressing frame. In a similar way, the rate of ingressing frames can be supervised. The main purpose is to protect against excess bandwidth usage and burst sizes, but also against malicious end devices.

With TSN these concepts have been extended by supporting the shaping and policing of scheduled data traffic (per stream filtering and policing). To keep the determinism of scheduled traffic also in the case of network and end device failures, situations like buffer overflow, leading to frame losses, must be strictly avoided. Therefore, a strong data policing is strictly required.

Token Bucket algorithm

Rate limitation is defined by assigning maximal rate to the sender. Because the sender emits Ethernet frames which need to be sent in full wire speed (e.g. 100MBit/s), rate limitation ensures that the number of send Ethernet frames per second and the number of bits sent with these frames do not exceed the limit. As it is furthermore required to prevent bursty data traffic, emitted Ethernet frames need to be spread over time by varying the inter-frame gap.

The standard technology used for this is the Token Bucket algorithm. Here, a counter, representing the tokens in a bucket (see Figure 31), is incremented with a constant rate until a defined limit and decremented each time a frame is sent. The decrement depends on the frame size. A frame of a given size is only sent if the number of tokens is sufficient (= frame is conformant).

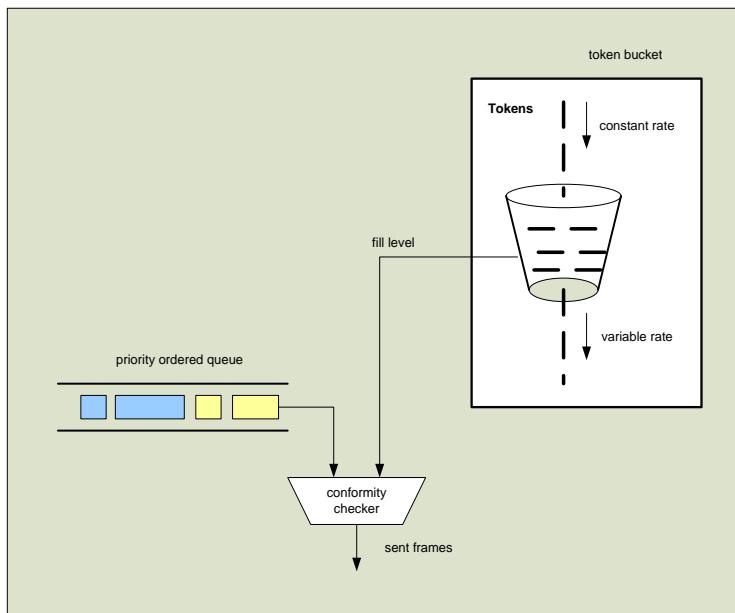


Figure 31: Token bucket algorithm (illustration)

The burstiness of the data traffic is determined by the bucket fill level and the number and size of queued Ethernet frames.

In order to preserve QoS it is important that the egress rate shaping is QoS aware, meaning that Ethernet frames are sent according to priority.

IEEE 802.1Q Credit based shaper

The credit-based shaper defined in IEEE 802.1Q, which bases on the token bucket algorithm, was introduced to bound latency and reduce jitter in the transmission of video and audio streams (Audio Video Bridging, AVB) and by this ensuring that frames of the individual streams are evenly distributed over time (burst avoidance). Two stream classes are defined, class A with a frame frequency of 8 KHz (125 µs period) and class B with a frame frequency of 4 KHz (250 µs period).

IEEE 802.1Q reserves IEEE 802.1p priorities 2 for Class B and 3 for Class A and recommends to map those priorities to the two highest traffic classes 6 and 7. This however is in contradiction to the recommendation given in 3.2.4, which assigns those traffic classes to TSN and management frames. In principle it would be sufficient to map the two stream classes to traffic classes 2 and 3, because the higher traffic classes are reserved for TSN (management frames are negligible), which have a time aware shaping and therefore do not enforce bursts.

Due to the fact that critical audio and video streams could also use scheduled traffic (see below), there is no real need to use the credit-based shaper in NG-TCN. If for any reason credit-based shaping is required, it must be ensured that all Ethernet switches along the transmission path support it. Especially for ETB the consequence would be that this behaviour must be standardized to ensure interoperability.

IEEE 802.1Qbv Scheduled Traffic

Using time scheduled traffic is another form of traffic shaping as it allows frame transmission only at predefined times. The concepts behind scheduled traffic are explained in 3.2.8.

Conventional Ingress rate limiting

Conventional ingress rate limiting uses similar techniques than egress shaping (token bucket or leaky bucket algorithms). The expectation however is that limited traffic is received, so that under normal conditions all incoming frames are accepted, and buffer overflow is avoided. Conventional ingress rate limiting has therefore only the role of a supervision, which aims to detect abnormal situations. Abnormal situations can be:

- Broadcast storm (caused by system fault)
- Wrong ED configuration (caused by ED systematic fault), leading to a higher frequency of received data than expected (and maybe with a higher priority)
- ED defect (caused by ED random fault), leading to a higher frequency of received data than expected (and maybe with a higher priority)

Most managed switches support those features nowadays. For the case of NG-TCN those features should be used for connected conventional ED.

Per stream filtering and policing (PSFP)

The IEEE 802.1 Qci sub-standard defines a possibility to filter frames on ingress ports based on arrival times, burst rates and used bandwidth. The policing of received Ethernet frames comprises three steps:

1. Stream filtering. Stream Ethernet frames exceeding a defined size are filtered.
2. Stream gating. Stream Ethernet frames arriving the wrong time are filtered and frames not belonging to the stream are filtered when arriving at a time reserved for the stream.
3. Stream metering. Stream Ethernet frames exceeding a defined reception rate are filtered.

Especially stream gating shall be used to support TSN as defined in 3.2.8 to ensure that only frames of a scheduled stream pass a switch in a defined time window. Hence the configuration of scheduled traffic shall also include the configuration of the corresponding policing actions.

Networking failures leading to frame loss due to policing must be diagnosable. IEEE 802.1 Qci defines a set of diagnostic counters which allow to pin-point the location of a network defect. Those counters shall be used in network monitoring and diagnostic, see 3.5.6.

Asynchronous traffic shaping

Asynchronous traffic shaping (ATS) as defined in [26] is a new concept with the objectives of providing bandwidth reservation for registered data stream (as with scheduled traffic) but without the need of time synchronization between the network components. Instead of using a global synchronized time, a local time is used to switch between time slots (called “epochs”). Four queues are used per port and traffic class, and those queues are assigned to a “prior”, “current”, “next” and “last” epoch. Frames are transmitted from the prior queue (while any remain on that queue) and then from the current queue. Received frames associated with any given stream reservation are added to the current queue, until the addition of a frame would exceed that reservation’s bandwidth allocation for an epoch, then to the next and finally to the last queues, discarding any additional frames. When a new epoch begins, the current queue becomes the prior queue, the next and last queues (and their remaining allocation for each reservation) becomes current, and next respectively. The former prior queue should then be empty, is given a fresh set of reservations, and becomes the new last queue.

ATS is in an early stage of specification and was therefore not further considered in CTA WP3.

3.2.6 Virtual LANs

The usage of VLAN as specified in [23] is compulsory for traffic segregation within the NG-TCN. Table 25 defines a set of predefined VLAN for NG-TCN. Besides those predefined VLANs there might be additional VLANs solely used for network management purposes (e.g. for ring redundancy protocol). ED connected to NG-TCN shall only use those predefined VLANs. Conventional ED, which do not support VLANs (VLAN tagged Ethernet frames) are automatically mapped to one of the default VLANs ECN-TCMS, ECN-OOS or ECN-COS by their local CS.

Table 25: Predefined VLAN for NG-TCN operation (preliminary)

No	Name	VLAN ID	Description
1	ECN-TCMS	2	Consist level VLAN used by connected eligible devices for non-TSN TCMS data traffic.
2	ECN-OOS	16	Consist level VLAN used by connected eligible devices for OOS data traffic.
3	ECN-COS	20	Consist level VLAN used by connected eligible devices for COS data traffic.
4	ECN-TSN-A-X	X = 32 ... 287 (256 IDs)	Consist level VLANs used by TSN devices for TSN data streams.
5	ECN-TSN-B-X		
6	ETB-TCMS	5	Train level VLAN used by all ETBN for non-TSN data traffic. This VLAN is configured on both ETB Line A and ETB Line B, see 3.2.10.
7	ETB-OOS	24	Train level VLAN is used by all ETBN for OOS data traffic. This VLAN is configured on both ETB Line A and ETB Line B, see 3.2.10.
8	ETB-COS	28	Train level VLAN is used by all ETBN for COS data traffic. This VLAN is configured on both ETB Line A and ETB Line B, see 3.2.10.
9	ETB-BEACON	6	Train level VLAN used by all CCU (TI Validator) for side selective BEACON telegrams (see 3.5.4). This VLAN is configured on both ETB Line A and ETB Line B.
10	ETB-TSN-A-X	X = 288 ... 543 (256 IDs)	ETB level VLANs used by ETBN for ETB TSN data streams. TSN data streams use identical VLAN-IDs on both ETB planes.
11	—	3 ... 4, 7 ... 15, 17 ... 19, 21 ... 23, 25 ... 27, 29 ... 31, 544 ... 4094	Reserved for future use
12	—	0, 1, 4095	Reserved (not for application use)

For the configuration of VLANs and the connection of ED the following rules apply:

1. All CS ports configured for connecting to COS ED shall be statically configured for ECN-COS. Ingressing tagged Ethernet frames with other VID than ECN-COS shall be filtered, untagged frames or frames with priority setting only (VID=0) shall be allocated to ECN-COS.
2. For CS ports configured for connecting to OOS ED two alternatives exist:
 - a. are statically configured for ECN-OOS. Ingressing tagged Ethernet frames with other VID than ECN-OOS shall be filtered, untagged frames or frames with priority setting only (VID=0) shall be allocated to ECN-OOS.
 - b. Are configured for ECN-TCMS and ECN-OOS. Ingressing VLAN tagged frames with another VID than ECN-OOS or ECN-TCMS are filtered. Ingressing VLAN tagged

frames with ECN-OOS or ECN-TCMS VID are allocated to corresponding VLAN. Ingressing untagged frames or frames with priority setting only (VID=0) are allocated to ECN-OOS. This alternative can be used by hybrid ED (ED with both TCMS and OOS capabilities).

3. All CS ports configured for connecting to TCMS ED shall be statically configured for ECN-TCMS, ECN-TCMS-A or ECN-TCMS-B. Ingressing tagged Ethernet frames with other VID shall be filtered, untagged frames or frames with priority setting only (VID=0) shall be allocated to ECN-TCMS.

3.2.7 Clock synchronization

General

Clock synchronization uses gPTP defined in IEEE 802.1ASrev [27] which is based on IEEE 1588. Precisely synchronized clocks are elemental for TSN. Without a clock synchronization, the data traffic cannot be scheduled. There are existing software implementations of PTP for Linux e.g. the Linux PTP Project.

At least every ED in a NG-TCN that uses TSN must run a PTP implementation. To achieve a better synchronization quality, it is recommended that all network devices such as bridges (and switches) are PTP-capable. Non-critical EDs may not implement a clock synchronization.

To be able to transmit safety data without a loss in a running TSN the clocks must be able to synchronize to microseconds precision in a time frame of one millisecond with small frequency adjustments in a steady state.

After a train (re)inauguration, the ETB time base might change since the master clock role can be assigned to another device by the Best Master Clock Algorithm (BMCA). If the master clock role is set statically, BMCA is not used, then the new recognized devices on the ETB must synchronize to their new master clock.

The consist clock domains shouldn't be affected after a train inauguration since the topology there doesn't change. Some consist clock domains might change, depending on the clock synchronization architecture.

Clock types used in ECN and on ETB

NG-TCN shall support different clock types inside a train.

- Master Clock (MC). It acts as the primary time source. For redundancy reasons IEEE 802.1ASrev allows multiple master clocks to be present. Each master clock (also hot standby master clock) is disseminating time in a gPTP domain. A fail-over mechanism guarantees that the redundant master clocks take over in case the currently active master fails. The ETBN is the preferred device to carry the master clock (as part of its boundary clock functionality) as typically at least two ETBN are available per consist.

A new “GlobalMC” concept proposed by Safe4RAIL (see 2.9) establishes a fault-tolerant system based on multiple GlobalMCs representing multiple gPTP domains that span the ETB.

- Slave Clock (SC). End devices are typically the only devices with just Slave Clock functionality. They adjust to the ConsistMC clock or to an average of multiple GlobalMCs. Also consist switches supporting TSN implement a slave clock in addition to their transparent clock functionality.
- Boundary Clock (BC). A boundary clock works as a master clock towards subordinate Slave clocks. Its master clock behaves as a slave towards a controlling higher-level master clock. As opposed to a transparent clock a boundary clock doesn't need a higher-level master clock on its slave-part to disseminate time on its master-part. The ETBN typically implements a boundary clock.
- Transparent Clock (TC). A transparent clock forwards timing packets, transparently adjusting time code fields during transitioning from one port to another. The adjusting is such that a receiving slave device does not see any variable delay caused by the transparent clock. A transparent clock functionality can be reached using the bridge (either one-step or two-step) mechanism as illustrated in Figure 34. Syntonization of the transparent clock to the GlobalMC is desired (but not mandatory) in order to more exactly measure the port-to-port delay. Intermediate consist switches typically implement a transparent clock.

Synchronization Protocol

Figure 32 shows the principle of PTP and gPTP time synchronization. Using time stamps T1 to T4 taken on egress and ingress respectively the slave clock can calculate its current time offset and act upon by tuning its clock frequency to get in sync with the master clock. gPTP may use this “two-step” timing approach where the timing frame payload as send by the CPU is conveyed unchanged. Instead the egress time stamps taken are sent in an additional follow up frame.

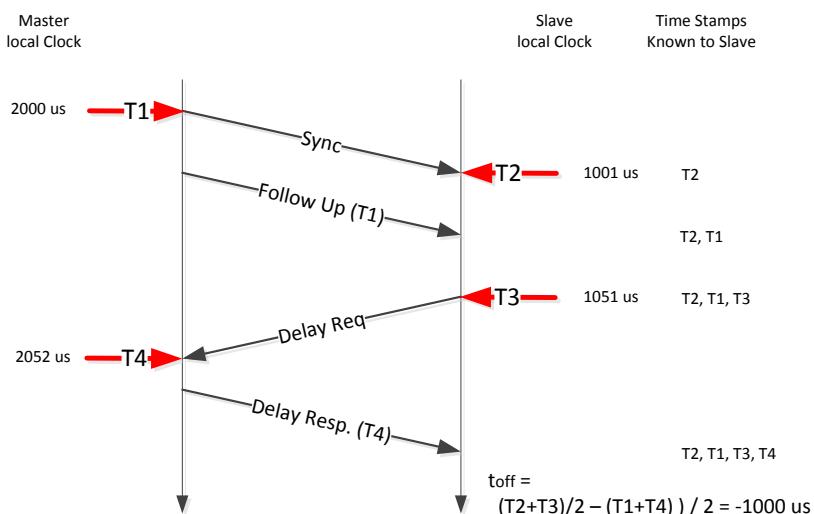


Figure 32: IEEE1588/IEEE802.1AS two-step timing protocol

Figure 33 shows the same principle for “single-step” timing, where egress timestamps are transparently patched into the timing frame. The gPTP protocol allows this variant also.

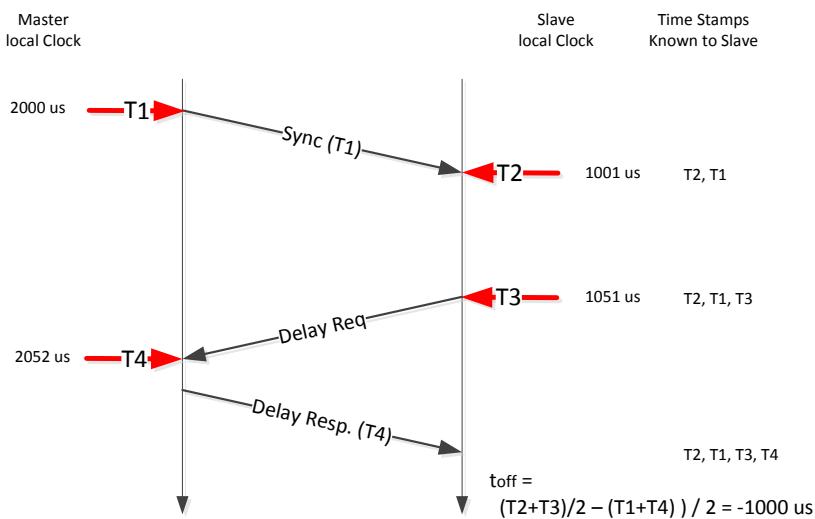


Figure 33: IEEE1588 one step timing protocol

Figure 34 shows how time synchronization of a bridge (or switch) works. The bridge adds information on how long the frames have been delayed inside the bridge (port-to-port). The slave does use this information to correct the time stamps and accurately calculates its timing offset towards the master clock. Functionally that implements a transparent clock (as opposed to a boundary clock which implements a slave/master clock pair). In addition, the switches in the NG-TCN synchronize in parallel their own clock with the master clock time

Note that the bridge itself does not need to be synchronized as it only sends time deltas rather than absolute times. Ideally it would be syntonized to the master clock though for time delta measurement accuracy. For lower accuracy it may also use a free running clock.

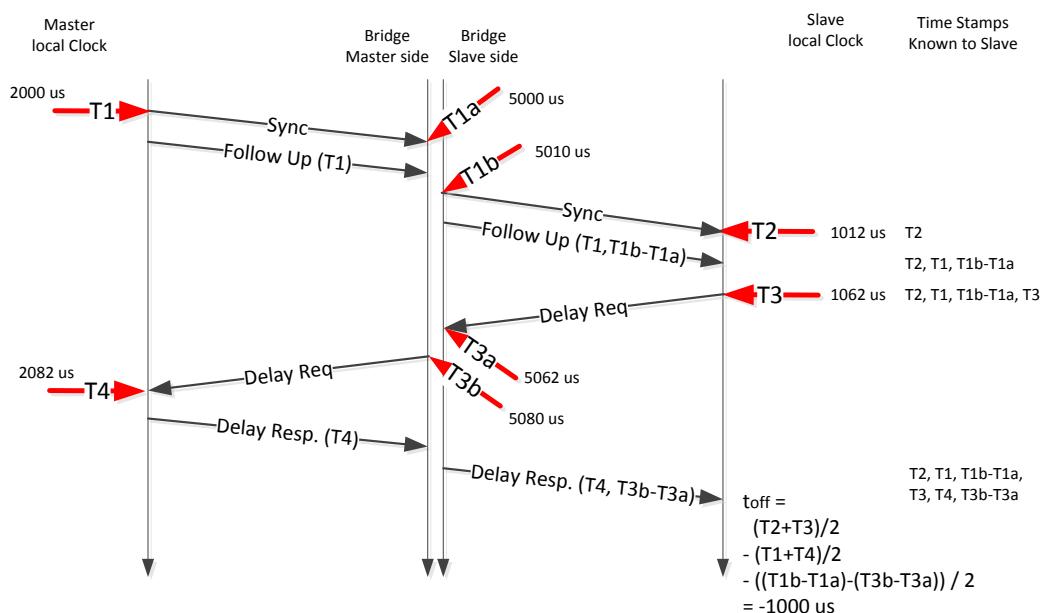


Figure 34: IEEE1588/IEEE802.1AS two-step bridge

Another option for a bridge (or switch) to avoid the varying time a frame is delayed inside the bridge (port-to-port), is the peer delay mechanism. Figure 35 shows how the peer delay (link delay) between

two Clocks (e.g. TC and SC) is measured. The delay is measured by ports on both ends of a link. This allows delay corrections to be made immediately upon reconfiguration of the network in case a bridge (or switch) fails. The “PDelay Resp Follow up” telegram is only used with the two-step protocol.

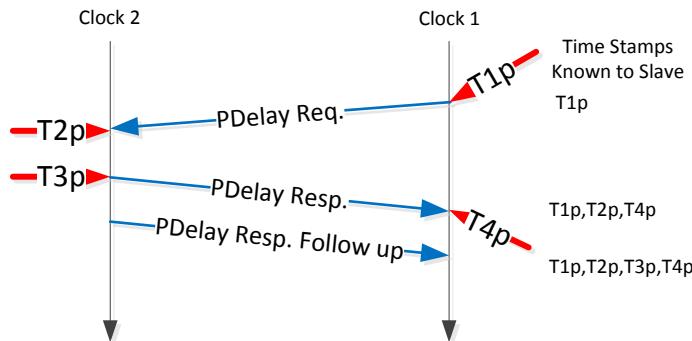


Figure 35: IEEE1588 peer delay mechanism

When the two-step timing protocol is used, and a Sync message is received on an ingress port, then the peer delay of this port is added to the value of the correction field of the following “Follow Up” message before it egresses on another port. Through this the slave knows the total delay of the telegrams without time influences of switching and can accurately calculate its timing offset towards the master clock

The peer delay mechanism is used instead of the “Delay Req.” and “Delay Resp.” messages shown in Figure 32, Figure 33 and Figure 34.

Configuration possibilities

In general, the time synchronization protocol can be configured. Especially the time cycle intervals of the telegrams (e.g. Sync, Delay Req) can be adjusted. Through this the behaviour of the synchronization can be influenced.

For each ED, clock quality and priority parameters can be set. This can be used to describe a clock of an ED and to mark clocks as preferred master clocks.

The PTP standard doesn't define how the measured synchronization fault should be corrected. It is up to the developer to implement a controller. The correction mechanism can be realized with a PI controller using a PLL or with different methods.

In some software implementations of PTP, the telegram network transport protocol can be configured. Possible protocols can be UDP and raw layer 2 ethernet. Raw layer 2 ethernet (with PTPv2, Ethertype 0x88F7) is the preferred protocol, as it is for a switch easier to handle in regard to port-to-port time measurements.

Requirements

An overall requirement for the network is that the general network infrastructure should boot faster than the EDs on start up. Ideally the time in the network is synchronized before the EDs start. At the latest after a few seconds a consist network should be ready and synchronized.

If an ED joins the network after booting, the local clock should synchronize to the master clock as fast as possible. A good value to synchronize to the master clock out of a random state is five seconds.

When a train (re)inauguration takes place, the ETB time base might change. The resulting resynchronization should reach an accuracy of microseconds after for example one seconds.

Error handling

To get a good constant common time base inside a clock domain, the synchronization process must be reliable and fault tolerant. An error can be imposed by many components. S4R presents a detailed assessment of the failure modes in deliverable D1.7. An overview is shown in Figure 36.

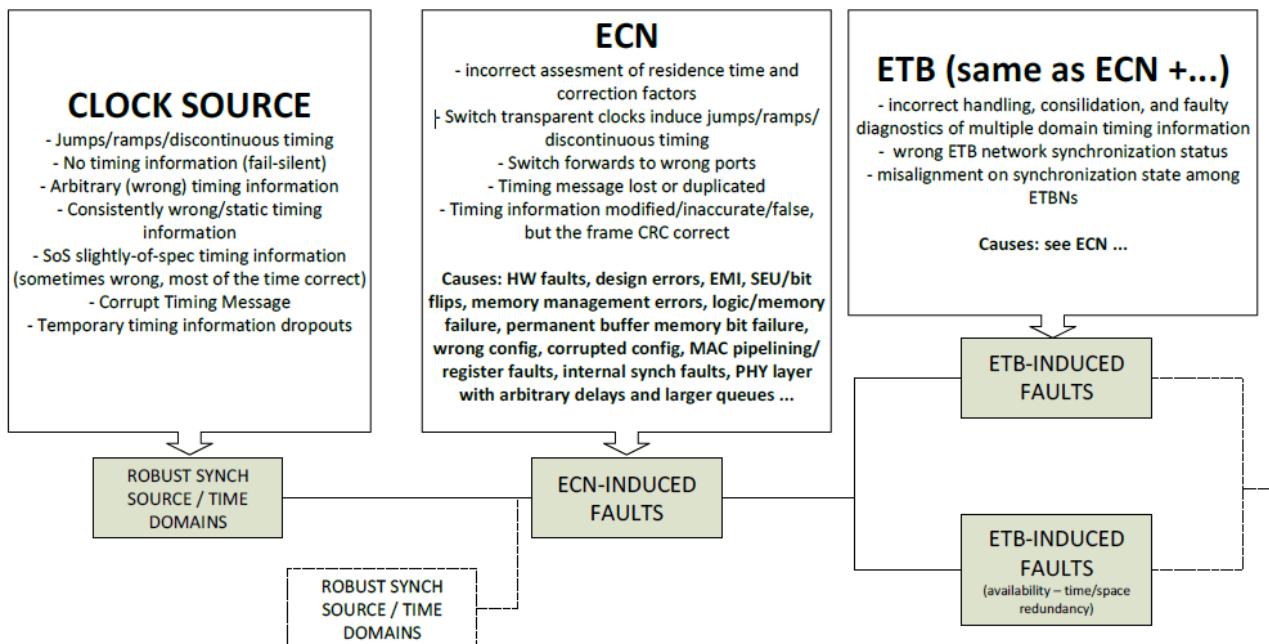


Figure 36: Error sources in the NG-TCN network

A failure can occur by writing wrong values in the telegram fields. An error can also occur during the transmission of the telegram after it egresses a device. This can happen due to flipping of a bit. This kind of error should be detected by the CRC-checksum of the ethernet frame. If an error in a telegram is detected, it should be discarded. A single error or missing telegram doesn't have much influence of the synchronization quality and can be easily handled by the implemented controller algorithm.

A flipping of a bit after the CRC-checksum is removed and the data is interpreted by the application results in an undetected error. The effects of such an error depend on where it occurs. Critical information is for example the timestamps, the correction value. A single error of timestamps and correction values can be caught by the application. For example, with filters or through averaging the last values. A constant or systematic error will result in a wrong calculated offset or delay. This will lead to a wrong adjustment control which will cause the clock to get out of sync. A high-integrity clock could recognize this and retreat from operation. In addition, the FT-AVG method on ETB can find one clock source which is faulty.

A wrong timing information on ECN in one clock domain can be recognized by an ED-S because it receives the information from several gPTP domains and over redundant paths.

If there appears an error on one ETB-Line which leads to a failure in the transmission path or the failure of an ETBN, then the communication (including clock synchronization communication) fails on this line. But all data can still be send over the redundant ETB-Line and Clock synchronization can operate there without any restrictions.

ETB Synchronization

The clock synchronization on ETB-level uses four GlobalMCs. Before they operate as democratic clocks calculating a fault-tolerant average of time based of the information of these four clocks, they need to have the same perception of time. This is reached with a hierarchical synchronization.

Each GlobalMC has a priority assigned (not BMCA). This avoids the situation where every master clock shares their properties and the master clock is afterwards selected based on those. The assignment can base on the inauguration result. For example, GlobalMC1 = Consist 1 Side A, GlobalMC2 = Consist 1 side B, GlobalMC3 = Consist n Side A and GlobalMC4 = Consist n Side B, where Consist n is the last consist of a train. The GlobalMC with the highest priority will initiate the synchronization and inform the other clocks about his local time, as shown in Figure 37. The other GlobalMC will follow sequentially, based on their priorities, and will spread their time to the lower prioritised GMCs.

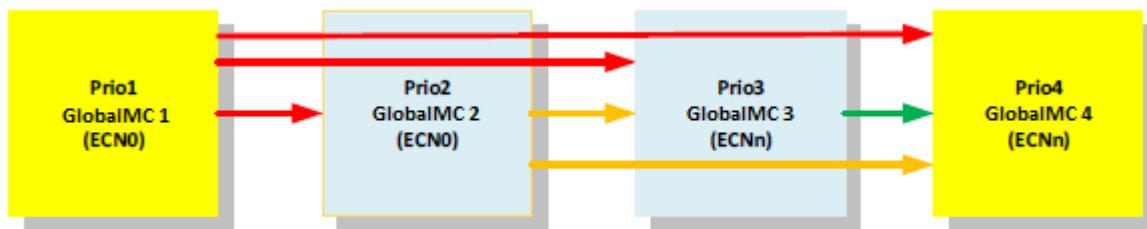


Figure 37: GlobalMC synchronization startup according to assigned priorities

Once all GlobalMCs have adjusted their time to their higher priority GlobalMCs and after each of them has the same perception of time in the system, they can be considered synchronized. Now they lose their priorities and disseminate their time to all ETBNs. All GlobalMCs calculate a fault-tolerant average out of four GlobalMC time values and perform a plausibility check. The valid value will be used to synchronize the local clock.

Network component requirements

Each component of the NG-TCN must fulfil a minimum of requirements to manage their tasks. The following paragraphs list what roles and capabilities a network component needs regarding clock synchronization and TSN.

ETBN

Each consist needs at least one ETBN. Because every consist in a train can become first or last consist, each ETBN must have one clock which can act as GMC with the properties defined in 2.9.6. This clock must also be able to act as a Boundary Clock (BC) and Slave Clock.

The ETBN links the train-wide ETB with the ECN and therefore must establish an interface for the clock domain(s) and TSN traffic between them. This leads to a gateway functionality for TSN and time information. This can optionally be realised on a separate gateway.

For independent clock domains in an ECN an independent master clock is required. This can be placed in a CS of the ECN or in the ETBN. Placing the ConsistMC in the ETBN has the benefit that no external interface between GlobalMC and ConsistMC domain is needed as they are in the same device. This makes the exchange of information easier. Optional but recommended is to include the CS functionality inside the ETBN device. This has the benefit that the ETBN device can be part of the ECN which simplifies the communication between the different MCs. Moreover, the CSs then can be designed in the same way without the need of clocks with special roles (ConsistMC or GlobalMC) because the ECN master clock resides in the CS-part of the ETBN device.

The ETBN must be able to calculate a FT AVG out of four clock domain sources and adjust its local clock accordingly. Depending on the architecture either this time information needs to be disseminated in the ECN or the time information of the independent second clock.

CS

In synchronization terms the CS has the role of a Transparent Clock (TC). It has to forward the gPTP messages of every clock domain on the ECN and to the ED.

To adjust its local clock the CS must handle two clock domain sources.

If the ECN master clock is not located in the ETBN device, a CS shall be able to take this role. Because of standardisation reasons every CS should have a suitable clock available. It must be checked if the normal build-in clock of a switch is good enough.

ED

Every (critical) ED which wants to participate in the TSN must synchronize its clock. Therefore, it receives up to four clock domain information. These include redundant time information. The ED must be able to synchronize its clock with the input of up to four clock domains.

Every device that participates in TSN must support the following TSN-relevant requirements: IEEE802.1Qbv (TSN), IEEE802.1Qbu, IEEE 802.1Qca and IEEE 802.1Asrev.

3.2.8 Scheduled traffic (TSN)

General

TSN aims to mitigate the drawbacks of AVB (see [04]) by introducing a synchronized data traffic (“scheduled”) and thereby avoiding interference of streams originating from different sources. This concept makes it possible to reserve bandwidth for critical data streams, which is key for a high reliability of critical data transmission.

The basic principle behind TSN is quite simple:

Each switch has a precise clock, and all clocks within a TSN domain are synchronized. Then all-time sensitive traffic can be scheduled. How this works in detail is shown in Figure 38.

A finite gate control list associated with each Ethernet port contains an ordered list of gate operations, which is stepped through and, when reaching the end, paused and restarted after a defined cycle time. Gate operations can be:

1. Open (o) the port for normal frame egress (best effort or credit shaped) for a defined time

2. Close (C) the port for normal frame egress for a defined time. Only frames marked as TSN frames are allowed to egress during this time.

Each gate operation changes the transmission gate state for the gate associated with each of the Port's traffic class queues. In an implementation that does not support enhancements for scheduled traffic, all gates are assumed to be permanently in the open state.

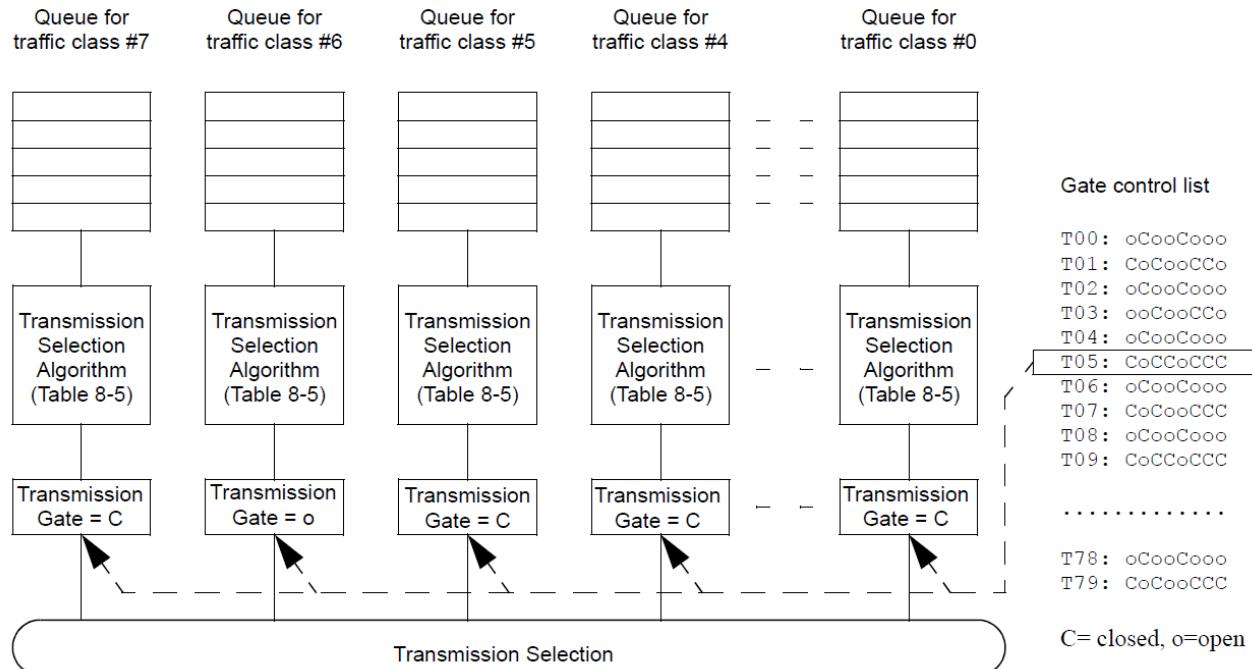


Figure 38: Port control for scheduled traffic (source: IEEE802.1Qbv)

To guarantee minimal latency, a port must be idle (not transmitting) when a time sensitive frame is selected for transmission. Because the time when the port shall be closed next time is known, it can be ensured that any other frame ready for transmission is not selected for transmission if its transmission time would exceed the port's close time. This mechanism is implemented by introducing a guard time just before the port closing time, during which only frames can be sent which terminate before the port's closing. The latency time can be further reduced by using cut-through instead of store-and-forward during switching. IEEE is presently investigating this.

The idea behind TSN is that if a time sensitive frame arrives at a switch, its destination port is known and already in closed state, so the frame can be directly forwarded to the destination port and egress the switch. This ensures minimal latency, and even more important, a deterministic behaviour, which practically means no or only a low jitter.

The important aspect here is that

- The destination port is known
- The time at which the time sensitive frame arrives is known

It requires a precise knowledge (“scheduling”) of the traffic, and this scheduling must be harmonized between all the switches for all the different traffic in the network.

Furthermore, this scheduling will be affected when there are changes in the network. In NG-TCN, basically two cases have to be considered:

- Network topology change on ECN level caused by redundancy switch-over
- Network topology change on ETB level caused by train inauguration or by ETBN failure

Each of these cases leads to changes of the transmission paths, and the scheduling must be adapted correspondingly.

Traffic scheduling configuration parameters

As mentioned above, scheduling the traffic in a NG-TCN means to establish a time-table for all involved ED and ND. How this works can be shown with the example of Figure 39. Depicted are three ED, each one producing one dataflow F_x ($x = 1, 2$ or 3) of scheduled data packets with a defined cycle time of C_x ($x = 1, 2$ or 3). The dataflows F_1 and F_3 are directed to all other ED and are splitting up somewhere in the network, forming derived dataflows F_{12} , F_{13} , F_{31} and F_{32} . Dataflow F_2 is only directed to ED1. The entity of a dataflow originating from one sender and directed to one or multiple destinations can be said to form a “virtual link” (according to ARINC 664).

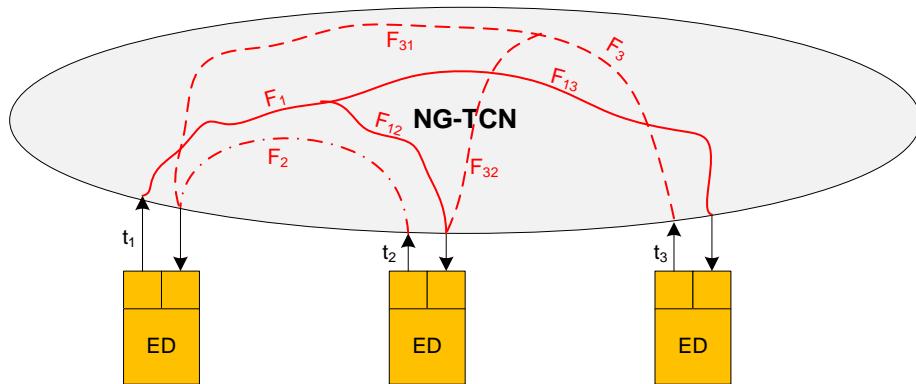


Figure 39: Scheduled flows

The point in time t_x ($x = 1, 2$ or 3) when a new packet of a dataflow shall be sent by the ED must be selected in a way that contentions in the network switches along the dataflow path are avoided.

We can denote the set of all sending Ethernet ports of ED and ND as $P = \{P_1, \dots, P_m\}$, the set of flows originating from ED as $F = \{F_1, \dots, F_n\}$, and the set of dataflow scheduling times as $t = \{t_1, \dots, t_n\}$. The times of gate open/close operations of all ports along the path of a given dataflow can be calculated when the start time t_x of a given dataflow is known. This calculation must consider the sequence of the P_x along the dataflow path as well as the propagation latency times on data links and in switches, meaning that a precise knowledge of the actual active network topology is essential. Furthermore, any contentions in the network (switches) between the different dataflows F must be avoided. Thus the task will be to define the set of data flow scheduling times t in a way that no contention between the different dataflows occurs.

The principle of this calculation is shown in Figure 40. A scheduling calculation algorithm reads in the actual network topology and the dataflow configuration (= set F), and generates a time table as a $m \times n$ matrix which defines for all P the gate open/close times for the related dataflow frames.

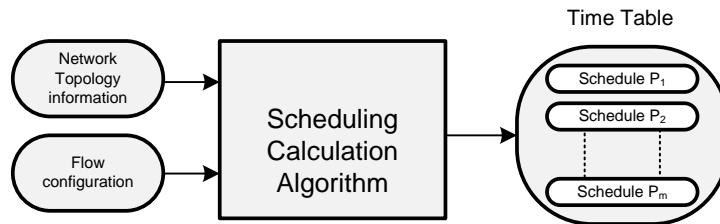


Figure 40: Time Table computation

As already mentioned in [04], the scheduling calculation is a complex task, mostly only solvable using heuristics and therefore unpredictable with respect to execution time (which in fact can take several seconds or even minutes of computation time, depending on the number of flows). This of course is not a suitable solution. The subsequently described approaches for TSN in consist networks and TSN over ETB try to avoid or at least to minimize time schedule re-computations while a train is in operation.

TSN in consist network

A-Plane/B-Plane concept

To avoid a time-consuming time table computation in case communication paths change caused by a failure in the ECN, a concept similar to the concept used in AFDX (see [04]) is proposed. The physical consist network (e.g. ring topology) is overlaid with a virtual A-Plane and B-Plane as shown in Figure 42. Each plane constitutes a set of VLANs, and all Ethernet ports assigned to a plane become member of that set.

This architecture offers two possibilities to connect critical end devices. The first one is more conventional and uses two redundant devices, each one connected to one of the planes (see Figure 41). Only one of the two is actively sending, the other is in stand-by. The problem here is the redundancy management because it has to be ensured that all devices of one plane are active, while devices of the other plane are in standby. Mutual supervision is done the conventional way using the default ECN-TCMS VLAN. After a device fails in one plane, all devices in this plane need to be deactivated and the devices in the other plane need to be activated. This takes time and is error-prone.

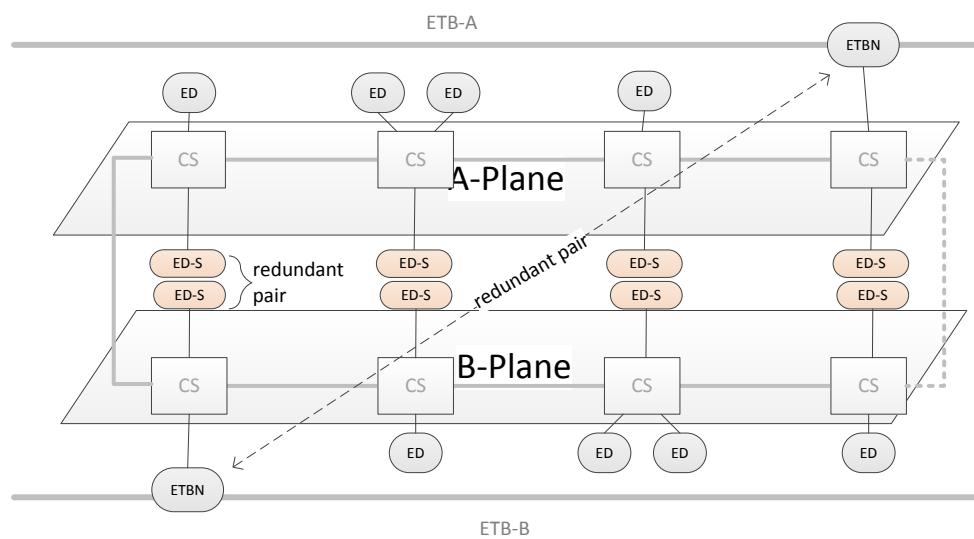


Figure 41: A-Plane and B-Plane with redundant devices (ETB Topology D₁)

More robust and seamless redundant is to use critical end devices with two Ethernet interfaces, each connected to one plane (Figure 42). For sending critical data from one critical end device to another critical end device in the consist, the frame carrying the critical data is replicated (see below) and both replica (A-frame and B-frame) are sent over the related plane. The destination end device receives both frames, eliminates the duplicate and forwards the remaining frame to its application.

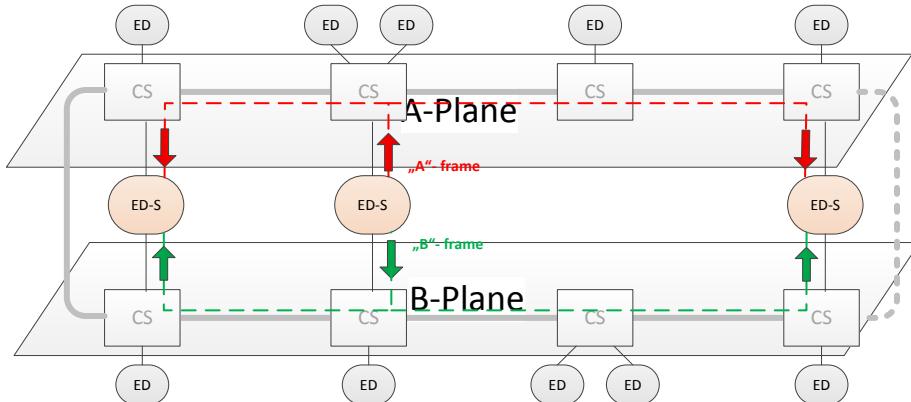


Figure 42: ECN overlaid with A-Plane and B-Plane

Ordinary end devices, which are not supposed to send scheduled data, do not become members of the plane's VLANs and are not aware of the existence of any plane. For communication, they use the predefined default VLANs (e.g. ECN-TCMS VLAN, ECN-OOS VLAN, ETB-TCMS, ETB-OOS) for consist internal and train wide communication.

Because a plane is statically defined, a time table can be predefined for all Ethernet ports belonging to the plane. Figure 43 demonstrates what happens in case of a link failure. A single fault can only hit one plane. If there is such a failure, not all destinations might be reachable anymore. Even for the case that the sent frame is redirected to another path to the destination (e.g. forced by a layer 2 protocol like ARP), the frame cannot leave the plane because it is confined to the plane's VLAN. Consequently, that destination will receive only one replica over the still intact other plane.

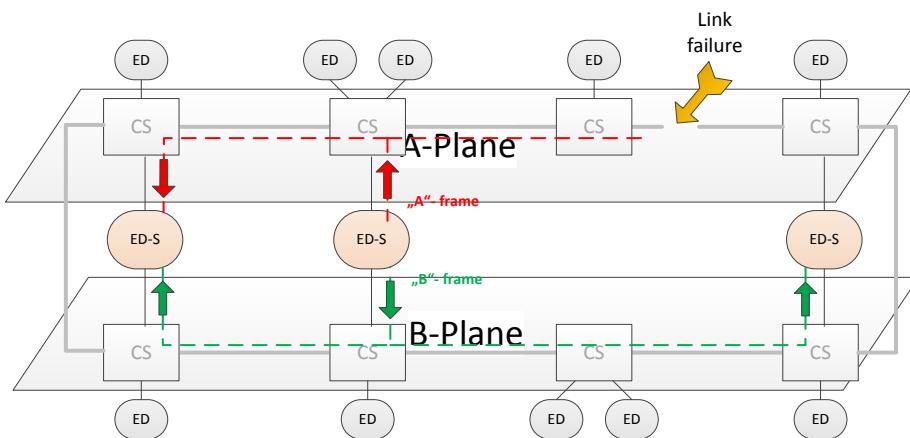


Figure 43: Link failure in a plane

Frame replication and elimination

The A-Plane/B-Plane concept requires that an application TSN frame is replicated at sender side, each replica sent over the related plane, and the duplicate is eliminated at receiver side. There are potentially two possibilities for implementation:

- a) Use a standard protocol like FRER as defined in IEEE802.1CB¹⁰ for this purpose
- b) Implement this function in the communication&network services of the FDF in the CCU.

The principle of FRER is that in a switch core at sender side a TSN frame is split in two member streams. The operation of FRER at sender and receiver side is shown in Table 26.

Table 26: Frame replication and elimination in IEEE802.1CB

End point	Action	Reference in IEEE802.1CB
Sender	1 Frame passed from user	
	2 A redundancy tag (R-TAG) is added to the frame which contains the sequence number	7.4.1, 7.8
	3 The frame is copied yielding two member frames	7.7
	4 Each copy is manipulated to receive a specific stream id (which requires change of MAC address and/or VLAN ID)	7.7
	5 The frame is send over the port which is related to defined VLAN	
Receiver	1 The frame is received over the port which is related to defined VLAN	
	2 Stream id is extracted (parameter "stream_handle")	6
	3 Sequence information is extracted	7.6
	4 Duplicates are discarded	7.4.2, 7.4.3
	5 Frame is passed to user	

¹⁰ Alternately PRP as defined in IEC62439 and supported as an option by IEEE802.1CB could be used. For details refer to [04].

At the time being IEEE802.1CB is still in draft state, which means that it is no option for short term solutions, although because of unavailability of suitable components. Another point is that it cannot be used for independent consist orientation detection as it is defined in 3.5.4. The reason is that the information, which plane is used for transmission, can only be retrieved from the stream id information. The stream id however is manipulated in the link layer, which belongs, by definition, to the black communication channel.

These circumstances do however not out-rule the usage of FRER in a long-term perspective, because this protocol has the advantage to automate frame replication and elimination in a standard way. For the time being, an alternative is to use possibility b) for implementation.

TSN over ETB

General

Supporting TSN on ETB level has the advantage that a defined bandwidth and a bounded latency can be guaranteed for the transmission of operational and safety critical process data. For the transmission of those time critical and safety critical process data some constraints and conditions can be defined:

- Operational critical process data sent by a consist are multicast to all other consists.
- Each consist sends an identical set of process data streams (identical means the same number of streams, identical cycle times and identical Ethernet frame size).
- The interface between consists must be well defined and standardized to achieve interoperability between consists of different manufacturers.

Architecture

The simplest way to introduce TSN over ETB is to prolong the A-Plane/B-Plane concept over ETB as it is shown in Figure 44. Corresponding to the definition of 2.5.3, the related train wide planes can then be called Left Plane and Right Plane. Left/Right Plane are logically defined and mapped to the consist A-Plane/B-Plane according to the train direction and orientation as defined in 2.5.3 (Figure 9).

Communication in the train-wide planes follows the same principles as consist plane communication: TSN data traffic is confined to the respective plain, and this is implemented with VLANs (3.2.6).

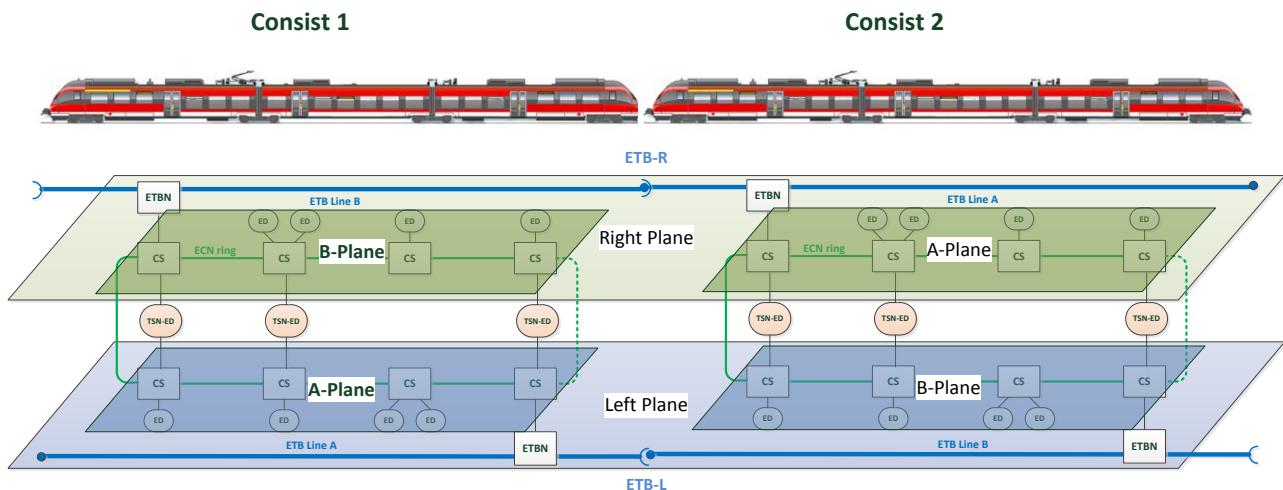


Figure 44: Train-wide TSN Planes

Scheduled Traffic

One consequence is that the number and size (bandwidth) of all ETB wide scheduled stream channels must be predefined, also with respect to the timely behaviour. The latter aspect is important, especially because the ETB topology, contrary to the ECN, might frequently change (train inauguration). As we saw above, each change of the topology means a change of the time table, which normally is a time-consuming effort. But here we can benefit from the fact that the ETB has a line structure. If number and size of scheduled stream channels are given, then the absolute time values of the time table depend only on the position of the consist in the train.

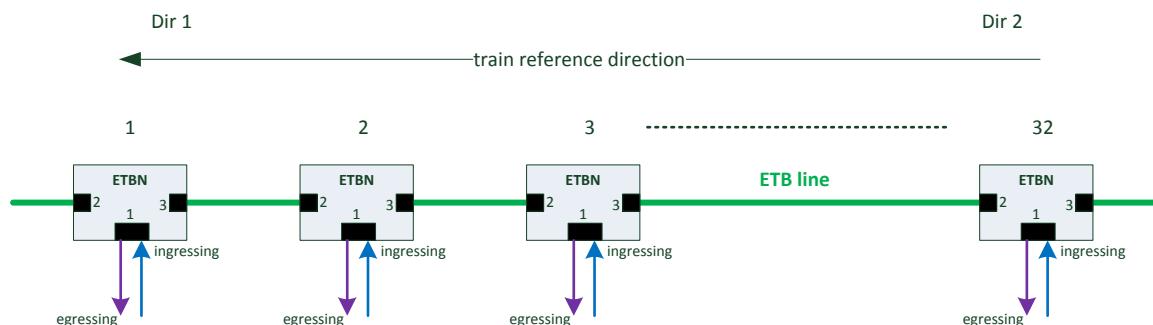


Figure 45: TSN over ETB

Let's assume that each consist is egressing over its ETBN (port 1) an equal number of n flows $F_{j,n}$, where $j \in \{1, \dots, cstCnt\}$ is the consist sequence number obtained after inauguration, and $cstCnt$ is the number of consists ($1 \leq cstCnt \leq 32$). The total number of flows over ETB is then $cstCnt * n$.

A consist (ETBN) in an intermediate position receives flows from both train reference direction 1 and direction 2. As shown in the example of Figure 45, where all consists have equal orientation, flows from direction 1 are received over port 2 and flows from direction 2 are received over port 3.

A consist (ETBN) in position j receives then dataflows as shown in Table 27.

Table 27: Flows on ETB

	Flows $F_{j,\text{dir}2}$ received at ETBN (port 3) in position j from ETBNs in the train reference direction 2.	Flows $F_{j,\text{dir}1}$ received at ETBN (port 2) in position j from ETBNs in the train reference direction 1.
j = 1	$F_{2,n}, F_{3,n}, \dots, F_{\text{cstCnt},n};$	None
$1 < j < \text{cstCnt}$	$F_{(j+1),n}, F_{(j+2),n}, \dots, F_{\text{cstCnt},n}$	$F_{1,n}, F_{2,n}, \dots, F_{(j-1),n}$
j = cstCnt	None	$F_{1,n}, F_{2,n}, \dots, F_{(\text{cstCnt}-1),n}$

The computation of the schedules $S_{j,m}$ for all Ethernet ports $P_{j,m}$ ($m = 1, 2$ or 3) follows an iterative algorithm. The task is to compute the schedule S for each port 1, 2 and 3 of the own ETBN (see Figure 45).

The schedule $S_{j,m}$ is defined by the vectors:

$$S_{j,1} = [\dots, t_{F\text{dir}1}, \dots, t_{F\text{dir}2}, \dots]$$

$$S_{j,2} = [\dots, t_{F\text{dir}1}, \dots]$$

$$S_{j,3} = [\dots, t_{F\text{dir}2}, \dots]$$

with:

$t_{F\text{dir}1}$ being the time window for each flow from train direction 1 (Table 27)

$t_{F\text{dir}2}$ being the time window for each flow from train direction 2 (Table 27)

Algorithm:

```

 $S_{1,m} = \text{predefined};$ 
For ( $i=2; i++; i \leq j$ )
{
   $S_{i,m} = f_s (S_{(i-1),m}, D_{i,(i-1)})$ 
}
  
```

It is important to have a predefinition of the schedule for the ETBN in consist 1. These initial values are used as a starting point in the iterative schedule computation.

The function f_s computes the schedule using as input information the schedule computed for the preceding ETBN ($S_{(i-1),m}$) and information about the transmission and storage delay between this ETBN and the preceding ETBN ($D_{i,(i-1)}$). The latter information depends on technology and physical configuration (e.g. Ethernet link length), and this information must be exchanged during train inauguration as a part of the consist properties (see IEC61375-2-3) to be known to the ETBN. This implies that the related parameters must be standardized.

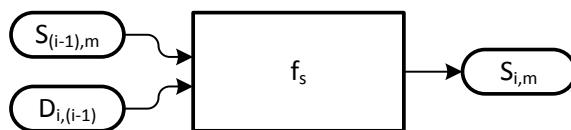


Figure 46: Function f_s

Connecting TSN between ECN and ETB

The connection between ECN and ETB is insofar critical as ECN and ETB may belong to different time domains. This requires a buffering of TSN frames in the ETBN device. Further details of this “ETB Gateway” function can be found in 3.5.5.

3.2.9 Redundancy management

The redundancy management described in this chapter focuses on network redundancy. Various redundancy protocols are presented and evaluated for use in the ECN with special consideration of the topologies presented in chapter 2.6. Redundancy protocol on ETB is covered by train inauguration.

General

Why is redundancy management needed?

Ethernet switches operate by storing and forwarding traffic between their ports. The switch examines each Ethernet frame and records the MAC source address and the port on which it resides. Subsequently, when a frame arrives for a given MAC destination address, the switch knows on which outgoing port to send the frame. If a frame arrives and its destination MAC address is unknown or is a broadcast, the switch will flood the frame out all of its ports.

If switches in an Ethernet network are connected in a loop or in a ring a broadcast storm will ensue where a single broadcast frame will circulate endlessly. This condition consumes all available bandwidth on the loop making the network unusable.

The general idea of media redundancy and redundant paths is almost as old as the use of Ethernet for industrial communications, and so is the dilemma that – by definition – Ethernet technology’s broadcast nature does not permit physical loops and therefore effectively forbids redundant communications paths.

However, fault tolerance or increased availability, which necessitates the use of redundant structures, is a basic requirement of NG-TCN at ETB and at ECN-Level (see [03]).

This means that the use of Ethernet for TCMS applications calls for protocols that are able to resolve the physical loops generated by the introduction of redundant pathways.

To facilitate the use of redundant communications structures in office environments, the IEEE (Institute of Electrical and Electronics Engineers) specified the spanning tree protocol (STP), which was published in the 802.1D 1990 standard. For the first time this enabled all Ethernet switches to employ an algorithm to facilitate interconnected network structures, albeit with switchover times of the order of many tens of seconds. Further protocols based on the underlying STP mechanisms were subsequently developed, and these were better tailored to the specific requirements of an industrial environment, in particular with markedly reduced switchover times. The Spanning Tree

Protocol (STP) allows the physical network to contain loops by forcing some links into a hot standby mode.

Reasons for media redundancy

Media redundancy is primarily used to avoid single points of failure in communications networks. Wherever there is a single point of failure it is possible for the communications network, to be completely disabled by a single technical fault. If redundant structures are used, then a single failure merely causes the network to fallback to a degraded state. Communications via the network remain viable, and the redundant system makes it possible for a repair to be carried out to restore the previous fault-free state. Additional detailed information about high-availability systems, media redundancy, failure and repair models are described in [59].

Redundant network structures are used for two separate purposes:

1. Load balancing:

The data traffic over a network path within a specific interval is greater than the bandwidth that a single data cable is able to handle. Introducing additional redundant connections increases the effective bandwidth of the original connection. The IEEE's link aggregation control protocol (LACP) [31] is typically used for this purpose.

2. Fault tolerance:

Additional media connections between network subscribers are introduced to enable the system to switch over to a secondary network path in the event of a failure in the primary path.

For ECN, fault tolerance is far more important than load balancing, which is why the following redundancy protocols should ensure high availability.

Component failure, which can never be entirely ruled out, needs to be dealt with in such a way as to minimize its impact on the system as a whole. As described in the Introduction of the chapter the focus is on network redundancy.

One fundamental requirement for any Ethernet network is the avoidance of loops. There must at all times be exactly one path between a message source and the corresponding sink. Any loops will result in data packets that circulate endlessly and eventually overload the network, which is why Ethernet does not permit alternative active paths to its devices. But media redundancy needs these alternative paths. Resolving this conflict calls for a protocol to monitor the redundancy.

Such a protocol must guarantee that, at any one time, there is only a single logical path from application point of view to each device, even if there are a number of physical pathways. The protocol achieves this by making sure that only one of the possible pathways is active at any one time and all the others are in standby mode.

The solution, which was realized for the first time with STP, depends on monitoring the links, detecting interruptions in communications and switching to an alternative path as soon as a failure is detected. Note that this principle means that communications will be interrupted for a certain time, because the failure first needs to be detected before the network can be switched over to the alternative path and communications are restored.

Depending on the complexity of the network, the duration of such interruptions may be difficult to predict.

The following fundamental requirements apply to media redundancy protocols in a train network environment:

1. Switchover-time determinism:

In the event of a failure, the time the protocol needs to switch from the primary logical path to a secondary alternative path and to restore communications must be predictable. *

2. Installation requirements:

If using the protocol and/or complying with required switchover times impose any constraints on the installation, for example the physical topology or the maximum number of useable network switches, then these must be clearly specified.

3. The protocol must be based on a **standardized method**. This is the only way of guaranteeing transparency, compatibility and hence security of investment.

The first requirement is absolutely essential for the use within time-critical applications or time sensitive applications. In this case seamless redundancy is the best solution to achieve zero switch over time.

A media redundancy protocol can be used only where reliable and calculable figures are available to specify the absolute worst-case upper limit for network switchover time in the event of a failure. This is the only way of ensuring that the network will fulfill the requirements of the application that is using it as a transmission medium:

If the media redundancy protocol can switch over fast enough to enable the protocol traffic and application to continue operating without impairment, then its redundancy mechanism is transparent to the application functionality and the timing requirements are fulfilled.

Technologies and solutions

STP / RSTP / MSTP

The Spanning Tree Protocol was defined in the IEEE Standard 802.1D editions prior to year 2004. It was designed to solve the fundamental problem of traffic loops and prevent accidental loops in poorly structured and managed wiring closets. The key idea in STP is to force some links into a hot standby mode in order to reduce the network topology to that of a tree. The resulting tree spans (i.e. connects) all switches but eliminates loops. The steps in order to best accomplish this process are:

1. Allow all switches to send messages to each other that convey their identity and link cost.
2. Elect a single switch, among all the switches in the network to be a root, or central switch.
3. Let all other switches calculate the direction and cost of the shortest path back to the Root using messages received from switches closer to the root. Each switch must have only one best way to forward frames to the Root.
4. If two switches servicing the same LAN exchange messages with each other, the one with the lowest cost to the Root will service the LAN. The other switch will discard all frames received from that LAN, thus opening the link and blocking a traffic loop.

STP introduced a few terms which are frequently used:

- a) Bridge Protocol Data Unit (BPDU):
specially formatted Layer 2 frame used by STP to exchange information between switches.
- b) Bridge diameter:
the maximum number of switches between any two end stations.
- c) Root port:
the port that offers the lowest cost path to the root bridge.
- d) Designated port:
the port that propagates Root information to the attached network segment.
- e) Alternate port:
the port that offers the next best cost path to the root bridge and will become Root Port, if the current Root Port loses connectivity with the root bridge.
- f) Discarding port state: the state in which the port is only sending and receiving STP BPDUs while blocking any regular network traffic.
- g) Forwarding port state: the state in which the port is sending and receiving both STP BPDUs and regular network traffic.

Over the last few years the (STP) spanning tree protocol mentioned earlier has been largely superseded by the rapid spanning tree protocol, RSTP. This is an optimized version of STP that was definitively described in the IEEE 802.1D 2004 standard [30]. RSTP implementations operate in a variety of topologies, support a higher number of switches and achieve improved switchover times of the order of about one second.

However, RSTP still does not guarantee deterministic failure behaviour. Reaction times depend on the location in the network where the failure occurs, and also on the approach taken by the individual implementation.

For this reason, there have been a number of attempts to optimize RSTP by restricting it to ring topologies and using fixed predefined parameters. To date, these optimizations have made it possible to demonstrate switchover times of the order of 100 ms or less.

The rapid spanning tree protocol, as its name implies, creates a tree structure from the connections between the Ethernet switches and disables all those paths that are not a part of the active tree.

This results in exactly one active path between any two devices. This protocol uses what are called bridge protocol data units (BPDUs) to communicate between the switches. One root bridge is defined as the root of the tree, and the optimal network paths are determined from there. If the network is changed in any way, for instance by the failure of a physical connection, this is reported to the network by means of topology change notification BPDUs.

The response to this is to recalculate the tree, activate the appropriate alternative paths and thus restore communications.

MSTP [23] is a further development of RSTP and works on the same principle. However, while RSTP operates independently of virtual local area networks (VLANs), MSTP always operates within VLANs and therefore facilitates more flexible network structures, for instance in order to implement load balancing over a variety of VLANs and network paths. MSTP and RSTP are mutually compatible and can be used together in a single network structure. Multiple instances of a Spanning Tree protocol can be active in virtual LANs with this new protocol. It logically groups individual RSTP structures into so-called VLANs (virtual LAN). As a result, the reconfiguration of the connection paths

in the network affects only one section. Neighboring subnetworks remain unaffected by the reconfiguration. MSTP requires a careful VLAN configuration and it can make troubleshooting complex and time-consuming in such networks.

Use of RSTP/MSTP in ring structures

If the topology is restricted to a ring, then it is possible to achieve deterministic and predictable switchover times with RSTP, provided the RSTP timing of the switches is known. The IEC 62439-1 standard contains a sample calculation that also demands additional protocol restrictions. For example, to prevent disruptive influences from outside the ring, the RSTP may not be configured on switchports other than ring ports.

Since RSTP was not primarily developed for ring topologies its design does exhibit a number of disadvantages compared to the MRP described below. For network devices that support both MRP (with a parameter set of 200 ms or better) and RSTP, and have no installation requirements that prescribe specific protocols, MRP is preferable to RSTP.

It should also be noted that RSTP possesses built-in overload protection to prevent individual network segments from being overloaded by large numbers of event-driven BPDUs. In a worst-case situation this overload protection has the effect of greatly increasing the reconfiguration time caused by lost BPDUs, up to the order of seconds. This restriction is less apparent in ring structures because of the less flexible topology, but it may still occur.

And it may happen quite frequently in meshed networks, particularly in the case of complex topologies with a high number of switches and media connections.

Use of RSTP/MSTP in meshed networks

One great strength of RSTP is its support for all kinds of meshed topologies. The resulting flexibility regarding the installation is a clear advantage over the stringent restrictions that are imposed by ring protocols such as MRP and ring installations.

However, this flexibility harbors one great disadvantage, namely the reconfiguration time, which for an interconnected network will depend – among other things – on the complexity of the network topology and the location in the network at which the failure occurred. Since RSTP, unlike MRP, is a decentralized protocol, it may also provoke highly unpredictable race conditions in the establishment of new communications paths, particularly when choosing a new root bridge.

This gives rise to network reconfiguration times that can be estimated only very roughly, and this does restrict the use of RSTP, particularly in meshed networks. In the case of meshed networks with very little complexity (such as ring networks with two or three additional loops or subrings), a detailed analysis can make it possible to determine upper limits, but these will always need to be worked out individually. Unlike with the protocols MRP, HSR and PRP, it is not possible to make a general statement.

MRP – Media Redundancy Protocol

One protocol that particularly addresses for example industrial applications is the media redundancy protocol, MRP. This protocol is described in the IEC 62439 2 standard, which is the industry standard for high-availability Ethernet networks. MRP is specified only for ring networks with up to 50 devices and guarantees fully deterministic switchover behaviour. Its absolute worst-case upper limit for

switchover times in response to a failure are 500 ms, 200 ms, 30 ms or as low as 10 ms, depending on the chosen parameter set.

Typical switchover times for MRP vary between half and a quarter of these worst-case times. Thus, under typical network load conditions, an MRP ring that is configured for a 200 ms worst case will need between 50 ms and 60 ms to switch over from the primary to the secondary path; under typical conditions an MRP ring with a 10 ms switchover time will react correspondingly faster.

Every MRP node requires a switch with two ring ports connected to the ring.

Under MRP, one of these nodes functions as a media redundancy manager (MRM). The MRM monitors and controls the ring topology so that it can react to network failures. It does this by sending Ethernet redundancy test frames to one ring port and receiving them at the other, and vice versa.

In a non-failure state, the MRM blocks all network traffic on one of its ring ports, with the exception of MRP protocol traffic. At a logical level, this converts the physical ring structure to a linear structure for ordinary network traffic, thus avoiding loops. If the MRM fails to receive its test frames, indicating a transmission failure in the ring – for example because of a device failure or a defective media connection – then it will open the previously blocked stand-by ring port to normal protocol traffic. All the devices will then be accessible via the secondary network path. All the other nodes in the ring have the role of media redundancy clients (MRC).

An MRC conveys the redundancy test frames fed into the ring by the MRM from one ring port to the next. It also reacts to any received reconfiguration frames (topology change) from the MRM, detects changes in the state of its port and reports this to the MRM. If such a state change report reaches the MRM before it has been able to detect the ring failure on the basis of missing test frames, then it uses the information received from the MRC to detect the failure. This ensures that the switchover in the MRM from primary to secondary network paths is always carried out within the shortest possible time. This flexibility in the matter of switchover times and the distinction between the dedicated manager (MRM) and the resource efficient clients (MRCs) enable the MRP ring to cover a very large number of practical requirements and be optimally configurable to suit them.

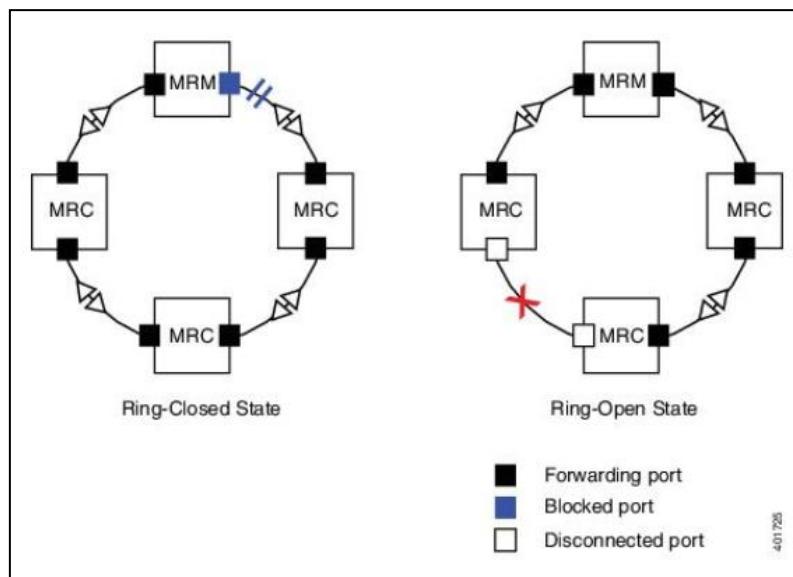


Figure 47: MRP Ring States (Source: [60])

PRP – Parallel Redundancy Protocol

Although a fast MRP ring can now cover a very large number of requirements, there are still applications that cannot tolerate any switchover time at all. To fulfill such requirements, we need to take an entirely new approach to the question of guaranteed high availability.

The basis of this new approach to network redundancy is to have two independent active paths between two devices. Both sender and receiver use two independent network interfaces. The sender transmits the same data simultaneously via the two independent active paths. The redundancy monitoring protocol then makes sure that the recipient uses only the first data packet and discards the second. If only one packet is received, the recipient knows that a failure has occurred on the other path.

This principle is employed by the parallel redundancy protocol (PRP), which is described in the IEC 62439-3 standard. **PRP uses two independent networks** with any topology and is not limited to ring networks. The two independent parallel networks may be MRP rings, RSTP networks and even networks without any redundancy at all. The principal advantage of PRP is its interruption-free switchovers, which take no time at all to switch over in failure situations and thus offer the highest possible availability. Naturally this applies only provided both networks do not fail simultaneously.

PRP is implemented in the end devices, while the switches in the networks are standard switches with no knowledge of PRP. An end-device with PRP functionality is called a double attached node for PRP (DAN P) and has a connection to each of the two independent networks. These two networks may have the identical structure or may differ in their topology and/or performance.

A standard device with a single network interface (single attached node, SAN) can be connected directly to one of the two networks. Naturally, in this case, the device will have no redundant path available in the event of a failure. A SAN can alternatively be connected to a redundancy box (RedBox) that connects one or more SANs to both networks. SANs do not need to know anything about PRP, they can be standard devices. In many applications, only critical equipment will need a dual network interface and less vital devices can be connected as SANs, with or without a redundancy box.

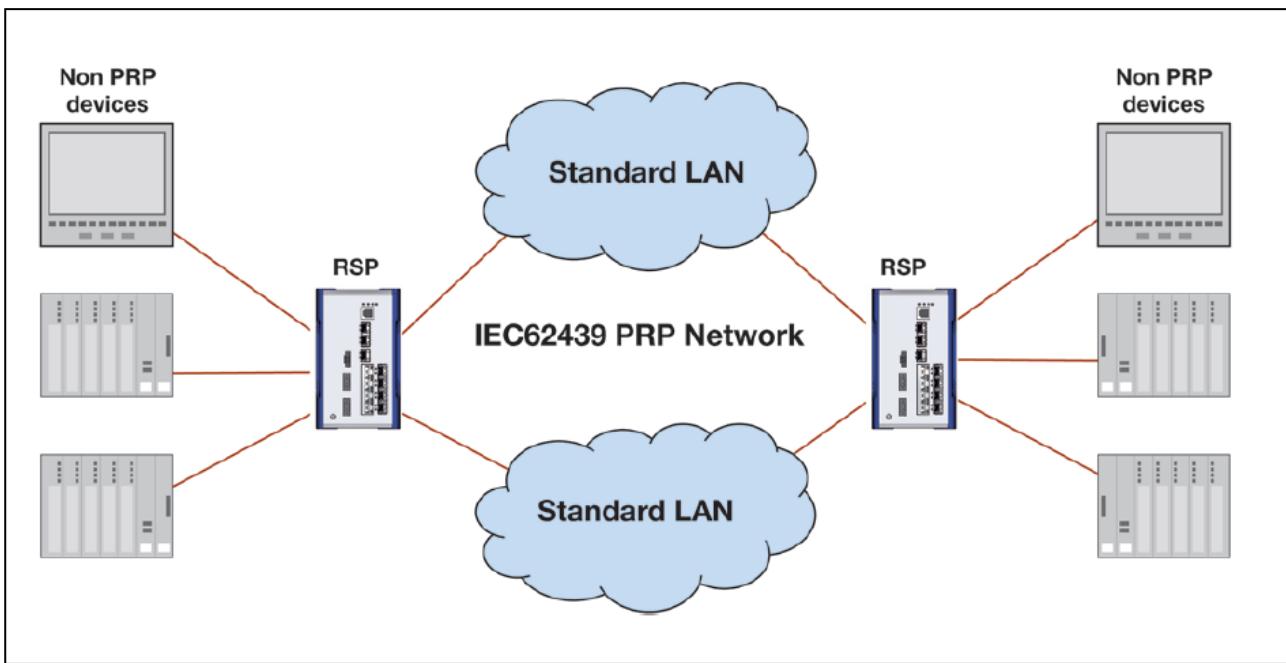


Figure 48: Identical data packets are transmitted simultaneously to both networks
 (Source: [58])

A DAN P implementation controls the redundancy and deals with duplicates. When the upper layers receive a packet for transmission, the PRP unit sends this frame to the network via both ports simultaneously.

When these two frames traverse the two independent networks they will normally be subject to different delays on their way to the recipient. At their destination the PRP unit passes the first packet to arrive to the upper layers, i.e. to the application, and discards the second one. The interface to the application is thus identical to any other Ethernet network interface.

The redundancy box implements the PRP protocol for all the attached SANs and thus operates as a kind of redundancy proxy for all types of standard equipment. Duplicates are recognized by means of the redundancy control trailers (RCT) introduced into each frame by a PRP connection or RedBox. In addition to a network identifier (LAN A or B) and the length of the user data contained in the frame, these 32-bit identification fields also contain a sequence number that is incremented for each frame sent by a node. A RedBox or DAN P connection can thus recognize duplicates, and if necessary discard them, based on the clearly identifiable features contained in each frame (physical MAC source address and sequence number).

Since the RCT is inserted at the end of the frame (see Figure 49), all the protocol traffic can still be read by SANs, which interpret the RCT merely as additional padding with no significance. This means that a SAN that is connected to a PRP network directly, i.e. without a RedBox, is able to communicate with all the DAN Ps and with any SANs in the same network (either A or B). It lacks only connections to the nodes of the other network because a DAN P does not pass any frames from one LAN to the other one. PRP switchover times fulfil the very highest demands, and it is also extremely flexible with respect to network structure and possible topologies, but it does always need twice the installed infrastructure of switches and other network components.

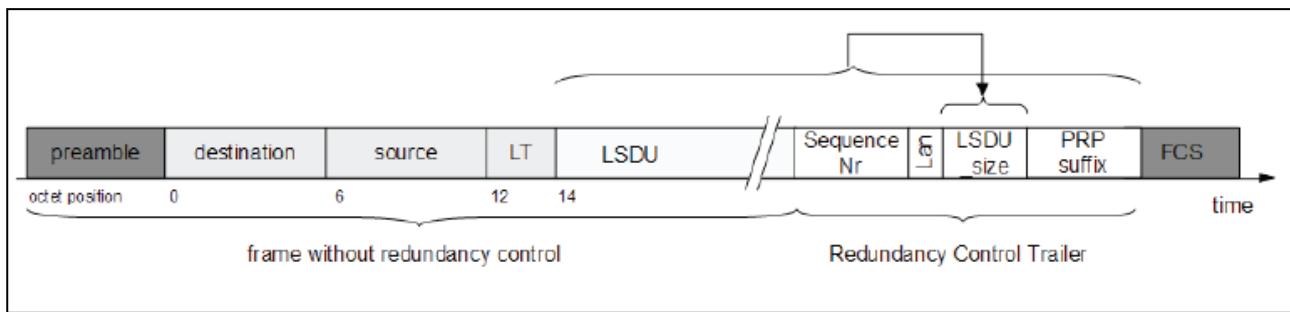


Figure 49: PRP frame format with no VLAN tag (Source: [58])

HSR – High Availability Seamless Redundancy

High availability seamless redundancy (HSR) is a further development of the PRP approach, although HSR functions primarily as a protocol for creating media redundancy while PRP, as described in the previous section, creates network redundancy. PRP and HSR are both described in the IEC 62439-3 standard.

Unlike PRP, HSR is primarily designed for use in (redundantly coupled) ring topologies. Like PRP, it uses two network ports, but unlike PRP, an HSR connection incorporates a DAN H (double attached node for HSR) that connects the two interfaces to form a ring (see Figure 50).

A frame from the application is given an HSR tag by the HSR connection. Like the PRP RCT, this contains the length of the user data, the port that transmitted it and the sequence number of the frame.

However, unlike PRP, the HSR header is used to encapsulate the Ethernet frame (see Figure 51). This has the advantage that duplicates of all frames are recognized in all devices as soon as the HSR header has been received. There is no need to wait for the whole frame and its RCT to be received before a duplicate can be recognized as such. This means that, similarly to cut-through switching, individual HSR connections and RedBoxes can begin forwarding the frame to the second ring port as soon as its HSR header has been completely received and duplicate recognition carried out.

Each HSR node takes from the network all frames that are addressed only to it and forwards them to the application. Multicast and broadcast messages are forwarded by every node in the ring and are also passed to the application.

In order to prevent multicast and broadcast frames from circulating for ever, the node that initially placed the multicast or broadcast frame on the ring will remove it as soon as it has completed one cycle (see HSR data flow in Figure 50).

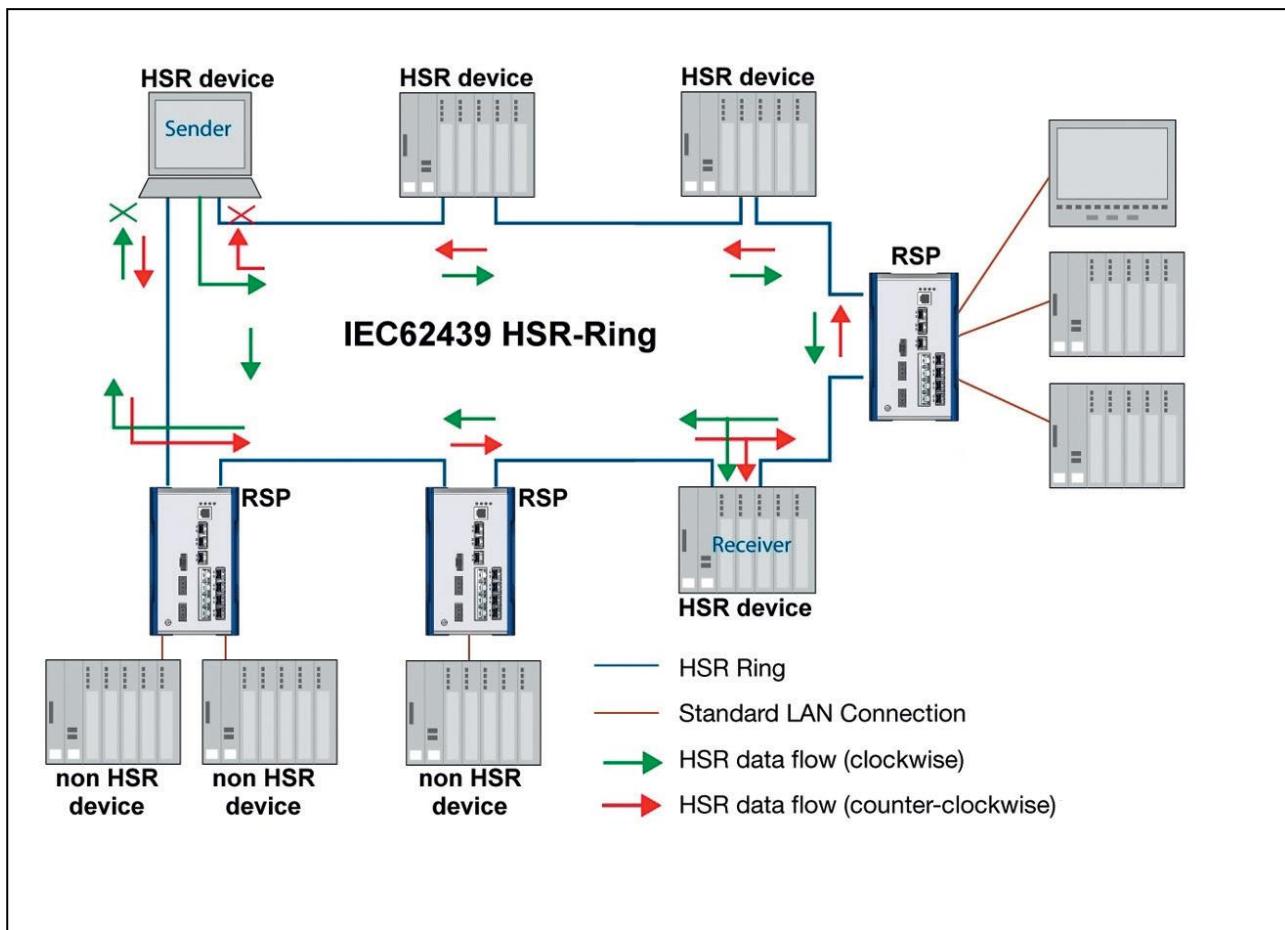


Figure 50: Duplicate data packets are transmitted simultaneously in both directions (Source: [58])

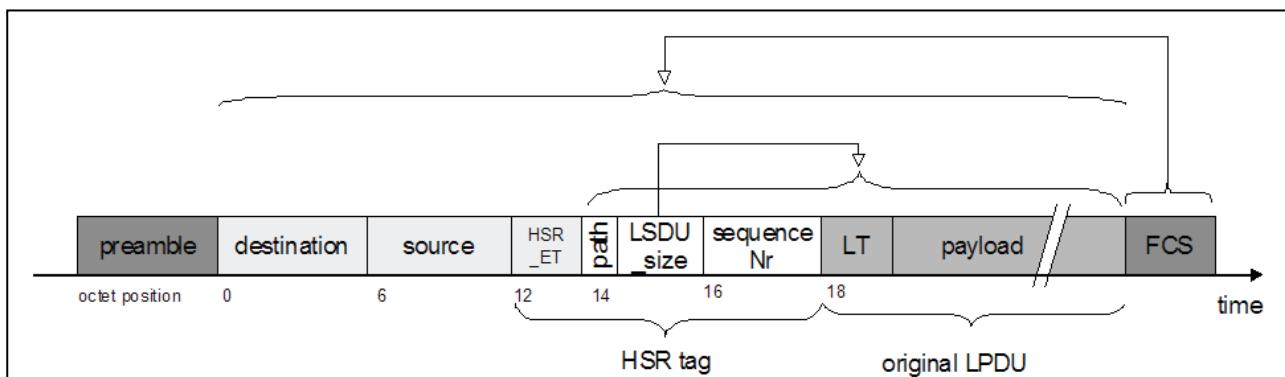


Figure 51: HSR frame format with no VLAN tag (Source: [58])

In contrast to PRP, it is not possible to integrate SAN nodes directly into an HSR network without breaking the ring: a SAN lacks the second network interface necessary for a closed ring. This is one reason why SANs can be connected to HSR networks only via redundancy boxes. The second reason is the encapsulation of the network traffic on the ring effected by the HSR header. Unlike with PRP, this prevents ordinary network nodes from participating in the HSR traffic. While SAN nodes interpret the PRP RCTs as padding, this is not possible for the HSR tag: its position in the frame

means that it is always interpreted as valid layer 2 frame information, and this prevents SAN nodes from correctly reading out the frame's user data.

Because some HSR devices may need to communicate with a management station or notebook for purposes of configuration and diagnostics, HSR connections will temporarily accept devices that transmit standard Ethernet frames, even on ring ports. In this case the HSR connections communicate without HSR header encapsulation, although this traffic is not passed to the HSR network – it merely provides bidirectional communications between the configuring management station on an HSR port and the HSR device.

Normal HSR communications is not restarted until the ring has been closed. Couplings between two HSR rings are always implemented by means of two ring coupling elements, known as QuadBoxes. These facilitate a coupling between two HSR with no single point of failure (see Figure 52).

About switchover times, HSR behaves just like PRP: by sending duplicate frames from both the ports of an HSR connection, in the event of a failure one frame will still be transmitted via whichever network path is still intact.

This means that the redundancy again functions with zero switchover time and, unlike PRP, does not require two parallel networks.

An HSR network, however, always has the form of a ring, or a structure of coupled rings, which means that it is less flexible than PRP at the installation stage. The duplicate transmission of frames in both directions also means that effectively only 50% of the network bandwidth is available for data traffic.

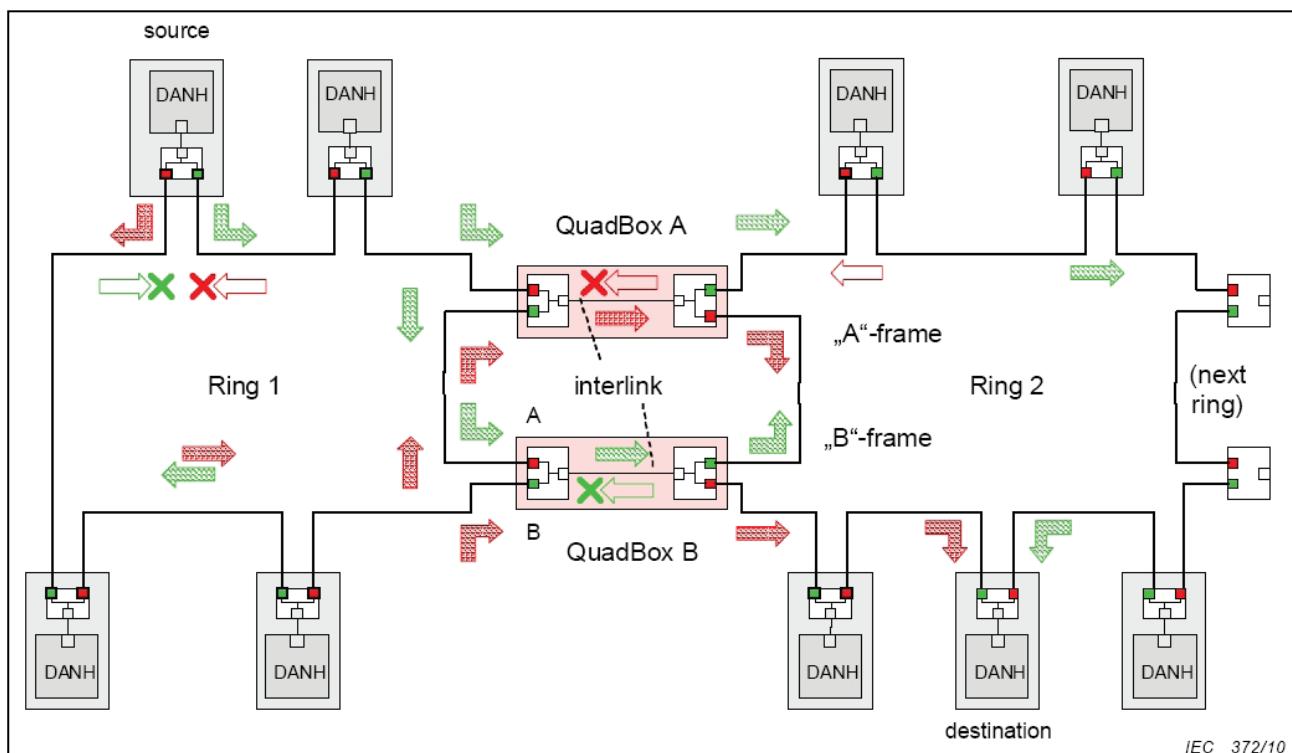


Figure 52: Coupled HSR rings (Source: [58])

IEEE802.1CB – Frame Replication and Elimination for Reliability

To prevent the packet loss when TSN is used resulting from interruption, the IEEE is currently developing a redundancy protocol with IEEE P802.1CB that uses mechanisms similar to the already established seamless redundancy mechanisms, High Availability Seamless Redundancy (HSR) and the Parallel Redundancy Protocol (PRP).

One goal is to maintain compatibility to HSR and PRP that is specified in IEC 62439-3. IEEE802.1CB involves static redundancy procedures, in which the redundant transmission paths are permanently active. In the case of a failure, switchover times from one path to another can be avoided.

To achieve seamless redundancy with IEEE P802.1CB, the Ethernet frames that need to be transmitted are replicated at the beginning of a redundant transmission path and subsequently forwarded through the network via multiple paths.

Usually, the replication occurs either directly on the sending device or, if the end device does not support redundant network connections, such as the one illustrated in Figure 52, at the first network device on the transmission path. When the data arrives at the destination, the first redundant data packet is forwarded in the direction of the application layer. Packet duplicates received after the first packet are recognized via a redundancy field in the Ethernet header and discarded. Thus, it is ensured that the redundant data transmission with IEEE P802.1CB is transparent for higher layers in the network stack and do not need to be considered.

In comparison to HSR and PRP, the redundancy mechanisms developed in the context of the IEEE P802.1CB offer the advantage that they can be used in any topology. Thus, IEEE P802.1CB is not limited to the otherwise absolutely required ring topology or topologies with completely independent networks. Additionally, IEEE P802.1CB is not restricted to exactly two redundant paths. In order to reduce the probability of packet loss, it is also possible with IEEE P802.1CB to utilize numerous redundant transmission paths. However, in this case, it must be ensured that all redundant paths can support the latency guarantees that are required by the application. The convenient management of requirements and configuration of TSN network paths is thus an important component of a functioning TSN ecosystem consisting of network devices and network management.

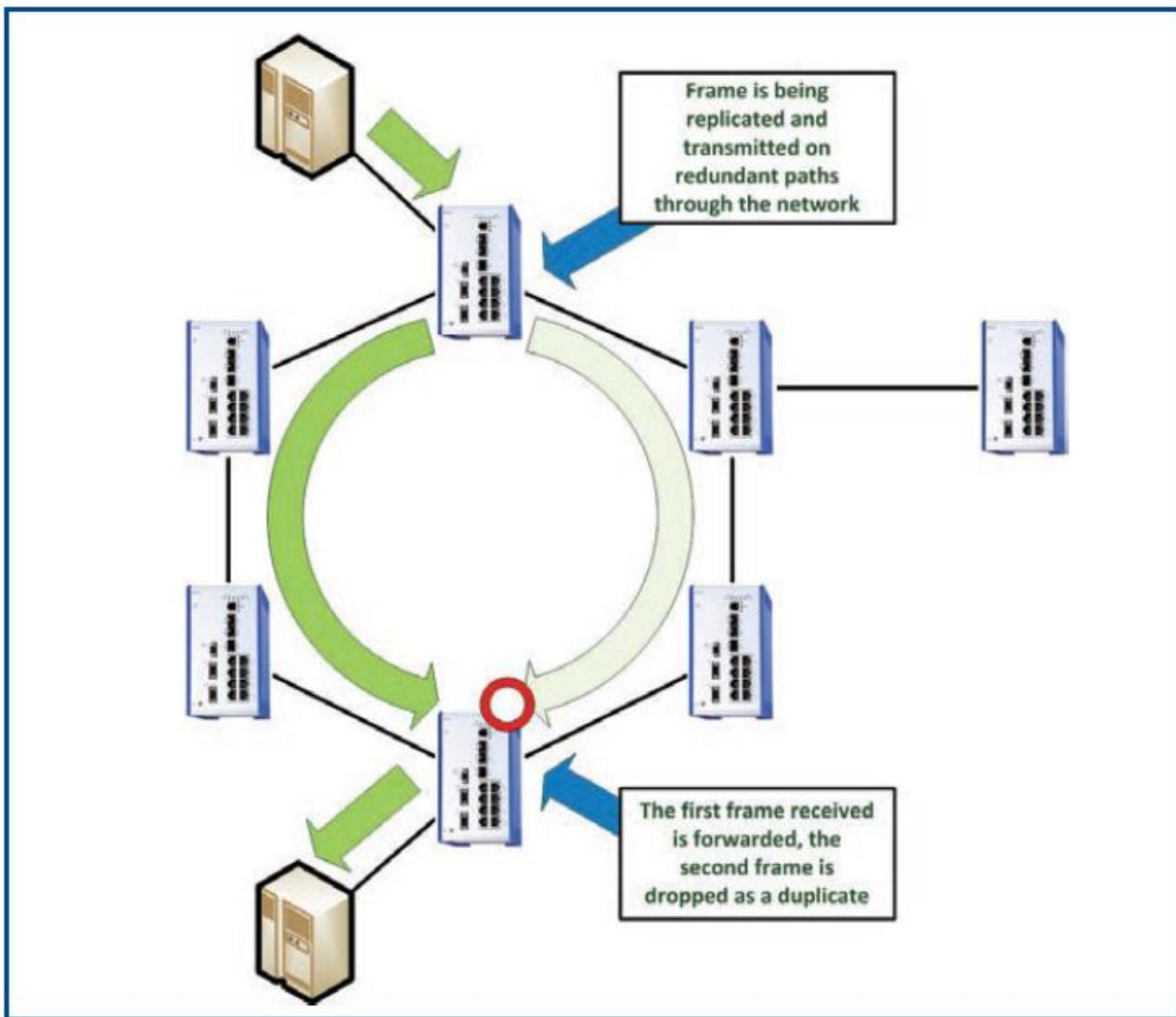


Figure 53: Frame replication and elimination (Source: [61])

Conclusion:

In practice, there is no perfect network topology nor perfect media redundancy protocol that precisely covers all applications and requirements.

The right choice of topology and protocol will always depend on additional factors, such as the physical installation requirements and/or the switchover times demanded by the application.

As an overview, the following table summarizes the protocols and principal parameters of the redundancy technologies covered in this chapter.

	RSTP	MRP	HSR	PRP	IEEE P802.1CB
Deterministic reconfiguration	no	yes	yes	yes	yes
Topology	any	ring with subrings	ring with subrings	any parallel networks	any
Worst-case reconfiguration time	>2s	10ms/30ms/200ms/500ms	0s	0s	0s
Standardized in	IEEE 802.1D-2010	IEC 62439-2	IEC 62439-3	IEC 62439-3	IEEE P802.1CB
Max. devices	Any (40 in ring topology)	50	512	any	any

Table 28: Standardized redundancy protocols

Selection of the redundancy protocol for ECN

The best solution of the network topology introduced in 2.6 for ECN is to use a physical ring topology superimposed with a logical parallel linear topology (A-Plane/B-Plane). In combination with TSN it is necessary to use the IEEE P802.1CB technology for the A-Plane and B-Plane VLANs as well as for the non-TSN components to create the possibility to communicate with each other in the non-TSN VLAN without causing a topology change by ring separation.

So, MRP seems to be the first choice, either with some modifications (selection of the preferred blocked port) or with a suitable placement (between A-Plane and B-Plane) of the MRM, but further investigations into the use of MSTP should be pursued¹¹.

HSR and PRP have the disadvantage of the non-flexible topology and DAN P, or SAN are needed to connect ED with one Connection to the network. Furthermore, HSR and PRP are not time-aware and thus not usable in combination with scheduled traffic.

3.2.10 Train backbone topology discovery

Chapter 2.5 proposes different train backbone architecture variants, which deviate more or less from IEC61375-2-5 ETB. This chapter discusses possible implementations of the train topology discovery (train inauguration).

Relation to TSN

It is anticipated that the next generation IP based TCN will deploy Ethernet real-time extensions currently standardized by the IEEE under the working title “Time Sensitive Networking” or “TSN” for

¹¹ Use of VLANs and (scheduled) routes with the different planes and in parallel a ring topology assumes MSTP to handle the interruption of different VLANs at different logical points across the rings!

short (IEEE802.1), see also sub-chapter 3.2.8. In context with this document the following TSN features require an A-Plane/B-Plane approach as detailed below.

Firstly, scheduled traffic and time slots (IEEE802.1Qbv), which allow to reserve time slots for critical communication. The time slots are referred to a common time base and need to consider the propagation delays through the network. Here the A-Plane/B-Plane approach allows for a static network configuration.

Secondly, seamless redundancy (IEEE802.1CB) based on duplication and deletion of frames. Here the A-/B-Planes are the redundant communication channels between source and sink. The redundant planes impose close timing behaviour between each other.

Unless specifically stated “TSN” refers to these TSN features in the following text.

A “TSN-aware device” is a device relying on one or both above features. A conventional device (non-TSN-aware) uses neither feature.

Train Backbone Topology Variants

Chapter 2.5.2 defined different ETB Topology variants ‘A’ until ‘E’.

The proposed network topologies have the following properties in common:

- Ability to “inaugurate”
The sequence and direction of vehicles need to be detectable
- ETB line redundancy
A failure of a single ETB line shall not disrupt communication
- Train backbone node redundancy (besides variant A)
A failure of a single train backbone node shall not disrupt communication.
- ECN and ETB shall be on separate subnets
The broadcast domains shall not extent over a single consist. That rules out a flat layer 2 network.

Variants A and B correspond readily to the IEC61375-2-5 architecture. Variants C, D and E differ from it since the redundant lines are no longer fed to a single node. As discussed in 2.5.2 especially variant D is of interest for a future TSN based network as it allows for a “compile-time” TSN IEEE802.1Qbv configuration using an A-Plane, B-Plane approach. That is during run-time, no dynamic recalculation is required in case one of the redundant backbone nodes per consist fails.

Therefore, this approach is further discussed below, concerning the implementation options for train inauguration.

A-Plane / B-Plane Approach for ECN

For the application of TSN it is beneficial to have a static network architecture as opposed to a dynamic one. A static network architecture keeps the way Ethernet packets are forwarded through the network constant but unfortunately forbids some established redundancy schemes such as ring protocols (e.g. MRP) and spanning tree protocols (e.g. RSTP). A static network architecture allows for a calculation of TSN IEEE802.1Qbv time slots beforehand, that is already during the planning

and configuration of the system. No change of time slot arrangements is required during network operation. A dynamic network architecture would require to seamlessly change time slots during operation, which is considered impractical.

On the other hand, a complete renunciation of a dynamic network architecture would make the well-proven ECN ring architecture unusable even for non-TSN devices connected to the network.

A solution is to combine features of the static and dynamic ECN network architecture using the following “A-Plane / B-Plane” approach (Figure 54):

- One common physical ring. The physical ring incorporates a logical ring and two logical “planes”. The separation can be done using separate VLANs.
- A ring architecture (e.g. MRP) is delivering redundancy for non-critical, non-TSN end devices (ED). Ethernet packets for those devices are eventually forwarded differently in case the ring breaks. If the physical ring is complete there will be a logical interruption at the Master Ring Switch (RS on the left in Figure 54). If there is an actual interruption in the physical ring the logical interruption will be closed.
- A-Plane and B-Plane are logically separated halves on the physical ring. A physical defect within the ring network renders one of the planes incomplete. To achieve redundancy the plane connected end devices (ED-S) are connected to both planes with separate interfaces. Ethernet packets are always forwarded in the same predictable way. That allows for the static configuration of TSN IEEE802.1Qbv time slots.

To allow a static TSN IEEE802.1Qbv time slot configuration on ETB, the ETB lines should be associated to one plane each. (I.e. A-Plane over ETB line A. B-Plane over ETB line B.)

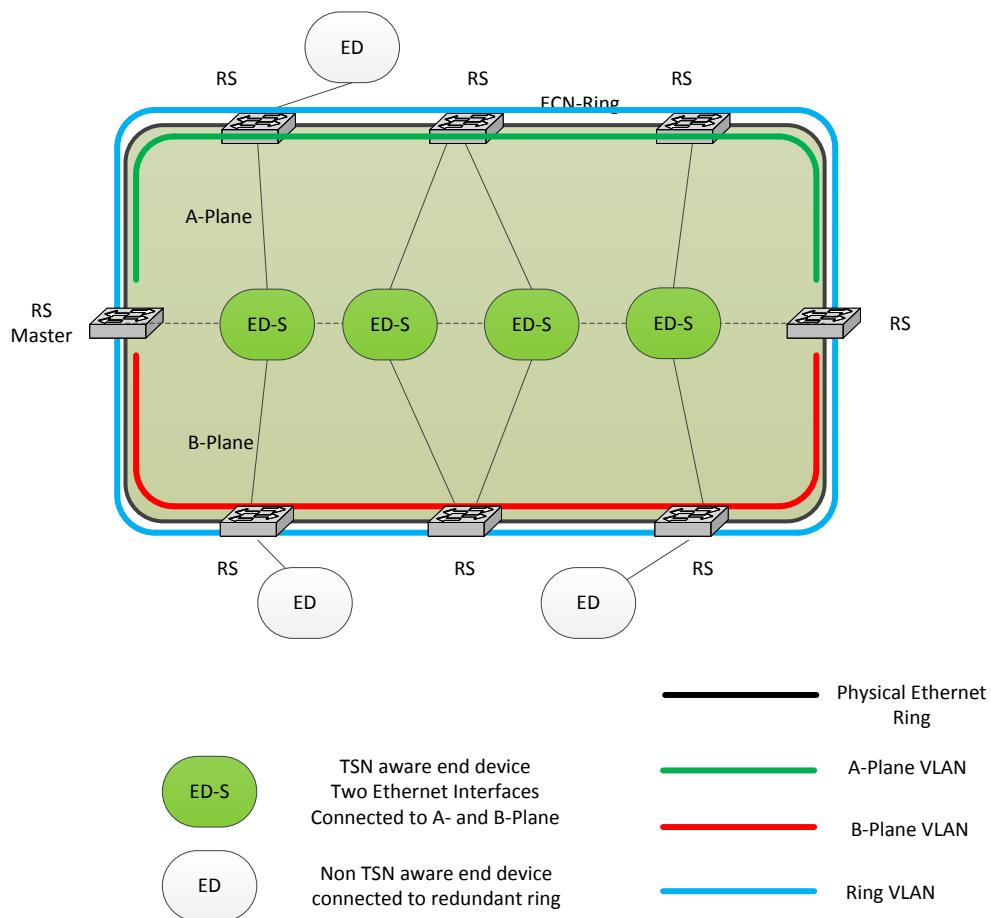


Figure 54: Combination of ECN ring and A-Plane / B-Plane

Line Redundancy

The ETB typically uses line redundancy, that a failure in a single ETB line (e.g. if a wire breaks) does not stop the ETB from functioning. Rather it seamlessly continues to function but asserts a maintenance alert in the diagnostic system. Two different implementations are discussed in more detail below. The method chosen has implications on how or if an A-Plane/B-Plane architecture can be realized over the ETB. There are also implications whether the redundant lines originate from the same ETBN or not.

Link aggregation for ETB line redundancy

The most standard approach for line redundancy as deployed so far is using link aggregation. While link aggregation is typically used to benefit from a higher ("aggregated") bandwidth it also doubles as a line redundancy mechanism. In fact, for the ETB application with 2 parallel links, redundancy is the only functionality used. The links are alternatively used with only one being actively transferring ETB traffic. This allows for coping with a "flickering line" where one line constantly changes state between good and bad. In this scenario the aggregated link would constantly be reconfigured (switching from one to two active lines) while losing frames during the transition. With a mode where only one line is active at a time a failure in the currently chosen line would just cause a single switch over to the standby line.

Implementation of line aggregation requires hardware support in the switch core as well as a controlling software process. On hardware side a group of ports (2 for the discussed ETB case) are

logically considered as one (so called “trunk”). On ingress all ports of a trunk are handled identical. On egress only one port of the trunk is egressing a certain frame. Generally, the function which determines the egressing port is a hash function over the Ethernet header (so that a somewhat equal distribution can be achieved based on MAC source and destination). Task of the control process is to update this hash function based on the availability of lines (defunct ports are not chosen for egressing frames). Typically, a controlling process according to IEEE802.1AX is implemented in software. IEC61375-2-5 uses a tailored control process, which uses the existing HELLO frames for detecting defunct links and additionally works with faster cycle times.

Also, in an ETB setup with 2 lines only one line is active at a time (i.e. the hash function always yields either line independent of the Ethernet header data). This is illustrated in Figure 55. Note that the selection of the ETB line is the same for all logical links (i.e. all VLANs). That implies that compatibility with Plane-A/Plane-B would require consolidating (i.e. time multiplexing Plane-A and Plane-B TSN traffic) the planes on one Ethernet link (in conflict with the Plane-A/B isolation idea). If the trunk ports are part of the same switch core (which is typically the case for ETB topology variant B) redundancy switch over could be done without changing TSN time slots.

The situation is different if trunk ports are connected at different ETBNs (cross switch trunking, which could be used with ETB topology variant D). In this case timing depends on which ETB line is chosen and TSN implementation cannot be kept static.

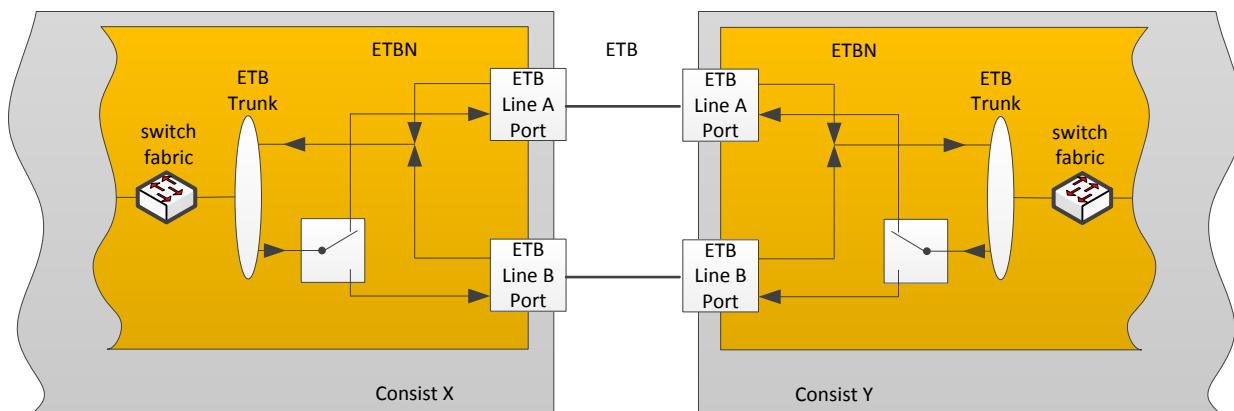


Figure 55: ETB line redundancy based on link aggregation

ETB line redundancy using dynamic VLAN configuration

Link aggregation as defined in IEEE 802.1AX is well established in existing ETB systems and its use is standardized in IEC61375-2-5. Yet in the context of TSN limitations show up:

- It is not possible to dedicate the redundant lines for right/left plane respectively. Right/left plane traffic needs to take the same line. Time multiplexing right/left plane traffic would be the only option.
- Time multiplexing of right/left plane though possible contradicts the idea of isolated planes. Support for variant D is not easily possible.

To overcome those limitations a different line redundancy scheme would be required the implementation of which is discussed below (Figure 56):

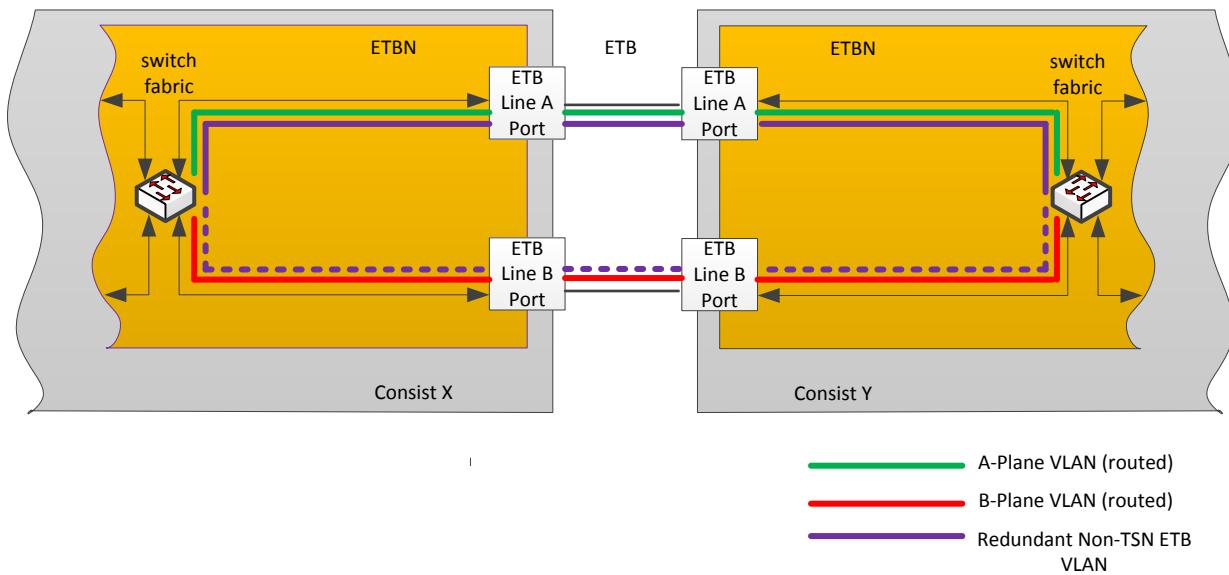


Figure 56: ETB line redundancy using VLAN reconfiguration

Left Plane and Right Plane, or from a consist local perspective A-Plane and B-Plane, are statically mapped to ETB line A- and B-ports respectively. Consequently, for A-Plane and B-Plane networks there is no line redundancy.

An additional VLAN (violet) carries non-TSN traffic for which line redundancy is implemented by using either ETB line A or B. This is done by reconfiguring the VLAN members based on a line integrity test mechanism (in turn based on Ethernet management frames periodically sent on all ETB ports. Same as for link aggregation). Either ETB Port A or ETB port B of a certain ETB Direction is part of the “violet” VLAN. That is the configuration for the “violet” VLAN is dynamically changed during run-time. At no point in time both ETB ports shall be part of the “violet” VLAN to prevent a broadcast or multicast storm from appearing. The redundant non-TSN connection, which is also used for inauguration frames (TOPO) can cope with multiple line errors if at least one redundant line is working between any two neighbouring ETBNs. This allows for a reliable inauguration result even if neither line A nor line B is complete (in which case TSN traffic is impacted and system could only be operated in a degraded mode).

Using VLANs makes it also easy to distribute the ETB ports among two ETBNs as shown in Figure 57. Basically, each ETB connection between two consists builds a redundant ring for just the ETB VLAN.

Having the ETB ports on two discrete ETBNs make it even possible to reuse the same VLAN IDs for A-Plane and B-Plane routed traffic as the VLAN IDs are not forwarded across planes. This is allowing for an easy turning of the consist (swapping Dir1 and Dir2), when the consist implements symmetry along its diagonal. In this case turning the consists swaps Dir1 and Dir2 of the consist but also swaps redundant line A and line B of the turned consist. With two different VLAN IDs this would otherwise disrupt the Plane VLANs.

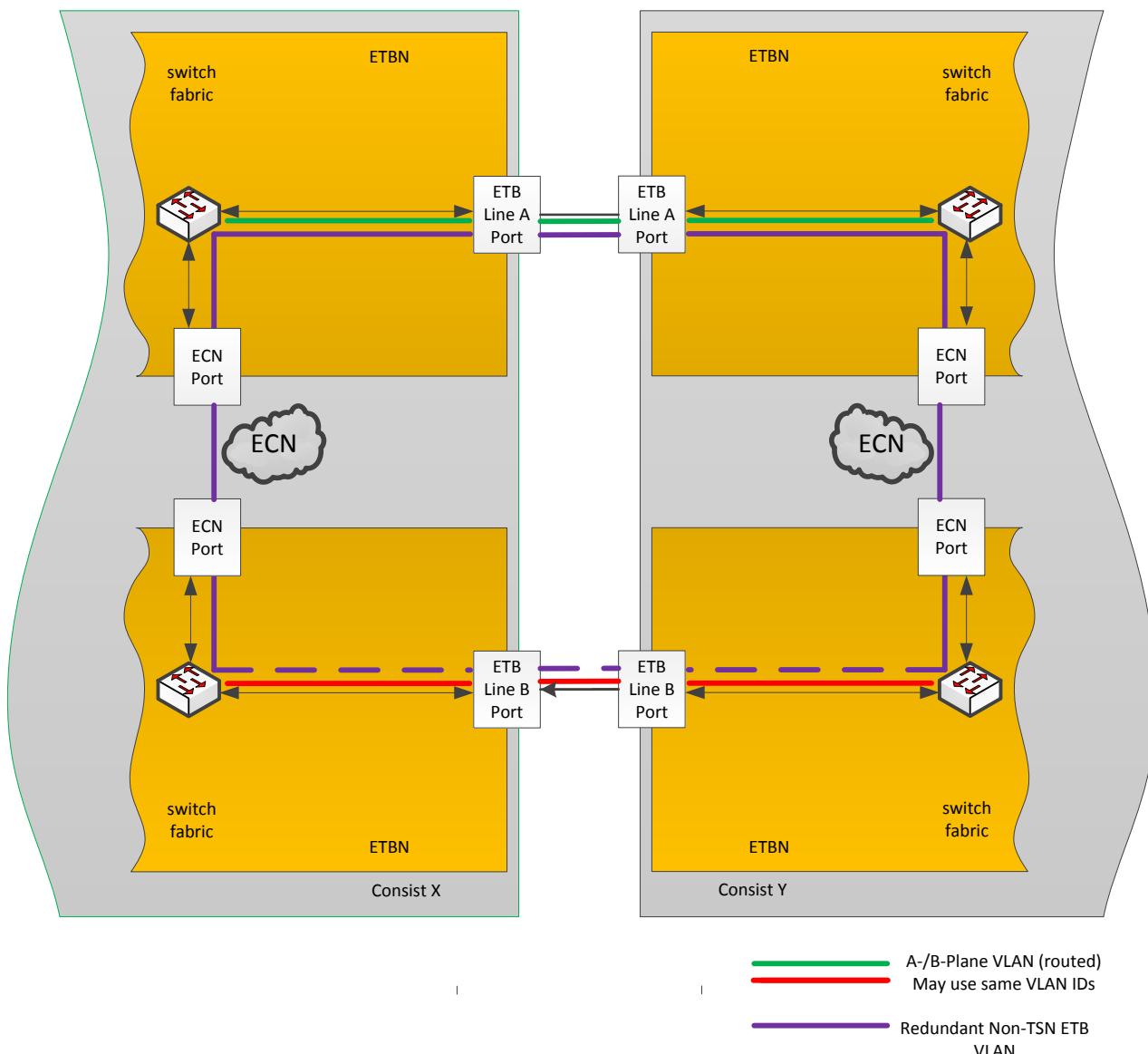


Figure 57: ETB line redundancy using VLAN across ECN

IEC61375 Inauguration Overview

Figure 58 shows a simplified train backbone architecture for IEC61375-2-5 which also corresponds to variant B [1]. ETBN redundancy and line redundancy are completely separated mechanisms.

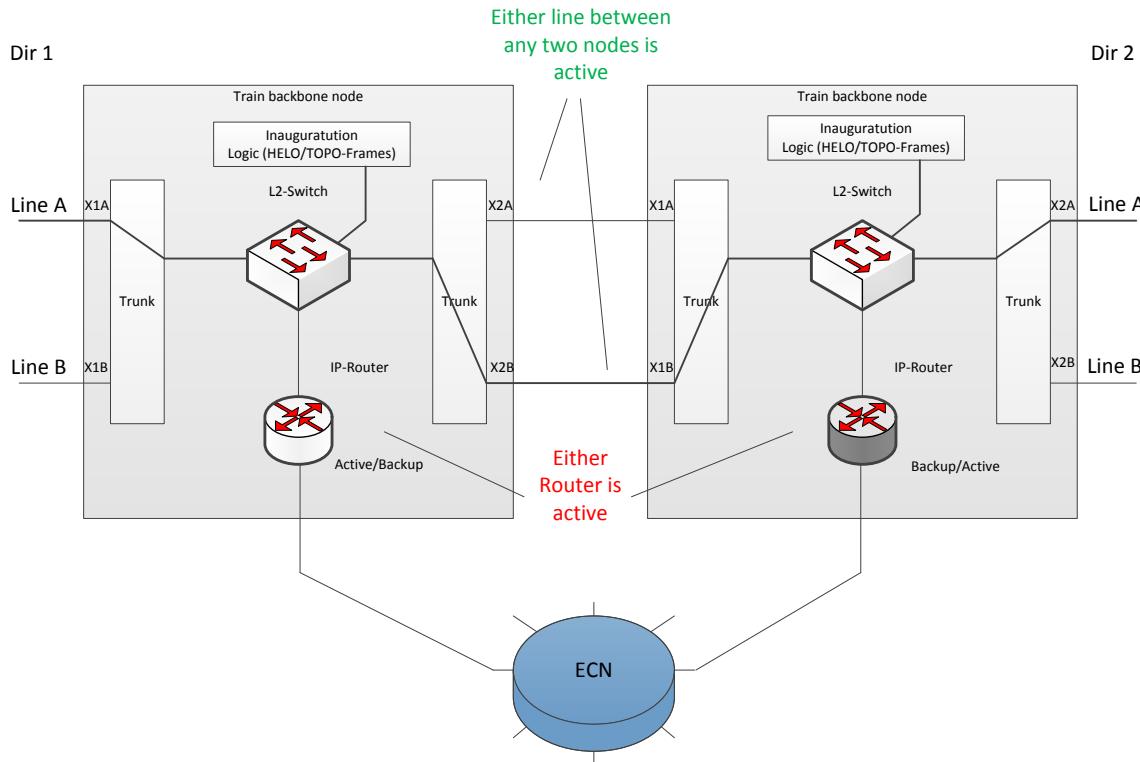


Figure 58: ETBN setup IEC61375-2-5 or “variant B”

Line redundancy works by using trunking, that is using multiple physical lines (here: two, A and B) to form a single logical line. The logical line is switched through the ETB nodes. Between the ETB nodes either physical line is chosen. As shown as an example in Figure 58 a different line can be chosen along the path. It is not required for either line A or B to be completely working within a train. Rather it is sufficient that at least one line between any two ETBNs is intact.

ETBN redundancy works by having more than one ETBN per consist (here: two). One being active, one in backup as chosen by a redundancy protocol (VRRP). The routing part is disabled on the backup node. The inauguration logic is always active.

Concerning the use of TSN with variant B there are the following issues:

- Node redundancy: Failure of node changes timing. It is not possible to use fixed TSN time slot timing on the backbone.
- No separation of planes on ETB level. Though, as discussed in 3.2.8, a consolidation of A-/B-Plane on a single link is feasible but not of real use as the problem with node redundancy still exists.

Consequently, “variant B” is not a feasible option for TSN use.

Train Inauguration for Variant D, A/B-Plane Approach

Figure 59 shows a consist network according to variant D using A-Plane / B-Plane approach. The basic difference is that the redundant lines are no longer fed to a single ETBN. That makes it more complicated to separate the ETBN redundancy from the line redundancy. One of the options presented below combines ETBN and line redundancy (“parallel inauguration”) the other tries to still handle line redundancy independently (“centralized inauguration”).

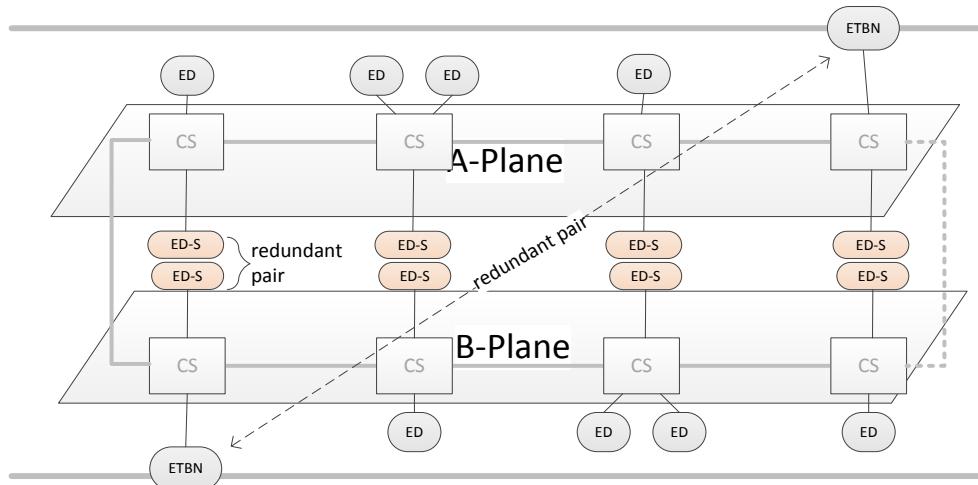


Figure 59: Variant D, A-Plane/B-Plane

Parallel Inauguration

As shown in Figure 60 one option is to basically duplicate the standard IEC61375-2-5 architecture but omit line redundancy. Line A and line B will independently inaugurate and yield independent results. Only in case of fully intact Line A and B networks the inauguration results will be identical. In case the result is identical either network can be chosen to be used. Otherwise the “more complete” network could be chosen. A/B-Plane data is routed by the associated ETBN router connected to the respective line (Line A or line B). For non-critical data, the “chosen” network is used (This allows redundancy for EDs only connected to either plane).

The drawback of the parallel inauguration is that for the system to work at least one of the redundant lines need to be complete. This significantly reduces the availability compared to the IEC61375-2-5 approach.

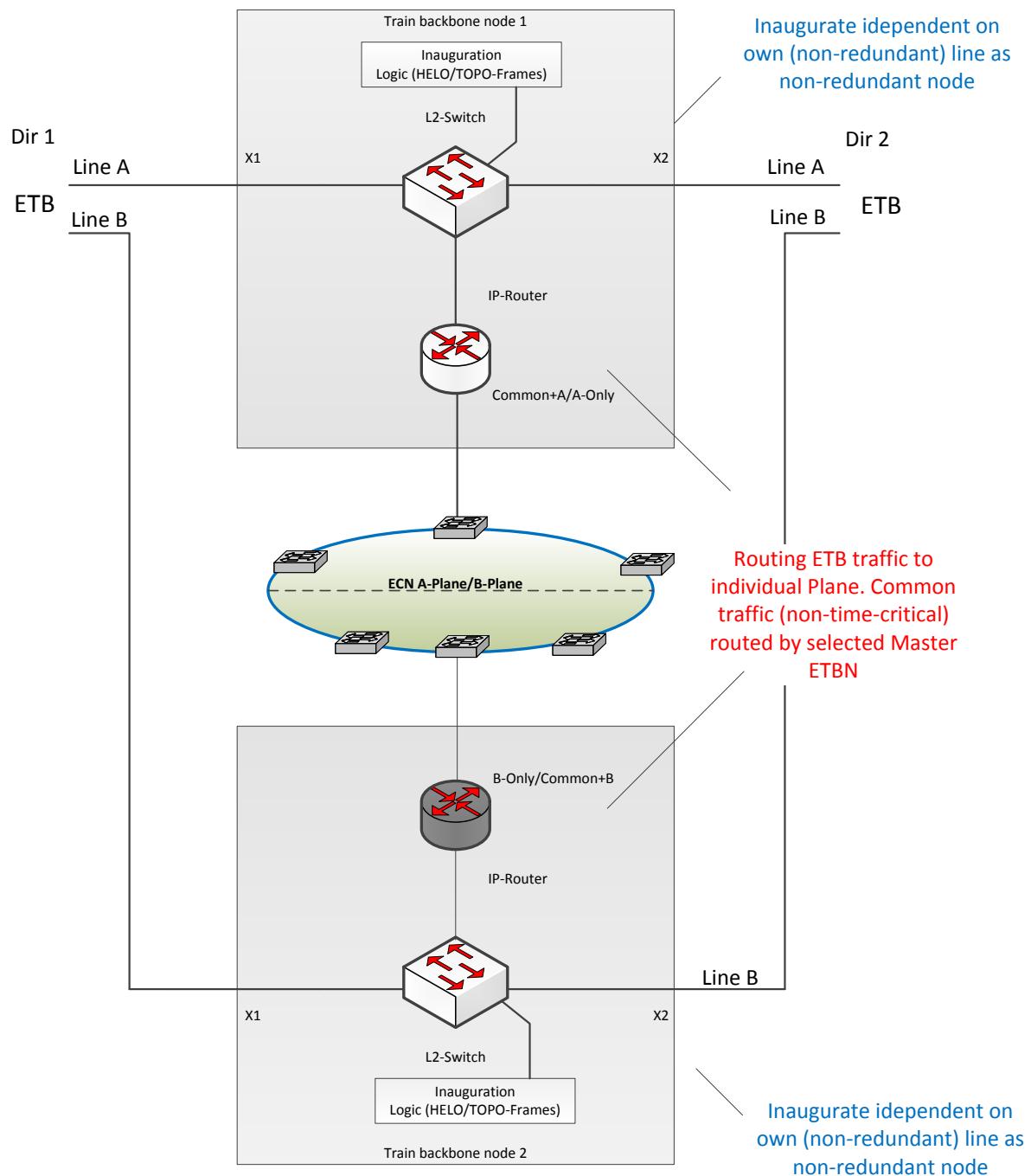


Figure 60: ETBN setup Variant D, parallel inauguration

Centralized inauguration

The architecture shown in Figure 66 tries to overcome the availability limitation caused by the parallel inauguration, described in the previous paragraph. It also allows to be nearer to IEC61375-2-5. The picture looks very similar to Figure 60. The difference is that the two ETBNs are no longer performing an independent inauguration but are logically put in series as detailed below.

Adapting IEC61375-2-5 inauguration to variant D

Consider the variant B approach according to IEC61375-2-5 depicted in Figure 61: The 2 ETBNs per consist are connected in series facing to consist ends 1 and 2 respectively. Each ETBN emits HELLO frames with its own MAC address. The HELLO frames are LLDP frames which allow the detection of switch interconnections based on ingress and egress ports. The neighbour relationship (“connectivity vector”, left neighbour MAC, own MAC, right MAC) is sent as a TOPO frame using multicast to all other ETBNs on the ETB. The consist can be considered as a “black box” (Figure 62) and the goal is to mimic its behaviour concerning TOPO and HELLO frames when moving from variant B to variant D.

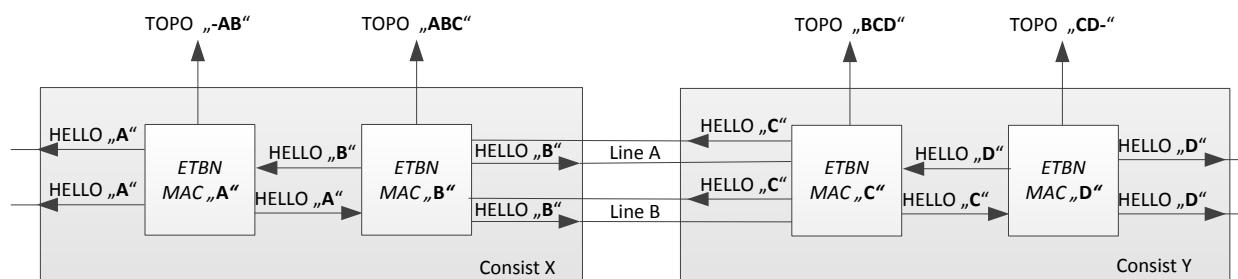


Figure 61: ETBN nodes in series (variant B)

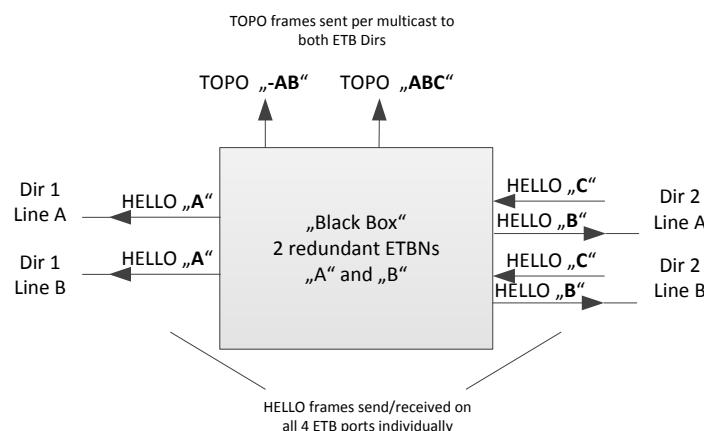


Figure 62: Consist as a “Black Box”

Figure 63 shows the lay-out of the redundant ETBNs for variant D. Physically the two ETBNs are in parallel, serving one redundant ETB line each. As far as inauguration is concerned the two ETBNs are logically still connected in series as shown in Figure 64. The blue line shows the emulated connection to exchange HELLO frames between the two redundant ETBNs of one consist. The ETBNs for redundant line A, B have a direct connection to the local Dir1, Dir2 ETB ports respectively (Figure 64, shown in red). They have a proxied connection to the non-local Dir2, Dir1 ETB port

respectively (Figure 64, shown in red/green). The HELLO frames exchanged between the ETBNs of a consist and the proxied HELLO frames are tunneled through the ECN.

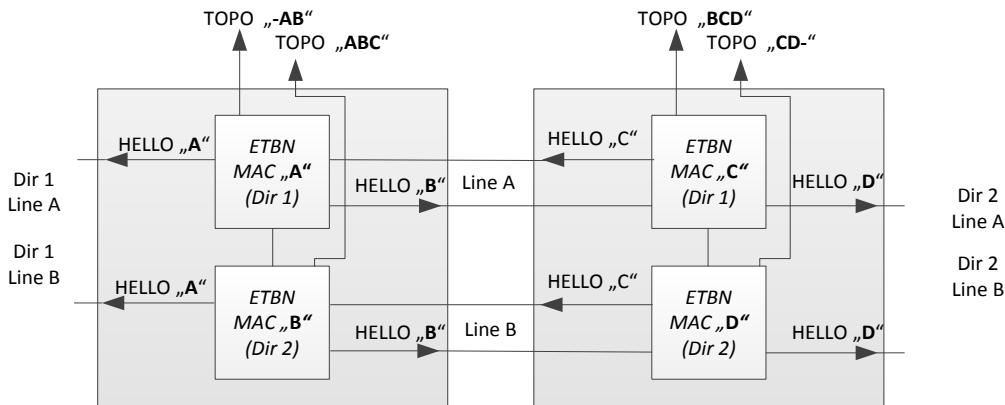


Figure 63: ETBN nodes emulating a serial topology (variant D, centralized inaug.)

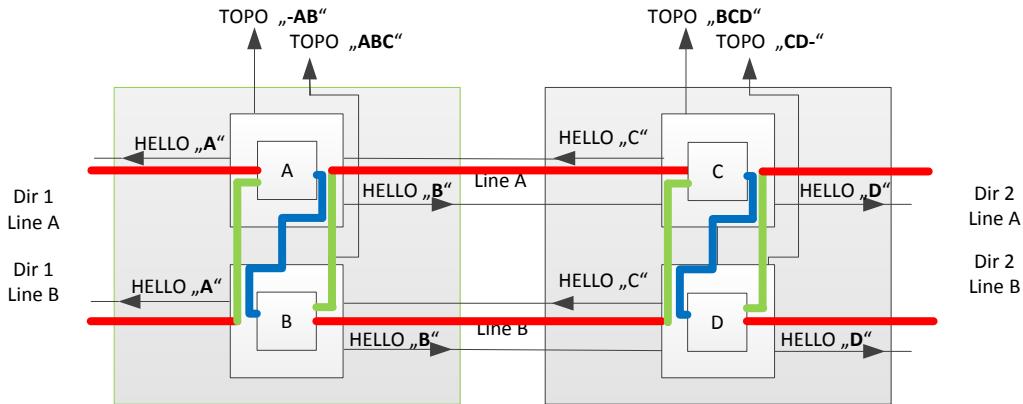


Figure 64: Logical connections between ETBNs

Node redundancy

For variant B as well as for variant D the ETBNs build a redundant pair with one node being a master and the other being a slave (hot standby). Only the master node has the ECSP interface active for communicating with the consist CCU. Typically, only the master node is doing the ETB-ECN routing. Both nodes take place in the inauguration and emit their own TOPO frame. In case of the failure of the master node the slave node takes over the master role (assuming the ETBN slave node was present prior to the failure).

For variant B a failing ETBN node closes its bypass relay so that the remaining (master) ETBN emits its HELLO frame to both ends of the consist. If the failing ETBN was a master prior to the failure, mastership changes. If the failing ETBN was a slave prior to the failure no functional changes occur to the existing (master) ETBN. Redundant lines are handled independent of an ETBN failure.

For variant D a failing ETBN changes the remaining ETBN to become a master (if not already master, behaviour just as for variant B). In any case (even if the remaining ETBN already was a master), the now single ETBN stops proxying and send its HELLO frames directly to both (Dir1, Dir2) ends (Figure 65). From a “black box” point of view the behaviour is mostly identical to an ETBN failure for variant

B, except that an ETBN failure always leads to a failure of the associated line (which is not the case for variant B).

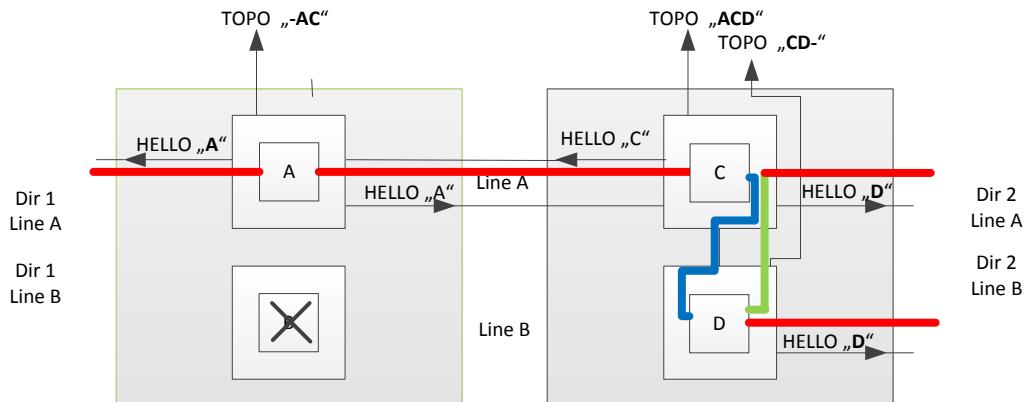


Figure 65: ETBN B failure scenario

Line redundancy

Since either line A or line B is used to handle the non-TSN traffic (including inauguration frames. A/B-Plane traffic may be statically mapped to ETB lines A/B respectively) between any pair of consists there need to be a cross connection between line A and line B inside the consist. This cross connection could be implemented by a VLAN connection between both lines. The VLAN will bypass the routers and requires the ECN to reach the opposite redundant line, which is an integral weakness of the centralized inauguration setup.

One major challenge is the implementation of trunking. That is either line A or line B shall be used for ETB traffic and distribution of the TOPO frames. A first idea could be to use cross-switch trunking, where the ports of the trunk can be on different switches. That would require to correctly handle proprietary tagged frames over all intermediate switches (e.g. same vendor for all the switches). This approach would allow true compatibility with the existing IEC61375-2-5 standard. Unfortunately, this approach is hardly feasible since a line redundancy switch over would change the frame timing as discussed above.

The suggested method is to use VLAN reconfiguration as it was detailed before. A “redundant ring” is formed by the ETB VLAN when connecting two consists together (see violet VLAN in Figure 67). This method also readily allows to use Line A / Line B for plane A / plane B traffic respectively.

The discussion so far assumed that the consists are connected in the same orientation relative to each other (say all consists are in train direction). In practice consists maybe oriented arbitrarily to each other. Figure 68 shows the scenario where two consists are oriented opposite to each other. Planes A/B of a consist are mapped to train sides left/right depending on the orientation of the individual consists. This allows for a simple method to figure out the consist side, e.g. by sending out beacon frames¹² (“left side”, “right side”) broadcast on the respective plane of one consist (e.g.

¹² See 3.5.4

leading consist) to all consists. This method is independent of the IEC61375 inauguration which also gives this information. Both results can then be checked against each other.

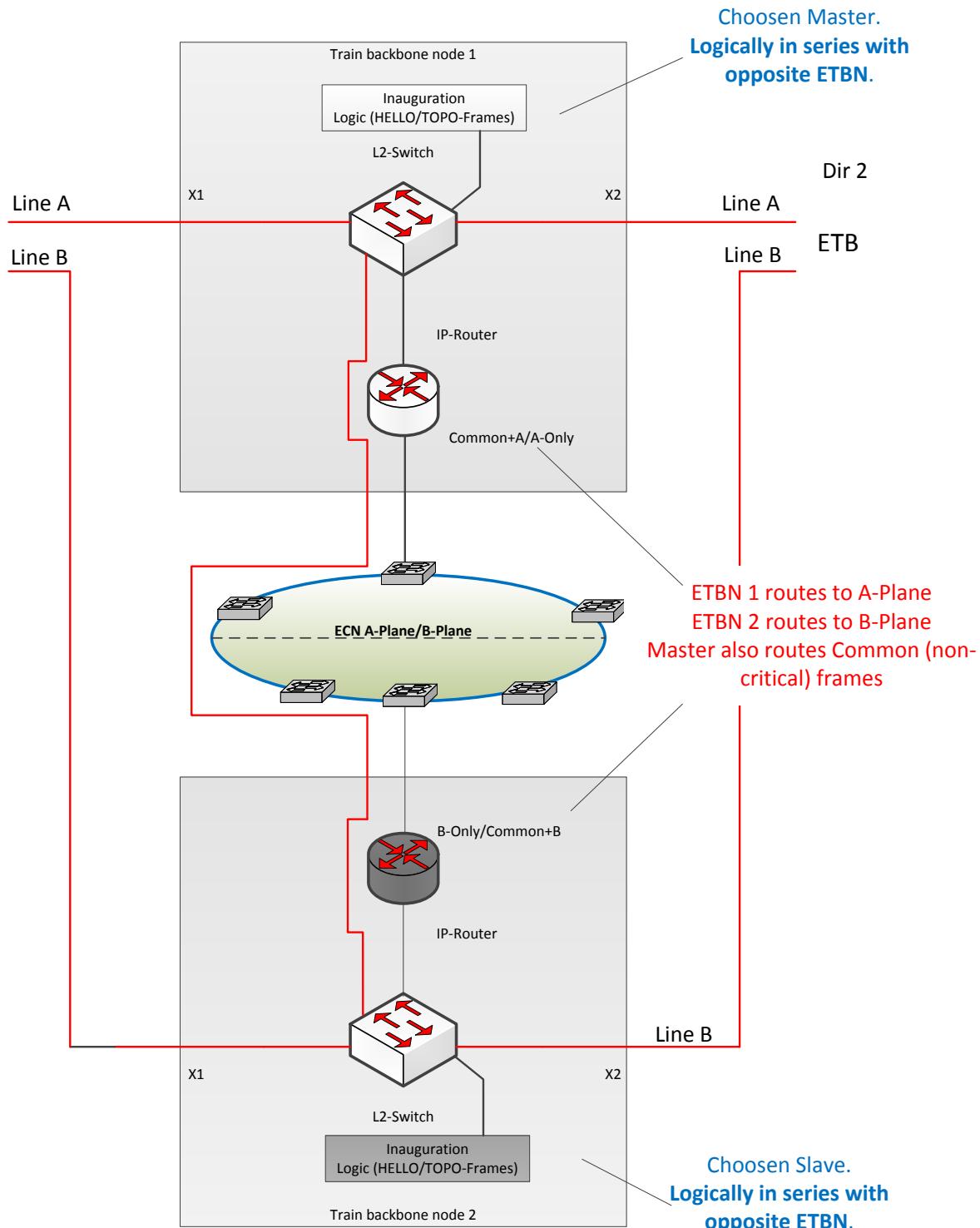


Figure 66: Variant D, "centralized" inauguration

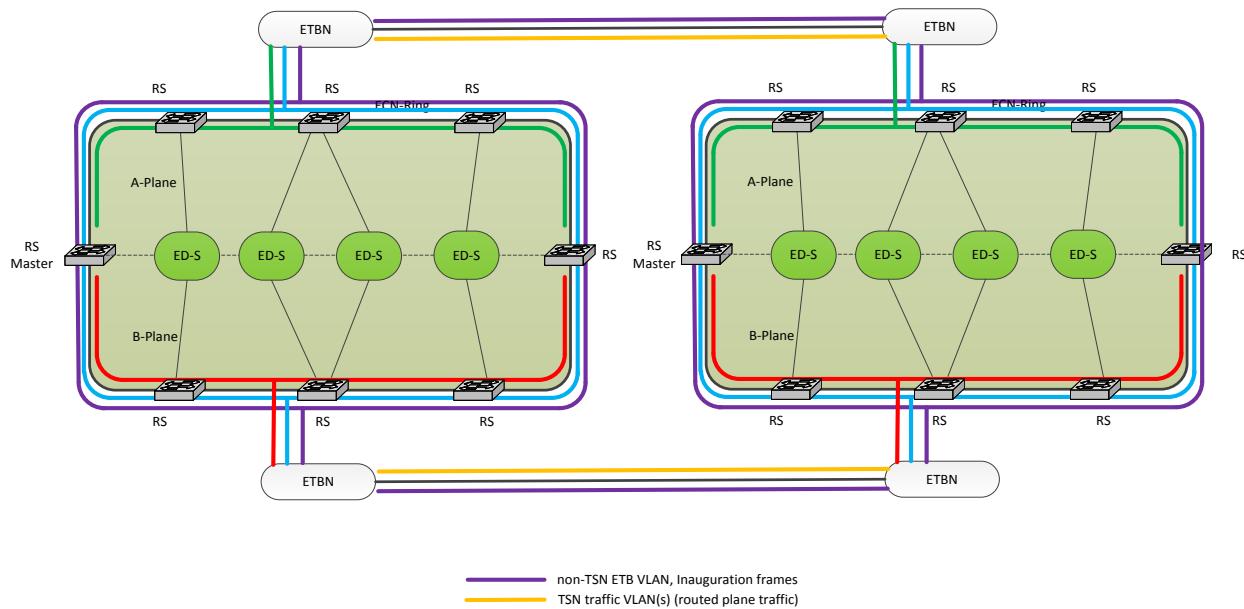


Figure 67: Variant D, “centralized” inauguration, coupled consists

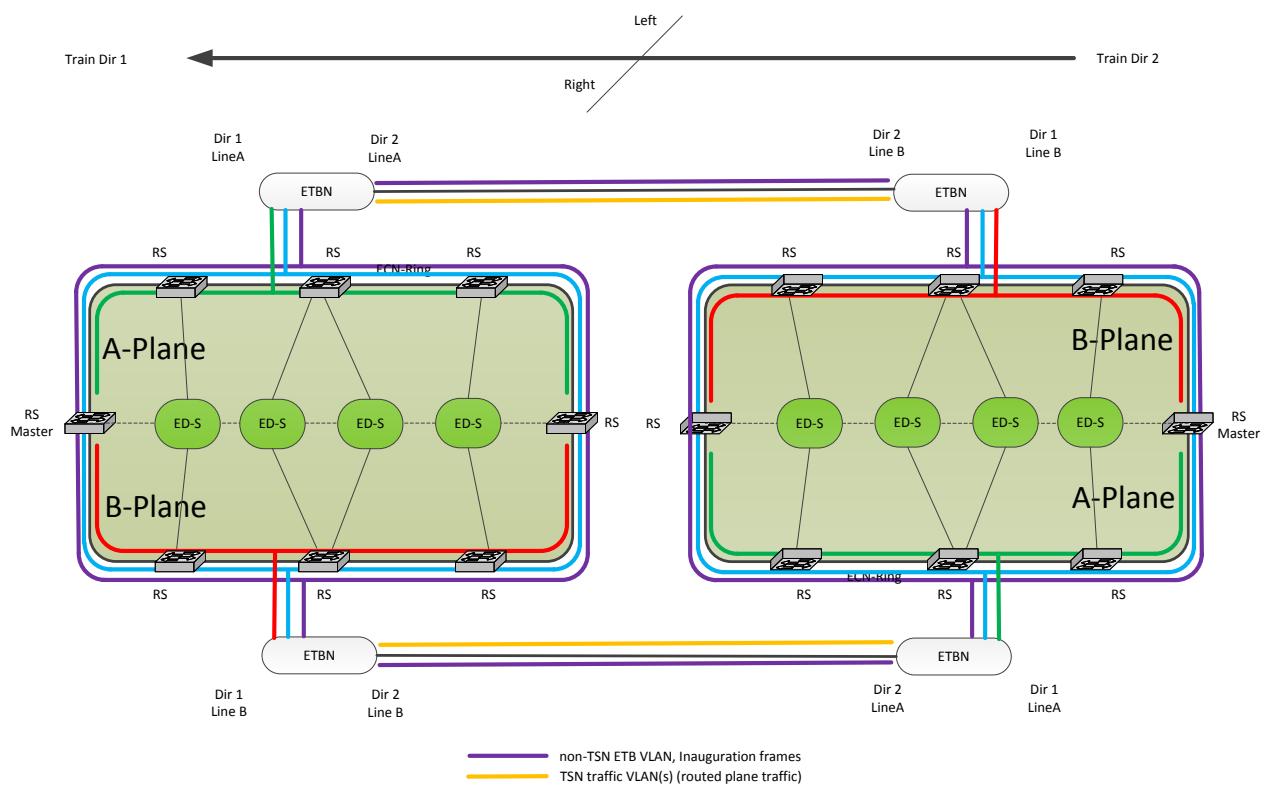


Figure 68: Variant D, “centralized” inauguration, rotation of consist

Summary

The architecture variant D, “centralized inauguration” with a line redundancy scheme based on VLAN reconfiguration has many advantages over the other variants due to

- Variant B ETB backbone cannot use static TSN timeslots as node redundancy changes timing
- Variant D “centralized inauguration” is much nearer to the IEC61375-2-5 inauguration than the “parallel inauguration”
- a line redundancy scheme based on VLAN reconfiguration in that it can handle TSN-Plane-A/B traffic different from conventional traffic

One caveat still exists with the necessity to have either redundant line fully functioning for train wide scheduled traffic.

3.2.11 Security aspects

On data link layer two mechanisms are proposed to increase security: Media Access Control Security (MACsec) and Port Based Network Access Control (PNAC). MACsec as defined in IEEE 802.1AE is used to encrypt traffic point-to-point for data confidentiality and integrity. PNAC, which is standardized in IEEE 802.1X, is an authentication mechanism to allow only privileged devices joining the network. Both standards are interconnected since the PNAC authentication can be used to exchange security keys, which are needed for MACsec to establish an encrypted link. In addition, key management needs also to be considered: For dynamic key exchange a server infrastructure is needed. The commonly used RADIUS protocol is therefore suggested. See chapter 3.5.7 for further information.

Since equipment of all end devices with these mechanisms is cost intensive these features should only be implemented in sectors where it significantly increases the security level. This applies particularly to end devices and connectors which are easily accessible by an attacker like CCTV cameras in passenger compartment.

Furthermore, traffic shaping, which is described in chapter 3.2.5, can also be used as a security mechanism to prevent the network against denial of service attacks.

3.3 NETWORK LAYER

3.3.1 IP addressing

IP UC addresses

All devices connected to NG-TCN have at least one IP address, which is used as source address in all transmitted IP packets and which is present as destination address in all received unicast IP packets.

The network layer addressing scheme for NG-TCN is defined in IEC61375-2-5 (train level) and IEC61375-3-4 (end device level).

IP MC addresses

NG-TCN allows the definition of IP MC groups. For addressing IP MC groups, the limited scope address range defined by the IANA (IETF RFC 2365) is used.

This address range is subdivided into (IEC61375-2-5, IEC61375-3-4):

ECN range: 239.255.0.0/16 (for groups inside one ECN)

Train range: 239.192.0.0/14 (for train wide groups)

Train wide addressing, R-NAT

IP addresses must be unique within an ECN, but different ECNs may overlap in IP addresses because all ECNs in a train use the same ECN IP address range. To have train wide unique IP addresses, ECN range addresses are translated to train range addresses when transmitted over ETB by using a railway specific network address translation (R-NAT).

R-NAT works like this:

1. While routing an IP telegram from ECN to ETB the IP source address is translated to a train range IP address. This is done for unicast and multicast.
2. While routing an IP telegram from ETB to ECN the IP destination address is translated to an ECN range IP address. This is done for unicast only.

As train range addresses may change after each train inauguration, the IP routers within the ETBN must be reconfigured after each train inauguration.

3.3.2 IP to MAC address resolution

Ethernet frame addressing is based on MAC addresses, and for IP packets encapsulated into Ethernet frames, destination IP addresses must be associated to the corresponding MAC addresses.

In IPv4, the Address Resolution Protocol (ARP) as defined in IETF RFC 826 is used for resolving IP addresses to MAC addresses.

For resolving an IP address, an ED is broadcasting an ARP request with the IP address in the payload, and the ED holding this IP address responds by broadcasting an ARP response. This association of IP address and related MAC address is then cached in the IP layer of the requesting ED, so that it is ‘learnt’ for future transfers.

Sometimes it is necessary to change this association, e.g. when the original device got out-of-order and a redundant device takes over (with same IP address, managed by VRRP for instance). Then the new device sends a ‘gratuitous’ ARP response which changes the associations.

IPv6 uses the Neighbor Discovery Protocol (NDP) for IP address resolution.

3.3.3 IP routing

General

Physical or virtual LANs are interconnected by IP routers. Contrary to Ethernet switches, which route Ethernet frames within a LAN on the base of the MAC destination address (OSI layer 2), are IP packets as defined in RFC 791 routed between LANs on the base of the IP destination address (OSI layer 3).

Within NG-TCN, two types of IP routers are used:

- Dedicated IP router for connecting ECN and ETB VLANs (ECN/ETB Gateway), e.g. ECN-OOS with ETB-OOS. This type of router is located in the ETBN device.
- IP router between different ECN VLANs (ECN/ECN Gateway), e.g. between ECN-OOS and ECN-COS.

All types are able to route unicast and multicast IP packets.

Static versus dynamic routing

Routing in the internet is supported by dynamic routing protocols like for instance OSPF, which continuously check the network for the best possible path between any two ED and which dynamically change the IP router configurations to adapt to the actual network situation. NP-TCN does not make use of dynamic routing protocols, because the only network changes occur after train inaugurations and these are very railway specific. So, the ETBN takes care about IP router reconfiguration by removing old route entries and adding new static routes after train inaugurations.

ECN/ETB Gateway (ETBN)

Contrary to the communication inside an ECN or ETB, which is Ethernet frame based (ISO OSI Layer 2), are conventional data exchanged between ECN and ETB by a Layer 3 routing of IP packets (ISO OSI Layer 3). This routing is necessary because ECN and ETB are separate Layer 2 networks, which can only be connected on Layer 3. The routing process differs slightly between IP unicast routing and IP multicast routing.

Transmitted IP unicast packets are first routed, and the source IP address is translated (R-NAT) before they are forwarded to the ETB. Thereafter they are routed in the destination ETBN and the destination IP address is translated. R-NAT here translates the train IP destination address to the corresponding const IP address.

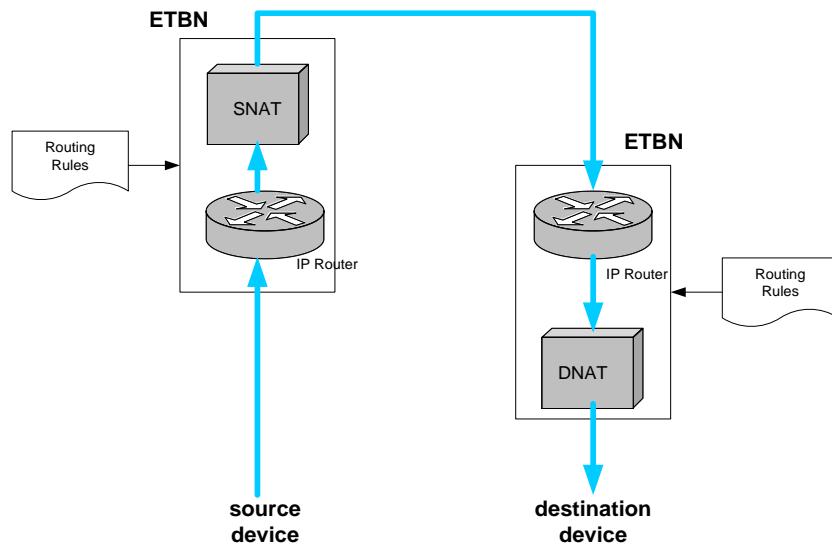


Figure 69: IP Unicast Routing

As IP multicast group addresses are never translated (R-NAT), there is no destination address translation at the destination ETBN. There is however another particularity: contrary to unicast routing, where the routing decision is only taken on the base of the destination IP address, require routing decisions of IP multicast group packets both source IP address and destination IP address. As a consequence, it is required to configure for all train-wide multicast groups the related consist local source devices.

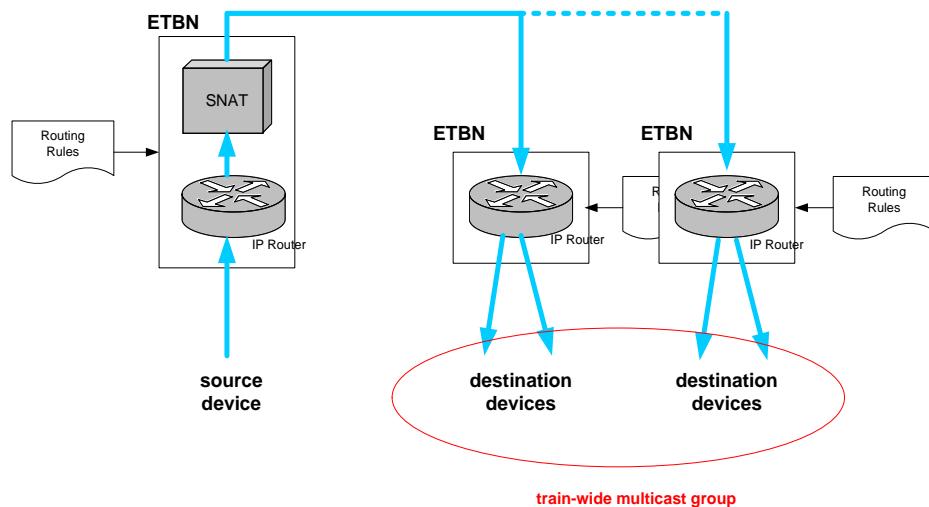


Figure 70: IP Multicast Routing

ECN/ECN Gateway

The ECN/ECN Gateway connects two consist VLANs, e.g. the ECN-TCMS and the ECN-OOS. Besides IP routing, the ECN/ECN Gateway shall provide firewall capabilities for filtering IP telegrams which do not meet the security policy. The ECN/ECN Gateway shall be able to filter IP telegrams at least based on

- IP source address
- IP destination address
- Source port (UDP/TCP)
- Destination port (UDP/TCP)
- ComId

The operation of an ECN/ECN Gateway is demonstrated with the block diagram shown in Figure 71. Routing and forwarding of IP packets is performed by the OS kernel (for example Linux), which is configured with the aid of for example "iptables".

iptables is a user-space application program that allows to configure the tables provided by the Linux kernel firewall (implemented as different Netfilter modules) and the chains and rules it stores.

A chain contains a ruleset of rules that are applied on packets that traverse the chain. Those rulesets are allocated to different tables, and each table has a specific purpose (see Table 29).

A rule defines a condition (e.g. a specific value within an IP packet) which, if matched, leads either to the acceptance of the IP packet or defines to drop it.

An IP packet ingressing a router firewall via the Ethernet interface is first passing a PREROUTING stage, during which rule chains from the raw, mangle and nat table can be applied. If not discarded, it then passes the IP router which decides whether to forward the packet towards the egressing Ethernet interface (FORWARD) or to pass to the local managing CPU. In the FORWARD stage, rule chains from the mangle and filter table are applied. This is the stage where the firewall filtering occurs. If not discarded yet, the IP packet is further passed to the POSTROUTING stage, where rule chains from the mangle and nat table are applied. Finally, the IP packet egresses the ECN/ECN Gateway over the second Ethernet interface.

Note that the ECN/ECN Gateway does not use mangle and nat tables (no generic rules defined for those tables) in standard configuration to restrict the ECN/ECN Gateway functionality to that what is absolutely necessary for standard IP routing and security firewall. This is also the part which is covered in the generic product test. However, the ECN/ECN Gateway allows defining "**user defined rules**" as part of the ECN/ECN Gateway configuration. Those user defined rules have to follow the syntax defined by iptables and in principle allow implementing all functions which are supported by iptables. In the case user defined rules are applied, the user takes the responsibility for the correct functioning of the ECN/ECN Gateway.

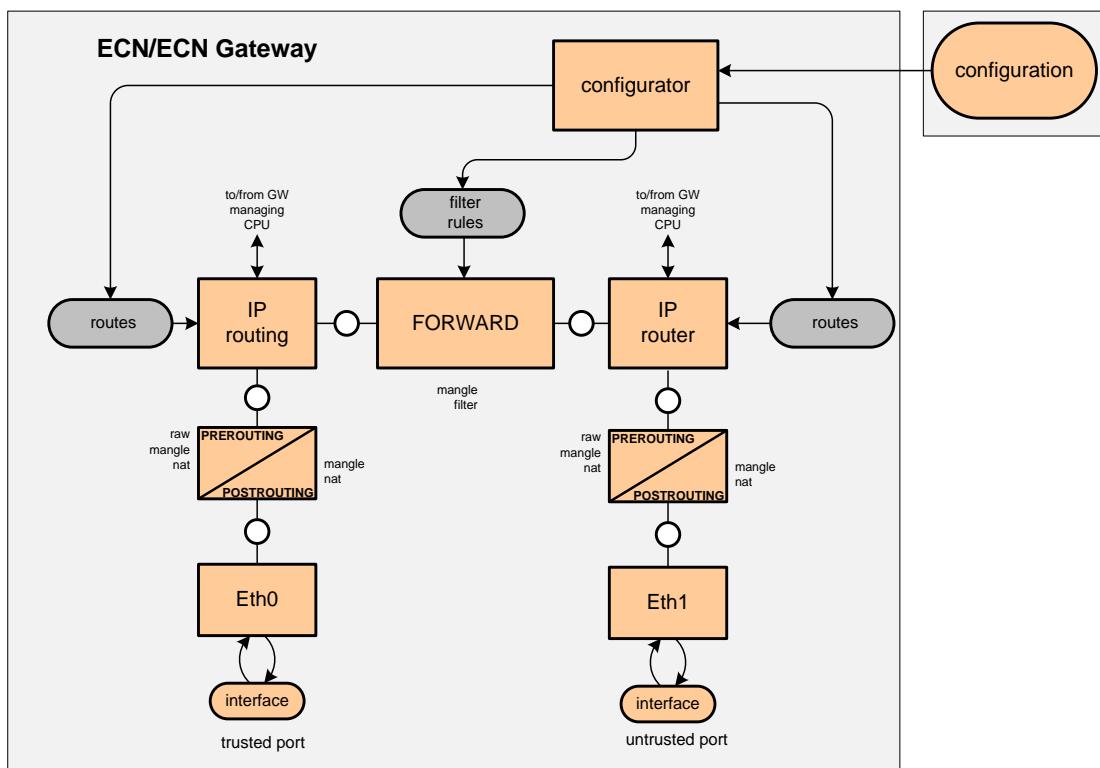


Figure 71: Routing and filtering IP packets

Table 29: iptables

Table	Description
Filter	The filter table is mainly used for filtering packets (firewall). Packets can be matched and filtered in whatever way. This is the place where action against packets is taken and where they are DROPPed or ACCEPTed, depending on their content.
Mangle	This table is intended for mangling packets, e.g. to change ToS (Type of Service) or TTL (Time To Live) fields and the like. Mangling is not explicitly supported by the ECN/ECN Gateway, but can be applied with user defined rules.
Nat	This table is intended to be used for NAT (Network Address Translation) on different packets. Nat is not explicitly supported by the ECN/ECN Gateway (it is supported in the ETBN however as described above), but can be applied with user defined rules.
Raw	The raw table is mainly only used to set a mark on packets that they should not be handled by the connection tracking system. Raw tables are not supported by NG-TCN (not implemented).

Connection tracking

Connection tracking is a feature build into the OS kernel (netfilter) which allows a stateful inspection of communication sessions. A typical example is a TCP session, which is opened with a SYN packet,

and then answered with a SYN/ACK return packet. Thereafter the connection tracking system knows that this is an established connection.

This feature allows the supervision of communication sessions. If for instance a SYN/ACK is seen from a non-known (not established) connection this packet will be discarded.

This feature also allows defining powerful firewall rules. If a connection shall only be initiated from a trusted network, e.g. the TCMS network, one can define a rule that does not accept SYN from the OOS network, but would let pass SYN/ACK packets from the OOS network for established connections.

For working, connection tracking needs to know the protocol internals. Connection tracking supports standard stateful protocols like TCP, but also stateless protocols like UDP and ICMP. With corresponding OS configuration also other protocols could be supported.

IP routing performance

The routing performance is determined by two values:

- 1) The throughput rate R_{RT} , which determines the number of IP packets (of minimal size) routed per second.
- 2) The routing time T_{RT} , which determines the time it takes for a routed IP packet from router ingress until router egress. The variance of the routing time defines the jitter.

The throughput can be limited if routing is performed in software. The parameters influencing the throughput are:

- CPU load caused by other processes
- Number of IP routing rules
- Network address translation
- If enabled, number of firewall rules
- Routed IP packet is UC or MC

As CPU load varies over time, also the throughput rate may vary.

In case of a CPU overload situation, temporary or permanent, latency will increase (theoretically until infinity). There is then also a high risk that QoS is violated and that Ethernet frames are discarded. This risk can be minimized with a careful configuration of the system.

Avoidance of this risk is only possible with a full wire speed capable IP router.

3.3.4 ICMP

ICMP as defined in IETF RFC 792 is a mandatory part of the IP protocol stack. It supports functions which are helpful and necessary for IP traffic operation. Important functions are:

- Destination unreachable indication

- Redirection to another IP router
- Echo server
- Traceroute

3.3.5 MC group management

General

ED can form a “Multicast Group”, which allows sending data to that group by one telegram in a one-to-many relationship. The advantage is that a data telegram (e.g. TRDP-PD) needs not to be send to each group member individually, which would require much bandwidth. The handling of multicast groups is performed by a standardized protocol, the IGMP.

IGMP Protocol

IGMP (Internet Group Management Protocol, RFC 2236) is a protocol used by IP hosts to dynamically register membership in Multicast groups to the closest multicast router.

An IGMP querier periodically broadcasts a “Host Membership Query message” to remain updated about group membership for the local network. Group members will respond with a “Host Membership Report message”, which lists the IP MC addresses they intend to join (this membership report can also be sent voluntarily).

All CS shall implement IGMP querier up to IGMP v3. Instead of operating one IGMP querier per ECN (concept recommended by IGMP), IGMP queriers are by default active on all managed switches.

NG-TCN IGMP implementation

As mentioned before, all NG-TCN managed switch devices have an active IGMP querier. A query message received from a directly connected ED is processed by the local querier and not further forwarded to the remote multicast router.

After receiving a report message, the querier adds the related IP MC address(es) to the switch address database together with the information to which switch ports received IP MC telegrams should be forwarded (“IGMP snooping” function, see below). These are the ED port, it received the report message from, and the ECN ring ports.

If the switch receives an IP MC telegram with a known destination address, the telegram will be forwarded to registered ports (except the port it arrived from).

If it receives an IP MC frame with an unknown destination address, this frame is only forwarded to ECN ring ports.

IGMP Snooping

IGMP snooping as defined in RFC4541 can very effectively reduce multicast traffic from streaming and other bandwidth intensive IP applications. By default, all switches flood multicast packets within the broadcast domain (e.g. all switch ports or the ports belonging to the VLAN the ingressing MC frame belongs to). With IGMP snooping frames are only forwarded to ports where a member of the related group is connected. This reduction of multicast traffic reduces the packet processing at the switch (at the cost of needing additional memory to handle the multicast tables) and also reduces

the workload at the end hosts since their network cards (or operating system) will not have to receive and filter all the multicast traffic generated in the network.

The information, which MC group member is reachable over which port, is retrieved by intercepting IGMP membership reports¹³. As IGMP periodically sends IGMP membership queries, this information is constantly updated. When a switch hears an IGMP report from a host for a given multicast group, the switch adds the host's port number to the multicast list for that group. And, when the switch hears an IGMP Leave, it removes the host's port from the table entry.

All managed CS shall support IGMP snooping (configurable).

3.3.6 Security aspects

Only packet filters as implemented by network firewalls are recommended to strengthen security on network layer. See chapter 3.5.7 for further information about firewall technologies.

In addition, there is an encryption technology existing on this layer called Internet Protocol Security (IPsec). However, as analyzed by Safe4Rail in [10], IPsec is not well suited for NG-TCN since there is no support for multicast communication. Therefore, encryption is proposed on data link layer as mentioned in chapter 3.2.11.

3.4 TRANSPORT LAYER

This chapter describes the transport layer protocols to use for the data transmission in the NG-TCN.

The current series of the standard IEC 61375 already defines the transport protocols and the versions to support for the end devices and the network devices within the network. In IEC 61375-2-3 [18] it is defined that the TRDP protocol runs above the transport protocols TCP or UDP for data communication. Thus, devices connected to the train backbone, and end devices and network devices connected to the consist network shall support these transport protocols.

In IEC 61375-2-5 [19] and IEC 61375-3-4 [20] the protocols to use in the transport layer are defined, where apart from the TCP/UDP protocols, the versions of the protocols ICMP (Internet Control Management Protocol) and IGMP (Internet Group Management Protocol) to use are defined. Although ICMP and IGMP protocols are not exactly from the transport layer (see previous paragraph), in the standard they are defined there as if they run above the IP protocol.

In the following chapters, the requirements for the transport layers TCP and UDP for TRDP communication are defined as ruled by the IEC 61375-2-3 [18].

3.4.1 TCP/UDP

UDP protocol shall be used for process data transmission, where packet size shall be restricted to the size of the Ethernet frame (MTU) [18].

For message data communication instead, TCP or UDP could be used, where packets exceeding the maximum Ethernet frame size can be transmitted by TCP in order to avoid problems with packet fragmentation [18].

¹³ As CS have to support IGMP querier function IGMP snooping is then implicitly available.

3.4.2 UDP/TCP port assignment (Well-known or dedicated ports)

IEC 61375-2-3 Annex A [18] defines dedicated destination ports for process data and message data transmission to ensure an interoperable data communication. These well-known port numbers should be given as configuration parameters for the communication stack.

Protocol	Destination Port
Process Data (UDP)	17224
Message Data (UDP)	17225
Message Data (TCP)	17225

Figure 72: Dedicated destination ports for UDP/TCP [18]

The standard defines some requirements as well for the source and receiving ports definition.

3.4.3 Security aspects

The current standard considers TCN as a system of category 1 (preferably) or category 2 according to IEC 62280 and no security protocols are defined.

In the safety analysis for the NG-TCN carried out in the Task 3.3 [05], the system has been assumed as a closed system as well, and the required security mechanisms for possible future open systems (if wireless transmission is considered) have not been analysed. Nevertheless, the security analysis conducted in the same task will imply to define some security countermeasures according to the standard IEC 62443-3-3 which should be considered in the specification of the Safety Layer SDTv4.

Concerning the security mechanisms in the transport layer, a possible protocol above the Layer 4 is the Transport Layer Security (TLS) protocol, which secures communication typically for client server applications. However, this protocol runs above TCP hence it would not be feasible for process data communication [10]. Thus, in the transport layer specification, no specific security mechanisms are proposed.

3.5 APPLICATION LAYER

3.5.1 URI addressing

On application level, all the details of the communication network infrastructure shall be hidden. The communication network is seen as a cloud, which provides services to transport data from A to B. This is also valid for the addressing, as application just wants to speak to their partner applications somewhere attached to the network on the base of application level addresses. Those addresses can identify a specific ED which is the location of the partner application, or they can identify in a more abstract way just a “function”, without needing to know where this function is located in the network. A typical example is to address the driver’s display in the leading cab: here the sending application doesn’t need to know where the leading cab and where the driver’s display is located.

This basically means to abstract from the physical network addresses of a network (e.g. MAC and IP addresses), and use some “speaking names” for addressing instead. In the context of NG-TCN this way of addressing is called functional addressing because the intention is to address certain functions in the own or a remote consist without the need to know the physical network address of

the ED which implement these functions. If a function is moved to another ED, e.g. following a redundancy switch-over, or after a train inauguration, the application needs in most cases not to deal with it. The functional addressing scheme used for NG-TCN is defined in IEC61375-2-3.

NG-TCN functional addressing is designed to support real-time data exchange (TRDP-PD and TRDP-MD between TCMS applications. The functional addressing is defined by an URI scheme (Universal Resource Identifier, RFC 3986), which became a standard way of resource location in the Internet community. A resource means in the context of NG-TCN a specific application or system SW component implementing a particular function.

The URI scheme which is defined for the functional addressing in NG-TCN is called the “TCN Uniform Resource Identifier, in short “TCN-URI”.

In a very abstract way, the TCN-URI can be defined as “user@host”, where “user” identifies the communicating functions and “host” the location of that function in the network (network interface address of the device implementing the function). The communication middleware has to “translate” the TCN-URIs “host” to the physical IP address for sending. This translation might be dynamic due to the dynamic nature of NG-TCN. The communication middleware also has to interpret the “user” part, because it identifies the application component which is sourcing or sinking the data.

More specifically, the TCN-URI is defined as shown in Figure 73.



Figure 73: TCN-URI functional addressing scheme (IEC61375-2-3)

The host part of the URI identifies the device that hosts the function. This part is then translated to an IP address. The (optional) user part identifies the function located on that device.

The individual elements of the scheme are as follows (Table 30):

Table 30: TCN-URI elements

URI Element	Definition
trn	Each URI begins with a scheme name that refers to a specification for assigning identifiers within that scheme. As such, the URI syntax is an extensible naming system wherein each scheme's specification may further restrict the syntax and semantics of identifiers using that scheme. The scheme defined for NG-TCN is named “tcn”. The scheme can be omitted when the context of its usage is clearly defined.
:	delimiter of the scheme. Shall be omitted when “tcn” is omitted
//	double slash precedes the authority component as defined in RFC 3986. Shall be omitted when “tcn” is omitted
usr	predefined application/system function (implemented by an application/system SW component).
@	delimiter between user and host part. If function is not written, e.g. when only a range of hosts shall be notated, the delimiter must be omitted.
fctdev	identifies the ED which implements the function.
.	delimiter between device and vehicle. If vehicle is empty, also the delimiter must be omitted.

URI Element	Definition
vehicle	identifies the vehicle where the ED is located.
.	delimiter between car and consist. If consist is empty, also the delimiter must be omitted.
consist	identifies the consist where the ED is located.
.	delimiter between consist and train. If train is empty, also the delimiter must be omitted.
cltrain	identifies the closed train where the ED is located.
.	delimiter between cltrain and train.
train	identifies the entry point to the train where the ED is located.

EXAMPLE The following TCN-URI identifies the driver's display in the leading vehicle:

drvDisplay@hmi.leadVeh.leadCst.anyClTrn.1Trn

A comprehensive specification and the usage description of the TCN-URI schema can be found in IEC 61375-2-3 [18].

3.5.2 Real-time data communication (TSN, TRDP)

Data communication between consists over ETB must be standardized to guarantee interoperability between consists of different manufacturers. This comprises all type data traffic, be it control data, audio or video. For TCMS related data communication, IEC defined a specific protocol (TRDP) which is much related to the RTP protocol already used for legacy WTB and MVB (RTP is specified in IEC61375-2-1).

TRDP (Train Realtime Data Protocol) is an end-to-end application layer protocol standardized in IEC61375-2-3. A TRDP stack implementation has been done as an open source project ("TCNOpen") and is downloadable under '<https://sourceforge.net/projects/tcnopen>'.

TRDP supports 2 data classes, Process Data (PD) and Message Data (MD). SAFE4RAIL made the proposal in [35] to define a third data class for scheduled traffic (TSN-PD). With this proposal, TRDP could be extended (TRDPv2) as it is shown in Table 31:

Table 31: TRDPv2 Data Classes

Data Class	Definition
Process Data (PD)	<p>PD-PDUs are cyclically transmitted between a publisher and one or many subscribers using a connectionless and unconfirmed transport layer service (UDP).</p> <p>Communication patterns:</p> <ul style="list-style-type: none"> - Push - Pull (request of data out of interval)
Message Data (MD)	<p>MD-PDUs are transmitted on demand following the server/client model with one or multiple clients using connectionless (UDP) or connection oriented (TCP) transport layer services.</p> <p>Communication patterns:</p> <ul style="list-style-type: none"> - Notify - Request / Reply - Request / Reply / Confirm

Data Class	Definition
TSN Process Data (TSN-PD)	<p>TSN-PD-PDUs are cyclically transmitted between a publisher and one or many subscribers using a link layer service for scheduled traffic (IEEE 802.1Qbv).</p> <p>Communication patterns:</p> <ul style="list-style-type: none"> - Push

The proposal also foresees to reduce the TRDP header information for TSN-PD-PDUs. The structure of the TSN-PD-PDU is shown in Figure 74.

TSN-PD is an OSI Layer 2 protocol which does not require IP and UDP header. But not using IP header would require a specific EtherType value, which is unfavorable¹⁴.

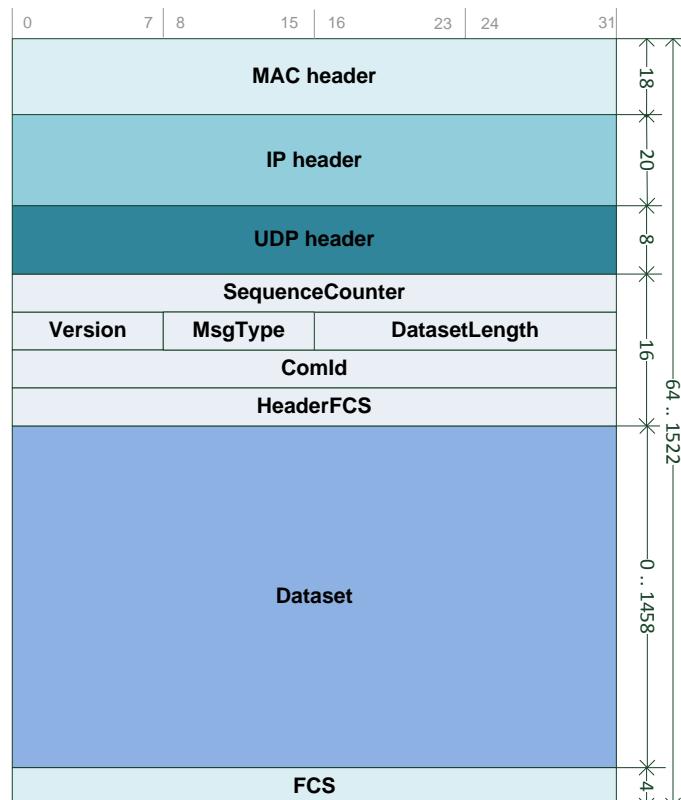


Figure 74: TSN-PD-PDU

Table 32: TSN-PD-PDU

Parameter	Description	Value
MAC header	Ethernet frame header	As defined in IEEE 802.3
IP header	IP telegram header as defined in IETF RFC 791 (IPv4)	
UDP header	UDP telegram header as defined in IETF RFC 768	

¹⁴ However, EtherType value “894C” could be used which is reserved for IP-TCN, see IEC61375-2-5.

Parameter	Description	Value
SequenceCounter	The sequence counter <ul style="list-style-type: none"> • Shall be incremented with each sending of the telegram (return to 0 on overflow) • Initial value: 0 	computed
Version	Protocol version	2
MsgType	Message type.	1: for standard PD (dataset ComId defined) 2: optional for ETB consist-indexed datasets (32 channels)
DatasetLength	Length of the user dataset in number of octets without padding bytes	0 ... 1458
ComId	Identifier of the user dataset	As defined in [18]
HeaderFCS	The header frame check sequence. <ul style="list-style-type: none"> • Shall be calculated for the TSN-PD-PDU header • Shall not include the HeaderFCS itself 	As defined in [18]
Dataset	User data. If the user data is not a multiple of 4 octets, octets with a value of 0 shall be appended until a multiple of 4 octets is reached (padding bytes).	Application specific
FCS	Ethernet frame check sequence, see 3.2.1.	computed

3.5.3 SIL4 Safe Data Transmission protocol (SDTv4)

The focus of this chapter is a description of the integration of the Safety Layer (SDTv4) into the proposed NG-TCN architecture, based on the “black-channel” approach and the failsafe-principle. Regarding the SDTv2 described in Annex B of IEC61375-2-3 and analyzed within D3.3 the SDTv4-Protocol must be extended and improved concerning the weaknesses identified to provide safe data transmission up to 1% of the THR of SIL4. The SDTv4 design should allow an easy integration into the NG-TCN architecture. To do this several changes and extensions have to be done.

General

SDTv2 Properties and weaknesses (taken from [05])

The design of a new safety layer considers the specification of SDTv2 but also addresses the main weaknesses of this protocol:

- THR is only proven up to SIL2
- No provision for security => depending on the network categorization (open or closed transmission system) in general and independent from the safety point of view. When NG-TCN or domains of NG-TCN is regarded as an open transmission system, additional measurements are necessary (recommendations could be found IEC 61784-3-3 chapter 9.8.3 Security measures [21]).
- Latency monitoring allows detecting slopes of latency time (t_L) increase or decrease, but not an already existing latency at the beginning of a measurement interval.

- Channel monitoring defined for SIL2
- Large packet size, increasing the probability of undetected bit errors
- The source has no information, that the message was received by the sink

NOTE: however, this is only necessary if the source also requires this information (for example, a control command on the sender side "Door open" expects a status : "Door open"). However, if safe input signals are sent to a processing unit, it is usually not necessary for the input module to know whether the receiver has also received the data, since the input module cannot derive a safe reaction in the event of an erroneous transmission; this is usually always done by the receiver.

Safe application and safe communication embedded in ISO/OSI-Reference

The embedding of the safe application and the safety layer (SDTv4) takes place in or above the upper layers of the ISO/OSI-Reference model as shown in figure 1 below, depending on the presence of layers in the communication architecture. This model guarantees the black channel approach through all layers of the ISO/OSI model in a manner, that integrated communication functions and services within ED-S or the use of external communication devices need not be considered in the certification process. Figure 75 shows a general representation of the embedding of the Safety Layer and the Safe Application on top of the Safety Layer independent of the subordinate communication layers.

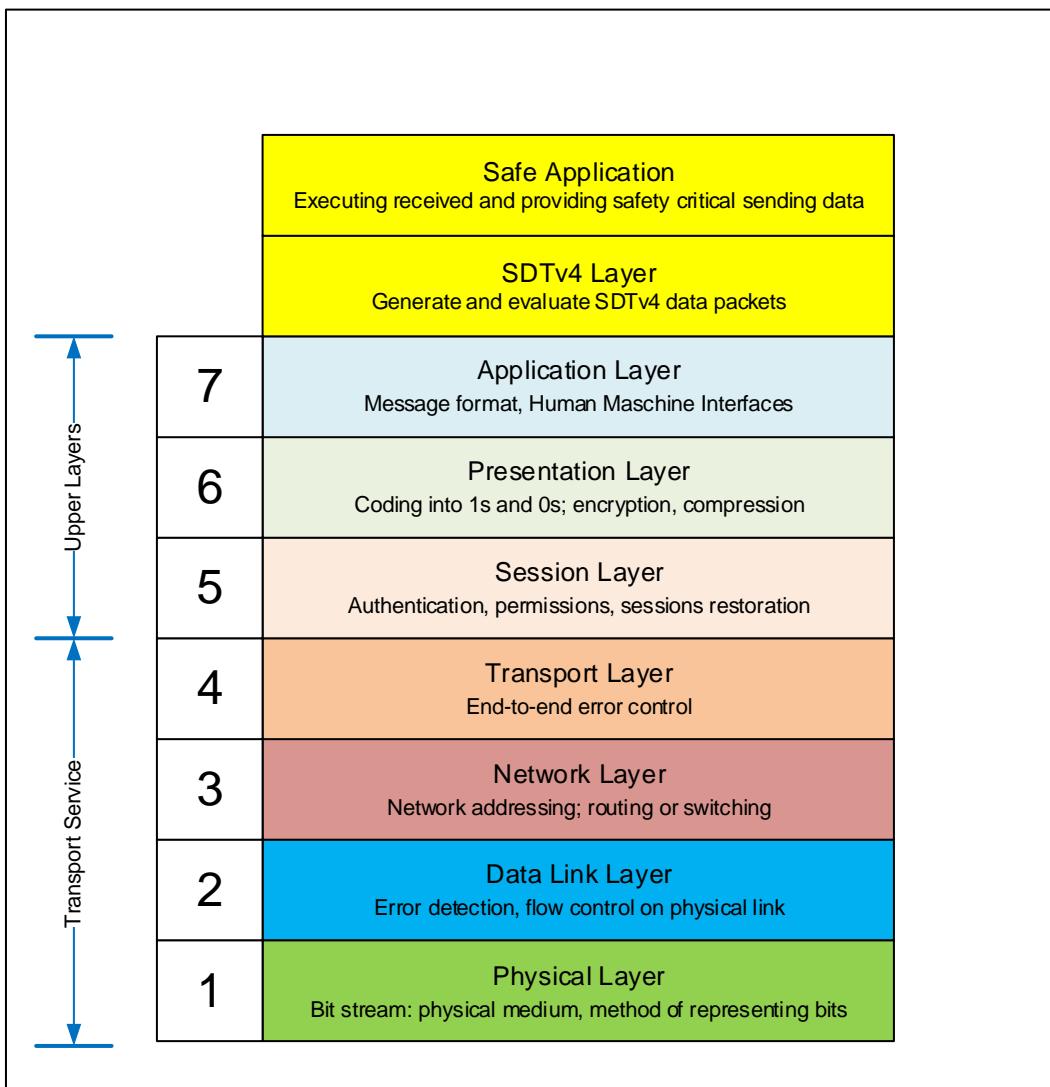


Figure 75: Safe application and safe communication embedded in ISO/OSI-Reference

Communication model when SDTv4 uses TRDP:

The communication model taken from Annex A (Train Real-Time Data Protocol (TRDP)) of IEC61375-2-3 should still be valid, especially for embedding the safety layer in the upper layers (5..7) or above Layer7 within NG-TCN. This type of integration of the SDTv4 should generally be used when safe **inter-consist** communication via ETB is required. TRDP could also be used within the ECN communication although it is not mandatory.

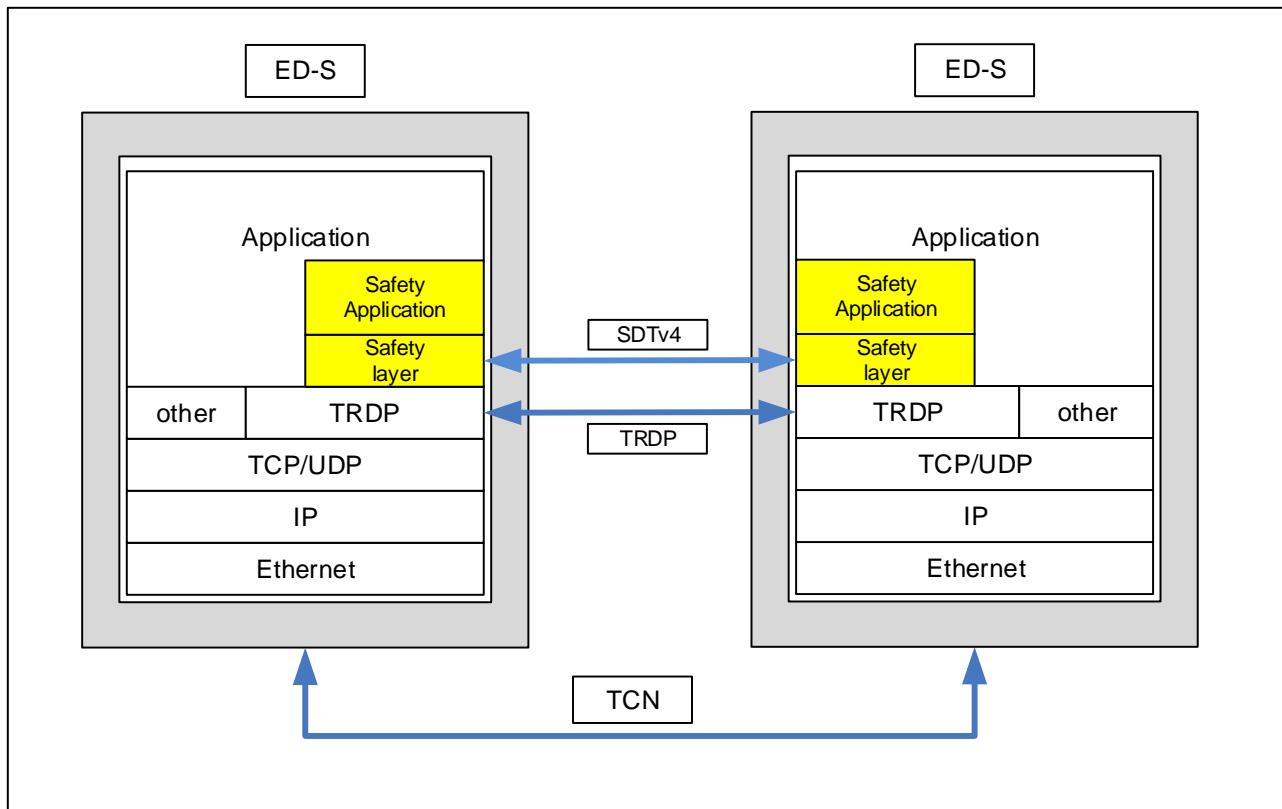


Figure 76: Communication model SDTv4 used TRDP

Nevertheless, the use of SDTv4 should not necessarily require the use of a subordinate TRDP protocol. In this case the following minimum requirements for the real-time protocol and address assignment must be met in order to demonstrate the safety requirements:

- Deterministic scheduling for sending and receiving data must be possible and configurable
- Unique addressing options for the safe end devices (ED-S) must be guaranteed.
- In the case of automatic address assignment of the ED-S, it must be possible to check the plausibility of the assigned address via a second independent path, or the address assignment itself has to be safety relevant up to SIL4.
- The time scheduling for the safe application as well as for the real time communication must be configurable in order to guarantee the calculation of the worst-case delay time of the safety related data end-to-end within the safety application of sender to the safe application of the receiver.

Communication model when SDTv4 uses other RT-Protocols:

As described before the use of SDTv4 should not require the use of TRDP. The design of SDTv4 should therefore be basically independent of TRDP, which means that both the communication and addressing parameters should be chosen generically. This type of integration of the SDTv4 could be used when safe intra-consist communication is required.

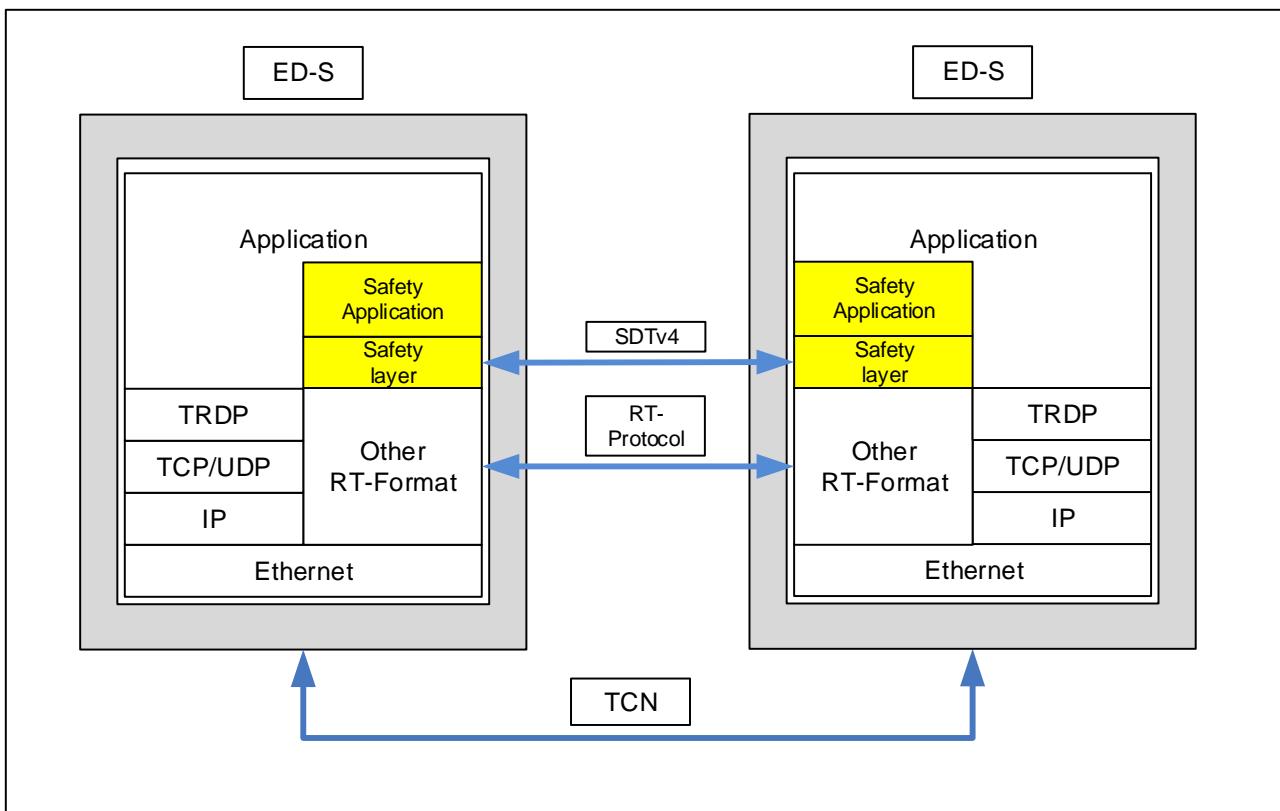


Figure 77: Communication model SDTv4 used other RT-Format

Figure 77 shows the communication model when SDTv4 uses other underlying RT-Protocol Formats. In this case it is possible that the ISO/OSI model is transparent between the layers 3 (Network Layer) and Layer 6 (Presentation Layer), depending on the used RT-protocol.

Source-Sink Communication Model

In the same manner as the SDTv2 protocol, the SDTv4 uses the source sink model as described in AnnexB of IEC61375-2-3. SDTv4 provides a safe communication path between a source of safety related (vital) data (SDSRC) and one or several sinks of those data (SDSINK). This safe communication path is called "SDTv4 channel". Figure 78 provides a logical model of such a SDTv4 channel. The SDTv4 channel starts and ends at safe applications and covers the entire path along from the SDSRC application to the SDSINK application(s). This includes the train communication network (NG-TCN) as well as the communication layers related to the NG-TCN which reside on the safe end devices (ED-S) hosting the safe application, and which both are considered not trustable from a safety point of view (=> "Black Channel" approach). A safe end device may contain one or a number of SDSRC or SDSINK, respectively. SDSRC and SDSINK itself can be described as a composition of the safe application and the SDTv4 protocol layer. The SDTv4 protocol layer provides two interfaces:

1. the communication channel interface
2. the SDTv4 application interface

The communication channel interface is defined by the communication technology underneath TRDP when TRDP is used or to another RT-Protocol type. This is the interface where SDTv4 protocol data units, called VDPs (= Vital Data Packets) are sent to or received from the NG-TCN.

The SDTv4 application interface, which is product specific, is the place where safety related process data are put to or get from the application. The SDTv4 Layer at SDSRC side has mainly the task to add protocol information, in such a way forming a VDP, which is necessary for a safe transfer of those data over the network, prior to sending. On receiver side, the SDTv4 layer validates received VDPs, and if validation is successful, contained vital data are exposed in the SDTv4 application interface.

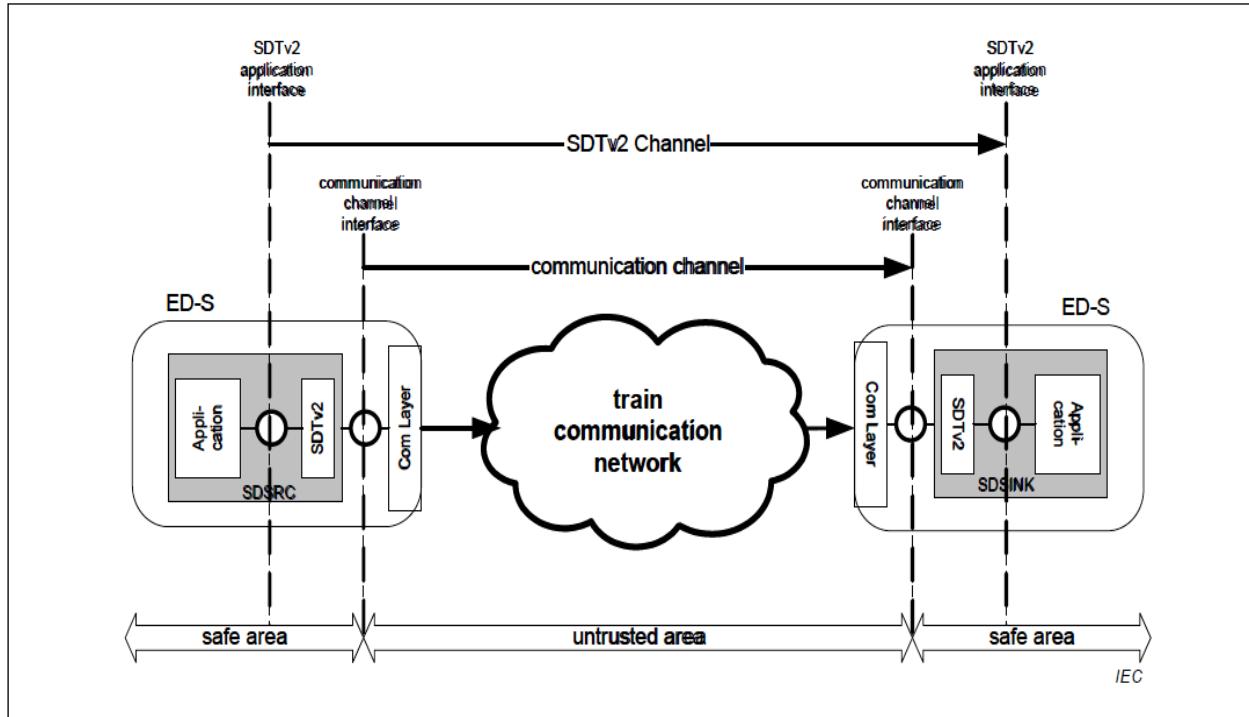


Figure 78: SDTv2 Channel valid for SDTv4

Safety functional requirements for SDTv4

The following requirements taken from IEC61375-2-3 Annex B have been partially adopted and modified in the necessary points which are mandatory for the development of the SDTv4 protocol:

- Safe communication and standard (regular) communication shall be independent. However, standard devices and safety devices shall be able to use the same communication channel.
- Safe communication shall be suitable for Safety Integrity Level SIL4 for continuous mode of operation (see IEC 61508-1).
- Safe communication shall use a single-channel communication system. Redundancy may only be used optionally for increased availability.
- Implementation of the safe transmission protocol shall be restricted to the communication end devices.
- Due to the dynamic nature of train compositions with a varying number of consists, a 1: n communication relationship between the safe data source and safe data sinks has to be supported.
- The transmission duration times shall be monitored.

- g) Environmental conditions shall be according to general railway requirements, mainly IEC 60571, if there are no particular product standards.
- h) Transmission equipment such as controllers, ASICs, Ethernet switch cores, cables, couplers, etc., shall remain unmodified (black channel). The safety functions shall be above OSI layer 7
- i) The safe communication shall not reduce the permitted number of devices.
- j) The safe communication shall support data exchange over the ETB in dynamically changing train compositions.

Safety measures

The safety measures mentioned in Table 1 for mastering possible transmission errors are one significant component of the SDTv4. The safety measures shall be processed and monitored within one safety unit.

Table 33: Deployed measures to Communication errors

Communication error	Safety measure					
	Safe Sequence Counter	Sink-time Supervision	Safety Code	Guard time	Source Identifier (SID)	Latency Monitoring
Corruption			X			
Unintended repetition	X					
Incorrect sequence	X					
Loss		X				
Unacceptable delay		X				X
Insertion	X				X	
Masquerade	X				X	
Addressing					X	
Revolving memory failures within switches	X					
Redundancy failure (active redundant sources)	X			X		

Operational states of the SDTv4 channel

A SDTv4 channel can be basically in two basic operational states (see Figure 79):

- State RegularCommunication: In this state, transmitted vital process data cannot be considered to be safe.
- State SafeCommunication: In this state, transmitted vital process data can be considered to be safe

The conditions under which state changes occur are specified in the following subclauses.

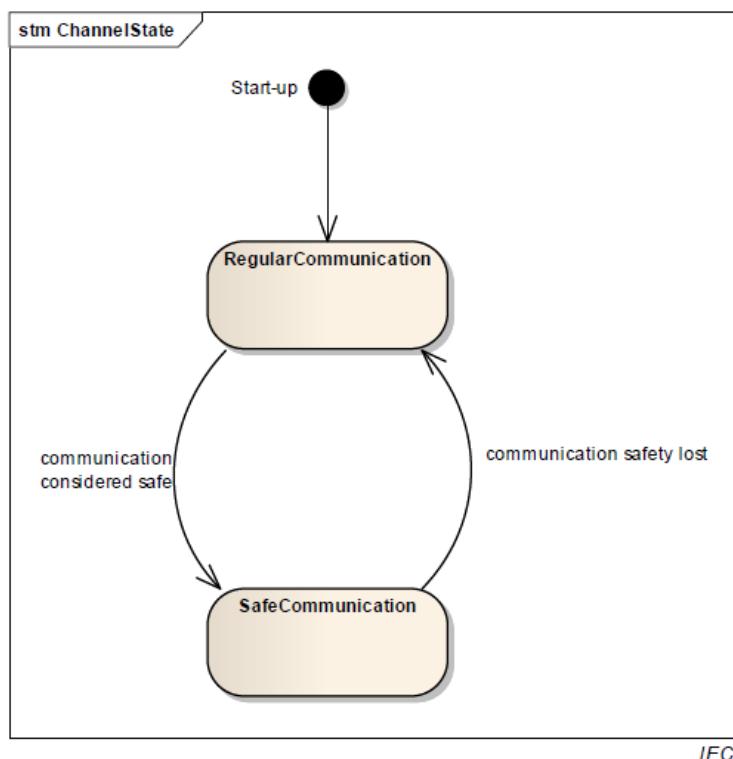


Figure 79: SDTv4 Channel States

Data presentation

All data within SDTv4 shall be transmitted in big-endian format (most significant octet of a data item first). All data structures used within SDTv4 shall be naturally aligned (data items stored at offset address which is a multiple of their size).

Variable length data structures (open arrays, records) shall not be used.

The VDP data elements of a structured type (record, sequence) shall be arranged in the order they are declared.

SID

All SDTv4 channels shall be identified by a unique Source Identifier (SID). The SID shall be an UNSIGNED32 value which is computed as a SC-32 signature (details in SID-Computation chapter below) of the following data structure. The initial (seed) value shall be 'FFFFFFFF'H.

```

SID_STRUCT ::= RECORD
{
  SDT4ProtVers      UINT16          -- version of the SDTv4 protocol, specify SID
                                     structure
                                     shall be set to '0001'H for first version.
  SDT4ProtVar       UINT16          -- variant of the SDTv4 protocol.
                                     '0001'H = small frames (8 Byte)
                                     '0002'H = large frames (max net data
                                     payload)
  SafeFuncID *      UINT16          -- Identifier used for FOC
                                     '0000'H = if no standardized safe
                                     functionality is used or for intra-consist
                                     communication
  SafeFuncVers *    UINT16          -- Version of safeFuncID used for FOC
                                     '0000'H = if no standardized safe
                                     functionality is used or for intra-consist
                                     communication
  SafeChannelID *   UINT16          -- Identifier for one unique safe channel of
                                     one SafeFuncID to ensure uniqueness if
                                     several channels of one function are
                                     required.
                                     '0000'H = if no standardized safe
                                     functionality is used or for intra-consist
                                     communication
  SafeChannelVers * UINT16          -- Version of SafeChannelID used for FOC
  SMI               UINT32          -- user defined Source Message Identifier.
                                     Shall be used if the uniqueness of a SDTv4
                                     channel is not indicated
                                     by combination of SafeFuncID and
                                     SafeChannelID
                                     and their versions and also for redundant
                                     SDSRC
                                     value: 1 ..'FFFFFFF'H (0 = reserved)
  reserved01        UINT16          -- reserved, shall be set to 0.
  reserved02        UINT16          -- reserved, shall be set to 0.
  cstUUID           ARRAY[16] OF UINT8
                                     -- unique consist identifier
  SafeTopoCount     UINT32          -- safe topography counter (STC), unique
                                     identification of the actual train
                                     composition. Provided by the
                                     communication subsystem. To be set
                                     to 0 for consist network internal
                                     communication
  reserved03        UINT32          -- reserved, shall be set to 0.
  reserved04        UINT32          -- reserved, shall be set to 0.
}

```

* Compared to SDTv2, the parameters should be more granularly selectable within SDTv4

SID Computation

The SafeTopoCount value shall equal the opTrnTopoCnt value as specified in IEC61375-2-3 chapter: 5.3.3.2.13 for train wide communication over ETB unless otherwise specified. SMI values from 1 until 999 shall be reserved for generic VDPs which are specified within the part of Annex B of IEC61375-2-3, describing the SMI of SDTv2.

SDSRCs and SDSINKs can compute the SIDs of expected VDPs with information retrieved from the TTDB. The parameters:

- SDT4ProtVers,
- SDT4ProtVar,
- SafeFuncID,
- SafeFuncVers,
- SafeChannelID,
- SafeChannelVers,
- SMI

need to be preconfigured.

SDSINKs expecting VDPs from a redundant SDSRC have to compute two SIDs because the SMIs must be different.

The computation has to be executed by using the CRC-Code: SC-32. The polynomial to be used is '1F4ACFB13' as defined in IEC 61784-3-3. The algorithm in C programming language notation depicted in Figure 80 (and defined in IEC 61784-3-3) for SC-32 computation should be used, see also Figure 81.

```
/*
 *  GLOBAL FUNCTION DEFINITIONS
 */

/**
 * @internal
 * Calculates and returns a 32-bit CRC.
 *
 * @param buf    Input buffer
 * @param len    Length of input buffer
 * @param crc    Initial (seed) value for the CRC calculation
 *
 * @return Calculated CRC value
 */
static UNSIGNED32 sdt_crc32(const UNSIGNED8 buf[], UNSIGNED32 len, UNSIGNED32 crc)
{
    UNSIGNED32 i;

    for (i = 0; i < len; i++)
    {
        crc = crctab32[((UNSIGNED32)(crc >> 24)^buf[i])&0xff]^((crc << 8));
    }

    return crc;
}
```

Figure 80: SC-32 Computation

CRC lookup table (0...255)							
00000000	F4ACFB13	1DF50D35	E959F626	3BEA1A6A	CF46E179	261F175F	D2B3EC4C
77D434D4	8378CFC7	6A2139E1	9E8DC2F2	4C3E2EBE	B892D5AD	51CB238B	A567D898
EFA869A8	1B0492BB	F25D649D	06F19F8E	D44273C2	20EE88D1	C9B77EF7	3D1B85E4
987C5D7C	6CD0A66F	85895049	7125AB5A	A3964716	573ABC05	BE634A23	4ACFB130
2BFC2843	DF50D350	36092576	C2A5DE65	10163229	E4BAC93A	0DE33F1C	F94FC40F
5C281C97	A884E784	41DD11A2	B571EAB1	67C206FD	936EFDEE	7A370BC8	8E9BF0DB
C45441EB	30F8BAF8	D9A14CDE	2D0DB7CD	FFBE5B81	0B12A092	E24B56B4	16E7ADA7
B380753F	472C8E2C	AE75780A	5AD98319	886A6F55	7CC69446	959F6260	61339973
57F85086	A354AB95	4A0D5DB3	BEA1A6A0	6C124AEC	98BEB1FF	71E747D9	854BBCCA
202C6452	D4809F41	3DD96967	C9759274	1BC67E38	EF6A852B	0633730D	F29F881E
B850392E	4CFCC23D	A5A5341B	5109CF08	83BA2344	7716D857	9E4F2E71	6AE3D562
CF840DFA	3B28F6E9	D27100CF	26DDFBDC	F46E1790	00C2EC83	E99B1AA5	1D37E1B6
7C0478C5	88A883D6	61F175F0	955D8EE3	47EE62AF	B34299BC	5A1B6F9A	AEB79489
0BD04C11	FF7CB702	16254124	E289BA37	303A567B	C496AD68	2DCF5B4E	D963A05D
93AC116D	6700EA7E	8E591C58	7AF5E74B	A8460B07	5CEAF014	B5B30632	411FFD21
E47825B9	10D4DEAA	F98D288C	0D21D39F	DF923FD3	2B3EC4C0	C26732E6	36CBC9F5
AFF0A10C	5B5C5A1F	B205AC39	46A9572A	941ABB66	60B64075	89EFB653	7D434D40
D82495D8	2C886ECB	C5D198ED	317D63FE	E3CE8FB2	176274A1	FE3B8287	0A977994
4058C8A4	B4F433B7	5DADC591	A9013E82	7BB2D2CE	8F1E29DD	6647DFFB	92EB24E8
378CFC70	C3200763	2A79F145	DED50A56	0C66E61A	F8CA1D09	1193EB2F	E53F103C
840C894F	70A0725C	99F9847A	6D557F69	BFE69325	4B4A6836	A2139E10	56BF6503
F3D8BD9B	07744688	EE2DB0AE	1A814BBD	C832A7F1	3C9E5CE2	D5C7AAC4	216B51D7
6BA4E0E7	9F081BF4	7651EDD2	82FD16C1	504EFA8D	A4E2019E	4DBBF7B8	B9170CAB
1C70D433	E8DC2F20	0185D906	F5292215	279ACE59	D336354A	3A6FC36C	CEC3387F
F808F18A	0CA40A99	E5FDFFCB	115107AC	C3E2EBE0	374E10F3	DE17E6D5	2ABB1DC6
8FDCC55E	7B703E4D	9229C86B	66853378	B436DF34	409A2427	A9C3D201	5D6F2912
17A09822	E30C6331	0A559517	FEF96E04	2C4A8248	D8E6795B	31BF8F7D	C513746E
6074ACF6	94D857E5	7D81A1C3	892D5AD0	5B9EB69C	AF324D8F	466BBBA9	B2C740BA
D3F4D9C9	275822DA	CE01D4FC	3AAD2FEF	E81EC3A3	1CB238B0	F5EBCE96	01473585
A420ED1D	508C160E	B9D5E028	4D791B3B	9FCACF777	6B660C64	823FFA42	76930151
3C5CB061	C8F04B72	21A9BD54	D5054647	07B6AA0B	F31A5118	1A43A73E	EEE5C2D
4B8884B5	BF247FA6	567D8980	A2D17293	70629EDF	84CE65CC	6D9793EA	993B68F9

NOTE This table contains 32 bit values in hexadecimal representation for each value (0...255) of the argument a in the function crctab32 [a]. The table should be used in ascending order from top left (0) to bottom right (255).

Figure 81: SC-32 Table

SDTv4 VDPs

A SDTv4 safe channel shall encapsulate safety critical data in a vital data packet (VDP). VDPs transferred over ETB (ETB-VDP) are transmitted within the user data part of a TRDP process data telegram. For communication relations within a consist, VDPs could also be transmitted by the use of other RT-Protocol-types.

Two different types of VDPs are possible to configure concerning the analysis done in [05]:

Variant 1: small safety frames with (1..8 Byte) homogenous data (see Figure 82)

Variant 2: large safety frames with (1..1500* Byte) homogenous data (see Figure 83)

Important note: * depending on PDU-Type: For TRDP the maximum is restricted up to 1432 Byte

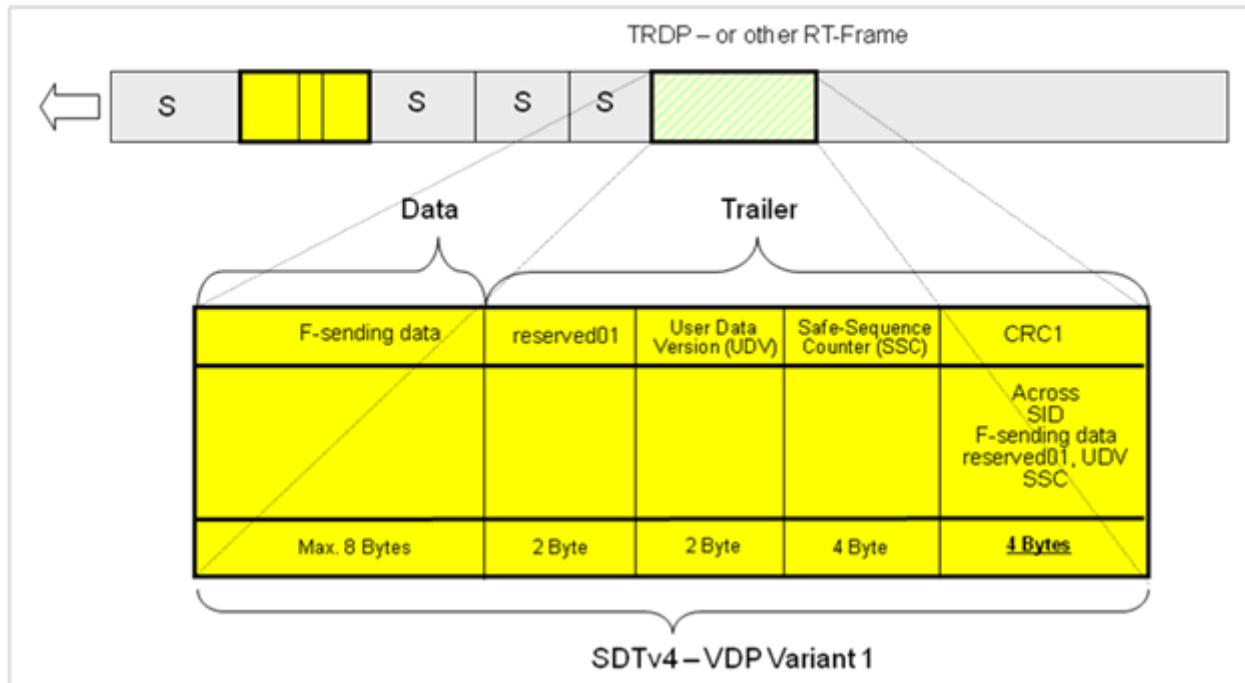


Figure 82: SDTv4 VDP Variant 1

If variant 1 is used this should be indicated via SID-data structure Parameter: "SDT4ProtVar". The value: '0001'H must be chosen for small frames.

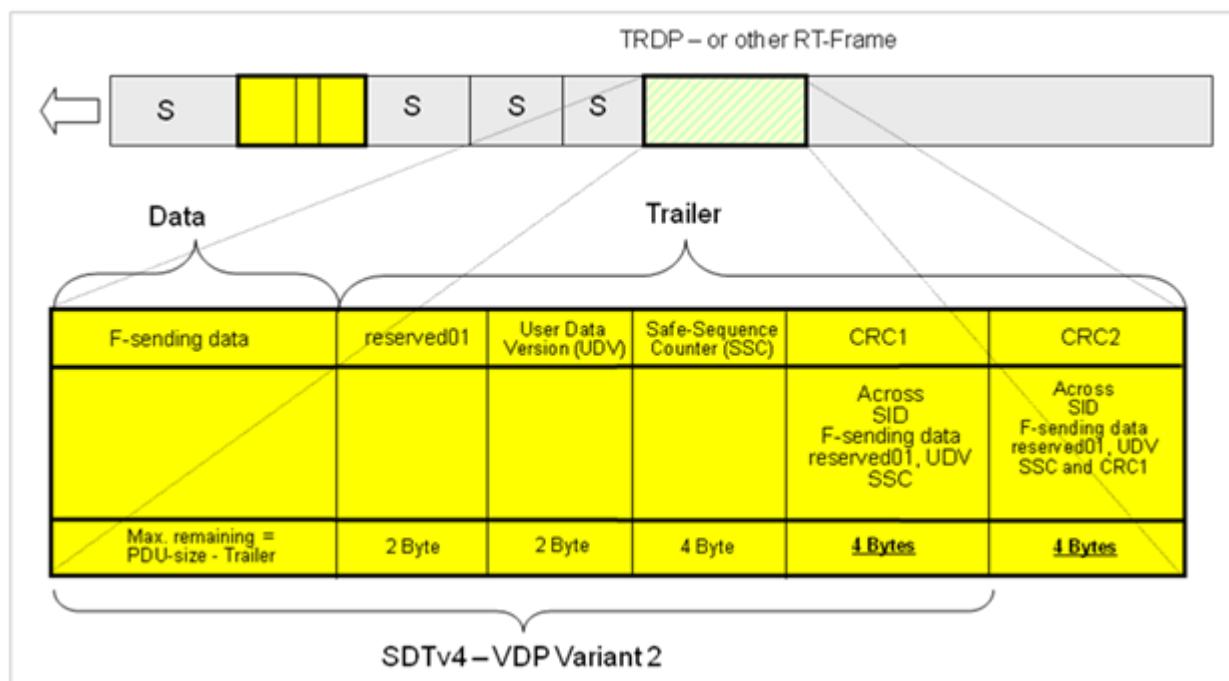


Figure 83: SDTv4 VDP Variant 2

If variant 2 is used this should be indicated via SID-data structure Parameter: “SDT4ProtVar”. The value: '0002'H must be chosen for large frames.

SDTv4 CRC Computation:

Depending on the used variants the CRC computation has to be executed once or twice. The CRC computation for variant 1 of the VDP uses the same polynomial as the computation of the SID. (see: subclause: SID Computation).

For variant 2 of the VDP, a second suitable generator polynomial should be chosen. When choosing the polynomials, care should be taken that at best the polynomials have no common factors. Furthermore, it is advantageous if only one of the two polynomials contains the factor $x+1$. (More information could be found in [05] chapter “Analysis of the Safety Layer”).

Regarding this requirement a good choice for CRC2 Computation could be the polynomial ‘D419CC15’ introduced within the Table1 of [57].

The notation corresponds to a 32-bit notation in [57], but in the IEC61375-2-3 standard the polynomials are represented by a 33-bit notation. To keep the polynomials comparable, the following table shows the respective polynomials in the respective representation:

Table 34: Representation of the used polynomials in 32 and 33Bit notation

Selection of the polynomial for:	32 Bit Notation [57]	33 Bit Notation [18]
CRC 1 Computation:	FA567D89	1F4ACFB13
CRC 2 Computation:	D419CC15	1A833982B

Variant 1 of SDTv4-VDP: CRC computation has to be executed once with result CRC1:

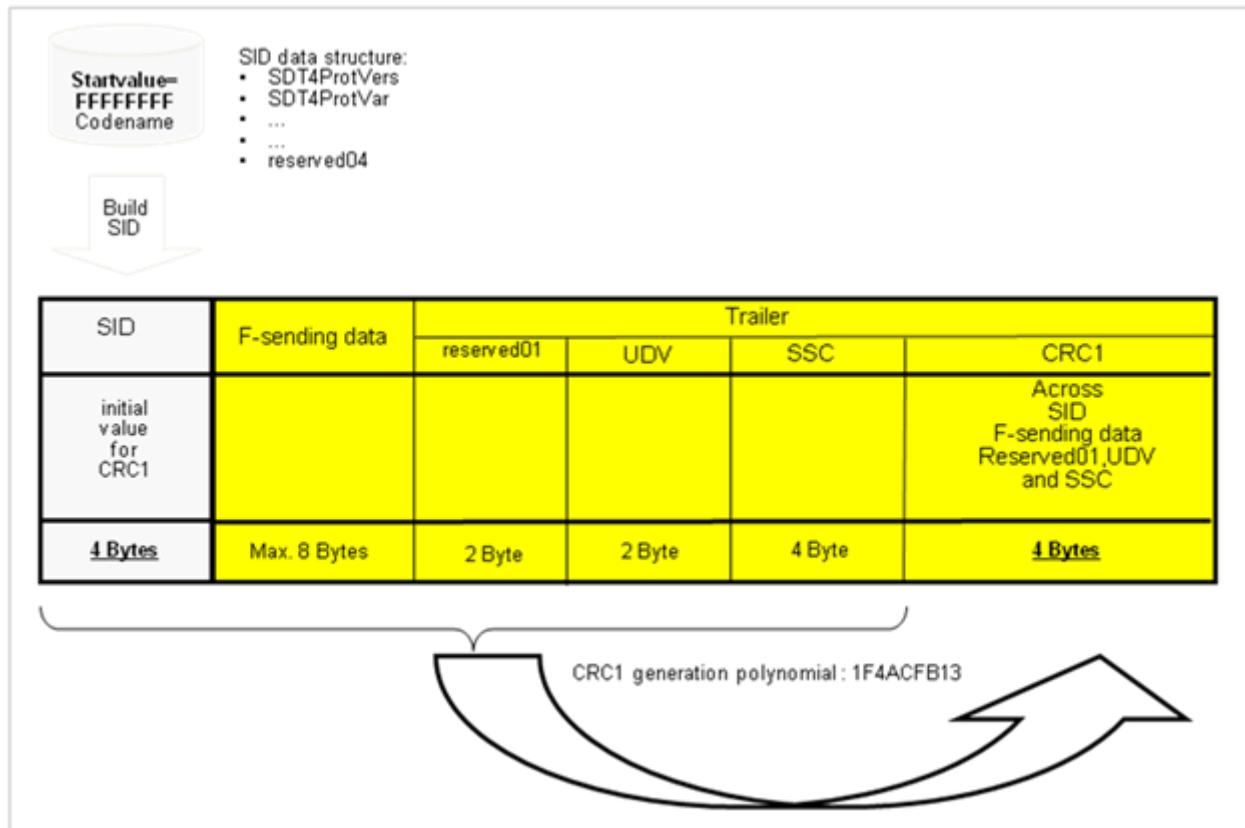


Figure 84: CRC1 Computation for VDP Variant 1

Initial value (seed) for CRC1 computation = SID

CRC-Source-Array=

1. F-sending data (depending on declaration) : 0...8 Byte
2. Trailer
 - 2.1 reserved01 : 2 Byte
 - 2.2 UDV : 2 Byte
 - 2.3 SSC : 4 Byte

Variant 2 of SDTv4-VDP: CRC computation has to be executed twice with result CRC1 and CRC2:

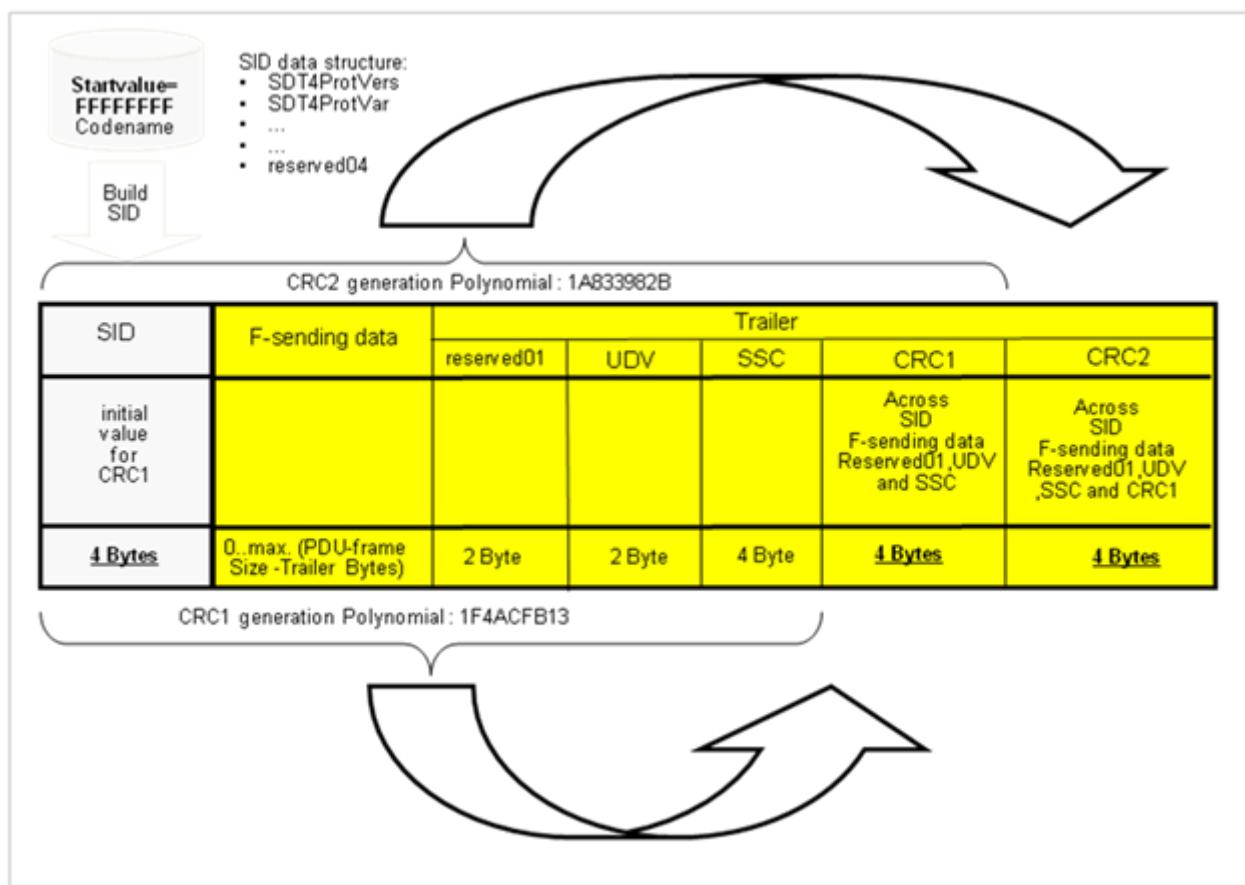


Figure 85: CRC1 and CRC2 Computation for VDP Variant 2

The CRC Computation for CRC1 has to take place as described above “Variant 1 of SDTv4-VDP: CRC computation has to be executed once with result CRC1”. In addition, this variant of VDPs (Variant 2) requires a second CRC (CRC2) to achieve the required THR (1% of SIL4) for the transmission of larger amount of safety relevant data (up to max. TRDP-frame size (1432-Trailer = 1416 Byte), or to max. of other PDU-frames).

CRC1: as described above for variant 1

CRC2: using polynomial (1A833982B)

Initial value (seed) for CRC1 computation = SID

CRC-Source-Array=

1. F-sending data (depending on declaration) : 0..max (PDU-Size – Trailer)Byte
2. Trailer:
 - 2.1 reserved01 : 2 Byte
 - 2.2 UDV : 2 Byte
 - 2.3 SSC : 4 Byte
3. CRC1 : 4 Byte

Configuring the system:

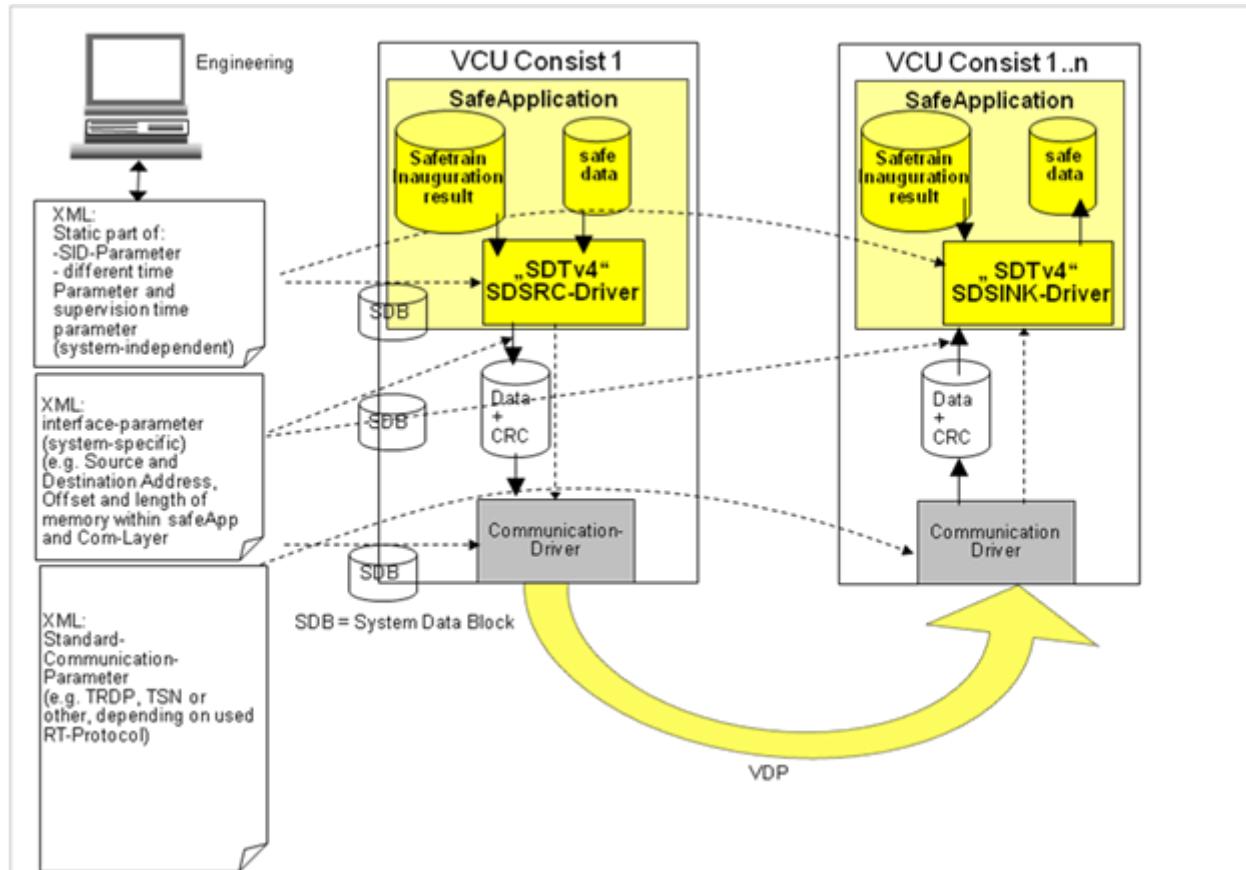


Figure 86: CRC1 and CRC2 Computation for VDP Variant 2

As shown in Figure 86 different safe parameters, communication parameters as well as interface parameters has to be configured during engineering phase. System-independent parameters, e.g. monitoring and sampling times, which the SDSRC and SDSINK require for processing, are described in more detail below.

In order to remain largely compatible with the architecture and description of the SDTv2 protocol when using the terms, they are used in strict compliance with Annex B of the IEC61375-2-3 standard, as long as there are no deviations.

Safe data source (SDSRC)

General

This part defines protocol requirements on safe data sources SDSRC. A safe data source has to produce VDPs, meaning that the VDPs are generated and are subsequently passed to the communication layer for transmission.

Configuration time parameters

SDTv4 requires a set of (configuration) time parameters which are listed underneath. A more detailed specification of those parameters is given in later sections.

T_{tx_period} Time period for sending VDP, as defined for SDSRC

T_{rx_period}	VDP receive (sampling) period, as defined for SDSINK
T_{rx_safe}	Maximal time for which SDSINK tolerates the absence of new (fresh) vital data
T_{guard}	Time used by SDSINK to detect the undesired presence of more than one active SDSRC in case of redundant SDSRC

Safe Data Preparation (Application)

The following requirements define some application conditions. In general, the application is responsible for providing the vital process data to be sent with SDTv4. Two input data classes are distinguished:

- a) **Continuous data.** Those data are characterized by changing their value more or less continuously over time (example: speed signal). Only samples of those data need to be transmitted. After sampling, the sampled data value is kept constant until the next sample (sample and hold principle). The time, during which such a sampled data value is constant, is subsequently called "signal sample duration time" (T_{sig}).
- b) **Discrete data.** Those data are characterized by changing their value on event (example: doors close/open signal). All different values of those data need to be transmitted, because otherwise safety related information might get lost. The minimal time during which the signal value is constant is as well referred to as the "signal sample duration time" (T_{sig}). Contrary to continuous input signals where T_{sig} is exactly one sampling period, can T_{sig} be a multiple of a sample period in the case of discrete signals.

By this, T_{sig} defines the time during which a data value sample is kept constant within the SDTv4 application interface of SDSRC.

In a VDP containing more than one discrete data item which might be typically the case, the signal sample duration time can be different for the individual data items, because it is a property of the source data items itself. The value of T_{sig_min} defines the lowest signal sample duration time occurrence of all the data items within a VDP.

The application shall ensure that all value changes of a discrete input data item (signal) are sampled and that the samples are kept stable in the SDTv4 application interface for a time T_{sig} .

Sampling rate of the application for sampling the input data item needs to be higher than the change rate (frequency) of the input data item.

NOTE T_{sig} can be different for the different input data items.

Safe data sending

Safety related data shall be sent within the VitalProcessData part of Vital Data Packets (VDP).

The producer (SDSRC) of VDP shall produce the VDP periodically with a cycle time of T_{tx_period} .

NOTE 1 T_{tx_period} will be defined by application, e.g. within IEC 61375-2-4, or within application profiles of FOC

The selection of T_{tx_period} shall comply with the following condition:

$$T_{tx_period} \leq T_{sig_min}$$

with T_{sig_min} being the lowest signal sample duration time of a sampled input data item (signal) exposed in the SDTv4 application interface.

NOTE 2 This ensures that all signal values are transmitted even in the case of two subsequent VDP losses during transmission.

VDPs shall not be produced if no valid SID can be computed.

NOTE 3 A valid SID can for instance not be computed if SID input parameters are missing.

VDPs shall not be produced if the end device hosting the SDSRC is not a safety device.

The SDSRC shall increment the SSC for each produced VDP:

$$SSC(i+1) = (SSC(i) + 1) \bmod 2^k$$

with $i = 0 \dots \infty$ and k being the cardinality of the safety sequence counter used (ETB-VDP: $k = 32$).

Redundant SDSRC

This subclause defines specific requirements on redundant safe data sources. The redundancy principle is to have two redundant source devices (SDSRC-A and SDSRC-B) forming one redundancy group. The input signal is read by both source devices, but only one device (redundancy leader) is actively sending to the sink (SDSINK), the other device (redundancy follower) is not sending. Both source devices supervise each other, and if the redundancy follower detects a failure of the redundancy leader it starts actively sending to SDSINK, see Figure 87.

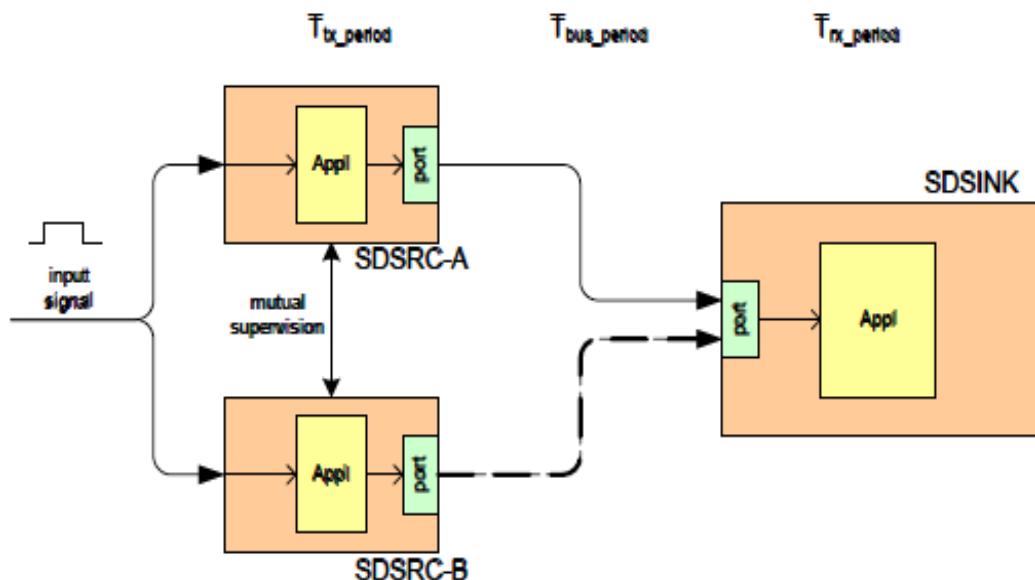


Figure 87: Redundancy Group (Example with 2 SDSRC)

NOTE 1 It is not defined herein how the mutual supervision between a redundancy leader and a redundancy follower, and how the switch-over from a redundancy leader to a redundancy follower is realized. This is an implementation choice.

In a redundant producer group of SDSRC (e.g. hosted by a redundant group of safety devices forming a redundancy group) only one SDSRC shall send VDPs.

All SDSRC of a redundancy group shall use different safety message identifiers (SMI).

The time span T_{red} between the redundancy leader ceasing to send VDPs and the redundancy follower start to send VDPs shall not exceed a value of:

$$T_{red} \leq T_{rx_safe} - 2 \times \max(T_{tx_period}, T_{rx_period})$$

NOTE 2 A violation of this rule may trigger the sink time supervision of SDSINK.

NOTE 3 For the definition of T_{rx_safe} and T_{rx_period} see below.

NOTE 4 T_{rx_period} might be longer than T_{tx_period} in case of undersampling.

It has to be considered that there might be multiple SDSINK connected to SDSRC, in which case the lowest value of T_{red} has to be used.

NOTE 5 By fault both SDSRC may send VDPs. This will be detected by SDSINK with the guard time check (see below).

Safe data sink (SDSINK)

This clause defines specific protocol requirements on safe data sinks. SDSINK has to receive ("sample") VDPs, to validate the VDPs, and to expose received process data in the SDTv4 application interface. "Sampling" of VDPs in this context means that the most recent VDP is read from the communication channel interface. The terms "sampling" and "receiving" are used synonymously.

Definitions – Variables

Variables:

For the subsequent specification, the following set of variables is used:

SSC	this is the non-stored SSC value of the actually sampled VDP
SSC _i	this is the SSC value of the last valid VDP
SSC	received SSC value of the actually sampled correct VDP
SSC _{initial}	SSC value of the initial VDP
SSC _{last}	this is the SSC value of the previously sampled valid VDP
SID _{initial}	SID value of an initial VDP

Definitions – VDP Classification

Duplicate VDP:

A VDP is considered a duplicate if it is identical to the VDP received before, meaning that the computed SafetyCode of that VDP is identical to the computed SafetyCode of the VDP received before.

NOTE 1 For VDPs already validated with correct SafetyCode (CRC1) and/or (CRC1 and CRC2) and correct user data main version, it is sufficient to compare the SSC in order to identify a duplicate: if $SSC = SSC_i$ or $SSC = SSC_{initial}$ then the VDP is a duplicate.

NOTE 2 "Computed" SafetyCode means that the SafetyCode computed by the SDSINK during reception is used, not the SafetyCode value written in the VDP.

Correct VDP:

A received VDP is considered correct, if:

- SafetyCode is correct (computed SafetyCode value is identical to the SafetyCode value contained in the VDP);
- UserDataMainVersion is correct (equals the expected user data version value).

Initial VDP:

A received VDP is considered initial in one of the following cases:

- a) it is not a duplicate;
- b) it is the first correct VDP received after power-up/reset;
- c) it is the first correct VDP received after a communication loss as indicated by the sink time supervision;
- d) it is a correct VDP, but where the SafetyCode evaluation has been done with the alternative SID of the redundant SDSRC (not the stored SIDinitial value of the previously received initial VDP).

NOTE A VDP with a different SID than SIDinitial may for instance be received when a redundancy shift occurs within a SDSRC redundancy group.

Fresh VDP:

A VDP is considered fresh if:

- it is correct;
- the VDP is not the initial VDP;
- the SID of the VDP is identical to SIDinitial;
- it is a real successor to the initial or fresh VDP received before, meaning that

$SSC \in \{(SSC_i + 1) \mid mod(2^k), \dots, (SSC_i + N_{SSC}) \mid mod(2^k)\}$, with $N_{SSC} = (\text{Trx_safe} / \text{T}_{tx_period})$, rounded up to an integer value, and k being the cardinality of the SSC.

Valid VDP:

A received VDP is considered **valid**, if it is a fresh VDP or a duplicate of the fresh VDP received before.

In all other cases it shall be considered invalid.

Discarded VDP:

To **discard** a VDP means to not expose its data to the application.

SDSINK States

The state diagram shown in Figure 88 defines the two possible main states a SDSINK can be in. The related triggers, guards and operations are defined in Table 35, Table 36 and Table 37.

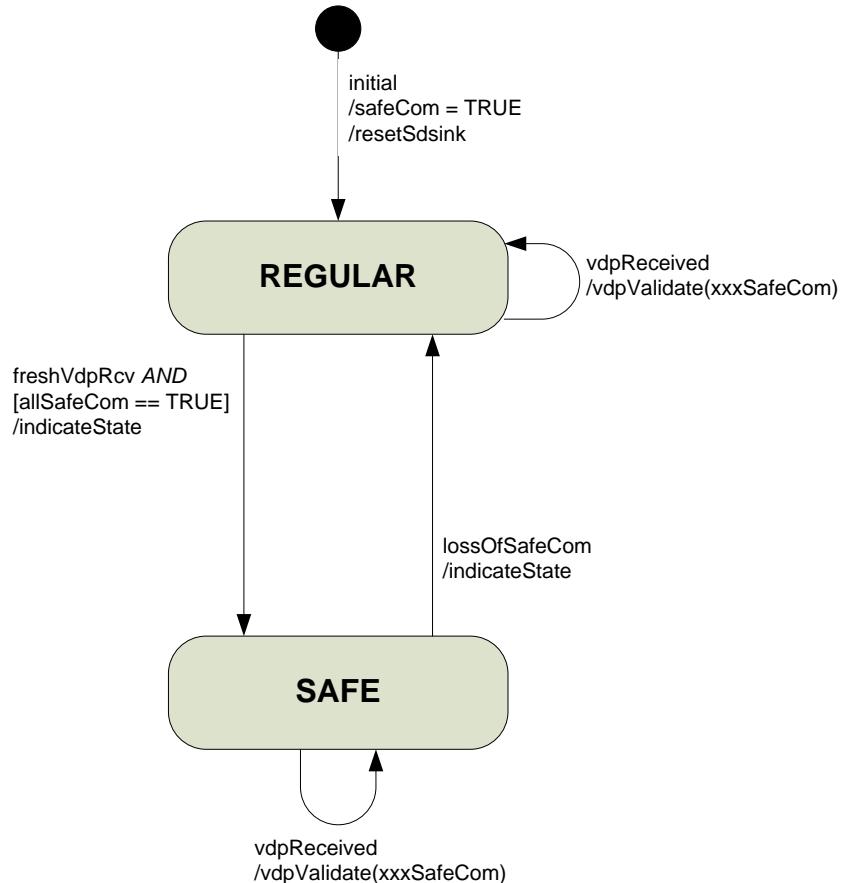


Figure 88: SDSINK state diagram

Table 35: SDSINK state diagram – triggers

Trigger	Description
Initial	Power-up or re-boot of SDSINK
vdpReceived	The most recent VDP is read from the communication channel interface
freshVdpRcv	A fresh VDP has been received
lossOfSafeCom	During VDP validation a loss of safe communication has been detected

Table 36: SDSINK state diagram – guards

Guard	Description
allSafeCom	Logical AND over the check results (variable 'xxxSafeCom', see below)

Table 37: SDSINK state diagram – operations

Operation	Description
vdpValidate	<p>Validation of received VDP, in particular:</p> <ul style="list-style-type: none"> • VDP integrity check • Sink time supervision check • Guard time check (result: gtcSafeCom), <p>The returned check results can have the following values:</p> <p>gtcSafeCom=TRUE: SDTv4 channel communication is considered safe</p> <p>gtcSafeCom=FALSE: SDTv4 channel communication is considered not safe (regular)</p>
resetSdsink	Reset the SDSINK
IndicateState	Indicate a state change to the application

VDP Sampling

A configurable time T_{rx_safe} shall be defined for detecting the loss of safe communication. By default, T_{rx_safe} shall be set in a way that the loss of two subsequently send VDPs is tolerated, e.g.

$$T_{rx_safe} := 3 \times T_{tx_period}.$$

Tolerances in timing should be considered for real implementations (e.g. T_{rx_safe} can be set to $3,5 \times T_{tx_period}$ to compensate tolerances in T_{tx_period} and to respect transmission jitter).

But if T_{rx_safe} is the limiting factor regarding the Safety Function Response Time (SFRT) of a safety loop then it must be checked whether the SDTv4 channel can even be used for this safety function and T_{tx_period} and T_{rx_period} may need to be adjusted.

The default setting of T_{rx_safe} might be changed in the case of under-sampling, see below.

A configurable time T_{rx_period} shall be defined which specifies the cycle in which SDSINK reads (samples) VDPs from the communication channel interface.

NOTE 1 T_{rx_period} defines the time between two samplings of the communication channel interface. The model of a periodic sampling of the communication channel interface is used for the purpose of this specification, but it does not imply a specific implementation. A real implementation can also use an event-driven VDP reception procedure.

The period T_{rx_period} of reading VDPs should be shorter than T_{tx_period} of the SDSRC.

NOTE 2 This is necessary to sample all received VDPs.

Under-sampling, meaning that T_{rx_period} is longer than T_{tx_period} , can be configured. If so, it shall be defined whether information loss is allowed or not.

If the SDSINK can calculate the relation between T_{rx_period} and T_{tx_period} , it is also possible to validate the VDP by calculating the right expectation of the next fresh SSC (see figure below, when $T_{tx_period} = 2 * T_{rx_period}$).

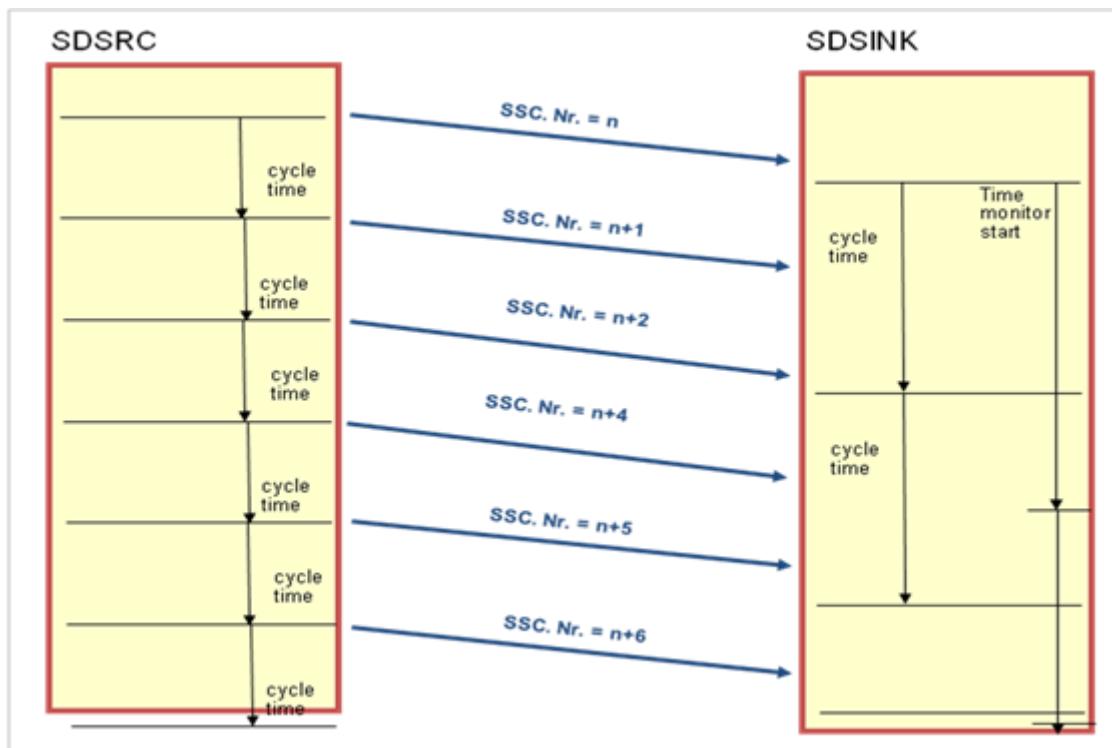


Figure 89: Under-sampling

Under-sampling without information loss might for instance be used if the SDSINK is only interested in specific discrete vital process data items (signals) within the received VDP, which will change their value less frequently as other data items (signals) in the same VDP.

Under-sampling with information loss might for instance be used when continuous signals are sampled (e.g. train speed signal) and a lower granularity is sufficient.

In case of SDSINK undersampling without data loss, the time T_{rx_safe} shall be shorter than the symbol sample duration time of the signal the SDSINK is interested in, but longer than T_{rx_period} .

NOTE 3 If T_{rx_safe} were longer than the symbol sample duration time, a signal change would get lost undetected.

VDP Integrity Check

General

The VDP integrity check aims to filter VDPs which are not correct, meaning that data are corrupted, or the user data main version is not the expected one. Data within those 'invalid' VDPs cannot be used (consumed) by the application.

After a power-up, reset, redundancy shift or a loss of safe communication, the receiver waits for the reception of an "initial" VDP. This initial VDP is used to "synchronize" the SDSINK with the SDSRC. Receiving the initial VDP is however not sufficient to indicate the reception of valid and safe data to the application: this will be done only with the next received fresh VDP, which matches the "window of expected SSC". This window defines a range of allowed SSC values which have to be matched by the VDPs following the initial VDP, in order to ensure that the received VDPs are in correct sequence. This window is shifted to the right with each received VDP carrying a new matching SSC (see Figure 90), so subsequent VDPs need to match the shifted window. In the example below, a

VDP with SSC = 9 has been received. The next VDP is expected to have an SSC in the range of 09 to 13. If the next received VDP has an SSC of 09, it is a duplicate to the previously received VDP. If it has an SSC of 10 to 13, it will be a fresh VDP.

All VDPs matching the window are called “valid”, but only those with a new SSC value are called “fresh”. After receiving the VDP with SSC = 10, the window is shifted by one covering now the range of 10...14 (not shown).

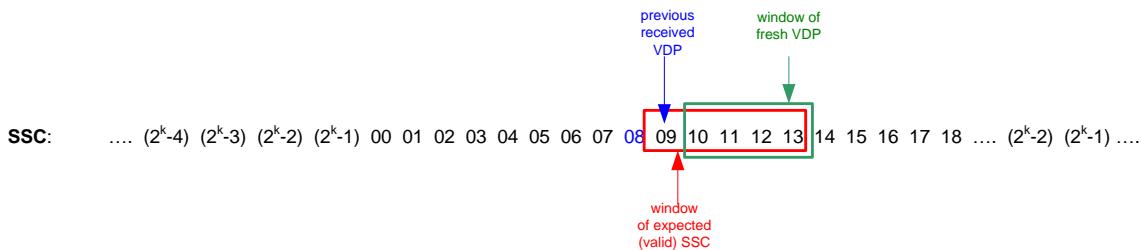


Figure 90: Window of expected SSC (example)

VDP processing

After reading a VDP from the communication channel interface, SDSINK shall first check the correctness of the VDP.

If VDPs from a redundancy group are expected, the correctness check shall be made with the expected SIDs associated to the SDSRC of the redundancy group.

NOTE In a redundancy group of two SDSRC, first a check can be made with the SID already known from the previously received VDP, and only if this fails it will be done with the second SID.

SDSINK shall check whether a received VDP is initial. Upon reception of an initial VDP, SSC_i and $SSC_{initial}$ shall be set to the SSC of this initial VDP and $SID_{initial}$ shall be set to the SID value used for the validation.

SDSINK shall check whether a received VDP is valid.

SDSINK shall check whether a received VDP is fresh. If the received VDP is a fresh VDP, SSC_i shall be set to the value of the SSC of the received fresh VDP.

This means that the receiver needs only to implement one sequence counter.

User data contained in fresh or valid VDPs shall be exposed to the application for consumption if SDSINK is in state ‘SAFE’.

User data contained in invalid VDPs shall not be exposed to the application for consumption (shall be discarded).

The application may consume the user data received from the most recently received valid VDP in those cases as long as data is indicated as safe.

Sink time supervision

With the reception of an initial VDP, the receiver shall start a timer which expires after a time T_{rx_safe} . ("sink time supervision timer").

The sink time supervision timer shall be retriggered with the reception of a fresh VDP.

If the sink time supervision timer expires, a loss of safe communication shall be indicated (trigger 'lossOfSafeCom') and the SDSINK shall wait for the next received VDP which is not a duplicate. This VDP shall be treated as an initial VDP.

Guard time check

General

The guard time check intends to detect two redundant active SDSRC (both sending VDPs). For this, a "guard time" is introduced which shall start with the reception of an initial VDP and shall last for a multiple of T_{rx_safe} (configurable). If a VDP with another SID than expected is received during that time, SDSINK assumes that both redundant SDSRC became active and shall indicate loss of communication safety. This situation is depicted in Figure 91. Here, SDSINK receives first VDPs with SID=A and then VDPs with SID=B. So SDSINK assumes that a redundancy shift at SDSRC side has taken place and expects to receive only VDP with SID=B further on. If it receives a VDP with SID=A now during the time T_{guard} , SDSINK assumes that the SDSRC sending SID=A is still active, which is a redundancy fault at SDSRC side. Such an event is called a "guard time violation". As mentioned, the guard time starts with the reception of an initial VDP. In the example, there are four initial VDPs: the first at the very beginning and the second after the redundancy shift. The VDP with the unexpected SID=A is as well interpreted as an initial VDP according to the rules defined for initial VDPs. This means, that the guard time supervision is retriggered in that case. The same is the case for the next received VDP with SID=B again. Consequently, guard time will be retriggered all the way and practically never expires if there is a mixed reception of VDPs with SID=A and SID=B. The guard timer will only expire if there is a stable reception from one SDSRC (again). So, with expiring guard timer, a loss of safe communication can be negated.

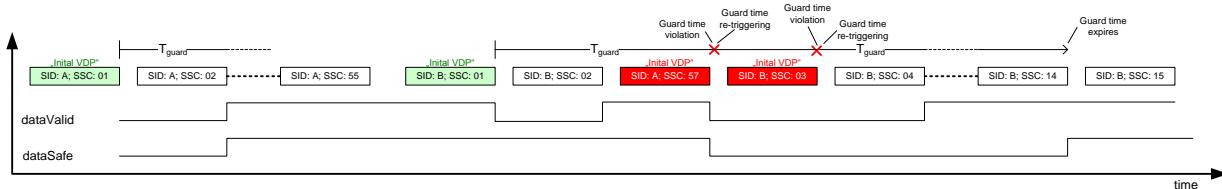


Figure 91: Guard time violation (example)

Requirements

With the reception of an initial VDP with a SID different to $SID_{initial}$, the receiver shall start a timer, which expires after a time T_{guard} (guard timer).

The receiver shall indicate a loss of safe communication (trigger 'lossOfSafeCom', 'gtcSafeCom = FALSE') if it receives, during the time the guard timer is active, an initial VDP with a SID different to $SID_{initial}$. This is called a "guard time violation".

NOTE 1 The intention with a guard time supervision is to detect two active redundant SDSRC sending VDPs, which normally never should happen.

The parameter T_{guard} shall be defined in a range of:

$$2 \times T_{rx_safe} \leq T_{guard} \leq 1000 \times T_{rx_safe}$$

NOTE 2 A good practical value will be $T_{guard} = 10 \times T_{rx_safe}$.

In case of a guard time violation, the guard timer shall be retriggered in order to start a new guard time supervision time interval.

The guard time supervision shall cancel the loss of safe communication indication (`gtcSafeCom = TRUE`) if the guard timer expires.

Latency monitoring

Latency monitoring is important if and only if the signals to be transmitted cannot be received "slowly delayed" by the receiver (SDSINK) from the sender's point of view (SDSRC), e.g. "control commands". In order to be able to ensure that the expected control command has been received, however, a second SDTv4 channel with the status information is required (see the example in Figure 111). This is the only way the sender SDSRC of the command can be sure that the recipient SDSINK has received this command within the expected or respected tolerance.

If it is not important from the sender's point of view (SDSRC) whether the telegrams slowly reach the receiver with a delay, then the sink time supervision is sufficient, because only within this time it can be guaranteed at all that a signal change of a transmission date has arrived at the receiver.

Condition for this: The signal change and the state of the signal change remains present at SDSRC (T_{sig_min}) for at least as long as the sink time supervision (T_{rx_safe}). Temporal signal changes at the SDSRC, which are shorter than the sink time supervision, cannot be guaranteed on the receiving side anyway.

For the "Contraction phase" shown in Annex B of IEC61375-2-3 "Latency violation sequence chart (example)" (in effect like transmission interval much higher than reception interval) there is also no guarantee that all VDPs have been received and sampled.

Channel monitoring

In contrast to SDTv2, SDTv4 does not require channel monitoring. This is due to the fact that the power of CRC error detection is given for both variants (small frames, large frames) and thus lies within the required residual error rate of 1 % of SIL4.

VDP-Variant 1:

For the integrity in general or for the detection of errors, however, the share of safety-relevant user data (max. 8 bytes) and the CRC itself play a decisive role, since the rest of the trailer does not lead to any direct dangerous state in the event of a corruption within the transmission. This can be explained by the fact that the Trailer carry at least: "reserved01: 2 Byte", "UDV: 2 Byte" more or less static data and the SSC with an expectation and a check within an interval. This means a data corruption of the SSC would remain undetected in general with the probability equal to $[(\text{window of expected SSC}) / 2^{32}]$ if the corruption remains undetected by the CRC mechanism. Furthermore, the HD of the Code = 8 with polynomial = "1F4ACFB13" in a range between "25-274" Bits "3...34 Byte"

(detailed information can be found within [57]). This lead to the result, that no data corruption remains undetected up to 7 Bits.

Taking that fact into account so for SDTv4 VDP Variant 1 (small frames) a resumed bit error probability (BEP) of 0.002 (assumption explained within [05]) lead to a residual error probability with a maximum VDP length of 12 bytes (max. 8 Bytes net data + 4 Byte CRC) below 10^{-19} .

Even if the entire VDP frame of 20 bytes is considered, with an assumed BER of 0.002 the residual error probability is 10^{-16} . So, with an assumed telegram rate of the sampled telegrams (others are not relevant) of 10ms (of 360.000 /h) this will lead to a residual error rate of $3,6 \cdot 10^{-11} /h$.

VDP-Variant 2:

For variant 2, assuming the two 32-bit CRCs are as good in their effect or error detection mechanism as a 64-Bit CRC (assumption explained within [05]) the residual error rate can be calculated by:

$$\text{THR} = 2^{-32} * 2^{-32} * 360.000 /h = 1,95 \cdot 10^{-14} 1/h$$

The residual error probability of the two combined CRC-32 is as good as a CRC-64, if at best the polynomials have no common factors and if only one of the two polynomials contains the factor $(x+1)$. This can be proven by combining two 8-bit polynomials analysed in [05] with a residual error probability below 2^{-16} . For details see “Figure 44 Residual error probability Vs bit error probability” in [05].

3.5.4 Safe train inauguration

General

“Train inauguration” as defined in the IEC61375 standards series and in UIC leaflet 556 [32] has the objective to discover the actual train composition and to establish a train-wide communication network (TCN). Historically, the train inauguration was split in two phases: first the train backbone topology discovery (WTB: IEC61375-2-1, ETB: IEC61375-2-5) and thereafter the discovery of the train composition (WTB: UIC leaflet 556, ETB: IEC61375-2-3). The first phase aims to establish a train wide communication network allowing end devices of different consists to communicate, while the second phase creates an application train view as a train composed of vehicles and consists. For the Ethernet based TCN, this train view is presented with the TTDB, which is a repository containing all relevant information about the actual train composition:

- Sequence of vehicles and consists
- Orientation of vehicles and consists
- Dynamic and static properties of vehicles and consists

NG-TCN maintains this split by defining the train backbone topology discovery, called “ETB inauguration”, and defining the train composition discovery, called “operational train inauguration”¹⁵. The challenge with NG-TCN is to provide the train composition information with a high safety integrity

¹⁵ In fact, the train composition discovery results in a train directory, showing the train as a sequence of consists, and the operational train directory, showing the train as a sequence of vehicles from a driver’s perspective. Both results are here subsumed under the terminology “operational train inauguration”.

level (SIL4). The protocols defined in the existing TCN standards (IEC61375-2-5 and IEC61375-2-3) are presumably only suitable for lower safety integrity (e.g. SIL2) as the analysis performed in [05] has shown¹⁶.

The approach of a safe train inauguration as defined in this sub-chapter follows the architectural approach of splitting the responsibility between different devices as it has been defined in 2.7.3 with the three architectural variants. Feasibility of architecture variant A has already been demonstrated in [05], but because this variant distributes ETBN and ECSP over different devices, this variant is not optimal. Architecture variant B has been rejected. Therefore, this sub-chapter bases on architecture variant C, which, if feasible, provides the optimal solution.

The safety concept behind architecture variant C is to use a kind of ‘diversity’ for the train inauguration. While the train inauguration is executed on the ETBN device with a lower safety integrity, the result of the train inauguration, namely the train directory (OTD), is validated by an independent instance (“TI Validator”) using independent input information for the highly safety critical parameters ‘consist orientation’ and ‘train end’. The combination of train inauguration and the independent validation of the result shall provide the high safety integrity with respect to the safety related inauguration functions (Figure 92).

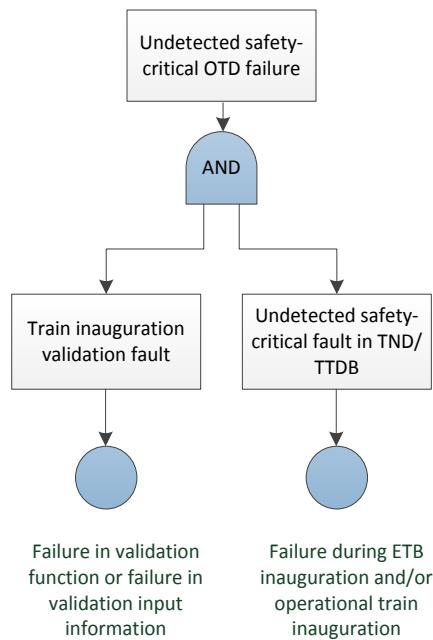


Figure 92: Train directory computation fault tree

With this concept, the train inauguration protocols as defined in the TCN standards can be maintained to a great extent, and modifications are made only where necessary,

- 1) The specification of the safe train inauguration within this sub-chapter is structured as follows:
- 2) Overview of architecture and services used for safe train inauguration

¹⁶ More precise, a formal proof that the protocols defined in existing standards are suitable for SIL2 has never been done. The analysis performed in [04] demonstrated its principle feasibility, although some weaknesses of the protocols have been revealed.

- 3) Description of the train inauguration process as it will be executed by low-SIL capable ETBN devices
- 4) Description of the train inauguration validation which will be executed on a high-SIL capable CCU device
- 5) Concept of independent sensors providing information about consist orientation and train end
- 6) User model of ETB – ETB operational states

Architecture

In architecture variant C (see 2.7.3), the whole train inauguration function is executed on the ETBN device, while the inauguration result validation is executed on a CCU. The different involved services are depicted in Figure 93. The services provided by the ETBN were already described in 2.7.1. The additional services running on the CCU are listed in Table 8.

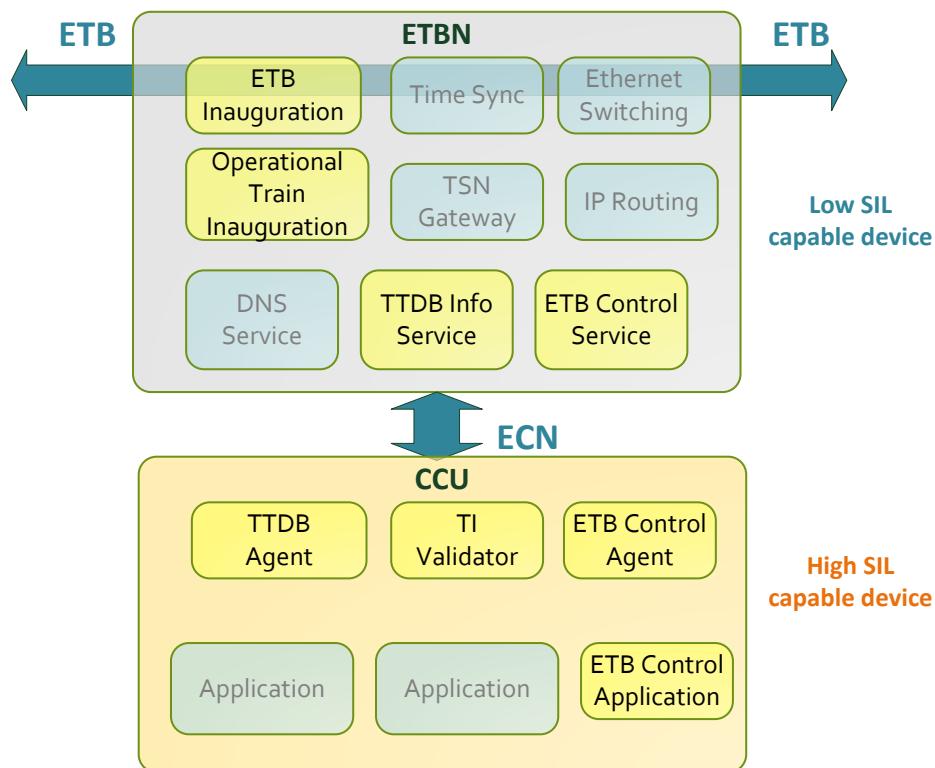


Figure 93: Services involved in safe train inauguration

Table 38: ED services involved in safe train inauguration

Service	Functions	IEC Service	Safety related	Related chapter
TTDB Agent	Establishes and maintains a local copy of the TTDB.	TTDB Info	no	-
TI Validator	Validates safety-critical TTDB parameters and ETB Control parameters	-	yes	
ETB Control Agent	The ETB Control Agent and the ETB Control application represent together the ECSC as defined in IEC61375-2-3. The ETB Control Agent provides a generic interface to the ETB Control service.	ECSC	yes	3.5.5
ETB Control Application	The ETB Control Agent and the ETB Control application represent together the ECSC as defined in IEC61375-2-3. The ETB Control application implements the application specific control of the ETB.	ECSC	yes	-

Train Inauguration

The safety-related train inauguration function, which is responsible to determine the train composition, can be split into three sub-functions (see block diagram shown in Figure 94), which are related to the computation of the TTDB and the notification of a train topology change. These three functions are:

- ETB inauguration (as specified in sub-chapter 3.2.10).
- Train directory computation (as specified in IEC61375-2-3)
- Operational train directory computation (as specified in IEC61375-2-3)

After the ETB inauguration, train wide communication based on IP (and IP addresses) is possible. But train applications need also information about the train composition itself, which is provided by the operational train inauguration in two different views. First the train directory (TrainDirectory), which in combination with the consist information (ConsistInfoList) provides the information about the train length, sequence and orientation of consists and rail vehicles. It will only change if the train composition is changed (adding/removing consists). Second the operational train directory, which adds information about the operational train reference direction which is determined by the position of the leading vehicle. As the position of the leading vehicle can change during train service (changing leading cabs), the operational train directory can also change during service.

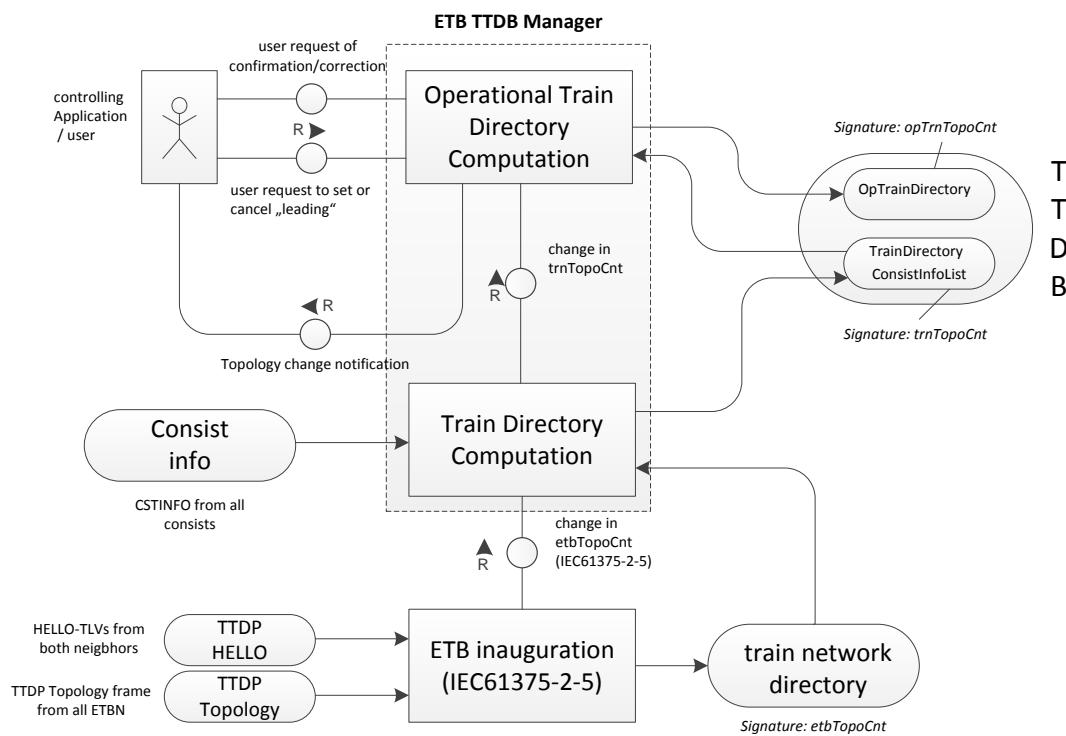


Figure 94: TTDB computation block diagram (based on IEC61375-2-3)

The execution of these functions is allocated to two logical instances: the ETB inauguration is allocated to the ETBN, and the OTD computation to the ECSP. This distinction has been made in the standards because the functions themselves can be allocated to different OSI layers: the ETB inauguration belongs to logical link control and networking (OSI Layers 2 and 3), and the (operational) train directory computation is a service allocated to the application layer (OSI Layer 7).

While the ETB inauguration needs to be adapted to the chosen NG-TCN ETB topology (Variant D₁), there is actually no need to make adaptations to the operational train inauguration sub-functions, with the exception that the correction is no longer needed. The analysis performed in D3.3 has demonstrated that the existing design is sufficient for a SIL2.

Train inauguration validation (TI Validator)

General

The basic principle of a safe train inauguration has already been sketched in chapter 2.7. To achieve higher safety integrity levels, diversity with respect to the determination of safety critical parameters is compulsory because otherwise freedom from systematic failures cannot be proven. The proposal is to compute the TND (architecture variant A) or the TTDB (architecture variant C) for a defined TFFR and to perform an independent check of the safety critical inauguration parameters (train inauguration validation).

Determine safety related inauguration parameters

In order to identify the safety related inauguration parameters, which require an independent validation, the TTDB data structures defined in IEC61375-2-3 shall be analysed¹⁷. A parameter is considered safety critical if a wrong value may lead to an inauguration safety function failure. The result is shown in Table 39.

Table 39: TTDB safety critical parameters

TTDB data structure	Safety critical parameter	Relevance ¹⁸				Remarks
		SE	OR	INT	TD	
ETB_INFO	No					
CLTR_CST_INFO	No					Open whether closed trains should be supported
PROPERTIES	No					Correctness checked with integrity check of pre-defined CONSIST_INFO
FUNCTION_INFO	No					Correctness checked with integrity check of pre-defined CONSIST_INFO
VEHICLE_INFO	vehOrient cstVehNo	x	x			Correctness checked with integrity check of pre-defined CONSIST_INFO
CONSIST_INFO	cstUUID vehCnt cstTopoCnt	x	x	x x	x	Pre-defined data structure (content not changed during inauguration) For cstUUID it is only required that it is unique.
CONSIST_INFO_LIST	No					
CONSIST	trnCstNo cstOrient cstUUID cstTopoCnt	x	x	x	x x	
TRAIN_DIRECTORY	cstCnt trnTopoCnt	x	x	x x	x	trnTopoCnt is included in OpTrnTopoCnt
OP_VEHICLE	opVehNo isLead leadDir trnVehNo vehOrient	x			x x	trnVehNo indicates vehicles inserted by correction
OP_CONSIST	cstUUID opCstNo opCstOrient trnCstNo	x	x		x	For cstUUID it is only required that it is unique. trnCstNo indicates vehicles inserted by correction
OP_TRAIN_DIRECTORY_STATE	trnDirState opTrnTopoCnt	x	x	x	x x	

¹⁷ An identification of safety related inauguration parameters in the TND has already been done in [05]. However, the analysis of the TTDB is more comprehensive.

¹⁸ SE=Sequence, OR=Orientation, INT=Train Integrity, TD=Train Directions

TTDB data structure	Safety critical parameter	Relevance ¹⁸				Remarks
		SE	OR	INT	TD	
OP_TRAIN_DIRECTORY	opTrnOrient opCstCnt opVehCnt		x	x x	x	opCstCnt and cstCnt differ when consists have been inserted by correction, otherwise they are identical.

Some conclusions:

- 1) All parameters contained in CONSIST_INFO (which includes VEHICLE_INFO) are statically preconfigured and can be verified by checking the signature for error detection and by comparing to the signature of the local copy¹⁹ of CONSIST_INFO for checking identity.
- 2) For ETB Topology Variant D₁ inauguration correction is not defined. This means that cstCnt equals opCstCnt and that trnVehNo, trnCstNo, cstOrient have a 1:1 relationship to opVehNo, opCstNo and opCstOrient.
- 3) It is sufficient to check the structure OP_TRAIN_DIRECTORY with its sub-structures OP_VEHICLE and OP_CONSIST because it covers all the information contained in structure TRAIN_DIRECTORY (which contains structure CONSIST).

Train inauguration validation process

The train inauguration validation process aims to check that safety critical inauguration parameters are correct. All relevant safety critical inauguration parameters are stored in the TTDB, so the task is to examine the TTDB for completeness and correctness (TTDB validation). One possible process is sketched in Figure 95 and described in Table 40. Prerequisite is that this process is executed with the same safety integrity level as it is requested for the train inauguration function (SIL4).

It should be mentioned that herein only an architectural view with the objective to demonstrate feasibility is described, real implementations may choose another approach.

The overall validation is divided in two phases, the TTDB pre-validation phase and the train inauguration validation. There is no guarantee that after a successful TTDB pre-validation no parameters still indicate a wrong value because the test coverage of the TTDB pre-validation is limited (example: a wrong consist orientation information is not always detectable by TTDB pre-validation). For this reason, the TTDB pre-validation is supplemented with the train inauguration validation which uses independent information sources during examination.

¹⁹CONSIST_INFO shall be (independently) loaded on ETBN and CCU. By comparing the signatures after inauguration it can be validated that the correct CONSIST_INFO has been distributed by ETBN to all other ETBN and that the CONSIST_INFO stored to ETBN is not corrupted.

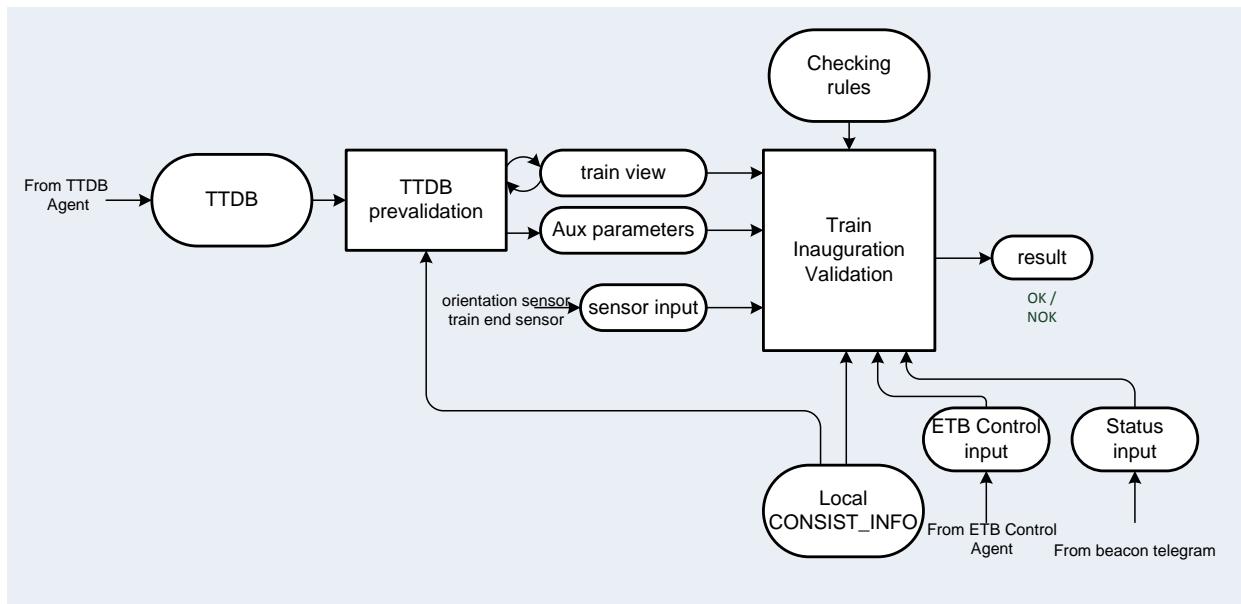


Figure 95: TI Validator block diagram

Table 40: TI Validator entities

Entity	Description
TTDB	A safely stored copy (or extract) of the TTDB. Retrieved from ETBN after inauguration using a safe data transmission protocol, e.g. SDTv2.
TTDB pre-validation	Function for consistency checking, generation of auxiliary parameters and validating train view (see below for a more detailed description of the pre-validation process).
Train view	<p>This is a representation of the operational train view which is subject of examination.</p> <p>The train view is an ordered list of all train vehicles, where each row contains the following parameters with “Index” being the entry number (1...N):</p> <ol style="list-style-type: none"> 1. Index 2. cstUUID 3. opCstNo 4. opCstOrient 5. opVehNo 6. isLead 7. dirLead <p>The number of rows equals the number N of vehicles in the train.</p>
Aux parameters	<p>These are local parameters used for the validation:</p> <p>localIndex: Index of the local consist anyLead: TRUE if there is one entry where isLead == TRUE FALSE if there is no entry where isLead == TRUE ERROR if there is more than one entry where isLead == TRUE</p>
Sensor input	<p>These are the input values from independent sources (orientation and train end detectors, vehicle application):</p> <p>localOrient: independent orientation info of local consist localTrainEnd: train end indicator</p>

Entity	Description
ETB Control input	Input values from ETB Control Agent (see 3.5.5): etbCtrl_LeadingReq: TRUE if the local consist requests leadership etbCtrl_LeadingDir: requested leading direction etbStatus_Leading: leading status etbStatus_LeadingDir: leading direction etbStatus_OpTrnDir: TTDB status etbStatus_OpTrnTopoCnt: opTrnTopoCnt value
Status input	Input values from Beacon telegram (see below): sharedOpTrnTopoCnt: opTrnTopoCnt value reported by other consists
Train inauguration validation	This function performs the checking of the validation train view (see below for a more detailed description of the train inauguration validation process).
Checking rules	These are a set of rules used by the TI Validator to check the operational train view (see below).
Local CONSIST_INFO	This is a description of the local consist, which shall not be derived from the TTDB (independent storage) and which is trustworthy.
Result	Result of the validation activity. The result is used by safety vehicle application to determine whether train can be operated or has to be in safe state.

The following example (Figure 96, Table 41) of a train view used for examination shows a train with three consists, each consist with three vehicles. Orientation of the middle consist is inverse, and the left-most consist is the leading consist.

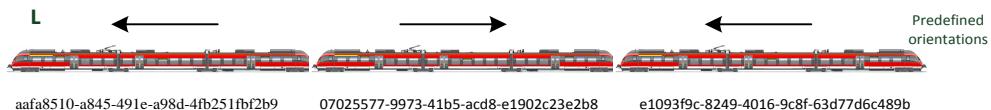


Figure 96: Validation train view (example)

Table 41: Train view for validation (example)

Index	cstUUID	opCstNo	opCstOrient	opVehNo	isLead	leadDir
1	aafa8510-a845-491e-a98d-4fb251fbf2b9	1	SAME	1	TRUE	1
2	aafa8510-a845-491e-a98d-4fb251fbf2b9	1	SAME	2	TRUE	1
3	aafa8510-a845-491e-a98d-4fb251fbf2b9	1	SAME	3	TRUE	1
4	07025577-9973-41b5-acd8-e1902c23e2b8	2	INVERSE	4	FALSE	0
5	07025577-9973-41b5-acd8-e1902c23e2b8	2	INVERSE	5	FALSE	0
6	07025577-9973-41b5-acd8-e1902c23e2b8	2	INVERSE	6	FALSE	0
7	e1093f9c-8249-4016-9c8f-63d77d6c489b	3	SAME	7	FALSE	0
8	e1093f9c-8249-4016-9c8f-63d77d6c489b	3	SAME	8	FALSE	0
9	e1093f9c-8249-4016-9c8f-63d77d6c489b	3	SAME	9	FALSE	0

TTDB pre-validation

During TTDB pre-validation four different activities are executed.

Firstly, it checks TTDB consistency, completeness and values of selected TTDB parameters by performing plausibility checks between TTDB parameter values or by comparing with pre-defined values, e.g. values taken from pre-defined CONSIST_INFO.

Examples:

- Verification of the checksums
- Completeness of dynamic arrays
- Check parameter ranges
- Correctness of own CstUUID value
- Uniqueness of CstUUID values
- Correct version info (pre-defined value)

Secondly, it derives from the TTDB the data for the train view and the aux(iliary) parameters.

Thirdly it checks that the number of entries for the own consist (identified by CstUUID) equals vehCnt value.

Fourthly it checks the operational train direction:

If the local consist is leading (isLead==TRUE) one of the conditions defined in Table 42 must be true.

Table 42: train direction conditions

opTrnDir	opCstOrient	Condition
cstUUID(Index=1) < cstUUID(Index=N)	SAME	cstOrient == SAME
cstUUID(Index=1) < cstUUID(Index=N)	INVERSE	cstOrient == INVERSE
cstUUID(Index=1) > cstUUID(Index=N)	SAME	cstOrient == INVERSE
cstUUID(Index=1) > cstUUID(Index=N)	INVERSE	cstOrient == SAME

If there is no leading consist, then the situation is more complex. For that case, IEC61375-2-3 defines in clause 4.2.4.3:

- b) If there was a previously leading vehicle, then this vehicle together with its previously operational train direction determines the operational train direction.
- c) If there were several previously leading vehicles, e.g. after a train lengthening, and all of these have the same viewing direction, then this viewing direction determines the operational train direction.
- d) If there are multiple consists in the train and a traction consist at one end, then this end defines the train head and traction consist includes vehicle 01 and determines the operational train direction.
- e) In all other cases, the operational train direction shall correspond to the ETB reference direction according to IEC 61375-2-5.

So additional information is needed, like the position of previous leading consists and consists with traction equipment. At least the information about previous leading consists is not contained in the TTDB, so an operational train direction check is not possible using information from the TTDB only.

To avoid a complex solution by adding a protocol to achieve the missing values, two alternatives are possible:

The first proposal here is to perform no additional check in this case. This is justified by the fact that if there is no leading consist, the train will be in a safe state (at standstill) and safety related driver operations like driving or door operation (release) will not be possible.

The second proposal is to restrict to rule e). This however may have some impact: if the driver leaves the cab, there will be no new inauguration due to rule b), but if this rule is replaced by rule e) there can be.

The conclusion drawn by T3.5 (in collaboration with S4R) was that the first proposal shall be selected. It was confirmed by railway operators that no safety related functions are executed while there is no leading consist.

Validation train view checking

The objective of the validation train view checking is to verify those safety critical inauguration parameters which can only insufficiently be checked during pre-validation and which require an independent information source. Table 43 lists the different checks, a more formal definition is given underneath.

Table 43: Validation train view checking – checks

Check type	Independent Information source	Objectives
Train view integrity	sharedOpTrnTopoCnt	Check that all consists share the same train view
Train integrity check	trainEnd	Check train ends and by this train completeness
Leading check	etbCtrl_LeadingReq	Check that a consist is only leading when requested
Orientation check	localOrient	Check correctness of consist orientation

The following check rules are given in a C like pseudo syntax.

```

// train view integrity
IF (opTrnTopoCnt== sharedOpTrnTopoCnt) THEN OK ELSE NOK;

// train integrity check (completeness, end vehicles)
IF localIndex==1 AND localTrainEnd==TRUE THEN OK ELSE NOK;
IF localIndex==N AND localTrainEnd==TRUE THEN OK ELSE NOK;
IF localIndex>1 AND localIndex<N AND localTrainEnd==FALSE THEN OK ELSE NOK;

// Leading check
IF isLead(localIndex)==TRUE AND etbCtrl_LeadingReq==FALSE THEN NOK ELSE OK;

//Orientation check
IF localOrient==OpCstOrient THEN OK ELSE NOK;
```

NOTE: This set of checking rules is generated from experience. Formally correct would be to derive those rules from a system FMEA analysing failure effects of inauguration and TTDB faults. This to perform is not in the scope of this task but may be subject of CTA-2.

Review of general failure modes

While exclusive errors in the local TTDB are detected with the exchange and comparison of the TTDB signatures and by the additional checks listed before, common mode failures affecting all TTDB are sometimes not detectable by this method. As explained earlier, common mode failures shall be detected by plausibility checks and by using independent information sources. Those checks primarily aim to detect faults in individual parameters, as for example the parameter ‘opCstOrient’ or ‘isLead’. What those checks do not cover are failures affecting complete entries (vehicle or consist entry) in the operational train directory, for instance missing, duplicated, reordered or unjustified inserted entries. Table 44 lists those “general” failure modes together with a hint on how to detect those failures. These ‘hints’ shall be respected during the TTDB validation design.

Table 44: OTD computation general failure modes

Failure mode	Cause (systematic failure)	Effect	Detectability by independent SIL4 checker
Values out of range or invalid	Computation or configuration error	At least one of the values in the table is out of its specified value range or has unspecified value.	Detectable during TTDB pre-validation
Insertion of vehicle entry	Computation error, for instance an old entry has been inserted.	Additional vehicle entry in validation train view	Detectable during TTDB pre-validation (doesn't fit number of consist parameter vehCnt value)
Insertion of consist entry	Computation error, for instance an old entry has been inserted.	Additional consist entry in validation train view	Detectable on application level (→ AC) There is a consist from which no telegrams are received
Duplication of vehicle entry	Computation error	Duplicated vehicle entry in validation train view	Detectable during TTDB pre-validation (duplicated opVehNo value)
Duplication of consist entry	Existing entry is doubled	Duplicated consist entry in validation train view	Detectable during TTDB pre-validation (duplicated cstUUID value)
Loss of vehicle entry	Computation error Entries have been deleted or were not produced.	Missing vehicle in validation train view	Detectable during TTDB pre-validation (missing opVehNo value)
Loss of consist entry	Computation error Entries have been deleted or were not produced.	Missing consist in validation train view	Detectable on application level (→ AC) telegrams received from a consist which is not listed
Missing consist entry	Powerless consist	Missing consist in validation train view	Detectable during validation train view checking (last indicated consist is no end consist)

Failure mode	Cause (systematic failure)	Effect	Detectability by independent SIL4 checker
			Works only for ETB topology variant D1! In ETB topology variant B, a powerless intermediate consist is not detectable.
Re-sequencing	Two or more vehicle entries are mixed up.	Vehicle sequence is corrupted in validation train view.	Detectable during TTDB pre-validation (incorrect sequence of opVehNo)
Re-sequencing	Two or more rows are mixed up.	Consist sequence is corrupted in validation train view.	Detectable during TTDB pre-validation (incorrect sequence of opCstNo)
Incorrect CstUUID value	Computation or configuration error	Unknown CstUUID value	Detectable during TTDB pre-validation or on application level (→ AC) No telegram with that cstUUID will be received
Incorrect consist orientation info	Computation or configuration error	Indication of wrong consist orientation	Detectable during validation train view checking

Frequency of train inauguration validation

The train inauguration validation is compulsory each time the OTD changes, which is indicated with a change of the opTrnTopoCnt value. Dependent on the train application, those changes may happen frequently (several times during a train service day) or less frequently (e.g. only one time per train service day). Dependent on this frequency and dependent on the reliability of the CCU, it might be helpful to execute the train inauguration validation also during periods where no change happens. For instance, the train inauguration validation could be executed when OTD changes but also in regular time intervals as a kind of a background self-test.

Independent Sensors

General

The train inauguration validation process as described above uses sensors to independently discover train end and consist orientation. Traditionally, those sensors are using conventional train lines as it is shown in Figure 97. As can be seen, two independent train lines are needed to identify the orientation of a consist (“physical coding”). In one possible implementation, the leading consist feeds a current in the train line on its side A, and by sensing this current other consists are able to discover their orientation with respect to the leading consist. Train end is discovered by reading the coupler state, which should state “open” for end consists and “closed” for intermediate consists.

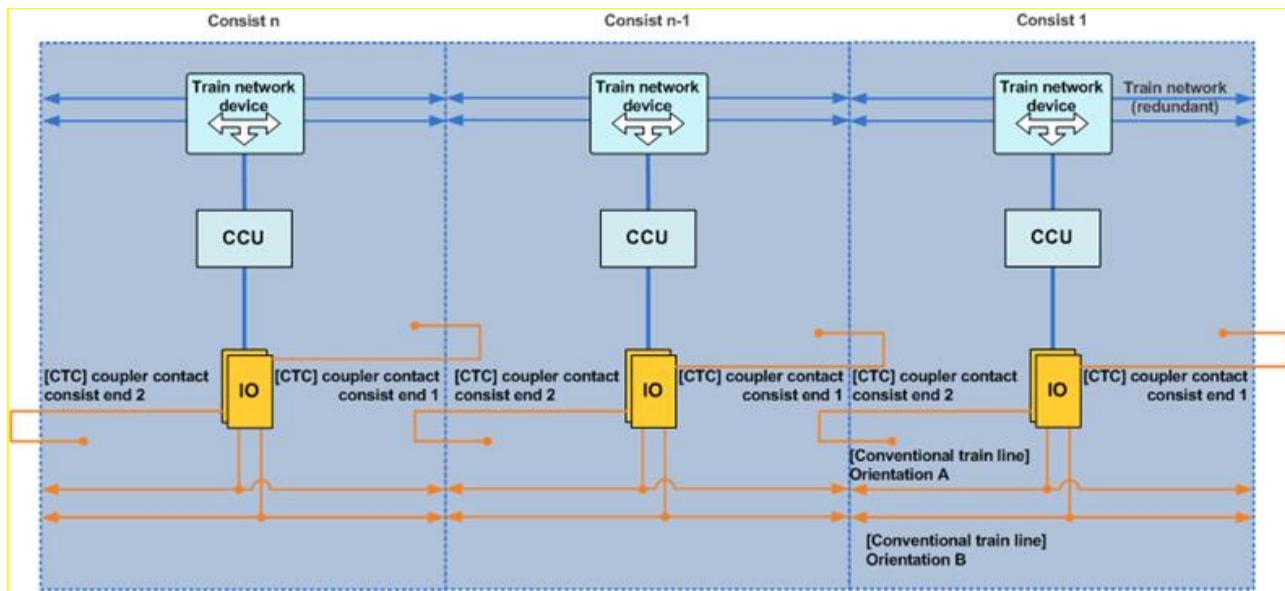


Figure 97: Independent check with train lines (traditional way)

When comparing this traditional way with train lines with the chosen ETB topology for ETB (ETB topology variant D₁), one can see similarities. In NG-TCN, there are two independent ETB lines (ETB-L and ETB-R) along the train. Those can be used in a similar way than train lines: every consist sends special “beacon” telegrams side selective, and other consists are then able to determine their orientation (see Figure 98).

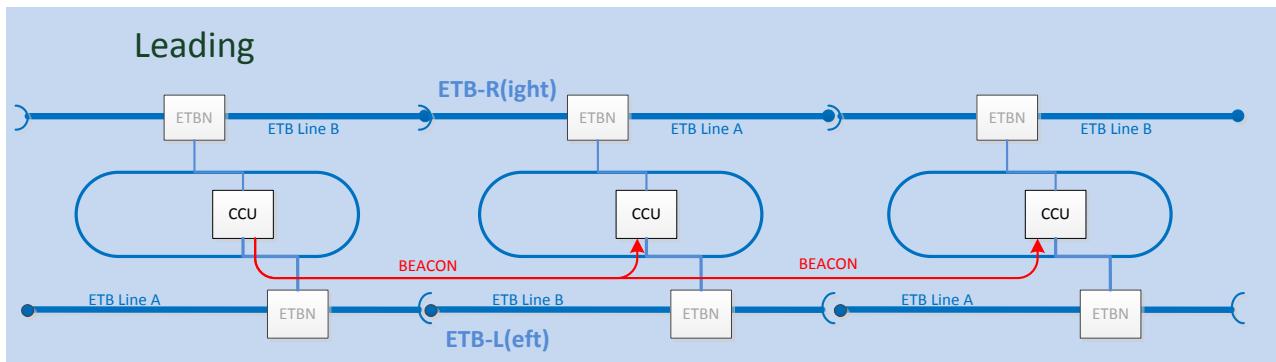


Figure 98: Independent check with “beacon” telegram

Train end detection depends on the way how consists are coupled. For physically coupled trains the traditional way can be kept as this doesn't require a train wide train line²⁰. For virtually coupled trains an equivalent mechanism needs to be defined.²¹

²⁰ But also other solutions for train end detection could be applied.

²¹ Virtually coupled train concepts will be developed in the Innovation Programm 2, but are as well subject of the CONNECTA-2 project.

Beacon telegram and frame replication

Contrary to general application TSN process data telegrams, which are replicated and sent over both ETB-L and ETB-R, “Beacons” are sent only over one ETB line as TSN process data telegrams²². For redundancy reasons it makes sense to send two distinct beacon telegrams, one over ETB-L and the other over ETB-R. To make the beacons distinguishable, the information to which ETB side they are sent (side A or side B) must be coded in the telegram (see Figure 99, side information illustrated by using different colors).

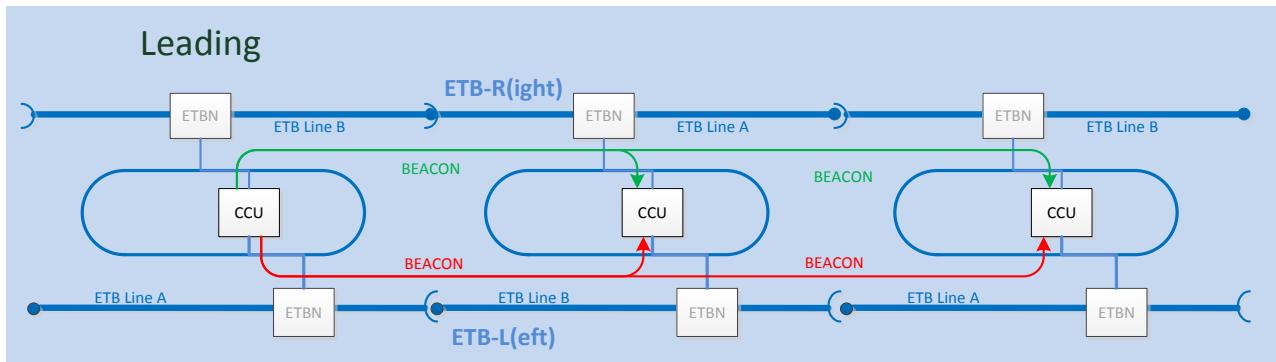


Figure 99: “Left” and “right” beacon

This requirement impedes the usage of a link layer-based replication mechanism as defined in IEEE802.1CB, because the link layer belongs to the non-safe black communication channel (see 3.2.8), but the insertion of the ETB side information is safety-related. So, instead of using IEEE802.1CB, one possibility is to replicate the beacon telegram in the FDF communication&network services and to add the information about the used ETB side in the telegram’s payload.

For safety reasons it shall be ensured that A-side telegrams cannot be sent to B-side by chance and vice versa. Similarly, it shall be prohibited that telegrams transmitted over ETB-L are not, by chance, transferred to ETB-R and vice versa. Those potential failure modes should be covered by the System FMEA.

Beacon telegram

The beacon telegram shall contain the beacon information but in addition also the status information required by the TI Validator. The structure of the beacon telegram is shown in Figure 100.

²² Beacon telegrams cannot be sent as routed conventional telegrams because then the IP router redundancy protocol, which belongs to the black communication channel, decides to which ETB line to route. Hence there is no control over which ETB line a beacon telegram is sent.

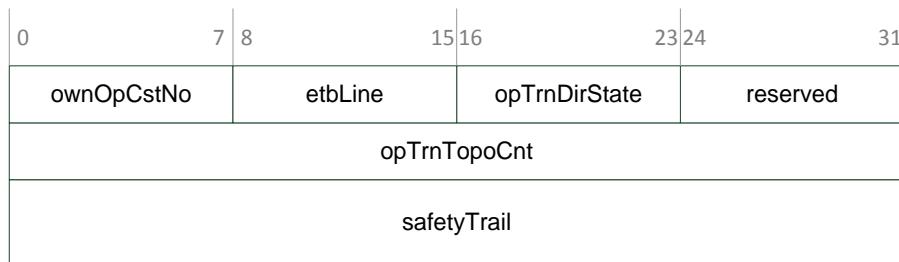


Figure 100: BEACON telegram

```

BEACON_TELEGRAM ::= RECORD
{
  cstUUID           UINT8[16]      -- UUID of the consist
  ownTrnCstNo      UINT8          -- own train consist number
                           value range: 1..32
                           0 = unknown (e.g. after inauguration)
  etbLine           ANTIVALENT8   -- ETB line selected for transmission
                           '01'B = Line A
                           '10'B = Line B
  opTrnDirState    UINT8          -- operational train directory state
                           1 = INVALID
                           2 = VALID
                           4 = SHARED
  reserved01       UINT8          -- reserved, shall be set to 0
  opTrnTopoCnt     UINT32         -- operational train directory topography
                           counter
  safetyTrail      ETBCTRL_VDP   -- ETB-VDP trailer (defined in [18])
}

```

NOTE: With this proposal, an independent way of comparing opTrnTopoCnt values from different consists can be implemented. OpTrnTopoCnt values are already distributed and compared within the ETBN using the ETBCTRL frame as defined in IEC61375-2-3. This frame is transmitted using SDTv2. With the SDTv4 compatible beacon telegram a more trustworthy comparison is available.

ETB Operational States

The ETB is seen in different states from the viewpoint of the ETB Control application (see 3.5.5) as it is shown in Figure 101. This state machine is triggered by the status signals received from the ETB Control agent, which itself is reacting on status signals received from the ECSP. The states and their related actions are described below.

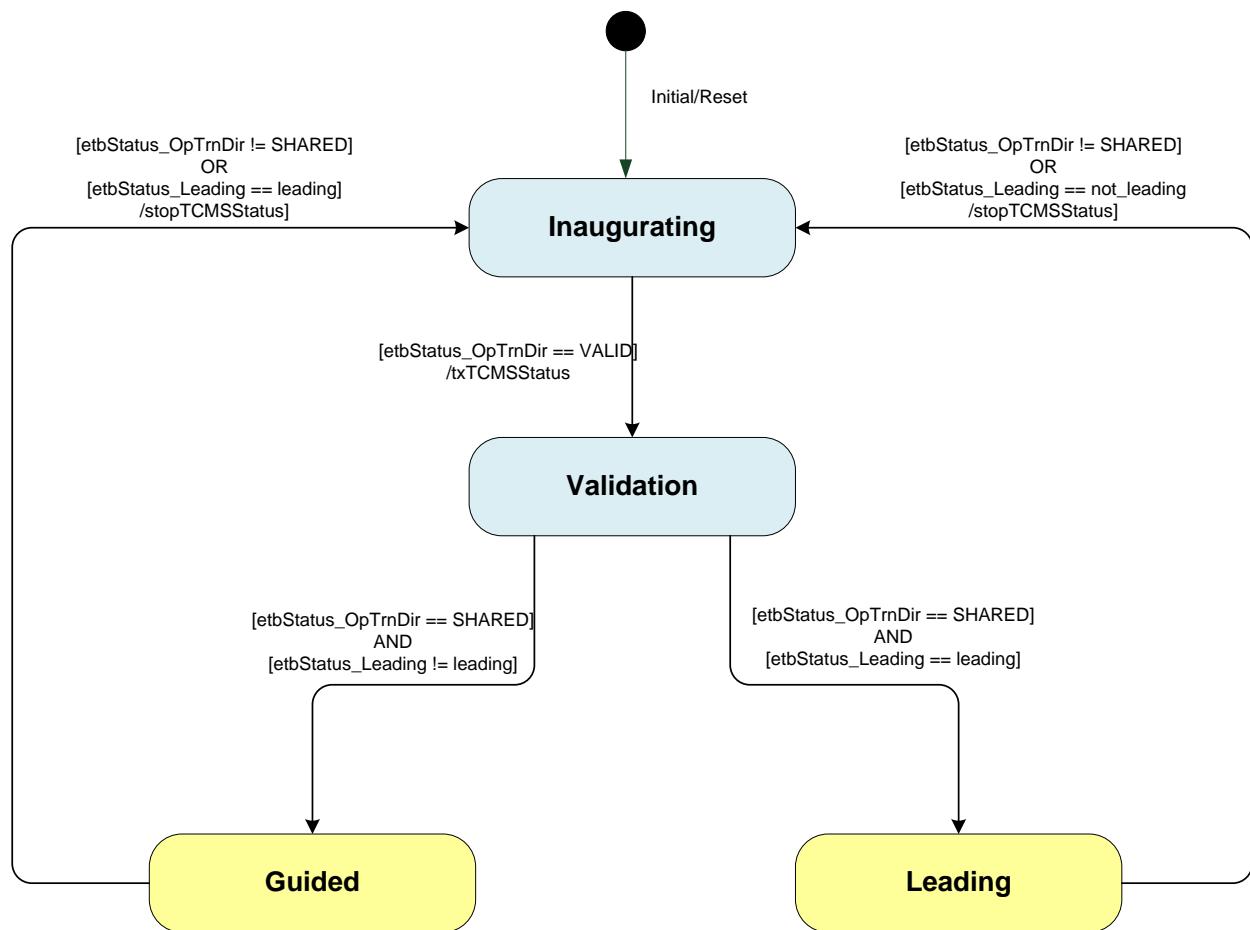


Figure 101: ETB user states

Inaugurating:

Discovery of the ETB topology and computation of the TND (see 3.2.10) and the TTDB.

No (TCMS) application ETB communication in this state (ETB/ECN IP routing and TSN-GW disabled), transmission of TCMS status telegram shall be stopped (action 'stopTCMSStatus').

This is also the defined state for the case an inauguration failure (inaugFailure) has been detected.

Validation

This state is entered when ETB inauguration (ETBN) and operational train inauguration (ECSP) are finished. TSN-GW and IP routers are (re-) configured and active. Upon state entering, TCMS status telegram exchange shall be launched (action 'txTCMSStatus') because these status telegrams are used during validation (for opTrnTopoCnt validation).

Guided:	Train network directory and TTDB are positively validated. (TCMS) application acts as guided consist (receiving commands from leading consist and sending status to leading consist). Leading requests only allowed in this state. Stays in state “Guided” when leading is requested until leadership is assigned.
Leading:	Train network directory and TTDB are positively validated. (TCMS) application acts as leading consist (sending commands to guided consist and receiving status from guided consists). Stays in state “Leading” during leading conflict until leading conflict is resolved.

3.5.5 Network application services

Network application services are those services which the network provides to connected ED. For using those services, a dedicated interface (interface protocol) is available.

DNS

The most basic task of DNS Service is to translate TCN-URI names to IP addresses. In very simple terms, DNS can be compared to a phone book. Briefly, the way DNS is used is as follows: To map an TCN-URI name onto an IP address, an application program calls a library procedure called the resolver, passing it the name as a parameter. The resolver sends a DNS query (UDP packet) to the DNS server residing in the ETBN, which then looks up the name and returns the IP address to the resolver, which then returns it to the caller. Armed with the IP address, the program can then establish a TCP/UDP connection with the destination.

The DNS server located in the ETBN maintains a host file where for all the ED the IP addresses and related TCN-URI names, as well as aliases to these names, are listed. A typical line in the “hosts” file looks like:

```
10.0.1.105      hmi.veh01.cst01 hmi.veh01.uiclabel hmi.uiclabel_slt951.cst01  
hmi.uiclabel_slt951.uiclabel hmi.uiclabel_slt951 hmi.veh01 hmi.veh01.1Cst
```

The “hosts” file is populated after CS booting up with the ED data of the local consist. Data of other consists are dynamically added/removed after each new train inauguration.

There are some special TCN-URIs which cannot be resolved by standard DNS, like:

- predefined IPT-URIs (e.g. “grpAll.aVeh.aCst”)
- IPT-URIs requiring computation: e.g. all IPT-URIs with “anyVeh”, “anyCst”, “leadVeh”, “leadCst”
- IPT-URIs requiring location information, like TCN-URIs containing “IVeh” label

For resolving those TCN-URI extensions to DNS are necessary, see for instance definition of “TCN-DNS” in IEC61375-2-3 Annex E.

DHCP

General

In cases where the manual configuration of the ED is inappropriate or not desirable for other reasons, an automated service may be used. The DHCP automates the process of configuring new and existing ED connected to the ECN. This is especially useful if for instance a defective ED shall be replaced by a new device from stock.

Configuring the ED for ECN access means to provide the ED with information, among it:

- IP Address
- IP Address Lease Time
- Subnet Mask
- DHCP server IP address

One special use case for instance is to assign an IP address which encodes the location of the ED in a consist (e.g. in which car of a consist it is located).

The DHCP service consists of three protocol machines (Figure 102):

The DHCP Server maintains the configuration database and selects the configuration dependent on the information in the dhcp_request message. There can be many DHCP servers in a consist: the protocol ensures that one DHCP server is selected.

The DHCP Client resides on the ED and is responsible to request new information each time the ED is powered, after communication link loss and after the IP Address lease time expired.

In between the DHCP Server and the DHCP Client is the DHCP Relay Agent, which is located on the CS where the ED is connected to. The main purpose of the relay agent is to add location/position information to DHCP Client requests (DHCP option 82).

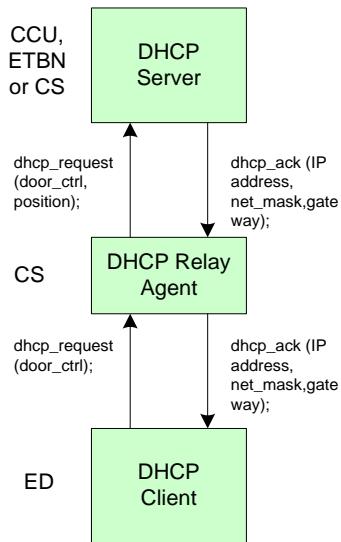


Figure 102: DHCP protocol machines

The DHCP server can be located anywhere in the consist, e.g. running on the CCU or on the ETCN device. A smart design would be to locate the DHCP server on CS together with the DHCP Relay Agent, in which case the DHCP server assigns the addresses to the locally connected ED only. Advantage of the latter solution is that there is no data communication to a remote DHCP server. In case of a device failure, only locally connected devices will be affected. As everything is handled locally, robustness (reliability) is increased.

There are three ways to assign a specific configuration to an ED:

Switch and Hostname Method	The combination of ED hostname and network switch identity is used to derive the configuration of the ED which is connected to (any) of the switch ports.
Network Switch Port Method	The combination of network switch port and network switch identity is used to derive the configuration of the ED which is connected to this switch port.
MAC Address Method	The MAC address of the ED is used as unique key to derive the configuration of the ED which may be connected to any switch.

But it is also possible to assign an arbitrary configuration (IP Address) out of a pool of dynamic IP addresses. This might be useful when connecting an ED temporarily, like a measuring device or a service PC.

Protocol

The IP telegram exchange between DHCP server, DHCP relay agent and DHCP client is defined in RFC 2131. An example session is shown in Figure 103 with the options listed in Table 45.

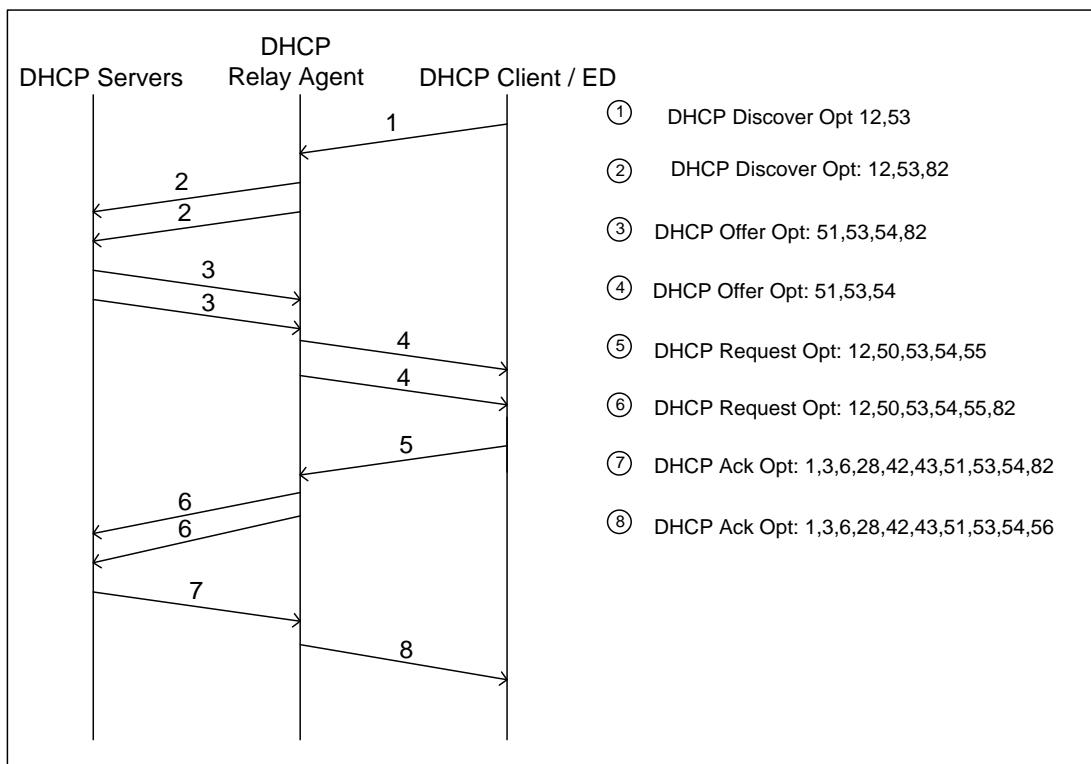


Figure 103: DHCP session example

Table 45: Used DHCP options

Option	Name
0	Pad
1	Subnet Mask
3	Router
6	Domain Name Server
12	Host Name
15	Domain Name
28	Broadcast Address
42	Network Time Protocol Servers
43	Vendor Specific Information (optional)
50	Requested IP Address
51	IP Address Lease Time
53	DHCP Message Type
54	Server Identifier
55	Parameter Request List
56	Message
57	Maximum DHCP Message Size
60	Vendor Class Identifier
72	Default World Wide Web Server
82	Relay Agent Information
255	End

Following are some typical situations described:

First IP address assignment

The ED sends the DHCP DISCOVER message.

If "switch and host name" method is used, DHCP option 12 will be included, containing the hostname of the ED. (The hostname must in this case be unique for the network switch connected to the ED.)

The DHCP Relay Agent receives the DHCP DISCOVER message, appends the option 82 field ("agent circuit id" = port number and "agent remote id" = MAC address of the network switch, see RFC 3146 for details) and forwards the DHCP DISCOVER message to the predefined DHCP Server, which may be redundant.

The DHCP Server(s) responds with a DHCP OFFER, which is sent to the corresponding DHCP Relay Agent, which in turn sets option 54 to contain the DHCP Relay Agent IP address and forwards the DHCP OFFER message(s) to the ED. (If redundant DHCP Servers are used, all DHCP OFFER messages are forwarded to the ED.)

The ED then sends the DHCP REQUEST message, including the DHCP option 12 ("switch and host name" method only), to the DHCP Relay Agent, which appends the option 82 field ("agent circuit id" = port number and "agent remote id" = MAC address of the network switch) and forwards the DHCP REQUEST message to the predefined DHCP Server(s).

The selected DHCP Server responds with a DHCP ACK message, which is sent to the corresponding DHCP Relay Agent. The DHCP Relay Agent sets option 54 to contain the DHCP Relay Agent IP address and forwards the DHCP ACK message to the ED.

The DHCP Relay Agent then initiates the configuration of the managed network switch connected to the ED.

Renew a Lease

Before the lease time of the IP address is expired, the ED is supposed to renew its lease.

The ED sends the DHCP REQUEST message, including the DHCP option 12, to the DHCP Relay Agent, which appends the option 82 field ("agent circuit id" = port number and "agent remote id" = MAC address of the network switch) and forwards the DHCP REQUEST message to the DHCP Server.

The DHCP Server responds with a DHCP ACK message, which is sent to the corresponding DHCP Relay Agent. The DHCP Relay Agent sets option 54 to contain the DHCP Relay Agent IP address and forwards the DHCP ACK message to the ED.

ETB Control

General

The network application service "ETB control" resides in the communication layers of the FDF as part of the communication&network services and provides functions for the control of the ETB to the applications within the FDF. ETB Control comprises the following functions:

- Request train leadership if demanded by application
- Set/reset inhibit inauguration dependent on train operational mode
- Provide status information about actual ETB state and train composition:
 - Inauguration inhibit state
 - Train shortening/lengthening detected while inauguration is inhibited
 - Train leadership
 - Operational train directory state
 - Operational train topography counter value
- Optional: Send confirmation message to ECSP if demanded by application

Architecture

The way how this is supported by ETB Control is defined in IEC61375-2-3. This standard defines an ETB control interface (called “ECSP interface” in the standard) between the ECSP and the ECSC, where ECSC represents the client side. In our case, ECSC can be split in two functions:

1. ETB Control agent, which is part of the communication&network services
2. ETB Control application, which belongs to the FDF application responsible for ETB control

Figure 104 shows the complete system architecture with the ETBN device part (with ETBN, ECSP, TTDB manager and DNS server) as it is defined in IEC61375-2-3 and the consist control unit implementing FDF and TCMS applications. The ETB Control agent sends cyclically the ECSP control telegram, receives the ECSP status telegram and, optionally, sends the ECSP correction message. Furthermore, the ETB Control agent interfaces with the ETB Control application (Figure 105). The interface between ETB Control agent and ETB Control application is implemented in the variable/message memory of the FDF and comprises a set of signals exchanged between the two instances (Table 46).

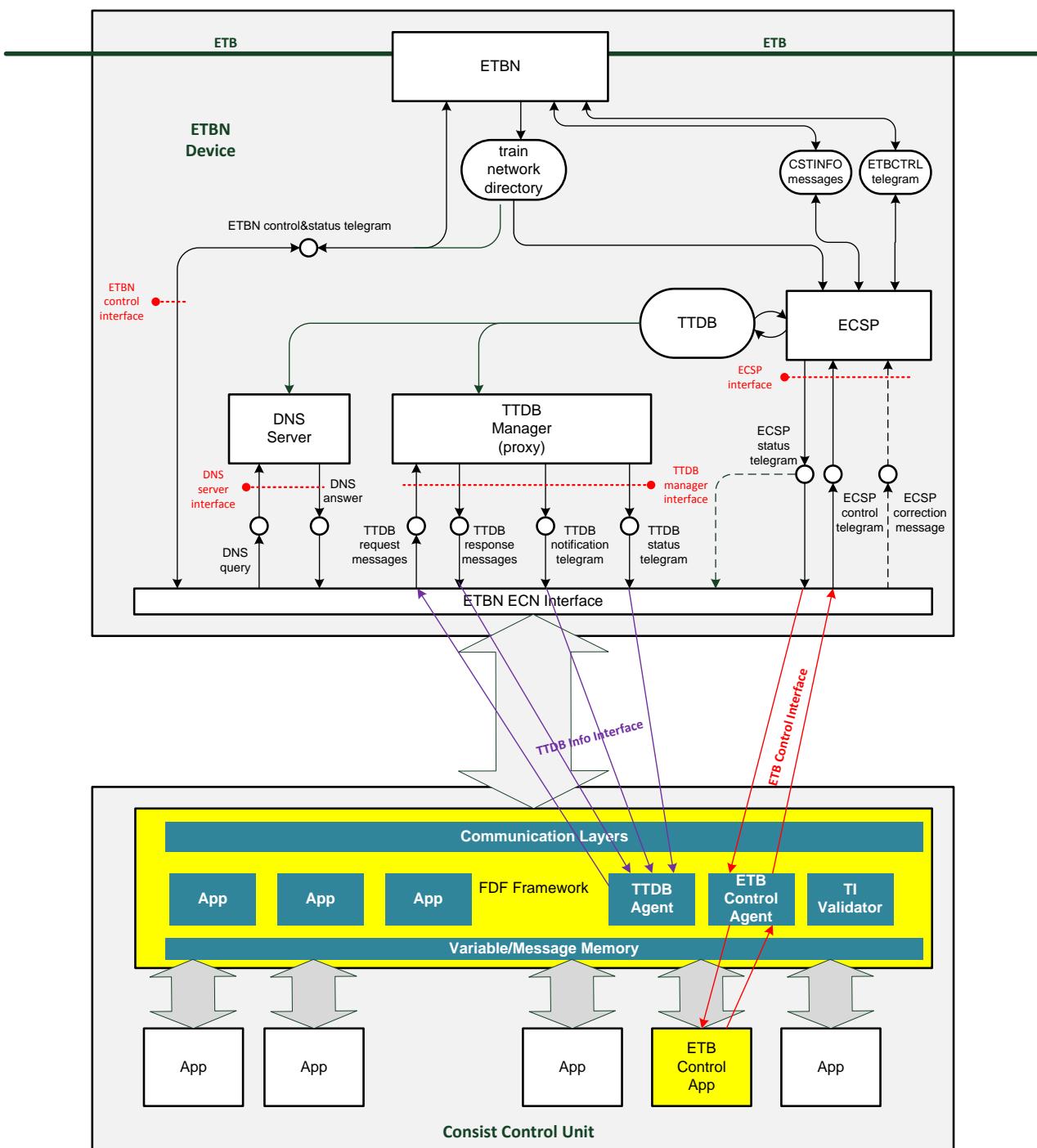


Figure 104: ETB Control system architecture

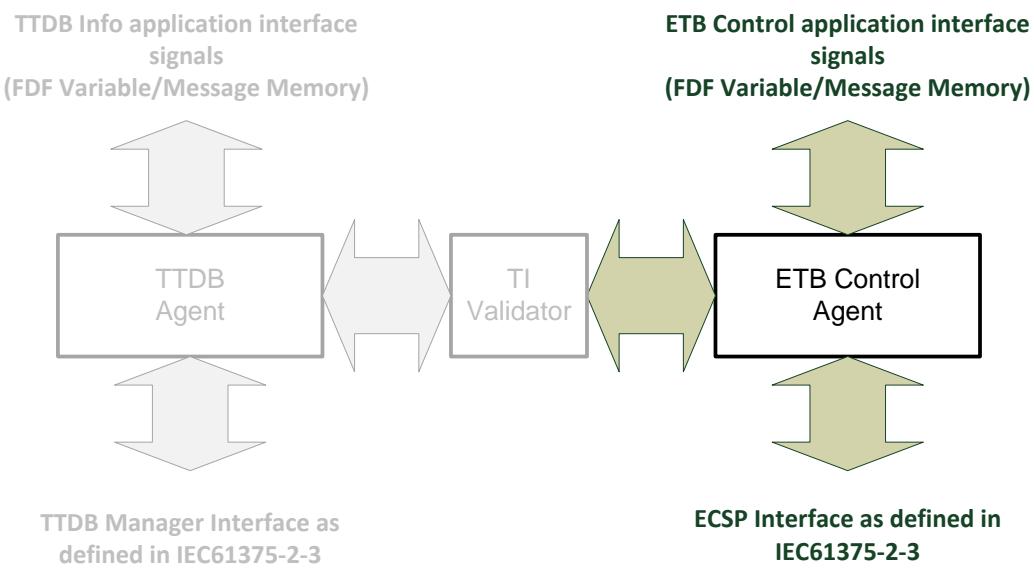


Figure 105: ETB Control Agent interfaces

Table 46: ETB Control agent/application interface signals

Signal	In/Out	Data type	Value range ²³	Comment
etbCtrl_InhibitReq	I	AV2	FALSE/TRUE	
etbCtrl_LeadingReq	I	AV2	FALSE/TRUE	
etbCtrl_LeadingDir	I	ENUM	0 = no leading request 1 = leading_dir1 2 = leading_dir2	
etbCtrl_sleepReq	I	AV2	FALSE/TRUE	optional
etbCtrl_confirm	I	AV2	FALSE/TRUE	optional
etbStatus_Inhibit	O	ENUM	0 = default 1 = inhibit_not_requested_on_ETB 2 = inhibit_set_on_local_ETBN 3 = inhibit_set_on_remote_ETBN 4 = inhibit_set_on_local_and_remote_ETBN	
etbStatus_Length	O	AV2	FALSE/TRUE	
etbStatus_Short	O	AV2	FALSE/TRUE	
etbStatus_Leading	O	ENUM	0 = not_leading 1 = leading_requesting 2 = leading 3 = leading_conflict	
etbStatus_LeadingDir	O	ENUM	0 = no leading request 1 = leading dir1 2 = leading dir2	

²³ For detailed description of signal values see IEC61375-2-3.

Signal	In/Out	Data type	Value range ²³	Comment
etbStatus_OpTrnDir	O	ENUM	1 = invalid 2 = valid 4 = shared	
etbStatus_OpTrnTopoCnt	O	UINT32	0 .. 2 ³²⁻¹	
etbStatus_isConfirmed	O	AV2	FALSE/TRUE	optional

Safety aspects

ETB Control has impact on the train operation (leading/guided consists) and operational train direction and therefore has to support a TFFR of less than 10⁻⁸/h, corresponding to SIL4. Consequences for the design are that at least two instances of ETB control agent and ETB control application with comparator (1oo2) have to be provided. Furthermore, the ETB Control Agent has to supervise its connection to the ECSP, and in case of communication loss shall enforce a safe state. This can be accomplished by using SDTv2 between ETB Control Agent and ECSP.

A specific problem is the downward slope to the ETB Control function implemented in the ETBN device if those devices are only designed for SIL2 functions or less. This specific issue has already been discussed in [05]. In this case, the output of ETBN is not sufficiently trustable and a validity check needs to be done. Affected interface signals are listed and evaluated with respect to their criticality in Table 47.

Table 47: ETB Control interface signals criticality

Signal/Datum	Train condition	Failure Mode	Failure Criticality	Justification
etbStatus_Inhibit	Not inhibited	Inhibit indicated	low	Consequence is that there can be a new inauguration despite inhibit is indicated. But this does not violate the integrity of train inauguration itself and can be considered as an availability issue.
	inhibited	Inhibit not indicated	low	Can lead to an availability issue if inhibit is requested by local consist, but not indicated. So local consist may continue requesting inhibit and by this preventing new train inaugurations.
etbStatus_Length	No lengthening	lengthening indicated	low	May lead to a situation that local consist removes a local inhibit request although not necessary. If thereafter a real lengthening occurs, this might lead to an unwanted immediate inauguration.
	Lengthening	lengthening not indicated	low	Leads to an availability issue if inhibit is set by local consist.

Signal/Datum	Train condition	Failure Mode	Failure Criticality	Justification
etbStatus_Short A train shortening, while inauguration is inhibited, indicates the communication loss to at least one end consist. Cause can be a failure in the end consist, but also the unintended decoupling of the consist (train integrity violation)	no shortening	shortening indicated	low	Could be false alarm (detectable) or communication loss to last consist, leading to fail-safe state.
	shortening	shortening not indicated	low	Shortening can be communication loss to last consist or a decoupling. In both cases the exchange of operational data to the last consist gets lost, which is detectable and forces fail-safe state. False alarm if operational data exchange still possible.
etbStatus_Leading	No consist is leading	Leading indicated	high	A leading consist is sending commands to guided consists, therefore a failure, where leading is falsely indicated, is critical.
	This consist is leading	Leading not indicated	low	Leading consist sends no commands to guided consists. Is an availability issue.
	Another consist is leading	Leading indicated	high	A leading consist is sending commands to guided consists, therefore a failure, where leading is falsely indicated, is critical.
etbStatus_LeadingDir	Direction 1 is leading	Direction 2 is indicated	high	A leading consist is sending commands to guided consists, therefore a failure, where leading direction is incorrect, is critical as it could lead to wrong direction information.
	Direction 2 is leading	Direction 1 is indicated	high	A leading consist is sending commands to guided consists, therefore a failure, where leading direction is incorrect, is critical as it could lead to wrong direction information.
etbStatus_OpTrnDir	Not all consists have computed valid opTrnDir	"SHARED" is indicated	high	Risk that commands are sent and executed although not all consists are prepared for.

Signal/Datum	Train condition	Failure Mode	Failure Criticality	Justification
	All consists have computed valid opTrnDir	"INVALID" or "VALID" is indicated	low	The local consist is not allowed to send valid safety critical data, so train enters (or stays in) safe state. Is availability issue, but no safety issue.
etbStatus_OpTrnTopoCnt	Train composition change or leadership change has happened	Value not updated	high	Train composition change may not be detected if also TTDB is not updated.
	Train composition change or leadership change has happened	Wrong (invalid) value	low	Differs from value stored in TTDB Unable to validate received SDT data
	No train composition change or leadership change has happened	Changed value	low	Differs from value stored in TTDB Unable to validate received SDT data
etbStatus_isConfirmed	Train composition not confirmed	Confirmation is indicated	low	The NG-TCN safety principle is that the driver is not in the safety loop for function 'safe train inauguration'.
	Train composition is not confirmed	No confirmation indicated	low	

A validity check is required for all faults with high criticality. The validity of those signals can be checked by performing plausibility checks and by comparing to the TTDB (TI Validator). The safety check of the TTDB was already discussed in sub-chapter 3.5.4. Its relationship to the control signals is shown in Table 48.

Table 48: ETB Control interface signal failure detection

Signal/Datum	Related OTD parameters	Detection
etbStatus_Leading	isLead	Plausibility checked during TTDB validation: a consist can only become ²⁴ leading if leading has been requested before and there is no other leading consist.
etbStatus_LeadingDir	leadDir	Checked during TTDB validation: indicated leading direction must equal the requested leading direction.
etbStatus_OpTrnDir	opTrnDirState	Checked with TTDB validation and comparison of opTrnTopoCnt values received from all consists in status telegrams.
etbStatus_OpTrnTopoCnt	opTrnTopoCnt	Checked with TTDB validation and comparison of opTrnTopoCnt values received from all consists in status telegrams.

TTDB Info

General

The network application service “TTDB Info” allows all interested ED to retrieve information from the consist local TTDB repository. For the CCU, TTDB Info resides in the communication layers of the FDF as part of the communication&network services.

Architecture

The way how TTDB Info is supported is defined in IEC61375-2-3. This standard defines a TTDB Info interface (called “TTDB Manager interface” in the standard) between the ECSP and interested client ED. In our architecture model, this client is represented by the TTDB Agent. (see Figure 104). The TTDB agent is considered part of the FDF communication&network services responsible for the interaction of with the TTDB.

Figure 104 shows the complete system architecture with the ETBN device part (with ETBN, ECSP, TTDB manager and DNS server) as it is defined in IEC61375-2-3 and the CCU implementing FDF and TCMS applications. The TTDB agent receives the TTDB status and notification telegrams and reads the TTDB if there are changes in the train leadership or in the train composition (change of opTrnTopoCnt).

The TTDB agent shall maintain a local TTDB repository which is used for the TTDB validation by the TI Validator (sub-chapter 3.5.4) and also used by the FDF to configure the train wide data exchange between local applications and remote applications via ETB (see [07] for details).

²⁴ However, once a consist is leading, there can be another leading consist (leading conflict)

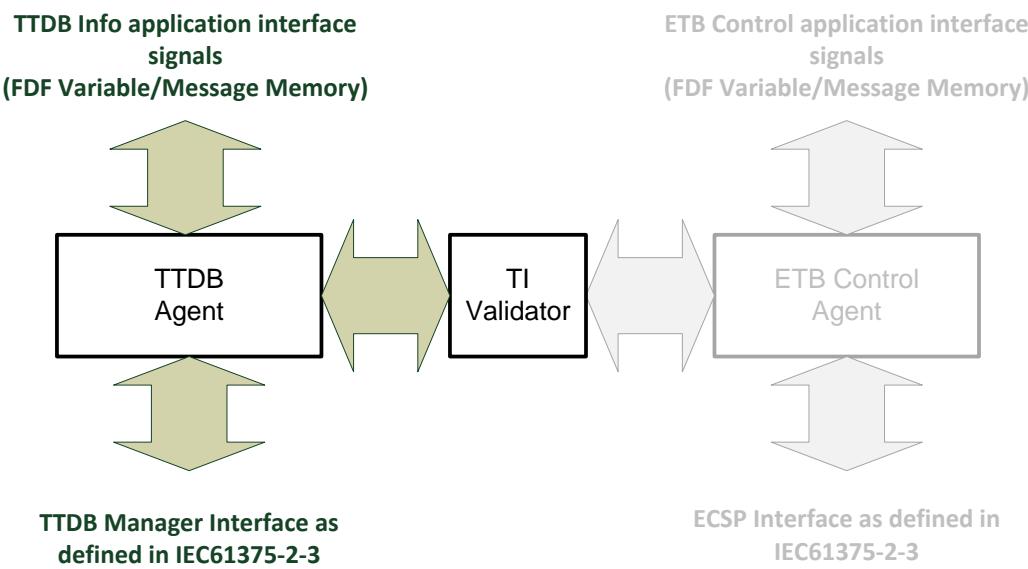


Figure 106: TTDB Agent interfaces

The TI Validator has the task, as defined in 3.5.4, to check the validity of the TTDB and to give clearance to high safety critical application for TTDB usage.

Clearance to ED-S supporting high safety integrity

The TI Validator is only active on the device that is responsible for ETB Control which is normally the CCU (the reason is that the TI Validator needs the information about leading requests). Other ED-S devices within the consist need to receive clearance from the TI Validator to use the TTDB. One possibility is that the TI Validator multicasts a status telegram (SDTv4 protected) to all interested ED-S within the consist which informs about:

- TTDB validation result (valid / invalid)
- The related opTrnTopoCnt value

For retrieving TTDB information, the TTDB manager interface as defined in IEC61375-2-3 can be used. Because its content (protected by the opCstCnt value) has already been validated by TI-validator, it can be used for high SIL applications.

ED-S cstUUID issue

For safe data transmission with SDTv2 or SDTv4, ED-S must know the cstUUID value of the own consist, because this parameter is part of the SID and not transmitted. This generates a problem for ED-S which cannot be (statically) preconfigured with the local cstUUID value and which are obliged to use a dynamic protocol to achieve this value. The standard way by making a TTDB inquiry will not work because TTDB inquiries are SDTv2 based and require the cstUUID – a classical hen-egg problem.

One solution could be that either ETBN or CCU distribute this information in an unsafe manner (non-safe data communication). Although this value is not trustable, it can be easily validated by using this value in the SDTv4 validation of the received TI-Validator status telegram.

It is proposed that the TTDB manager (IEC 61375-2-3) provides this information in a specific telegram.

SNMP

This sub-chapter uses references [52], [53], [54], [55] and [56].

General

The **Simple Network Management Protocol (SNMP)** is developed by the **Internet Engineering Task Force (IETF)** and it is the most popular protocol for monitoring and controlling of devices in an IP network, such as routers, switches, controllers, NAS appliances, and more, by a central **Network Management System (NMS)**. The most important tasks, for which SNMP is used, are

- **Monitoring of network components**, e.g. retrieval the number of received, sent or discarded IP packets of a specified ethernet port, internal measurements, such as CPU load, temperature, and so on.
- **Remote controlling and configuration of network components**, e.g. to bring an interface up or down, or to set an IP address.
- **Detection and reporting of failures**, e.g. to detect differences between the planned and the physically network topology or to take preventive measures by receiving an alarm when a defined threshold value has been exceeded.

Advantages of SNMP

The advantages of SNMP are as follows:

- Open protocol supported by many vendors.
- Widespread in Ethernet networks
- Many different network components are supported.
- Also supports event-driven communication with traps. This means less network load due to SNMP communication.

SNMP has a simple architecture, based on the manager/agent model consisting of a SNMP Manager, a SNMP agent, management information base, managed objects and the network protocol.

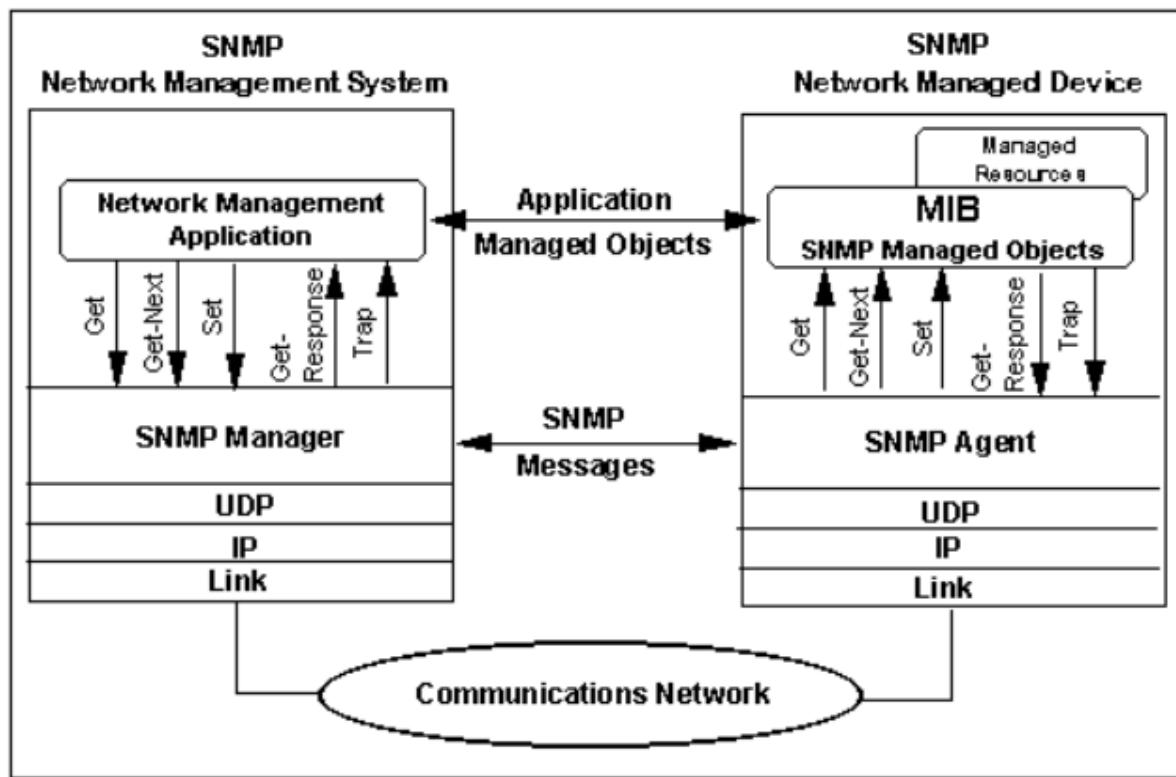


Figure 107: SNMP model

The **SNMP agent** is the software, runs on a managed device and maintains information about configuration and current state of database, containing the managed objects. It replies to the enquiry of the SNMP manager with the requested information.

The **SNMP manager** is an application program that contacts an SNMP agent to query or modify the database at the agent. It may be part of an NMS, or more simply, be a standalone tool known as an SNMP browser or MIB browser.

The manager and agent use a **Management Information Base (MIB)** and a relatively small set of commands to exchange information. The MIB is a collection of all MIB objects that can be called up or modified by the SNMP manager. It manages individual system aspects such as information about the managed nodes or statistical information about the throughput of packets, established connections, error messages, and so on.

The MIB objects are organized in a tree structure and formulated uniformly in an "Abstract Syntax Notation 1"-based collection of rules, the Structure of Management Information (SMI). The MIB objects are identified by a unique Object Identifier (OID). The OID describes the path through the hierarchically structured MIB tree to the required MIB object.

Example: The OID 1.3.6.1.2.1.1.1 is the path to the "sysDescr" object in the directory "system".

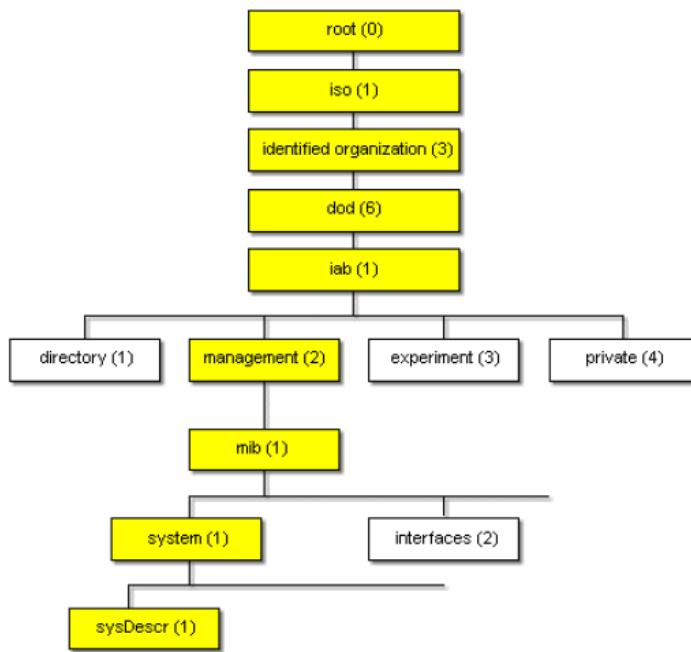


Figure 108: OID path to the “sysDescr” object

The MIBs are differentiated in two classifications:

Standardized MIBs are defined in RFCs and other standards.

With standardized MIB objects, the OID is fixed.

Two of the most important standardized MIBs are:

- MIB-II
- LLDP-MIB

Private MIBs are MIBs defined by vendors with product-specific expansions that are not included in the standard MIBs.

Private MIB objects are kept in the "enterprises" subdirectory. Within the private structure, the addresses are left up to the manufacturer. Only the manufacturer number needs to be registered to IANA. The OID can be represented as an ASCII character string.

SNMP protocol versions

SNMP has three official versions, SNMPv1, SNMPv2 and SNMPv3.

SNMPv1 made its first appearance in 1988 in a collection of RFCs starting with *RFC 1065* (updated in *RFC 1155 - 1157*). In 1991, *RFC 1156* was replaced by the *RFC 1213*, which defines the Version 2 of management information base (MIB-2). Version 1 has been criticized for its poor security. Authentication of clients is performed only by a “community string”, in effect a type of password, which is transmitted in cleartext.

SNMPv2 was introduced in 1993 with *RFC 1441*. Loosely speaking, SNMPv2 expanded on the basic information, starting with *RFC 1442* (currently *RFC 2578*). In general, SNMPv2 includes improvements in the areas of performance, security, confidentiality and manager-to-manager communication. Besides it introduced improved techniques for managing tables and two new PDUs (see Table 1).

SNMPv2 also included a proposed security mechanism, but it was largely rejected by the marketplace. Finally, with *RFC 1901* the version SNMPv2c, which used the SNMPv1 “community” security mechanism, was introduced.

SNMPv3 makes no changes of the protocol aside from the included model for reasonable effective security. In 2002 the final version of SNMPv3 is defined in *RFC 3414*. Due the weakness of security of SNMPv1 and SNMPv2, it is strictly recommended to use SNMP in the recent version 3.

SNMPv1 specifies five core PDUs to communicate between the manager and the agent. Two other PDUs, *GetBulkRequest* and *InformRequest* were added in SNMPv2.

Table 49: PDU types

PDU type	Description
GetRequest	A manager-to-agent request to retrieve the value of a variable or list of variables. Desired variables are specified in variable bindings. Retrieval of the specified variable values is to be done as an atomic operation by the agent. A response with current values is returned.
GetNextRequest	A manager-to-agent request to discover available variables and their values. Returns a response with variable binding for the lexicographically next variable in the MIB. The entire MIB of an agent can be walked by iterative application of <i>GetNextRequest</i> starting at OID 0. Rows of a table can be read by specifying column OIDs in the variable bindings of the request.
GetBulkRequest	A manager-to-agent request for multiple iterations of <i>GetNextRequest</i> . An optimized version of <i>GetNextRequest</i> . Returns a Response with multiple variable bindings walked from the variable binding or bindings in the request. PDU specific non-repeaters and max-repetitions fields are used to control response behaviour. <i>GetBulkRequest</i> was introduced in SNMPv2.
Response	Returns variable bindings and acknowledgement from agent to manager for <i>GetRequest</i> , <i>SetRequest</i> , <i>GetNextRequest</i> , <i>GetBulkRequest</i> and <i>InformRequest</i> . Error reporting is provided by error-status and error-index fields. Although it was used as a response to both gets and sets, this PDU was called <i>GetResponse</i> in SNMPv1.
SetRequest	A manager-to-agent request to change the value of a variable or list of variables. Variable bindings are specified in the body of the request. Changes to all specified variables are to be made as an atomic operation by the agent. A Response with (current) new values for the variables is returned.
Trap	Asynchronous notification from agent to manager. While in other SNMP communication, the manager actively requests information from the agent, these are PDUs that are sent from the agent to the manager without being explicitly requested. SNMP traps enable an agent to notify the management station of significant events by way of an unsolicited SNMP message. Trap PDUs include current <i>sysUpTime</i> value, an OID identifying the type of trap and optional variable bindings. Destination addressing for traps is determined in an application-specific manner typically through trap configuration variables in the MIB. The format of the trap message was changed in SNMPv2 and the PDU was renamed SNMPv2-Trap.
InformRequest	Acknowledged asynchronous notification. This PDU was introduced in SNMPv2 and was originally defined as manager to manager communication. Later implementations have loosened the original definition to allow agent to manager communications. Manager-to-manager notifications were already possible in SNMPv1 using a <i>Trap</i> , but as SNMP commonly runs over UDP where delivery is not assured and dropped packets are not reported, delivery of a Trap was not guaranteed. <i>InformRequest</i> fixes this as an acknowledgement is returned on receipt.

Example application of SNMP

- SNMP is suitable to take preventive measures when the discarded packets of an ethernet port of the network component rises sharply.
- port of a network component can be activated or deactivated using SNMP.

Authentication Server

The concept of network access control with the aid of an authentication server is described in 3.5.7.

TSN Gateway

The TSN Gateway (TSN-GW) is a function of the ETBN and is responsible for the transfer of scheduled data streams between ECN and ETB.

Concept

The fact that TSN telegrams are not routed between ECN and ETB (see 3.2.8) and the circumstance that ECN and ETB belong to different clock domains makes it necessary to define a TSN gateway function which is located in the ETBN (see 2.7).

All telegrams exchanged on ETB level are subject to standardization to achieve interoperability between consists of different types. This means that structure and content of ETB telegrams are defined. This restriction doesn't exist on ECN level – here it is up to the consist designer to define the telegrams to be exchanged between components on consist level. For generating the ETB level telegrams, basically two possibilities exist:

- 1) A CCU generates the ETB telegrams which are then 1:1 transferred to ETB. Reception is vice versa, received ETB telegrams are forwarded 1:1 to the CCU. This approach is useful in centralized consist designs, where all ETB communication is done by the CCU. Advantage of this approach is its simplicity, disadvantage is that subsystem data are first transferred to local CCU and then to ETB, which could be a problem for very time sensitive data.
- 2) ETB telegram data are generated by subsystems and shall be transferred to ETB without a CCU processing in the middle. Because a subsystem provides only a fraction of the data contained in an ETB telegram, a multiplexing function in the ETBN picks the relevant data from the subsystem telegram and places it into the ETB telegram. This leads to a n:m relationship used for the multiplexing (m = number of ECN telegrams, n = number of ETB telegrams). This approach is useful in decentralized consist designs. Advantage is the direct transfer of subsystem data to ETB, disadvantage is the complexity of a multiplexing function.

Possibility 2 inherently contains possibility 1 in the case of m,n = 1. As it is more flexible than possibility 1, possibility 2 is chosen for NG-TCN.

A further aspect is that the connection between the TSN-Gateway and an ED-S in the ECN must be configured as TSN link and must not interfere with possible other TSN links in that ECN. A CCU directly connected to a switch port of the ETBN based TSN Gateway would mitigate that influence.

Architecture

The principal design of the TSN-GW is shown in Figure 109 (the detailed design is task of the component developer, see also [10]). Because the TSN-GW connects two different VLANs (ETB-

TSN and ECN-TSN-A/B), see 3.2.6, and L3 routing cannot be used, the TSN-GW serves as a VLAN ED in both VLANs. Outbound TSN frames are sent from the ECN to the TSN-GW using the MAC address of the TSN-GW as destination address and are forwarded to the ETB with MAC address of the TSN-GW as source address. For inbound TSN frames it works vice versa. Clock domains are adapted by using schedulers on each side and buffers (telegram stores) in between for decoupling. Both the schedulers and the multiplexing need to be properly configured following application specific rules for train-wide TSN data transfer (see 3.2.8).

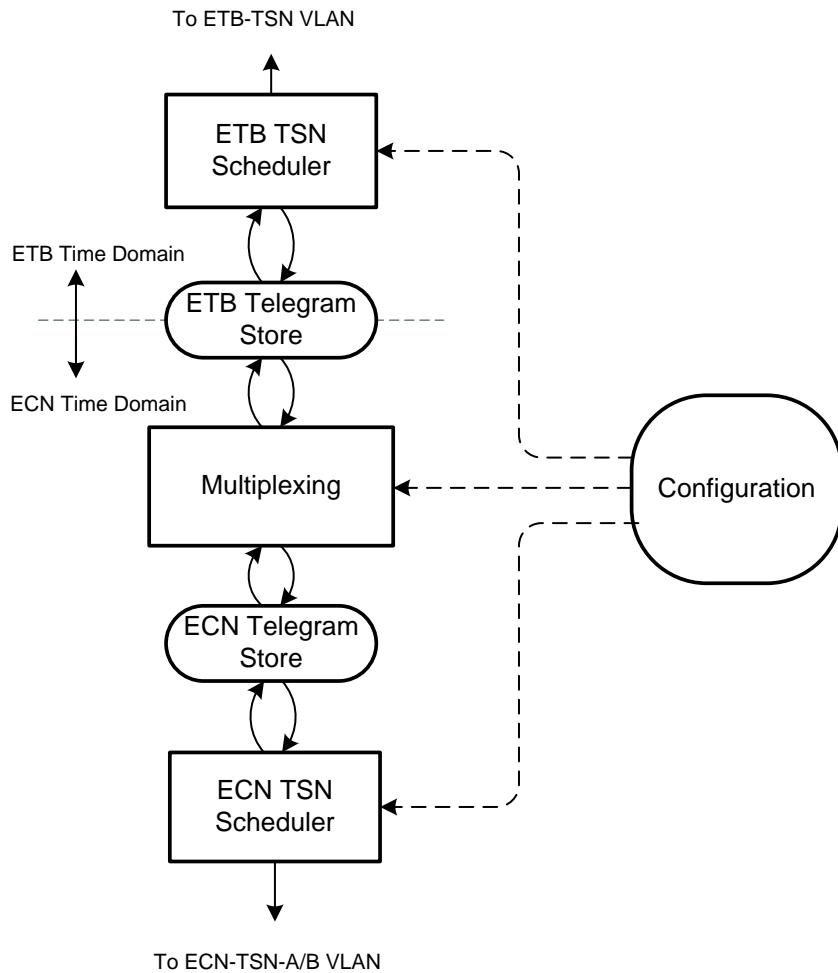


Figure 109: TSN Gateway architecture block diagram

Multiplexing

The Multiplexing function maps data blocks from ECN TSN-PD telegrams to ETB TSN-PD telegrams and vice versa. This process is illustrated in Figure 110 where the content of k ECN TSN-PD telegrams is mapped to one ETB TSN-PD telegram.

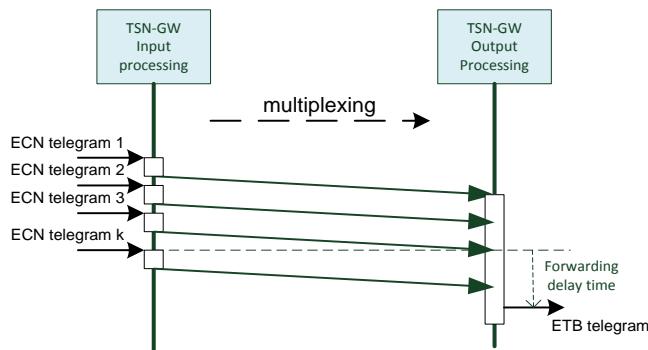


Figure 110: Multiplexing process

An important performance parameter is the forwarding delay time (FDT) of the TSN-GW. The FDT for the ECN to ETB direction is the time from the reception of the last ECN telegram, which contains data for the ETB telegram (telegram k in Figure 110), until the ETB telegram is prepared for sending²⁵. In ETB to ECN direction it is the time from reception of the ETB telegram until the last ECN telegram is prepared for sending.

ETB Scheduled Process Data

The definition of TSN-PD telegrams and related time schedules is primarily a task of CTA WP4. A simplified model of ETB scheduled traffic is shown in Figure 111. In this example, the leading consist is sending commands to all guided consits. All consists (including leading) send status data to all other consists.

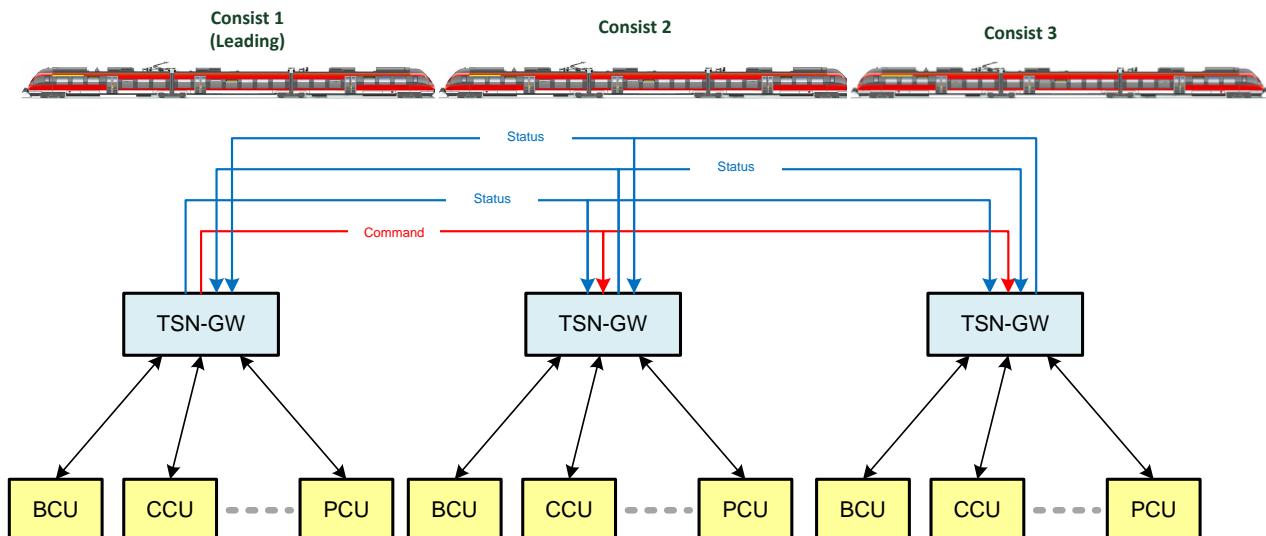


Figure 111: ETB communication pattern (example)

This model can be generalized:

- There can be multiple command/status streams

²⁵ The time when the telegram is actually sent depends on the schedule on ETB.

- The streams can also be video/audio, e.g. an audio announcement send to all consists
- Any consist holding a function master can send the commands

Because a consist can be in any position, there need to be predefined time slots on ETB which can be used. [10] proposed three time slots:

- Slot one repeating all 2.5 ms ($f_{slot} = 400$ Hz)
- Slot two repeating all 5 ms ($f_{slot} = 200$ Hz)
- Slot three repeating all 10 ms ($f_{slot} = 100$ Hz)

The bandwidth B_{slot} reserved for each time slot is defined by the gate opening time T_{slot} (see 3.2.8):

$$B_{slot} = T_{slot} \times f_{slot} \times B_{etb},$$

where B_{etb} is the ETB bandwidth in bit/s (NG-TCN ETB: 10^9 bit/s).

EXAMPLE: If T_{slot} of slot one is 0.5 ms ($5 \cdot 10^{-4}$ s), then $B_{slot} = 200$ Mbit/s

3.5.6 Network monitoring&diagnosis

Network monitoring and diagnosis system periodically records values of network performance metrics in order to measure network performance, identify performance anomalies, and determine root causes for the problems, preferably before NG-TCN performance is affected.

Network metrics

The most important performance metrics that are monitored include connectivity, delay, packet loss rate, and available bandwidth.

(1) **Network connectivity** is probably the most important metric for a network monitoring and diagnosis system, since the top priority of a network service is to guarantee that any pair of end nodes can communicate with each other. Due to its importance, all network layers, starting from the physical layer, should provide mechanisms to automatically monitor network connectivity.

(2) **Network delay** is perhaps one of the high significative performance metrics in regarding some ED application in NG-TCN. It could be monitored mainly at the end-to-end level using for example ping. Network delay to directly evaluate network path performance, especially for small data transmissions.

(3) **Packet loss rate** refers to the probability that a packet gets dropped on a network path. It is mainly monitored at router interfaces using SNMP packet statistics.

(4) **Available bandwidth** is another important performance metric, which directly captures data transmission speed. Although network delay can be used to evaluate the performance of a network path for small data transmissions, the available bandwidth metric is needed for larger data transmissions. However, available bandwidth is much less popular than the delay metric due to its high measurement overhead. People instead use the link load metric, which can be more easily measured (e.g., using SNMP),

Network performance measure

To capture available bandwidth information. Network performance metrics can either be measured at link level or at end-to-end level.

Link-level information is easy to obtain since most network devices support link level performance measurements. For example, link packet loss rate and link load can be measured using the SNMP protocol, and link connectivity can be monitored using routing protocol heart-beat messages. The problem with link-level monitoring, however, is that it is hard to extrapolate end-user performance purely based on link-level information.

- (a) fine-grain synchronization of the measurements on all the links along an end-to-end path is a hard-technical problem,
- (b) It is often not immediately clear how to assemble the performance information (e.g., path delay variance) from multiple links to infer that of the whole path.
- (c) The overhead of transmitting and managing each link-level measurement can be complex due to the large number of end users and the large number of links that each end-user may use.

End-to-end monitoring matches the experience of a real ED data transmission more closely.

Since end-to-end monitoring does not require network internal information, that's why end-to-end monitoring sometimes incurs much less measurement and management overhead. Despite, end-to-end monitoring also has an obvious problem: it is often hard to design a technique to measure end-to-end performance. Currently the two most popular end-to-end monitoring techniques are ping and traceroute. Both can be used for delay and connectivity measurements and traceroute is also popular for route measurements. It is much harder to obtain information on other metrics like packet loss rate and available bandwidth.

Active Monitoring:

The measurement device creates and injects some data into the monitored NG-TCN and observes the reaction of the network or/and a specific ND/ED. This approach allows to perform required tests whenever it is needed. On the other hand, it generates extra volume of an artificial network traffic. The examples of information discoverable by this technique are round-trip time, jitter.

Passive Monitoring:

The passive approach does not inject any data into the network line. The measurement device just silently watches all the data passing by. It records all the traffic or more often only a selected characteristic of the traffic passing by the device. This approach is typical e.g., for the flow monitoring.

Network monitoring technologies

This chapter introduces different technologies used for network monitoring. A network monitoring is the use of a system that constantly monitors a NG-TCN for problems caused by overloaded, crashed ND/ED, loose of network connections. In case of any trouble, the Network monitoring system should notify the failure to a network administrator via alarms for a proper management of the issue.

Monitoring Via SNMP

Monitoring via Simple Network Management Protocol (SNMP) is the most basic method of gathering bandwidth and network usage data.

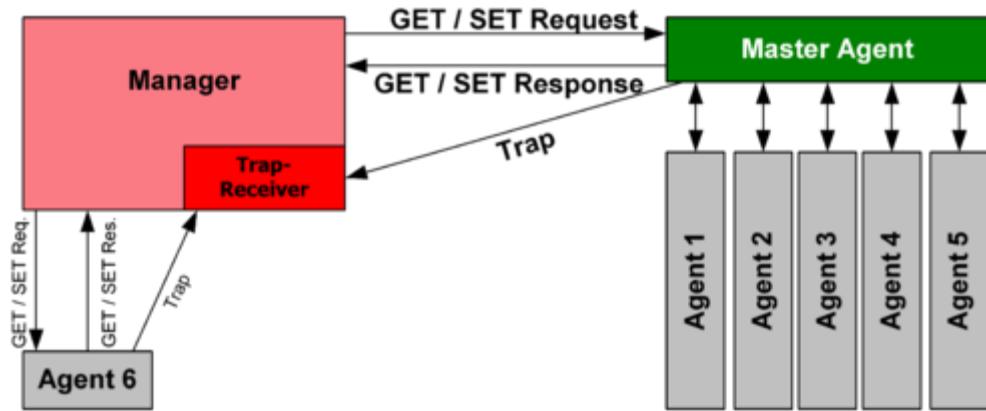


Figure 112: How SNMP Monitoring Works

In typical uses of SNMP, one or more administrative devices called Managers have the task of monitoring or managing a group of managed devices (network devices, EDs on NG-TCN). Each managed device executes a software component called an agent which reports information via SNMP to the manager.

An SNMP-managed network consists of four key components:

- Managed devices (any type of device, including, but not limited switches, routers, EDs)
- Agent— software which runs on managed devices
- Network management station (NMS)— software which runs on the manager
- Management information base (MIB)

A managed device is a network node that implements an SNMP interface that allows unidirectional (read-only) or bidirectional (read and write) access to node-specific information. Managed devices exchange node-specific information with the NMSs.

An agent is a network-management software module that resides on a managed device. An agent has local knowledge of management information and translates that information to or from an SNMP-specific form.

A network management station executes applications that monitor and control managed devices. NMSs provide the bulk of the processing and memory resources required for network management. One or more NMSs may exist on any managed network.

Management information base (MIB) SNMP agents expose management data on the managed systems as variables. The protocol also permits active management tasks, such as configuration changes, through remote modification of these variables. The variables accessible via SNMP are organized in hierarchies. SNMP itself does not define which variables a managed system should

offer. Rather, SNMP uses an extensible design which allows applications to define their own hierarchies. These hierarchies are described as a management information base (MIB). MIBs describe the structure of the management data of a device subsystem; they use a hierarchical namespace containing object identifiers (OID). Each OID identifies a variable that can be read or set via SNMP. MIBs use the notation defined by Structure of Management Information Version 2.0 (SMIv2, RFC2578), a subset of ASN.1.

SNMP Protocol Details

SNMP is the most commonly used method mainly because it is easy to set up and requires minimal bandwidth and CPU cycles. Besides network usage monitoring, another well-known feature of SNMP is the ability to also watch other network parameters such as CPU load, temperature, as well monitoring many other readings, depending on the queried device.

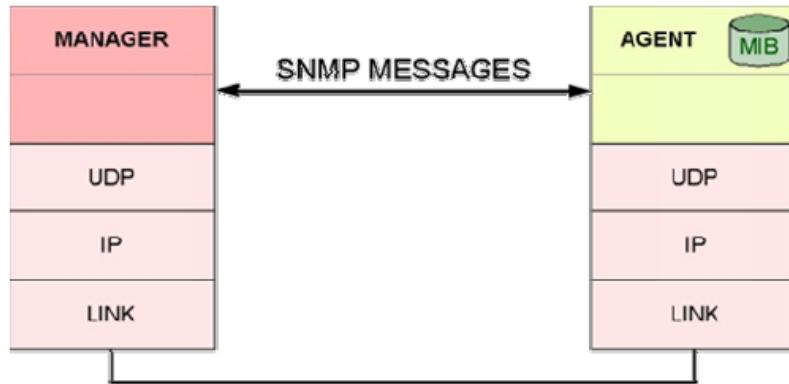


Figure 113: SNMP Details.

SNMP operates in the application layer of ND/EDs. All SNMP messages are transported via UDP. The SNMP agent receives requests on UDP port 161. The manager may send requests from any available source port to port 161 in the agent. The agent response is sent back to the source port on the manager. The manager receives notifications (Traps and InformRequests) on port 162. The agent may generate notifications from any available port.

SNMP implements three protocol versions:

- 1) SNMPv1 specifies five plus one core protocol data units PDUs: *GetRequest*, *SetRequest*, *GetNextRequest*, *GetBulkRequest*, *Response*, *Trap* (Asynchronous notification from agent to manager)
- 2) SNMPv2 added Two more PDUs, *GetBulkRequest* and *InformRequest*
- 3) SNMPv3 adds a *Report PDU*,

SNMPv3 focuses on two main aspects, namely security and administration. The security aspect is addressed by offering both strong authentication and data encryption for privacy.

SNMPv3 provides a secure environment for the management of systems providing protection at least against the following:

- Modification of Information – Protection against some unauthorized SNMP entity altering in-transit messages generated by an authorized principal.
- Masquerade – Protection against attempting management operations not authorized for some principal by assuming the identity of another principal that has the appropriate authorizations.
- Message Stream Modification – Protection against messages getting maliciously re-ordered, delayed, or replayed to effect unauthorized management operations.
- Disclosure – Protection against eavesdropping on the exchanges between SNMP engines.

Monitoring Bandwidth via Packet Sniffing

Packet Sniffing should come into consideration if ND/ED do not support SNMP or xFlow to measure bandwidth usage and it is requesting to differentiate the bandwidth usage by network protocol and/or IP addresses.

How Packet Sniffing works:

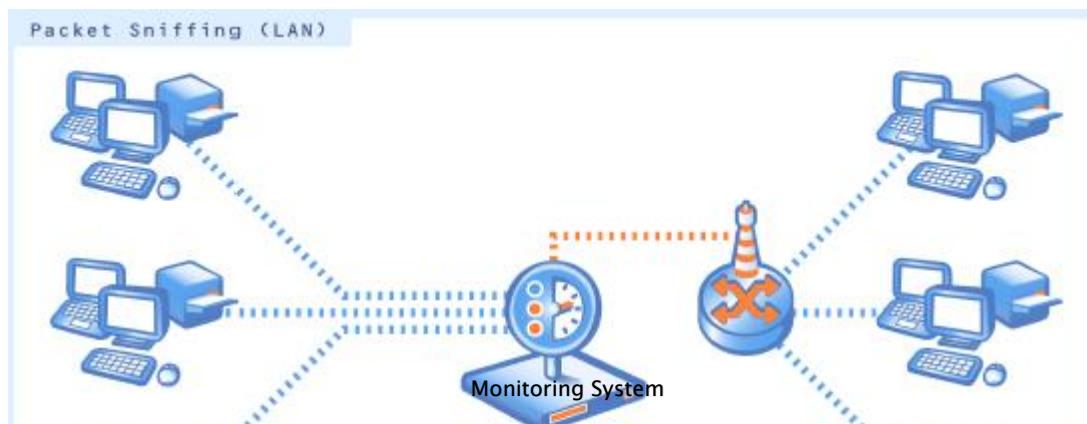


Figure 114: Packet Sniffing

Packet sniffer allows to know which applications or IP addresses are causing the traffic in NG-TCN network, Packet sniffer looks at every single data packet traveling through your network for accounting purposes.

In order to calculate bandwidth usage, the monitoring system can analyse and inspects all network data packets either passing network interface of ED (shown on the left side) or the data packets sent by a monitoring port of a switch (right side).

The packet sniffer can only access and inspect data packets that actually flow through the network interface(s) of the machine running the monitoring system software. This is fine if it is requested only to monitor the traffic of the monitoring system. If it is requested to monitor the traffic of ED/ND in NG-TCN, it must be used a switch that offers a "monitoring port" or "port mirroring" configuration. In this case the switch sends a copy to the monitoring port of all data packets traveling through the switch. As soon as monitoring system is connected to the switch's monitoring port, it is able to analyse the

complete traffic that passes through the switch. Another option is to set up the Monitoring system as the gateway for all ED/ND in the network.

Monitoring Bandwidth via Flows

Bandwidth usage by IP address or by application in a network, can be evaluated using one of the xFlow protocols. They are the best choice especially for networks with high traffic (connections with 100s of megabit or gigabits). For xFlow monitoring the router gathers bandwidth usage data (flows), aggregates them and sends information about these flows to Monitoring System using UDP packets. Because the switch already performs a pre-aggregation of traffic data, the flow of data to Monitoring System is much smaller than the monitored traffic. This makes xFlow the ideal option for high traffic networks that need to differentiate the bandwidth usage by network protocol and/or IP addresses.

NetFlow Monitoring

The NetFlow protocol is mainly used by Cisco devices. Once configured, the router sends for each data flow a NetFlow packet to the monitoring system. There the data can be filtered and evaluated.

There is different advantage of using NetFlow:

- NetFlow generates little CPU load on the router itself (according to Cisco 10,000 active flows create about 7% additional CPU load; 45,000 active flows account for about 20% additional CPU load).
- Generates less CPU load on the monitoring system, compared to packet sniffer sensors.

sFlow Monitoring

sFlow works similar to NetFlow monitoring. The router sends data flow packets to the monitoring system running. The most obvious difference between the two flow protocols: With sFlow, not all of the traffic is analysed, but only every n-th packet. The advantage is clear: There is less data to analyse, there is less CPU load needed and less monitoring traffic is generated.

Measurement Techniques

Measurement techniques can be classified based on the performance metric they measure. Since a same metric can be monitored at both the link-level and the end-to-end level, the corresponding techniques can be further labelled as link-level or end-to-end level monitoring techniques.

Link level network connectivity can be monitored using both physical-layer signals and IP-layer routing protocol heart-beat messages; while at the end-to-end level it is monitored using ping or traceroute.

The delay metric is measured using ping at both the link and end-to-end levels. However, link-level ping can only be done through the router command-line interface, i.e., manually, so it cannot be used directly by a monitoring system. That is a key motivation for developing link-delay inference techniques. One simple method is to ping the two ends of link and use the delay difference as an estimation of the link delay. Note that all these techniques measure the sum of propagation delay and queueing delay. None of them can directly quantify the queueing delay, which is an important metric for network congestion and delay variance. So far there have been no good techniques to quantify queueing delay, either at the link-level or at the end-to-end level-

The packet loss-rate metric at the link-level is measured using SNMP, which uses a counter to keep track of the total number of lost packets. End-to-end packet loss rate is hard to measure because packet loss is very bursty. A reasonable estimation of path loss often requires a large number of sampling packets, making overhead a major concern. Sting and Badabing are perhaps the two best known packet loss-rate measurement tools. Sting leverages the TCP protocol to identify packet losses on both the forward and reverse paths. It uses the fast retransmission feature of the TCP protocol to force the packet receiver to acknowledge each data packet, and then identifies packet loss by comparing data-packet sequence numbers and ack-packet sequence numbers. Badabing estimates path loss rate by measuring both the loss episode frequency and the loss episode duration, which are sampled using two-packet or three-packet probings.

Available bandwidth at the link-level is measured using link capacity and traffic load information. Internet link capacity is generally known a priori, and the traffic load can be calculated using the statistics collected by SNMP. At the end-to-end level, people generally use tools like iperf or ttcp which use TCP flows' transmission performance in order to quantify path available bandwidth. Note these tools measure TCP achievable throughput, not the available bandwidth (i.e., the residual bandwidth). This is because TCP achievable throughput is not only determined by the available bandwidth of the path, it is also affected by the level of multiplexing of background traffic flows and system configuration parameters such as TCP buffer sizes.

3.5.7 Security

Firewalls

Firewalls (see 3.3.3) monitor all network traffic and can be configured to either allow or block connections and communication based on specific criteria, which comprise among others IP addresses and TCP/UDP ports. A firewall enforces a set of rules what data packets will be allowed to enter or leave a network.

Firewalls are typically categorized in *network-based firewalls* and *host-based firewalls*.

Network-based firewalls

Network-based firewalls handle traffic between networks. They are not installed on the devices they are supposed to protect but on a separate machine which interconnects the untrusted public network and the trusted secured network. The devices within the trusted network are not affected by the firewall, they neither require installation of additional software nor specific configuration. Also, the firewall does not monitor or filter communication between devices within the trusted network.

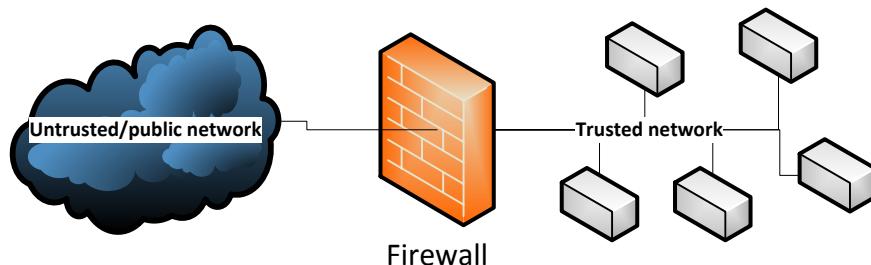


Figure 115: Illustration of a network-based firewall

Host-based firewalls

Host-based firewalls monitor and filter the traffic between the host device on which they are installed and the networks the host device is connected to. A trusted network does not necessarily exist. Host-based firewalls impose higher requirements on the host devices since they require installation of the additional firewall software as well as host-specific firewall configuration.

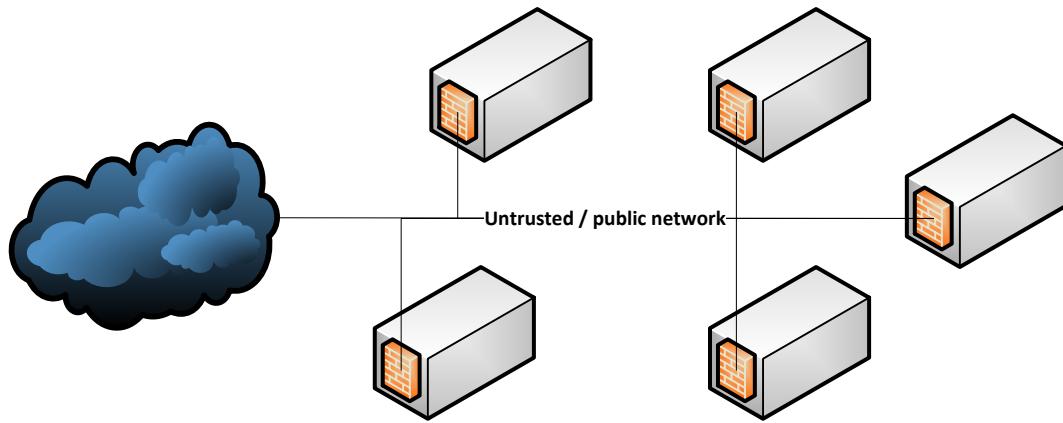


Figure 116: Illustration of a network with host-based firewalls

Topology

Within TCMS and OOS scopes, network-based firewalls could best be utilized in the conduits between various zones and the devices serving as gateways between the zones, respectively.

- Conduit TCMS_Constist_Regular_Safety
- Conduit RM_TCMS-Regular
- Conduit OOS_TCMS
- Conduit MAR_TCMS, Conduit MAR_OOS (or within MCG)
- Conduit RM_OOS_Wired, Conduit RM_OOS_Wireless
- Conduit COS_OOS
- Conduit ETBN_TCMS_Constist_R, ETBN_TCMS_Constist_S, ETBN_OOS

Figure 117 and Figure 118 show reasonable locations of firewalls within the TCMS and OOS domains.

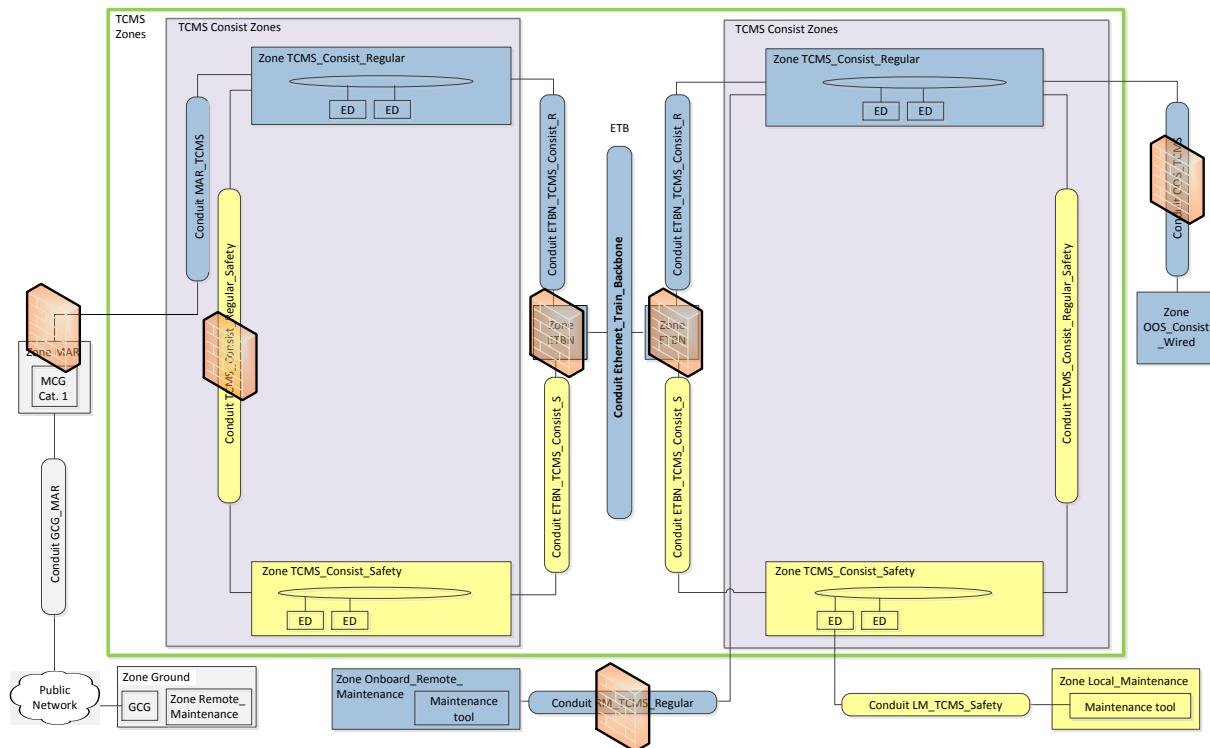


Figure 117: Firewalls in TCMS domain

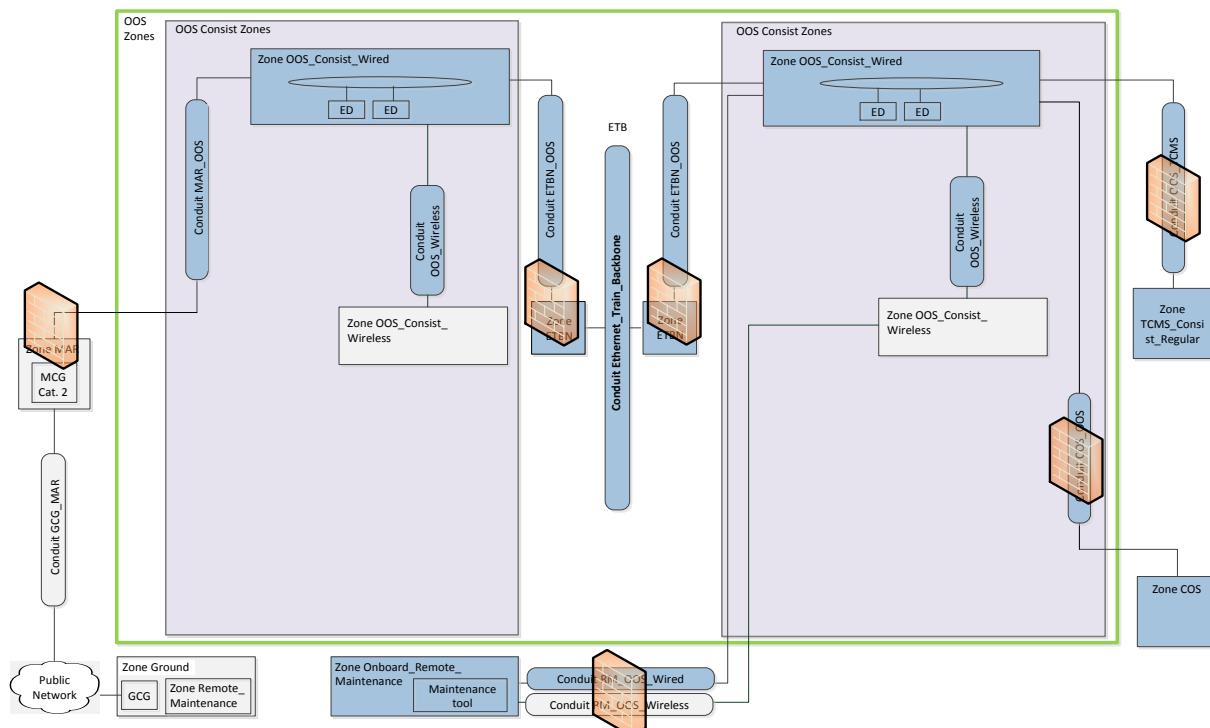


Figure 118: Firewalls in OOS domain

Security event detection

Besides preventive measures like firewalls and network access control, it is also important to be able to detect (potential) security violations and to track this information. This can then be used for further analysis, which is helpful for deriving of new measures or enhancing existing ones. That implies every network component and end device, which incorporates security related functions, needs to be able to detect certain kind of security events and to inform a central system with logging capabilities inside the consist in case of occurrence. As protocol for transmission of security events to this logging system the standard syslog is proposed. This gives also the possibility to use an existing software solution on server side like the open source software rsyslog.

The following events shall be supported by NG-TCN:

Table 50: NG-TCN security events

Topic	Meaning
Cabinet door opened	If a cabinet door (or cover panel) with devices behind is opened, a sensor system creates a log message including the location of sensor.
Cabinet door closed	If a cabinet door (or cover panel) with devices behind is closed, a sensor system creates a log message including the location of sensor.
Login Successful	If a user logs in, the concerned device creates a log message including the user name.
Login Fail	If a user login try fails, the concerned device creates a log message including the user name and the connection details of the client.
Account modification	An end device generates an audit log message whenever any of the following events occur: <ul style="list-style-type: none"> - Creation of a new user account; - Deletion of a user account; or - Modification of the privilege level, or group membership, of a user account
Privilege escalation	An end device generates an audit log message whenever any of the following events occurs: <ul style="list-style-type: none"> - A user spawns a shell, terminal or other application or command using different user credentials than his own (e.g. uses sudo); or - A user changes his effective user credentials, group membership, privilege level, or similar credentials (e.g. uses su).
Credential modification	An end device generates an audit log message whenever any of the following events occurs. <ul style="list-style-type: none"> - A user changes his password or any other persistent authentication token; - A user password or other authentication token is changed for any other reason, or - Grant, modify, or revoke access rights, including adding a new user or group, changing user privilege levels, changing file permissions, changing database object permissions
Firewall activation	When the firewall is taken up during system operation, the concerned device generates firewall log messages.
Firewall deactivation	When the firewall is taken down during system operation, the concerned device generates firewall log messages.
Firewall reconfiguration	When the firewall is reconfigured, reinitialized, or reloaded at runtime, the concerned device generates firewall log messages.

Topic	Meaning
Unexpected incoming traffic	<p>When unexpected traffic is received on the external interface, the concerned device generates a firewall log message.</p> <p>Note: The firewalls are configured via a white list. All traffic not included in the white list is unexpected.</p> <p>This applies only to the internal firewall between network zones.</p>
Application startup	An end device sends log messages whenever an application is started.
Application shutdown	An end device sends log messages whenever an application is shut down.
Application software update	An end device sends this log message whenever an attempt is made to update application software and specify whether the attempt was successful. The log message should also include the previous and current version numbers of the software
System service startup	A device sends this message whenever a security-related system service is started.
System service shutdown	A device sends this message whenever a security-related system service gets shut down.
System startup	A device sends this message whenever the system as a whole starts up or enters an operational state. Message shall include run level and firmware version.
System reboot	A device sends this message whenever the system gets rebooted.
System shutdown	A device sends this message whenever the system gets shut down.
System software update	A device sends this log message whenever an attempt is made to update the system software and specify whether the attempt was successful. The log message should also include the previous and current version numbers of the software.
Maintenance Mode Entry	A device that support a dedicated maintenance mode, used for testing, debugging, fault-finding or software updates or similar tasks, send this log message when entering this mode.
Maintenance Mode Exit	A device that support a dedicated maintenance mode, used for testing, debugging, fault-finding or software updates or similar tasks, send this log message when exiting this mode.
Valid PNAC credentials	Network devices generate a log message whenever a connected end device attempts to use a supported authentication method and uses valid credentials.
Invalid PNAC credentials	Network devices generate a log message whenever a connected end device attempts to use a supported authentication method but uses invalid credentials, or an unsupported authentication method.
Physical or link layer loss	Network devices generate a log message whenever a connection loss to an externally accessible device is detected on the physical or link layer. This only applies to the originator device to which the externally accessible device was directly connected.
Physical or link layer up	Network devices generate a log message whenever a connection to an externally accessible device is established on the physical or link layer. This only applies to the originator device to which the externally accessible device is directly connected.
Messages dropped	Devices generate this message when they drop log messages to prevent a flooding of the network. The text of the message should contain the number of messages dropped if known.
Unknown host identifier	Network devices which act as DHCP servers or relays generate a log message whenever a DHCP request message is received containing a host identifier which is either unknown, already active in use, or expected to be used on a different physical port.

Encryption

Encrypted transmission makes it unfeasible for attackers to read, reverse-engineer and falsify communication. Encryption could be either used throughout zones, i.e. also on all EDs or only for selected conduits. Using encryption on all EDs would be expensive, though, since encryption is compute-intensive and might be problematic for less powerful devices, such as for instance I/O units.

There are two basic encryption methods:

- Symmetric encryption

In this scheme, both sender and receiver of a transmission use the same key for encryption and decryption of the data. If attackers gain knowledge of this single key, they can both decrypt and encrypt any message.

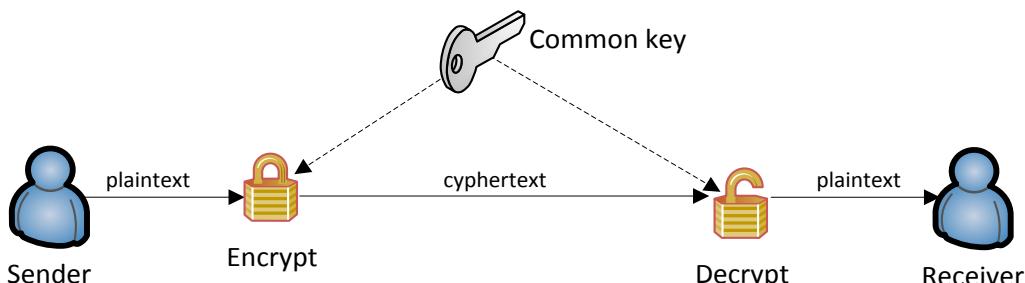


Figure 119: Symmetric encryption

- Asymmetric encryption (public-key cryptography)

In an asymmetric encryption scheme, multiple keys are involved. Each participant has a key pair consisting of a private key which is kept secret and a public key which can be known by every participant. When sending a message, the sender uses the public key of the intended receiver of the message to encrypt the transmission. Decryption of the message is only possible with the receiver's private key, thus only the intended receiver can decipher the message.

In addition, the sender can *sign* a message using his own private key. This enables the receiver to use the sender's public key to validate that the message did indeed originate from the claimed sender and not from an imposter.

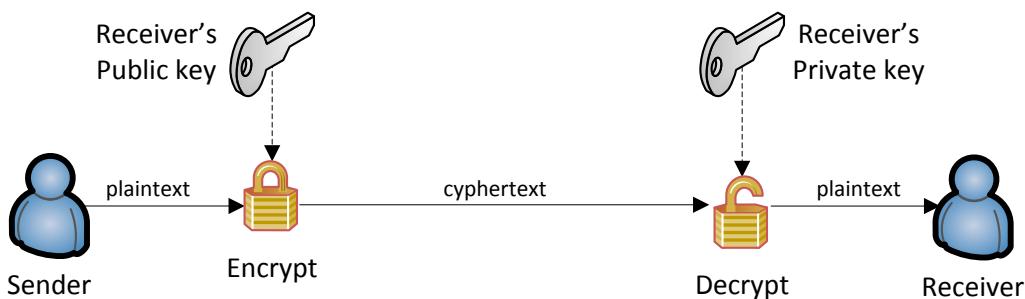


Figure 120: Asymmetric encryption

A problem common to both methods is the required key management, particularly for asymmetric encryption due to the higher number of keys involved.

As mentioned in 3.2.11 the proposed encryption technique for NG-TCN is Media Access Control Security (MACsec), which is based on symmetric cryptographic keys. However, these keys can be exchanged through an asymmetric encryption process as described in following chapter.

Network access control

As shown by security analysis done in CTA Task 3.3 [05], gaining access to the network is a necessary initial – but also elementary – step for subsequent activities which may be potentially harmful. Therefore, it is important to focus attention on accessing the network. A first measure for protection against local attackers are physical barriers as described in 3.1.5. However not every device and network port can be protected in this way like a PIS display, which is located in the passenger compartment. For such exposed devices (and network ports) further measures shall be considered. Sub-chapter 3.2.11 already introduced Port Based Network Access Control (PNAC) for this use case. As described also, PNAC can be used to exchange security keys for MACsec encryption. Therefore, it is appropriate to use encryption in conjunction with authentication.

The following figure depicts the different roles for authentication.

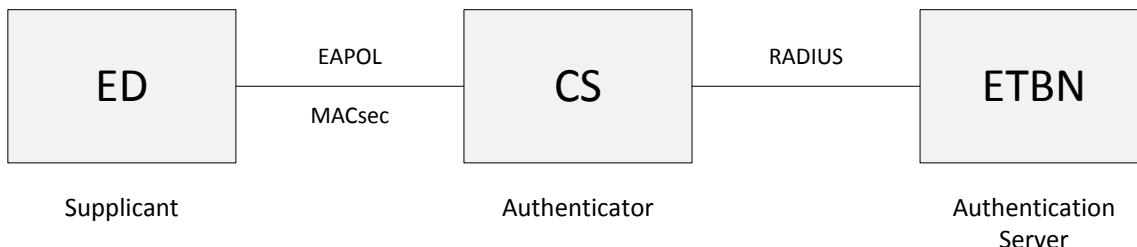


Figure 121: PNAC and MACsec overview

The **supplicant** is an End Device (such as a CCTV camera or service laptop) that wishes to attach to the network – though the term 'supplicant' is also used interchangeably to refer to the software running on the client that provides credentials to the authenticator. Supplicants need to support EAPOL as encapsulation technique and certain EAP methods (see below) to be able to authenticate. Furthermore, support for MACsec is needed preferably in hardware.

The **authenticator** is the network access device – in case of NG-TCN the CS, where the supplicant is directly connected – that facilitates the authentication process by relaying the supplicant's credentials to the authentication server. The authenticator enforces the network access policy, including MACsec. Like the supplicant, the authenticator must be capable of MACsec key negotiation and packet encryption. The authenticator shall integrate MACsec in hardware to support encryption at line rate.

The **authentication server** validates the supplicant's credentials and determines what kind of network access the supplicant should receive. The industry standard essentially is a RADIUS server, which is also sufficient for NG-TCN. At least two servers should be placed in a consist for redundancy reasons. Therefore, it makes sense to allocate this functionality to the CMS or to the CCU. Like the supplicant, the authentication server needs to support certain EAP methods as described in next paragraph. In MACsec, the authentication server plays an important role in the distribution of master keying material to the supplicant and authenticator. In addition, the authentication server can define the MACsec policy to be applied to a particular endpoint.

Authentication (EAP) methods

EAP is not only a protocol, but also a generic authentication framework that supports many different types of authentication methods with different characteristics. The additional use of MACsec reduces the amount of possible methods because MACsec requires an EAP method that supports the derivation of a master session key (MSK). Therefore, the following EAP methods are recommended for NG-TCN:

- EAP Transport Layer Security (EAP-TLS): This method uses a TLS handshake to mutually authenticate a client and a server. Hence, certificates need to be provided to servers as well as to clients.
- Protected EAP (PEAP) or EAP Tunneled Transport Layer Security (EAP-TTLS) with a chosen encapsulated protocol like Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAPv2): These two methods extend the EAP-TLS mechanism in the way that they use the TLS handshake to establish a secure connection. The secure connection is then used to authenticate the client. For this purpose, several mechanisms are available e.g. password-based authentication protocols like MSCHAPv2. Depending on server configuration mutual authentication during TLS handshake is applied. This allows to operate clients with and without certificates in parallel.

Key management

All the mentioned EAP methods are using certificates, which are used also at the end to generate the keys for encryption. Since certificates needs to be installed on clients as well as on authentication servers, key management needs to be introduced. Additionally, certificates are normally limited in time, so that an update concept needs also to be considered in key management.

4 NG-TCN CONFIGURATION AND SET-UP

4.1 START-UP / SHUT-DOWN

Startup

The network startup behaviour depends on the start-up of its individual network components. Even if all network devices are powered the same time, the time until individual network components become operational varies. Important in this context are the dependencies between ND and between ND and ED.

ND-ND dependencies:

- CS can become fully operational after the ECN ring has been established with all other CS. In that case the ring protocol has to smoothly integrate the CS.
- ETBN can become fully operational after train inauguration between other ETBN is finished and the TTDB is setup ('late insertion').

ND-ED dependencies:

- ED depending on DHCP can become fully operational before the DHCP server located in the network is setup. In this case the ED has to wait until DHCP is available and shall not start with a temporary or default IP address.
- In the same way, TSN-aware ED have to synchronize their time before starting any application data transfer.
- ED can become fully operational before the ECSP server located in the CMS is setup and started to send ECSP status telegrams (and is ready to provide TTDB access). ED should block application data transfer until ECSP is available and signals that everything is setup.

From an ED perspective the NG-TCN can be considered operational if ECSP status telegrams are received and the ED is informed about the train setup. This process is depicted in Figure 122 and described in Table 51.

ED functions with high safety integrity have in addition to wait for clearance by the TI-Validator.

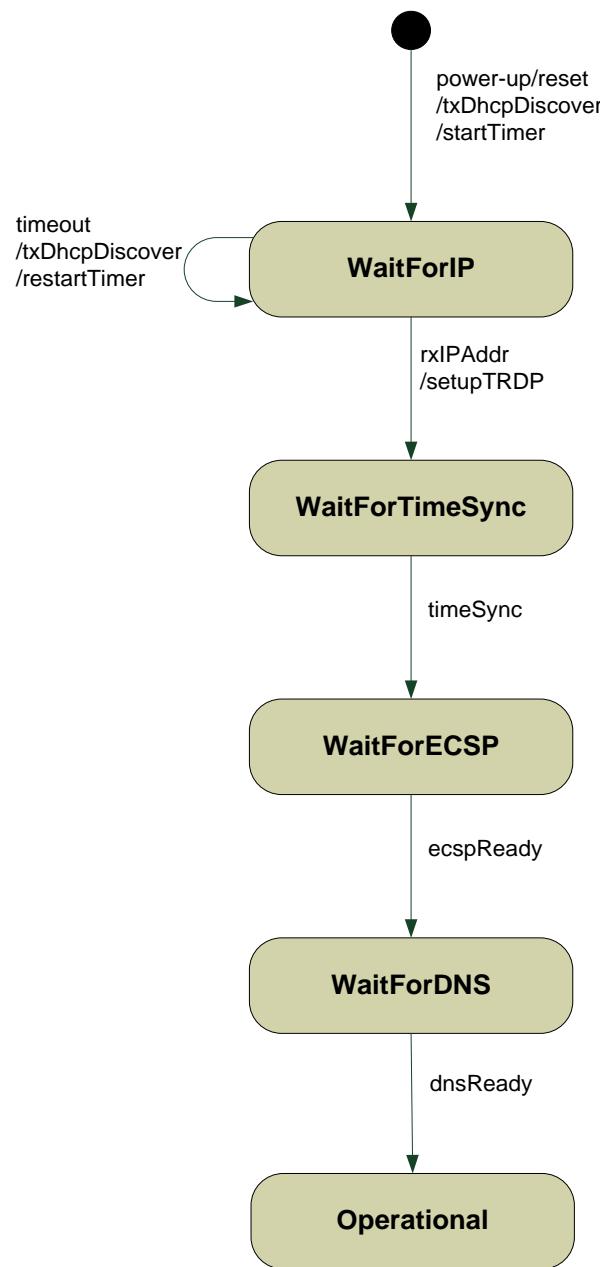


Figure 122: ED start-up state machine

Table 51: ED start-up state machine

Trigger	Description
powerup/reset	Power up or reset
rxIpAddr	IP address received from DHCP
timeSync	Time synchronized with master clock(s)
ecspReady	ECSP status telegram received and opTrnDirState == SHARED (see [18])
dnsReady	TDB status telegram [18] received indicating that TTDB is setup and DNS prepared for address resolution

Action	Description
(re)startTimer	Setup a timer
txDhcpDiscover	Send DHCP discover telegrams
setupTRDP	Configure TRDP for sending/receiving of TSN and conventional frames
State	Description
WaitForIP	Wait for IP address assignment (DHCP server)
WaitForTimeSync	Wait for time synchronization with master clock(s)
WaitForECSP	Wait for ECSP readiness
WaitForDNS	Wait for TTDB manager and DNS server
Operational	ED is operational, application data transfer can be started.

Shutdown

There exists no specific process for the shut-down of the network. This can be simply done by cutting the power to the ND. The NDs shall be designed in a way that a sudden loss of power will not lead to inconsistencies or corruption of permanently stored data²⁶.

4.2 NETWORK CONFIGURATION (STATIC)

This subchapter is focused on the static configuration of the network within the NG-TCN.

Configuration of the End Devices is out of the scope of this task and only configuration of the network devices within the NG-TCN (ETBNs and Consist Switches) is analysed.

In the context of NG-TCN, the configuration of the network cannot be completely static, in fact, coupling and decoupling of the consists forces to have a train wide dynamic network making the network configuration more complex. As the dynamic behaviour of the network due to new train topologies has been covered in previous chapters of the document, this chapter is focused on the static configuration of the network.

A detailed configuration depends on specific implementations; hence this chapter describes only some common aspects of the configuration to be considered in NG-TCN. On the one hand, the main aspects to configure in the network devices are briefly explained, and on the other hand, some rules for the method of configuration are proposed.

²⁶ Typical those devices have capacitors which hold the power for a couple of milliseconds after power loss. During this time some basic housekeeping can be done to ensure a proper shutdown of the device.

4.2.1 Static data to be configured

The services to configure statically in the network devices of the NG-TCN are listed in the following table although the detailed data for each of the functionalities is not specified.

Static configuration of NG-TCN network devices		
Device	Info	Description
- ETBN - Consist switch	IP address	Static IP addresses of the switches shall be set.
- ETBN	DHCP server	When DHCP is available for dynamic IP addressing and the ECSP is located within the ETBN, the DHCP server shall be configured.
- ETBN	DNS server	When ECSP is located within the ETBN, the DNS server shall be configured for translation of IP addresses.
- ETBN - Consist switch	Port settings	Port assignment and ingress and egress policing configuration shall be set.
- ETBN - Consist switch	VLAN configuration	For traffic distinction within the networks as well as for network management, VLAN configuration shall be set in the network devices ports. More detailed information about this configuration can be found in the chapter 3.2.6 of this deliverable.
- ETBN - Consist switch	TSN settings	Scheduled data streams must be predefined according to application specific requirements.
- ETBN	ETB Gateway	When the gateway is located within the ETBN, the configuration for ETB/ECN data mapping and the configuration of the ETB/ECN scheduled data shall be set.
- ETBN	Static consist information	When ECSP is located within the ETBN, the static consist information as detailed in [18] shall be configured.
- ETBN	Safe transmission of inauguration data	In case a safe transmission of the inauguration data between the ETBN and the CCU is needed as explained in the chapter 3.5.4, the SDT layer configuration for that communication shall be set.
- Consist switch	Ring protocol settings	Ring protocol settings for the ECN shall be configured such as the master or manager assignment, or the blocked port to interrupt the ring.

Table 52: Static configuration for network devices

4.2.2 Requirements and method for network configuration

As already stated, the configuration of the system will be implementation specific, and the methodology of configuration as well will be manufacturer dependant. Thus, this specification does not aim to define a specific way of configuring but only some general rules and recommendations.

On the one hand, regarding the configuration of safety-related data, it has to be taken into account that the generation and installation of this data, along with any tool to produce the data, shall follow the rules defined in the standards EN 50126-1/2 [13][14] in accordance to the SIL of the data to be configured.

On the other hand, when regarding security, as already defined in the requirements defined in D3.1[03], TCN resources shall be securely configured:

ID_60061	NG TCN shall provide following Security protections: 1) NG TCN shall Protect against malicious access to TCN resources 2) NG TCN shall ensure secure configuration of TCN resources 3) NG TCN shall Provide secure platform communication over all ED, ED-S 4) NG TCN shall Provide secure wireless train to ground communication 5) NG TCN shall Provide secure wireless intra consist communication
----------	---

Finally, for the installation of the static configuration data defined in Table 52, different use cases have been identified.

- Configuration at start-up phase.
- Configuration of a network device after a maintenance action.
- Configuration of consist switches when inserting new vehicles to the consist.

The idea is that all switches would have the complete configuration information of all the devices, so at start-up phase this data should be configured in all of them and each one would select the corresponding one depending on its location. Each switch should solve its location within the network and load the corresponding configuration among all the configurations.

In the second case, only the switches that have been repaired after an error need to be configured and it is assumed that the rest of the network devices have already the complete configuration of the network (uploaded at start-up). When replacing the device, this has to be configured again and there could be different methods to do it. In a similar way to the initialization, the complete configuration could be preloaded to the switch and then select the correct one. However, another option could be an auto-configuration through the neighbour network devices. The re-started switch could obtain its configuration from the neighbour switches that would know the location of it. In order to carry out this auto-configuration, a suitable protocol among the network devices should be defined and implemented. The idea behind is to avoid human errors that could occur when re-installing the network devices during maintenance phase.

The third case is similar to the previous one, when inserting new vehicles to the consist, the new consist switches need to be configured completely, and this could be done pre-loading directly the whole configuration or with an auto-configuration algorithm. The auto-configuration could be done

loading the required data from an existing consist switch. As mentioned previously, to carry this out, a suitable algorithm and protocol should be defined.

These configuration methods are only some possibilities to configure the required static data into the network devices of the NG-TCN in order to have a “simple” and reliable configuration method in such a complex system.

4.3 DOWNLOAD

The main goal of this section is to explore and analyse the download capabilities in NG-TCN. In particular, the focus is on the needed configuration aspects of the NG-TCN for assuring that downloading capabilities are available and properly configured.

This section first identifies the applicable scenarios, then evaluates possible download strategies and, finally, provides possible download configuration examples using the SNMP (Simple Network Management Protocol).

SNMP has been used because, as stated in A and in section 3.5.5, it is assumed that each device in the NG-TCN will run an SNMP agent; SNMP gathers all the data from network devices and allows to track issues, to make decisions based on real data, and to take control wherever necessary. SNMP fits use cases in which the network monitoring as well configuration is required, as per our scenarios.

The capability to allow download operations for remote diagnostic, as well as remote software updates, or for remote dynamic network configuration updates, is required in several stages of a train’s lifetime: from the manufacturing, through maintenance, till the operational stage.

Two main scenarios have been foreseen and, hence, considered for such analysis:

1. The download operation from a remote control room to the train. A practical example for this scenario is the case in which a bug is discovered in an ED, ED-S or ND and a software update (e.g., a software patch) shall be delivered (hence, downloaded) and installed. Other scenarios are:
 - The download of a remote NG-TCN configuration; when the train is in standstill or in maintenance, it could asynchronously receive a request for downloading network configuration updates;
 - The download of software updates (e.g., patches or new firmware versions) for NG-TCN ED, ED-S or NG (as reported at point 1);
2. The download operation from within the train (e.g., from an ED, ED-S or ND) to the outside (e.g., a remote control room); this is the case in which it is necessary to obtain, for example, diagnostic information from an ED, ED-S or ND. Therefore, it shall be possible to:
 - Download logs from ED, ED-S, NG in a NG-TCN;
 - Download diagnostic information for ED, ED-S or ND.

In order to assure that all those functionalities could be exposed and be available, proper configurations actions are required. As it is assumed the use of SNMP for network management and

diagnosis, the following diagram has been proposed for assuring that each of the ED composing the NG-TCN has the correct SNMP configuration.

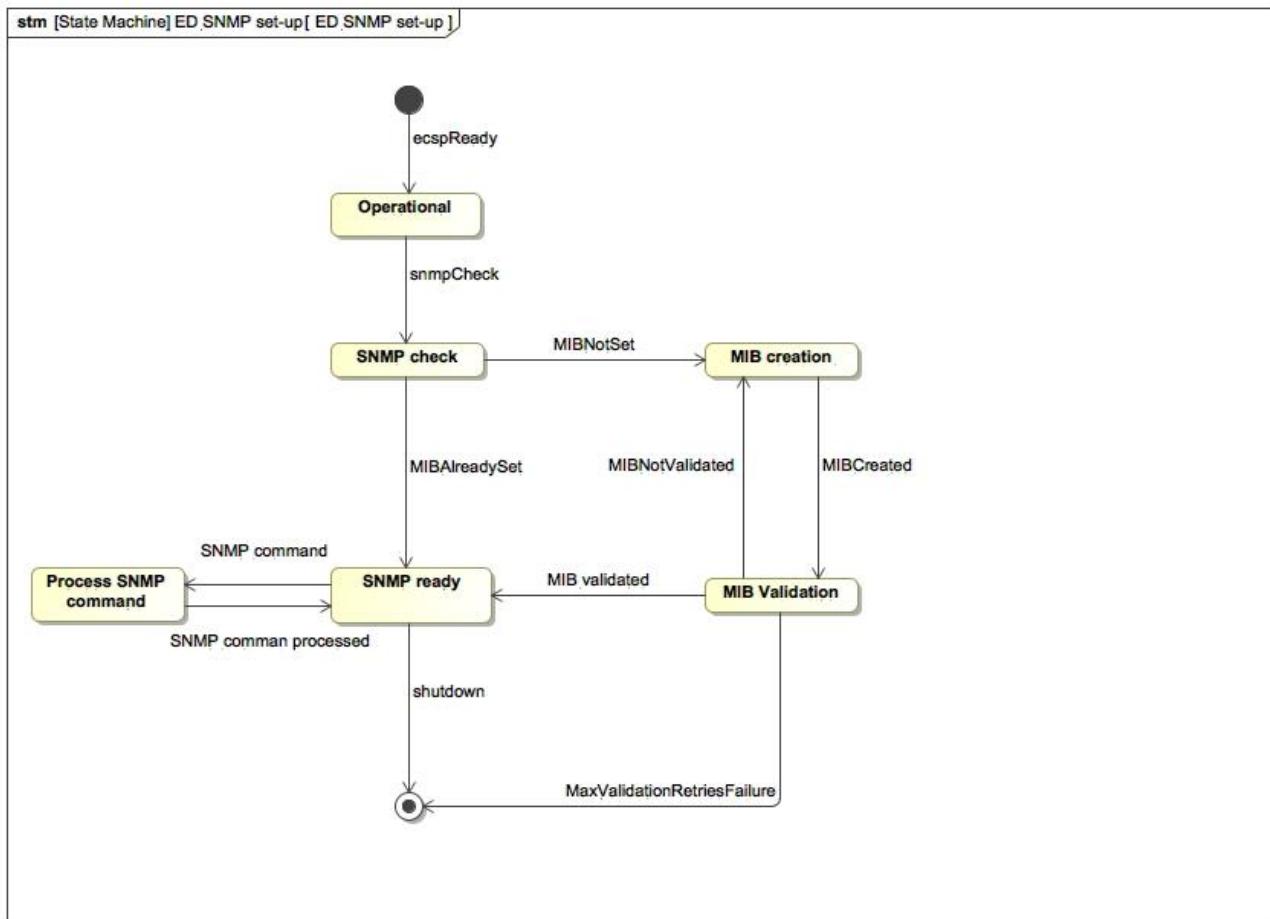


Figure 123: SNMP set-up for ED, ED-S and ND

In Table 53, the triggers are listed that enable state transitions and a description of each of the states characterising the diagram.

Table 53 - ED SNMP set-up state machine

Trigger	Description
ecspReady	ECSP status telegram received and opTrnDirState == SHARED (see [18])
snmpCheck	As soon as the ED, ED-S or ND is in the operational state a check on its SNMP configuration is requested
MIBNotSet	The MIB (Management Information Base) is not set on the ED
MIBAlreadySet	The MIB is present and up-to-date
MIBCreated	The MIB has been created
MIBNotValidated	The created MIB contains errors and, hence, has not been correctly validated. A re-creation shall be tried for <i>MaxRetries</i> times
MIBValidated	The MIB has been successfully validated
MaxValidationRetriesFailure	The MIB validation process has failed for a number of times equal to <i>MaxRetries</i>
SNMP command	An SNMP command has been received and shall be processed by the ED, ED-S or ND SNMP agent

State	Description
Operational	ED is operational, application data transfer can be started.
SNMP check	The SNMP agent of the ED starts a check on the integrity of its MIB. This includes also the verification that MIB exists.
MIB creation	The SNMP agent creates the MIB database defining MIB objects it will use for monitoring and network management
MIB Validation	The SNMP agent validates the created MIB checking that the structure of the database is correct
SNMP Ready	The SNMP agent is ready to receive commands or to generate traps
Process SNMP command	The SNMP agent has received a new command from an SNMP master. The command is processed.
Termination State	In the case of an ED shutdown or in the case the validation of the MIB has failed for <i>MaxRetries</i> times, the state machine goes to termination

As it can be noticed in Figure 123, the SNMP agent acts for assuring that the MIB has been correctly initialised. The SNMP master agent, by acting on MIB objects, using MIB Object IDs is able to monitor the ED and to download diagnostic information that can be processed and evaluated.

The initial configuration on the MIB includes also the configuration on the security aspects (e.g., define the access to specific MIB object views, as specified in SNMPv3) that will be further exploited in the next section 4.4.

In order to support the identified scenarios, the following MIB objects shall be present and available by the ED so that the SNMP agents are aware of software updates or changes in the configuration and the SNMP master knows which command it is able to send for monitoring and network management purposes.

The proposed structure matches the hierarchical composition of a MIB.

- **device:**
 - **type:** it contains information related to the type of the device (e.g., switch, gateway, hub, sensor, etc.);
 - **manufacturer:** the name of the manufacturer
 - **name:** the name of the device
 - **serial:** the serial number of the device
 - **firmware:**
 - **version:** an integer value representing the current version of the firmware installed on the device
 - **uri:** the uri from which the firmware binary is made available and can be downloaded;
 - **updateAvailable:** a boolean value indicating if an update to the firmware is available or not

- **configuration:**
 - **value:** the current value of the configuration
 - **uri:** the uri from which the configuration is made available and can be downloaded;
 - **updateAvailable:** a boolean value indicating if an update to the configuration is available or not
- **diagnostic:** it contains all the variables to be accessed for diagnosis purposes (e.g., the value of a sensor, the lifetime of an ED, the path to a log file, etc.);

Of course, this proposal does not exclude that other properties may have already been defined by ED manufacturer.

4.3.1 Remote configuration download

Assuming each ED, ED-S or ND has in its MIB the structure previously defined the necessary steps for receiving the configuration updates are:

1. The SNMP master agent (e.g., the one running in the remote control centre) sends an SNMP *set* command to an SNMP agent (e.g., the one running on the targeted ED);


```
snmp set HOST publicw device.configuration.uri CONFIGURATION_URI
          device.configuration.updateAvailable 1
```
2. The command sets the two variables in the MIB *device.configuration.uri* and *device.configuration.updateAvailable*;
3. The SNMP agent accesses to the MIB and checks the value of the variable *updateAvailable*. If the value is 1 means that an update in the configuration is available and the agent can access the *uri* variable for retrieving the host and the path to the configuration to be downloaded;
4. The ED can download the configuration (e.g., using a secure file transfer protocol, e.g. HTTPS as defined in IEC61375-2-6).

4.3.2 Download of software updates

As specified in section 4.3.1, the same approach can be used, by the ED, to verify if an update to the firmware is required. In particular, in the case the ED shall update its software, the following steps apply:

1. The SNMP master agent (e.g., the one running in the remote control centre) sends an SNMP *set* command to an SNMP agent (e.g., the one running on the targeted ED);


```
snmp set HOST publicw device.firmware.uri BINARY_URI
          device.firmware.updateAvailable 1
```

2. The command sets the two variables in the MIB *device.firmware.uri* and *device.firmware.updateAvailable*;

3. The SNMP agent accesses to the MIB and checks the value of the variable *updateAvailable*. If the value is 1 means that an update in the firmware is available and the agent can access the *uri* variable for retrieving the host and the path to the binary to be downloaded;
4. The ED can download the binary; It is important to remark that the SNMP protocol is used just for orchestrating and managing the firmware information of the device and the availability of an update of the firmware itself (via proper MIB objects). A different protocol shall be used for downloading the binary (e.g., for example via HTTPS);
5. The ED can install the new version of the software binary once the download has been completed.

4.3.3 Download of diagnostic information

The last scenario under evaluation refers to the capability, from a remote control centre, to access and download log information, as well as diagnostic ones, from an ED. In this case, the SNMP master (e.g., the one running in the remote control room) sends a *get* command to an SNMP agent running on the targeted ED. In details, the process is the following one:

Download of specific diagnostic information

1. The SNMP master agent (e.g., the one running in the remote control centre) sends an SNMP *get* command to an SNMP agent (e.g., the one running on the targeted ED);

```
snmp get HOST publicw device.diagnostic.VARIABLE_NAME
```

2. The SNMP agent processes the command;
 - a. it accesses the MIB hierarchy;
 - b. it locates the MIB object;
 - c. It retrieves its value and gives it back to the requestor;

Download of log files containing diagnostic information

The case in which the SNMP master requests the log file of an ED is equivalent to the case in which an ED has to download a software binary for updating its firmware. In particular:

1. The SNMP master agent (e.g., the one running in the remote control centre) sends an SNMP *get* command to an SNMP agent (e.g., the one running on the targeted ED);

```
snmp get HOST publicw device.diagnostic.log
```

2. The SNMP agent processes the command;
 - a. it accesses the MIB hierarchy;
 - b. it locates the MIB object;
 - c. It retrieves its value and gives it back to the requestor;
3. The SNMP master evaluates and processes the value of the retrieved variable which contains the *uri* to the log file to be accessed;

4. The SNMP master downloads the log; as already stated in the previous section, also in this case a protocol that differs from SNMP shall be used from log file download (e.g. HTTPS).

4.4 SERVICE ACCESS

This section provides an overview on the EAP protocol and how SNMP is used to configure the access to EAP-enabled devices. **Service access** consists of a set of authentication procedures used to access the NG-TCN services exposed to external user, as shown in Table 7. The protocols, which are considered in this section for service access, can be applied to access the services from the MCG, WPAN and WLANs.

The ECSP shall provide functions to manage the authentication of EDs, ED-Ss and NDs. To avoid forbidden accesses, the connected devices request authorization to the NG-TCN network Authorization Server, which implements EAP. The EAP-enabled devices shall be configured and accessed only by a restricted set of users who have the rights to modify the configuration status.

EAP is an **authentication protocol** for PPP that supports multiple authentication mechanisms that are negotiated during the authentication phase. The EAP protocol does not prescribe a particular authentication technology, it is an authentication framework within which a server provides authentication functionalities.

EAP allows a third-party authentication server to interact with a PPP (point-to-point protocol) implementation via a generic interface. The main goal of EAP is to allow network access authentication, where IP layer connectivity may not be available. EAP does not need IP connectivity to work, so that it provides just enough support for the reliable transport of authentication protocols.

Unlike TCP, EAP cannot efficiently transport bulk data so that it cannot be used to transport data. EAP does not select a specific authentication mechanism at Link Control Phase, but rather postpones the usage of such a mechanism until the Authentication Phase. The authenticator can request from more information before determining the specific authentication mechanism.

To implement EAP, the vendors of access devices develop the following abstraction layers:

1. **Lower layer.** The responsibility of the lower layer is to transmit and receive EAP frames, which are exchanged between the peer and the authenticator. For example, EAP can be executed on wireless IEEE 802.11 LANs. [RFC3748]
2. **EAP layer.** The EAP layer is responsible to receive and send EAP packets via the lower layer. This layer implements duplicate detection and retransmission mechanisms.
3. **EAP peer and Authenticator Layers.** This layer is responsible to multiplex the incoming messages via the Code field in the EAP packet. An EAP host can be both a peer or an authenticator
4. **EAP Method Layers.** EAP methods implement the authentication algorithms and receive and transmit EAP messages via the EAP peer and authenticator layers.

A widely adopted implementation of the EAP protocol is the IEEE 802.1X. The 802.1X adopts the client/server model. [43] shows the entities involved in the 802.1X authentication (see also 3.5.7):

- **Client (Applicant)**, which consist in a user terminal seeking access to the LAN. On the terminal there must be installed the 802.1X software to do the authentication procedures on the access device.
- **Access device (Authenticator)**, which authenticates the client to control access to the LAN. In a typical 802.1X environment, the access device uses an authentication server to perform authentication.
- **Authentication server**, which provides authentication services for the access device. The authentication server first authenticates 802.1X clients by using the data sent from the access device. Then, the server returns the authentication results to the access device to make access decisions. The authentication server is typically a RADIUS (Remote Authentication Dial-In User Service) server. In a small LAN, you can use the access device as the authentication server.

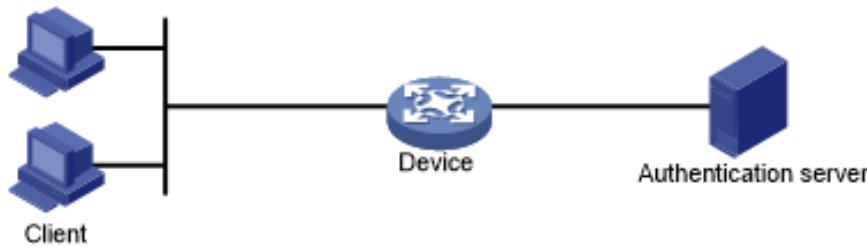


Figure 124: The three actors of the EAP protocol

802.1X defines EAP over LAN (EAPOL) for passing EAP packets between the client and the access device over a wired or wireless LAN. Between the access device and the authentication server, 802.1X delivers authentication information by either EAP relay or EAP termination.

EAP Relay

EAP relay is defined in IEEE 802.1X. In this mode, the network device uses EAP over RADIUS (EAPOR) packets to send authentication information to the RADIUS server, as shown in [45].

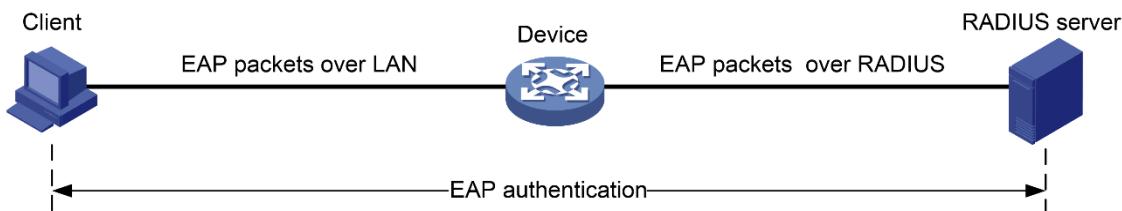


Figure 125: EAP relay mode

In EAP relay mode, the client must use the same authentication method as the RADIUS server. On the access device, you only need to use the `dot1x authentication-method eap` command to enable EAP relay.

EAP Termination

The access device performs a different bunch of operations in EAP termination mode. [45] shows the list of operations which are performed in EAP termination mode:

1. Terminates the EAP packets received from the client.
2. Encapsulates the client authentication information in standard RADIUS packets.
3. Uses PAP or CHAP to authenticate to the RADIUS server.

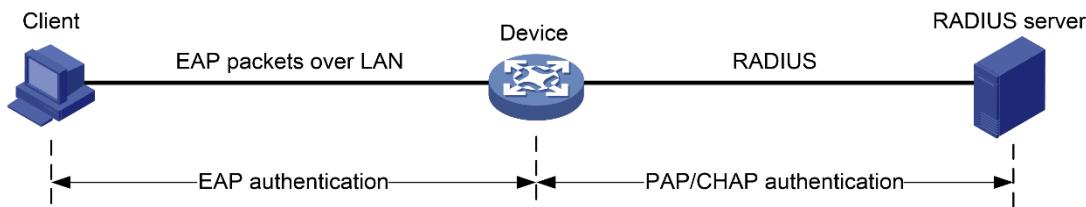


Figure 126: EAP termination mode

Table 54: Comparing EAP relay and EAP termination

Packet exchange method	Benefits	Limitations
EAP relay	Supports various EAP authentication methods. The configuration and processing are simple on the access device.	The RADIUS server must support the EAP-Message and Message-Authenticator attributes, and the EAP authentication method used by the client.
EAP termination	Works with any RADIUS server that supports PAP or CHAP authentication.	Supports only the following EAP authentication methods: <ul style="list-style-type: none"> - MD5-Challenge EAP authentication. - The username and password EAP authentication initiated by an iNode 802.1X client. The processing is complex on the access device.

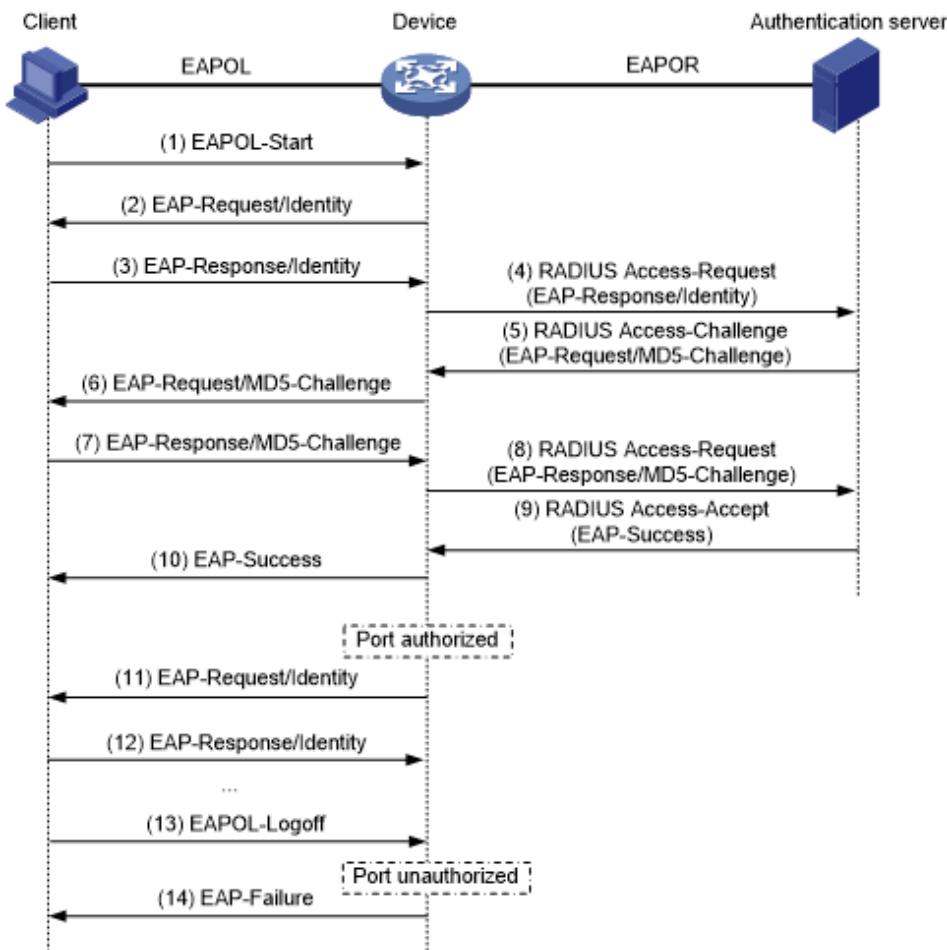


Figure 127: Sequence diagram of the 802.1X authentication procedure

1. After a user launches the 802.1X client, a user interface pops up. The user enters a registered username and password. Then, the 802.1X client sends an EAPOL-Start packet to the access device.
2. The access device replies back with an EAP-Request/Identity packet to ask for the client username.
3. In response to the EAP-Request/Identity packet, the client sends the username in an EAP-Response/Identity packet to the access device.
4. The access device relays the EAP-Response/Identity packet in a RADIUS Access-Request packet to the authentication server.
5. The authentication server uses the identity information in the RADIUS Access-Request to search its user database. If a matching entry is found, the server uses a randomly generated challenge (EAP-Request/MD5-Challenge) to encrypt the password in the entry. Then, the server sends the challenge in a RADIUS Access-Challenge packet to the access device.
6. The access device transmits the EAP-Request/MD5-Challenge packet to the client.
7. The client uses the received challenge to encrypt the password and sends the encrypted password in an EAP-Response/MD5-Challenge packet to the access device.

8. The access device relays the EAP-Response/MD5-Challenge packet in a RADIUS Access-Request packet to the authentication server.
9. The authentication server compares the received encrypted password with the encrypted password it generated at step 5. If the two passwords are identical, the server considers the client valid and sends a RADIUS Access-Accept packet to the access device.
10. Upon receiving the RADIUS Access-Accept packet, the access device performs the following operations:
 - a. Sends an EAP-Success packet to the client.
 - b. Sets the controlled port in authorized state.

The client can access the network.

1. After the client goes online, the access device periodically sends handshake requests to check whether the status of the client connection. By default, if two consecutive handshake attempts fail, the device logs off the client.
2. Upon receiving a handshake request, the client returns a response. If the client fails to return a response after a number of consecutive handshake attempts (two by default), the access device logs off the client. This handshake mechanism enables timely release of the network resources used by 802.1X users that have abnormally gone offline.
3. The client can also send an EAPOL-Logoff packet to ask the access device for a logoff.
4. In response to the EAPOL-Logoff packet, the access device changes the status of the controlled port from authorized to unauthorized. Then, the access device sends an EAP-Failure packet to the client.

Figure 128 shows the basic 802.1X authentication procedure in EAP termination mode, assuming that CHAP authentication is used.

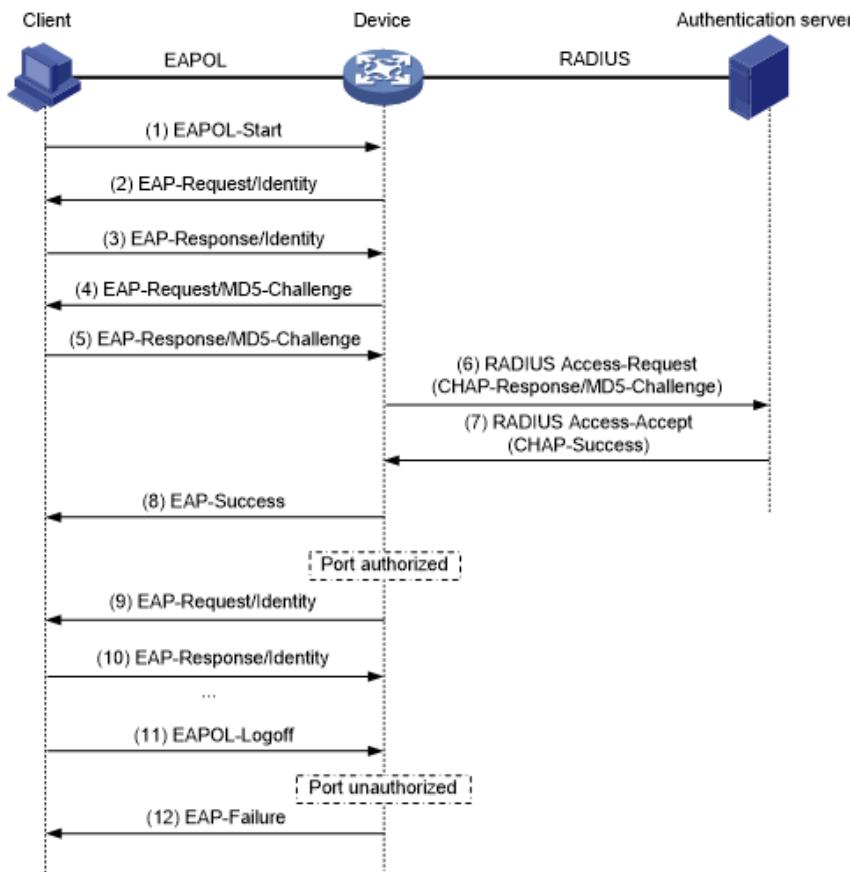


Figure 128: 802.1X authentication procedure in EAP termination mode

In EAP termination mode, the access device rather than the authentication server generates an MD5 challenge for password encryption. The access device then sends the MD5 challenge together with the username and encrypted password in a standard RADIUS packet to the RADIUS server

An EAP authentication device can be configured with SNMP. Network device vendors provide supports for many SNMP protocol versions. The access to the EAP devices management shall be secure and regulated over SNMP. The security model of the SNMP protocol changes over its versions.

This section focuses on the following SNMP versions:

- SNMP v1
- SNMP v2c
- SNMP v3

The SNMPv1 and SNMP v2c use a community-based form of security, which allows to a set of managers to access the agent MIB via an IP address access control list and password.

SNMPv2c includes also a bulk retrieval mechanism and a more detailed error message report mechanism to management station. One of the features of this mechanism is to support of the retrieval of tables and large quantities of information, which minimize the number of round-trips required.

A further improvement in the SNMPv2c protocol involves the error handling support, which includes the expansion of error codes to contain different kinds of error conditions. Error return codes with SNMP v2c also report the error types.

SNMPv3 is a security model, which is an authentication strategy that is set up for a user and the group in which the user resides. The security level is the permitted level of security within a security model, and it determines which mechanism is adopted when an SNMP packet is handled.

The security level determines if an SNMP message needs to be protected from disclosure and if the message needs to be authenticated. The various security levels that exist within a security model are listed as follows:

- **noAuthNoPriv**. Security level that does not provide authentication or encryption.
- **authNoPriv**. Security level that provides authentication but does not provide encryption
- **authPriv**. Security level that provides both authentication and encryption.

Table 55 reports the SNMPv3 security models and levels with their supported authentication procedures.

Table 55 - Security model of SNMP

Model	Level	Authentication	Encryption	What Happens
v1	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
v2c	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
v3	noAuthNoPriv	Username	No	Uses a username match for authentication.
v3	authNoPriv	HMAC-MD5 or HMAC-SHA	No	Provides authentication based on the HMAC1 -MD52 algorithm or the HMAC-SHA3 .

Model	Level	Authentication	Encryption	What Happens
v3	authPriv	HMAC-MD5 or HMAC-SHA	DES	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides DES4 56-bit encryption in addition to authentication based on the CBC5 DES (DES-56) standard
v3	authPriv	HMAC-MD5 or HMAC-SHA	3DES	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides 168-bit 3DES6 level of encryption
v3	authPriv	HMAC-MD5 or HMAC-SHA	AES	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides 128-bit AES7 level of encryption.

SNMPv3 provides secure access to devices by providing authentication, encryption and access control. These added security benefits secure SNMP against the following security threats:

- **Masquerade.** This threat considers that a SNMP user may assume the identity of another SNMP user, to perform management operations for which that SNMP user does not have authorization.
- **Message stream modification.** This threat refers to messages that might be maliciously reordered, delayed or replayed to cause SNMP unauthorized management operations.
- **Disclosure.** The threat concerns on the eavesdropping of SNMP messages exchanged between different SNMP engines.

SNMPv3 Costs

SNMPv3 authentication and encryption cause a slight increase in the response time when SNMP operations on MIB objects are performed. Table 56 contains the various SNMP version ordered from the least to the greatest response time requested to perform it.

Table 56 - Cost of SNMP implementations

Security Model	Security Level
SNMPv2c	noAuthNoPriv
SNMPv3	noAuthNoPriv
SNMPv3	authNoPriv
SNMPv3	authPriv

User-Based Security Model

SNMPv3 User-Based Security Model (USM) refers to SNMP message-level security and offers the following services:

- **Message integrity.** To ensure that messages have not been altered or destroyed in an unauthorized manner and that data sequences have not been altered to an extent greater than can occur non-maliciously.
- **Message origin authentication.** To ensure that the claimed identity of the user on whose behalf received data was originated is confirmed.
- **Message confidentiality.** To ensure that information is not made available or disclosed to unauthorized individuals, entities, or processes.

SNMPv3 authorizes management operations for configured users and enables encryption for exchanged SNMP messages. Only configured users can access ED, ND and ED-S devices.

USM uses two authentication protocols:

- HMAC-MD5-96 authentication protocol
- HMAC-SHA-96 authentication protocol

View-Based Access Control Model

The View-Based Access Control Model (VACM) enables SNMP users to control access to SNMP managed objects by supplying read, write, or notify access to SNMP objects. It prevents access to objects restricted by views. These access policies can be set when user groups are configured with the snmp-server group command.

MIB Views

To enforce security mechanisms, the ECSP administrator shall be able to restrict the access rights of a set of groups to only a subset of the management information within the management domain.

The access to a management object is controlled through MIB views, which contain the set of managed object types (and, optionally, the specific instances of object types) that can be viewed. Access Policy Access policy determines the access rights of a group.

SNMP includes the following three types of access rights:

- Read-view access. The set of object instances authorized for the group when objects are read.
- Write-view access. The set of object instances authorized for the group when objects are written.
- Notify-view access. The set of object instances authorized for the group when objects are sent in a notification

NOTE: this specification of the service access uses the references [42], [43], [44], [45], [46] and [47].

5 CONCLUSIONS

5.1 GENERAL

This report summarized the analysis results and specification work executed in Task 3.5 of CONNECTA for the definition of a NG-TCN architecture. The main achievements of this work are:

- Introduction of a new TRDP traffic class (TSN-PD) for scheduled data traffic based on standard IEEE 802.1Qbv.
- Time synchronization concept based on IEEE 802.1AS-rev as prerequisite for scheduled traffic.
- Definition of a new network architecture with separated ETB lines and diverse virtual data communication planes for scheduled data traffic.
- Safe Data Transmission protocol and safety layer definition for the transport of safety critical data up to highest safety integrity levels (SIL4).
- Safe train inauguration concept for train composition discovery with highest safety integrity levels (SIL4).
- Definition of a security architecture and security methods to achieve state-of-the-art cyber security in alignment with actual security standards.

This new architecture allows to replace conventional train lines for train control and provides the capabilities to integrate safety-related sub-systems like the Electronic Distributed Valve (EDV) brake and ETCS signalling. Due to its ability to transport data of mixed criticality, the same communication infrastructure can be used for TCMS functions and operator-/customer-oriented services. Furthermore, the possibility to reserve bandwidth for critical data supports the process of incremental certification: non-safety related communication cannot interfere with safety-related communication.

More in detail, the Technical Annex in the Grant Agreement [01] defines 8 aspects which should guide the work of WP3 Task 3.5 and which are cited here to check the completeness of the work:

(1) Define the network topology including end system”

Here, a new network topology has been defined which suits the specific needs of high reliable scheduled data traffic. On ETB level, a right and left ETB line have been introduced which is different to the nowadays used topology with aggregated ETB lines. On consist level, dual-homed critical end devices connecting to two virtual TSN planes have seamless communication also in the case of a network fault. Conventional and legacy devices are connected as today with a single Ethernet interface to the ECN ring network, which ensures backward compatibility to existing solutions.

(2) Define network services

Besides well-known services already present in existing implementations, NG-TCN introduces some modifications to some of them and also defines new services. To mention here are: data communication service for scheduled data traffic, modification of train inauguration service to

cope with the changed ETB topology and support of highest safety integrity, and a new safe data transmission protocol for connecting safety function classified for SIL4.

(3) Suitable communication protocols have to be selected or specified

The modified or new network services partly require new or adapted protocols, like the protocol for frame replication and elimination (IEEE 802.1CB), the modified train inauguration protocol or the safe data transmission protocol. Completely new is the precise time synchronization protocol based on the IEEE 802.1AS standard, which is a prerequisite to scheduled data traffic.

(4) Specify the network components that constitute the network

There are no really new network components compared to existing solutions, but most of the components have changed roles and provide additional functionality. First to mention is here the function of time synchronization and scheduled traffic, which affects most network components like consist switches and TSN-aware end devices. But also, the ETBN got new functionality. Chapter 2.3 provides a list of network components and a description of their roles.

(5) Specify requirements on and interfaces to end systems

This is accomplished with a special focus on TSN-aware end devices. To connect those end devices to NG-TCN, they need to implement services and protocols which have been mentioned before. Chapter 2.8 is dedicated to the network interfaces.

Requirements on end systems have been defined to an extend that allows to connect those end systems to NG-TCN

(6) Define the communication interface following a specific application profile for end systems (as specified in WP4)

To be generic, end devices interfaces defined herein are not application profile specific, but in their generality, they are parametrizable for all relevant profiles discussed in WP4, like Doors, HVAC and BMS. In addition, in discussions and meetings with WP5 it has been ensured that brake requirements are fulfilled as well.

(7) Specify how the whole network, including connected end systems, can be configured.

Network and end device configuration is very device specific and mainly in the responsibility of the component suppliers. But the defined network services and protocols constrain the functionality to be provided and by this the configuration demand. Some general rules and guidelines for network configuration are summarized in chapter 4.

(8) Possibilities of sharing resources (e.g. network) with the signalling system shall be defined.

NG-TCN as defined herein provides the necessary communication features for integrating the signalling system. However, the signalling system interfaces defined by UNISIG need to be adapted correspondingly. The analysis of possibilities and limitations are subject of E.

Summarized, the specification of NG-TCN architecture and interfaces carried out in this task T3.5 are considered appropriate for supporting the objectives of NG-TCMS with respect to reliable, low latency, safe and secure data communication. The concepts should be detailed enough to derive requirements for network component prototyping. The verification of the concepts is envisaged for

subsequent projects as it is outlined in F. In parallel, necessary standardization activities on international level will be launched.

5.2 KPIs

The contribution of the Drive-by-Data concepts to Shift2Rail objectives, expressed by the KPIs formulated in [02], shall be demonstrated:

Cutting the life-cycle cost of railway transports by as much as 50%	Due to its ability to integrate mixed-criticality devices, e.g. TCMS, OOS and COS devices, in one physical network, the number of network components will be lowered. With the introduction of scheduled traffic and high safety data communication integrity, train lines are not any longer needed and can be completely replaced by corresponding network services. All this will reduce material cost and maintenance cost. Furthermore, it's a weight reduction which also counts for cost reduction.
Doubling railway capacity	The low latency and low jitter data communication that is possible with introducing TSN enables fast reactions on events. This ability can be helpful in virtual coupling scenarios as it allows to run virtually coupled trains in low distances.
Increasing reliability and punctuality by as much as 50%	The reduced number of components and the optimization of the network topology increases the material reliability. Seamless redundancy provided by the A-Plane/B-Plane approach increases the functional reliability.

A quantification of these KPIs can be done during the proof-of-concept phase in subsequent projects.

5.3 OPEN ITEMS

During the course of the task some issues were identified which could not be closed and which remain to be solved either in subsequent projects or in other groups, like for instance standardization bodies. The following lists provides the identified items.

Table 57: Open Items

No	Open items	Related chapter	Remarks
1	Problem with the pin out of GbE X-coded M12 connectors defined in IEC 61076-2-109. The polarity of pins 7/8 is reversed compared to the other pairs.	3.1.1	Input to IEC WG43
2	Persistent errors in inauguration frames must be located to the ETBN causing them	Annex J	Input to CTA-2
3	A mechanism or protocol must be defined which selects the ETB line between consists used for non-TSN traffic	3.2.10	Input to CTA-2
4	Investigate the use of MSTP as a redundancy protocol for ECN	3.2.9	Input to CTA-2
5	An FMEA should be executed for the safe train inauguration in order to formally prove the suitability of the concept (proof of concept).	3.5.4	Input to CTA-2

No	Open items	Related chapter	Remarks
6	A quantitative analysis for demonstrating that the certification effort for a NG-TCN using ED-S is not higher than for legacy TCN using train lines should be done (see ID_60007).	Annex C	Input to CTA-2
7	For time synchronization there are actually 2 choices: 1. ETB and ECN clock domains synchronized (preferred solution) 2. ETB and ECN clock domains not synchronized (fallback solution) Measurements have to show robustness and timing behaviour of choice 1, before a final decision can be made.	2.9	Input to CTA-2

A Annex – Network device capability matrix

This matrix maps functional capabilities to network components.

Table 58: Network component capability matrix

OSI Layer	Capability	Component	ETBN	ETBR	CS	RT	ED (convent.)	ED (TSN)
1	100FDX						x	x
1	1GbE	x	x	x			(x)	(x)
1	10GbE	(x)	(x)	(x)				
1	ETB Bypass							
1	PoE			x			x	
1	Sleep mode	(x)						
2	Frame reception and transmission	x	x	x	x	x	x	
2	Frame relaying	x		x				
2	QoS	x		x			x	x
2	Traffic shaping/policing	x		x			x	x
2	Dual homing							x
2	VLAN	x		x	x	(x)	x	
2	Master Clock (GlobalMC/ConsistMC)	x		x				
2	Slave Clock	x		x				x
2	ETB Topology Discovery	x						
2	Scheduled traffic (TSN)	x		x				x
2	PNAC			x		x	x	
2	MACSec			x		x	x	
2	Redundancy: ring protocol			x				
2	ETB Repeater function		x					
3	IP protocol layer	x	(x)	x	x	x	x	
3	IP routing	x			x			
3	IGMP snooping	x		x				
3	ICMP	x		x	x	x	x	
4	TCP/UDP	x		x	x	x	x	
7	SNMP agent	x	x	x	x	x	x	
7	DHCP relay agent				x ¹			
7	DHCP server	(x)		x				
7	IGMP querier			x				
7	ECSP	x						
7	TTDB Manager	x						
7	DNS server	x						
7	ETB Control Agent						x	
7	TTDB Agent					x	x	

OSI Layer	Capability	Component	ETBN	ETBR	CS	RT	ED (convent.)	ED (TSN)
7	TI Validator							x
7	TSN-GW	x						
7	Device redundancy	x						x
7	Network monitoring						x	
7	Security Event Detection	x	x	x	x	x	x	x
7	Authentication Server			x				

(x) = optional

¹ if DHCP relay agent and server are on the same device, the relay agent is implicitly implemented by the server

B Annex – Network performance analysis

B.1 General

The performance of the data transmission between a sending ED-TSN and a receiving ED-TSN within a NG-TCN is determined by different factors.

A typical train wide data communication path is shown in Figure 129. Data have to pass three switched Ethernet segments (ECN + ETB + ECN) which are interconnected by two TSN-GW. The latency time for the transmission between the two ED-TSN depends, for the case of TSN traffic, only on the performance of the network components. For normal, priority-based traffic, it additionally depends on the network load which is created by the collective of connected EDs.

The signal path between sending ED-TSN and receiving ED-TSN is constant for a static network configuration, but may change if the network configuration changes, e.g. caused by the failure of a network device or a train inauguration. Hence, for designing the network configuration, worst case scenarios have to be analyzed.

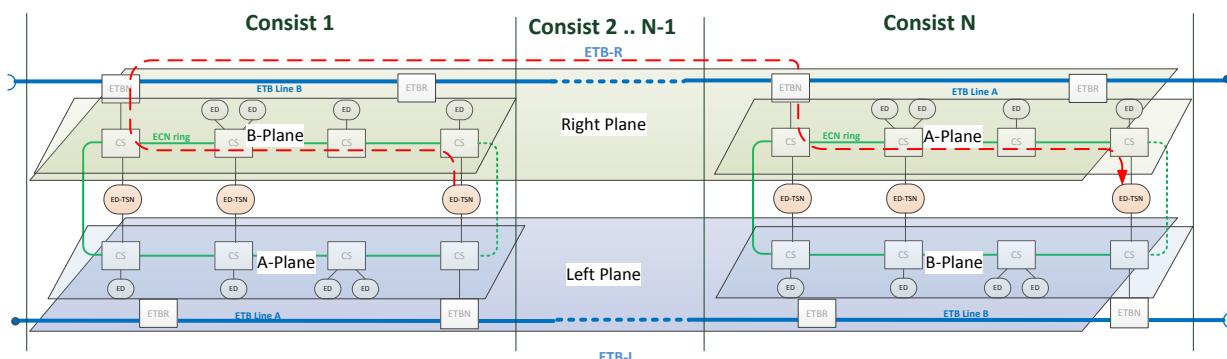


Figure 129: Train-wide data communication

B.2 Network performance principles

For the transmission of deterministic data traffic through the NG-TCN transmission latency must be bound. To analyze the transmission characteristics, the simple model as depicted in Figure 130 shall be used. Here, a critical data stream is sent from a talker to a listener through the network. Without any other network data traffic, the latency would only be defined by the type and number of network components (hops) the stream has to pass from talker to listener. In practice however, there will be interfering traffic, and how this traffic influences the latency depends on the transmission technology.

In conventional Ethernet as it is defined in IEC61375, QoS is mainly based on priorities. Critical data are given the highest priority, while other data have lower priority. When highest priority data interferes with highest priority data, frames are getting queued up in Ethernet switches, leading to a bursty traffic pattern unless traffic shaping is in place. When highest priority data interferes with lower priority data, higher priority data have preference, but if there is a lower priority frame transmission in progression, higher priority data transmission is held back until lower priority frame transmission terminates. The latency follows a probability density distribution with broad variance, similar to a

Gaussian distribution as it is indicated in Figure 130. Although there exists a theoretical maximal latency, it is hard to calculate. Due to the broad variance, the jitter is high.

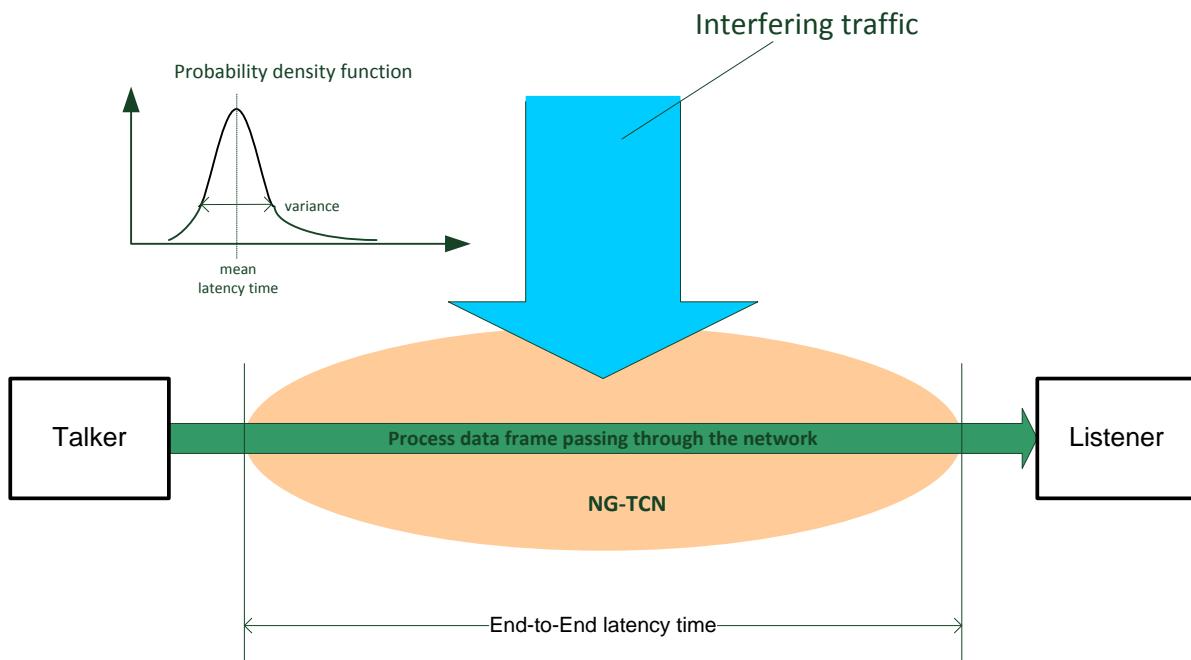


Figure 130: Data communication with interfering traffic

In TSN aware Ethernet a defined time slot, and with this a defined bandwidth, is reserved for critical data streams. Interference with other data traffic cannot happen, only potential interference with other critical data streams using the same time slot (which is a matter of configuration). Hence the expectation is that the probability density variance is much smaller, leading to a small jitter. The mean latency time depends on the number of hops and the individual transmission delays induced by the network components. This will be further explored in the next paragraphs.

B.3 Network Component Characteristics

The performance of the overall network depends on the performance of the individual network components. The performance of the components depends on different aspects:

- The inner architecture of the component
- The forwarding principle (cut-through, store-and-forward, data multiplexing)
- The data path through the component
- The transmission speed of the interface ports

The main characteristics of the NG-TCN components are listed in Table 59.

Table 59: Network component characteristics

Functional role	Characteristics	Data path (OSI Layer)
ETBN	Full wire-speed, store-and-forward switching for conventional and TSN data traffic along the ETB. IP-routing of conventional data traffic between ECN and ETB. TSN Gateway for TSN data traffic, asynchronous and synchronous mode.	i. ETB to ETB (L2) ii. ECN to ETB via IP router (L3) iii. ECN to ETB via TSN-GW (L7)
ETBR	Full wire-speed, cut-through or store-and-forward switching for conventional and TSN data traffic along the ETB Two design possibilities: <ul style="list-style-type: none">• L1 repeater• L2 repeater (with switching fabric)	i. ETB to ETB (L2)
CS	Full wire-speed, store-and-forward switching for conventional and TSN data traffic in ECN. GbE/10GbE in ECN ring 100FDX/GbE for ED connection	i. ECN ring to ECN ring (L2) ii. ED to ECN (L2)
RT	IP-routing of conventional data traffic between ECN VLANs. Routing algorithm can be implemented in SW (CPU) or in dedicated HW.	i. ECN VLAN to ECN VLAN (L3)

The performance measurement methodology of network components is defined in IETF RFC 1242, RFC 2544 and RFC 4689. For NG-TCN, especially the forwarding delay and the jitter, both as defined in RFC 4689, are important.

The forwarding delay t_{fw} measures the time from the last frame bit ingressing the network component until the last bit egressing the network component²⁷ (LILO principle). With this definition, the real forwarding delay is measured, but this means that the result depends on the frame size and the transmission speed. Indeed, for Ethernet switches, t_{fw} is composed of two time values, under the assumption that there is no interfering traffic²⁸ (TSN case):

$$t_{fw} = t_{fr} + t_{sw}$$

where t_{fw} stands for the total forwarding delay, t_{fr} represents the time for frame sending which depends on frame size and transmission speed, and t_{sw} represents the time for processing and queuing the frame.

The value of t_{fr} can be easily calculated. For t_{sw} , it is more complex, as it depends on the architecture of the network component and the data flow inside the components. There are measurement values

²⁷ RFC 4689 defines the last bit of an IP packet and by this coping with different link layer formats. As NG-TCN uses only Ethernet, the last bit of the Ethernet frame (last bit of CRC) can be used instead.

²⁸ In case of interfering traffic additional time might be spent for holding frames in buffers. Interfering traffic is excluded for TSN by definition.

reported in literature, see for instance [34]. An estimation of t_{fw} based on available data is listed in Table 60.

Table 60: t_{fw} estimated (Ethernet frame with 1530 octets, 1GbE, LILO, 2.5 ms ETB cycle)

Data path	Architecture	t_{fw} estimated
ETB to ETB (L2)	Switching fabric + line interfaces (Phys)	$\leq 18 \mu s$
ECN ring to ECN ring (L2)	Switching fabric + line interfaces (Phys)	$\leq 18 \mu s$
ED to ECN (L2)	Switching fabric + line interfaces (Phys)	$\leq 18 \mu s$
ECN to ETB via TSN-GW (L7), synchronous	ETBN switching fabric, traffic store and frame multiplexing Multiplexing in SW Multiplexing in HW	$\leq 200 \mu s$ $\leq 40 \mu s$
ECN to ETB via TSN-GW (L7), asynchronous ²⁹	ETBN switching fabric, traffic store and frame multiplexing Multiplexing in SW Multiplexing in HW	$\leq 2700 \mu s$ $\leq 2540 \mu s$
ECN to ETB via IP router (L3)	IP routing	$12.24 \mu s^{30}$
ECN VLAN to ECN VLAN (L3)	IP routing	$12.24 \mu s$

B.4 Estimated expected end-to-end latency in NG-TCN

With the figures presented before end-to-end latency can be estimated. This estimation is done for two scenarios shown in Table 61, which represent a minimal and a maximal configuration for train wide communication (see also 0):

Table 61: Scenarios for end-to-end latency estimation

Data path	Scenario 1 (min)	Scenario 2 (max)
Number of CS	2	64
Number of ETBN	2	63

This leads to the results for the two scenarios, differentiated for synchronous/asynchronous TSN-GW operation and HW/SW implementation of TSN-GW multiplexing (Table 62):

²⁹ For worst case one cycle time must be added to the values of synchronous transfer

³⁰ Equals the time for transmitting one 1530 octets Ethernet frame (full wire speed routing)

Table 62: end-to-end latency estimation (unit: μs)

Scenario	Synchronous Mode		Asynchronous Mode		
	HW	SW	HW	SW	
1	116	436	2116	2436	
2	2330	2650	4330	4650	

As can be seen, end-to-end latency is mainly determined by the TSN-GW operational mode. But in general, all those values are in an acceptable range.

C Annex – Requirement traceability matrix

The implementation of the NG-TCN requirements as set out in [03] by the NG-TCN architecture as defined herein is listed in Table 63. Listed are only functional and non-functional requirements, informal parts are left out. As well excluded are signalling related requirements which are subject of E.

Table 63: NG-TCN requirements implementation

ID	Requirement Text	Implementation
ID_60065	The NG (next generation) of TCN (Train Communication Network) shall provide one train-wide communication network for full TCMS support including the replacement of train lines, which ensure reaching the appropriate safety goals for highest safety levels.	Fulfilled, see definition of NG-TCN architecture in chapter 2
ID_60066	The NG-TCN shall enable the connection of safety functions up to SIL4 and shall support the ‘fail-safe’ principle in order to reach the required SIL and the ‘fault-tolerant’ principle in order to reach the required availability.	Fulfilled. SIL4 ‘fail-safe’ supported by SDTv4 safety layer and safe train inauguration concepts. Fault-tolerant principle is achieved with the A-Plane/B-Plane architecture.
ID_60067	The NG-TCN shall provide an optimal train network for TCMS and OMTS (on-board multimedia and telematics) services, by considering quality of service aspects like determinism, real-time behaviour, demand-response-time, guaranteed bandwidth or jitter.	Fulfilled. TSN guarantees the QoS for critical data traffic.
ID_60068	The NG-TCN shall ensure to end devices the requested end-to-end performance at least in term of demand response time, SIL, and availability. NOTE : The requested performances are end-devices function dependent	Fulfilled. Critical end devices use TSN and are connected to both A-Plane/B-Plane
ID_60069	The NG-TCN shall provide an interface for also for non-TCMS functions like signaling subsystems.	See E
ID_40004	NG-TCN shall support the quantities listed in Table 5 and Table 6 of Annex A.	Partly fulfilled. Due to the decision to stay with IPv4 and the IP address space allocations made in IEC61375-2-5 the number of network nodes per consist and per ECN has been reduced.

ID	Requirement Text	Implementation
ID_40009	<p>NG-TCN shall enable connected end device applications (ED) to communicate with each other within the train on the base of the Internet Protocol (IP) for OSI layer 3.</p> <p>Two use cases are identified:</p> <ul style="list-style-type: none"> i) communication between ED located in the same consist ("intra-consist communication") ii) communication between ED located in different consists ("inter-consist communication") <p>NOTE: this requirement only restricts the protocol used for OSI layer 3. Other layers are not affected, as for example the usage of a wireless link layer or PROFINET IO where the application layer (OSI layer 7) directly interfaces with Ethernet (OSI layer 2).</p>	Fulfilled. IP is defined.
ID_40010	If IPv4 (RFC791) is applied, then a train wide IP address as defined in IEC61375-2-5 shall be used for addressing end devices in a train.	Fulfilled. IP address as defined in IEC61375-2-5 is adopted.
ID_40011	<p>The NG-TCN may use wire based (IEEE 802.3 Ethernet) and wireless (IEEE 802.11 WLAN, LTE) technologies for interconnecting devices on OSI layers 1 and 2.</p> <p>NOTE 1: the conditions for communication to wireless devices are ruled by Roll2Rail project and CONNECTA WP2 and further initiatives of Shift2Rail.</p> <p>NOTE 2: wireless technologies can only be applied if they fulfill the RAMS and security requirement specified later within this document.</p>	Fulfilled. The architecture defined in chapter 2 defines a wire based backbone (ETB and ECN), but allows to connect ED wirelessly. LTE is not defined, instead WPAN can be used.
ID_40012	Wire based technology shall be Ethernet as defined in IEEE 802.3	Fulfilled.
ID_40016	The NG-TCN shall support the dynamic coupling or uncoupling of consists (train lengthening and train shortening) during service.	Fulfilled. Defined by train inauguration protocols in sub-chapters 3.2.10 and 3.5.4
ID_40017	The NG-TCN shall continuously discover the actual train composition and shall maintain the discovery result in the Train topology database (TTDB) as defined in IEC61375-2-3.	Fulfilled. Defined by train inauguration protocols in sub-chapters 3.2.10 and 3.5.4
ID_40018	The NG-TCN shall ensure that there is no more than one leading vehicle in the train during service.	Fulfilled. Defined by train inauguration protocols in sub-chapters 3.2.10 and 3.5.4
ID_40022	The IP-TCN shall support port based VLAN	Fulfilled.
ID_40023	IP-TCN ED ports shall be configurable to support VLANs in accordance to [IEEE802.1Q], meaning that an ingressing Ethernet frame with a valid Ethernet tag shall be allocated to the VLAN identified by the VID (VLAN Identifier) in the Ethernet tag.	Fulfilled.
ID_40024	An ingressing, untagged Ethernet frame, or tagged Ethernet frames with VID = 0x000, shall be allocated to the default VLAN associated to the ingressing Ethernet port.	Fulfilled.

ID	Requirement Text	Implementation
ID_40025	An ingressing tagged Ethernet frame with invalid VID shall be discarded. NOTE: this event leads to a security log, see ID_40071	Fulfilled.
ID_40026	Ethernet frame un-tagging/tagging during port egress as defined in [IEEE 802.3] clause 3.5 and [IEEE 802.1Q] (VLAN) shall be configurable for all ED ports, especially: i) Frames shall always egress untagged. ii) Frames shall always egress tagged. If the frame was untagged at ingress, it shall be tagged with the default VID. iii) Frames shall egress unmodified. If the frame was untagged at ingress, it shall egress untagged. If the frame was tagged at ingress, it shall egress tagged with the original VID	Fulfilled.
ID_40072	NG-TCN shall support a precise time synchronization based on the protocol defined in IEEE 1588.	Fulfilled. As defined in 2.9, IEEE802.1AS will be used.
ID_40028	TCN shall support a precise time synchronization within the network with a precision of $\leq 10 \mu\text{s}$ with a jitter of $\pm 1 \mu\text{s}$ (consist level) of $\leq 20 \mu\text{s}$ with a jitter of $\pm 2 \mu\text{s}$ (train level) NOTE: implies to use time-aware (IEEE 1588) switches	Fulfilled. See 2.9 and 3.2.7. Verification will be done in CONNECTA-2.
ID_40070	Setup of synchronized clock after startup or network reconfiguration (e.g. inauguration) shall not take longer than 1.0s	Partly fulfilled. Setup time could be more, see 2.9.4
ID_40030	The IP-TCN shall support ingress rate limiting (Traffic Policing) on ED ports EXAMPLE: dropping Ethernet frames exceeding the granted bandwidth priority-aware (lowest priority first).	Fulfilled. See 3.2.5
ID_40034	The maximal transmission latency time of transferred data shall be as specified in Table 9 of Annex B in [03]. NOTE: "latency" defines the network transfer time which means the time span between the sending of a Process Data frame by the source ED until reception by the destination ED	Fulfilled, see Annex B
ID_40036	Network Devices shall provide the possibility to limit the transmission rate of egressing data per data class ('traffic shaping'). NOTE: "shaping" means to reserve a guaranteed bandwidth for a data class. IEEE802.1Q defines two shaping techniques: 1) credit based shaping 2) traffic scheduling Which to apply depends on the data class and the required determinism	Fulfilled. See 3.2.5

ID	Requirement Text	Implementation
ID_40039	All Layer 2 ND ('bridge', e.g. Ethernet switches) shall switch in full-wire speed.	Fulfilled, see Annex B
ID_40040	All Layer 3 ND ('IP router') shall route in full-wire speed.	Partly fulfilled, see Annex B. "Full wire speed" not required, but a minimal performance.
ID_40042	NG-TCN shall at least support the following data rates for the ETB and the consist network as options: - 1 GbE - 10 GbE	Fulfilled.
ID_40047	Addressing on network layer shall use the IP address schema defined in IEC61375-2-5 (inter-consist) and IEC61375-3-4 (intra-consist) in case IPv4 is deployed.	Fulfilled See ID_40010.
ID_40048	Addressing on application layer shall use the TCN-URI schema defined in IEC61375-2-3.	Fulfilled. See 3.5.1
ID_40050	The TCN shall provide a service for dynamically assigning location specific IP addresses to end devices. NOTE 1: this feature can be implemented by using DHCP with option 82, but also other protocols are permitted. NOTE 2: this service might be obsolete for IPv6	Fulfilled. DHCP service defined in 3.5.5
ID_40052	The NG-TCN shall provide a DNS server (RFC 1034, RFC 1035) for resolving TCN-URI addresses (IEC61375-2-3) to IP addresses.	Fulfilled. See 3.5.5
ID_40055	The NG-TCN shall provide a server which informs ED about the actual train composition as it is defined in IEC61375-2-3 (train topology database TTDB) NOTE: This must be designed in a way, that a single point of failure in the addressing does not lead to a dangerous failure.	Fulfilled. See 3.5.5
ID_40056	The NG-TCN can provide a train topology database (TTDB) manager interface as specified in IEC61375-2-3 Annex E.	Fulfilled. See 3.5.5
ID_30107	The result of the train inauguration has to be published to those ED-S, who have a safety relevant communication channel, so that a 1:1 Connection of two ED-S in different consists can use it for a protection against random addressing errors in the black channel.	Fulfilled. See 3.5.5
ID_40059	The NG-TCN shall provide a user service to set/reset the local vehicle to/from status "leading" as it is specified in IEC61375-2-3.	Fulfilled. See 3.5.5
ID_40060	The NG-TCN shall provide a user service to inhibit a train inauguration. In case train inaugurations are inhibited, no new train network directory as for example defined in IEC61375-2-5 shall be computed.	Fulfilled. See 3.5.5
ID_40061	Train composition control shall only be granted to an authorized (dedicated) ED-S (or a redundant partner ED-S) in the consist.	Fulfilled. See 3.5.5

ID	Requirement Text	Implementation
ID_40062	The NG-TCN can provide an ECSP interface for train composition control as specified in IEC61375-2-3 Annex E.	Fulfilled. See 3.5.5
ID_40064	<p>NG-TCN shall support PoE on defined ED ports, compliant to [IEEE802.3], as an option (the number of PoE ports is product specific).</p> <p>NOTE: It has to be ensured that using PoE has no impact on any other subsystems on the train. This is a general principle, not limited to the safety or operational critical TCMS functions. It is also a general principle for EMC in the train that the subsystem shall resist to EM perturbations coming from any of the other subsystems AND shall not generate any EM impacting the any other subsystems. See EN 50121-2-3.</p>	Fulfilled. See 3.1.3
ID_40076	The NG-TCN shall provide precise time information based on IEEE1588 to connected ED / ED-S.	Fulfilled. See 2.9.
ID_40067	<p>ED sending process data shall support network scheduling of process data traffic as an option.</p> <p>NOTE: Traffic scheduling is defined in IEEE802.1Q</p>	Fulfilled. See 3.2.8
ID_40068	<p>End Devices shall provide the possibility to limit the transmission rate of egressing data per data class ('traffic shaping').</p> <p>NOTE: The correct ED traffic shaping can be supervised by the switch, see ID_40030</p>	Fulfilled. See 3.2.5
ID_60004	NG-TCN shall support the connection of ED-S implementing safety related function up to SIL 4	Fulfilled. See 3.5.3
ID_60005	ED-S connected to NG-TCN shall enter a defined safe state if the safe communication fails.	Fulfilled. See 3.5.3
ID_60006	ED-S connected to NG-TCN shall guarantee the same level of RAMS parameters as defined in section 4.1.	Fulfilled. See 2.11
ID_60007	The effort for certification of NG-TCN using ED-S for safety related functions shall not be higher than the effort for a legacy TCN using non-safe ED and train lines. This shall be demonstrated by T3.3 and T3.4 tasks	Partly fulfilled, see [06]. No quantitative analysis yet. Proposed for CTA-2.
ID_60008	ED-S shall implement their safety function using a NG-TCN considered as an untrusted transmission channel. ED-S and NG-TCN shall put in place all technological solutions in order to guarantee the safety level required by ED-S's safety applications.	Fulfilled. See 3.5.3
ID_60010	<p>ED-S connected to NG-TCN shall guarantee the compliance with EN50159 in order to enable the communication between ED using a non-trusted transmission system.</p> <p>NOTE: Compliance should be for category 2 or category 3, which category will finally be selected depends on the result of T3.3.</p>	Fulfilled. See 3.5.3

ID	Requirement Text	Implementation
ID_60012	ED-S shall use at least a single-channel communication system. Redundancy may be used optionally for increased availability	Fulfilled. See 2.2
ID_60013	ED-S shall implement a safety layer in between the safe application(s) and the untrusted communication channel. The safety layer shall provide safety services as defined in EN50159 at least to detect following Message characteristics: Message authenticity Message integrity Message timeliness Message sequence	Fulfilled. See 3.5.3
ID_60015	Due to the dynamic nature of train compositions with a varying number of consists, a 1:n communication relationship between the ED/ ED-S source and ED/ ED-S destination shall be supported	Fulfilled. See 2.7.1
ID_60016	ED-S and ED communication shall be independent. However, ED-S and ED shall be able to use the same communication channel	Fulfilled. See 2.2
ID_60035	Environmental conditions of NG-TCN shall be according to general railway requirements, mainly EN 50155, if there are no particular product standards	Fulfilled. See 2.11
ID_60036	When NG-TCN uses a black channel approach and no boundary constraints are defined (adopted bit-error-probability), the supervision by the safe data protocol must be able to detect errors/faults caused by Environmental problems (e.g. heat, humidity)	Fulfilled. See 3.5.3
ID_60037	NG-TCN shall support safety data communication between ED-S connected to different ECN of the same train	Fulfilled. See 3.5.3
ID_30100	The safety protocol should be able to detect error up to 1% of THR for SIL4 concerning the safety standards EN5012x (x=6,8,9), IEC61508, IEC6784-3, IEC61375 and EN50159.	Fulfilled. See 3.5.3
ID_30101	The Safety Layer of the ED-S should generate and supervise Safety-telegrams with all the relevant measures which belong to the table of EN50159 (Data corruption, Re-sequencing, lost repetition and so on).	Fulfilled. See 3.5.3
ID_60030	ED and ED-S connected to a NG-TCN shall have the a reliability value in order to satisfy the global NG-TCN reliability as defined in 4.1	Fulfilled. See 2.11
ID_60032	ED and ED-S connected to a NG NG-TCN may implement redundancy architecture to achieve the required reliability.	Fulfilled. See 2.2
ID_60033	NG-TCN shall support all traffic data as defined in EC61375-1 tab 7: Supervisory Data Process Data Message Data Stream Data – video – voice Best Effort Data	Fulfilled. See 2.8.3

ID	Requirement Text	Implementation
ID_20002	The architecture of the NG-TCN shall be designed to reach the required failure rate in a way that the NG-TCN can continue executing its functionality correctly in case of a failure which can lead to a service failure.	Fulfilled. See 2.11
ID_20004	The maximum failure rate of each function of the NG-TCN shall be: $\lambda \leq 10^{-7}$ failures/hour NOTE: only functions which may cause a service failure as defined in ID_20003 are affected	Fulfilled. See 2.11
ID_40019	Intra-consist communication shall not be interrupted during coupling or uncoupling of consists. NOTE: this might contradict the need of train wide clock resynchronization after inauguration	Fulfilled. See 2.2
ID_40020	A powerless or defective vehicle or consist shall not interrupt the train wide communication between consists which are not affected by the power loss/defect.	Partly Fulfilled. A powerless consist is not supported, see 2.5.3
ID_30000	A single point of failure in the network (e.g. wire-break, short cut, device defect) should not lead to a partial or complete communication loss of the entire NG-TCN. EXAMPLE 1: train wide communication shall not be affected by a ETBN being out-of-order EXAMPLE 2: a defective consist switch may only disrupt the communication of end devices directly connected to it, but not the communication between other end devices. EXAMPLE 3: a defective WLAN access point may disrupt the communication of wireless end devices associated to it, but not the communication between other end devices.	Fulfilled. See 2.11
ID_30001	A single point of failure in one ED or one ED-S should not lead to partial or complete communication loss of the NG-TCN.	Fulfilled. See 2.11
ID_30003	Special Environmental constraints should be defined to keep the bit error probability very low (wiring instructions) for a higher availability in general.	Fulfilled. See 2.11
ID_30004	Network Components only with reported MTBF by the supplier should be used in the network for a quantitatively calculation of the availability.	Fulfilled. See 2.11
ID_30006	An ED-S with main controlling functions of other ED (e.g. IO devices) should be redundant and operate in a "cold-stand by" mode with a maximal switch-over time.	Fulfilled. See 2.11
ID_30007	The maximum time for the permitted interruption of a communication over NG-TCN shall be less than 0.1s (consist network) and 1.0s for train backbone. NOTE: A possible solution for ECN could be the use of ring topology.	Fulfilled. See 2.11
ID_30011	The network quality should be traceable via standard tools and functions for providing early failure detection.	Fulfilled. See 2.11

ID	Requirement Text	Implementation
ID_30012	In case of a replacement of an ED or ED-S, it should be possible, that the network itself provide the necessary configuration (include addressing) parameter, so that the device replacement without removable media can take place. NOTE: Intention is to reduce mean-time of repairing	Fulfilled. See 2.11
ID_30014	The ED or ED-S should have the possibility to be connected to a redundant power supply without interferences to each other.	Fulfilled. See 2.11
ID_40069	It shall be possible to manufacture consists with identical NG-TCN configuration, except for the consist identifier which must be unique for each consist.	Fulfilled. See 2.11
ID_60034	ED-S and ED shall implement an alarm to request specific maintenance operations NOTE: 1) ED shall provide an alarm-service for internal malfunction of ED 2) In the context of preventive maintenance, ED-S shall provide an alarm-service for internal malfunction of ED-S. 3) ED-S and ED shall provide an alarm-service for internal deviations of their operation limits (for example range temperature)	Fulfilled. See 2.11
ID_30102	The HW of the ED-S has to fulfill a hazard rate THR of ED-S = 2 10E-11.	Fulfilled. See 2.11
ID_30103	SW executing safety related functions have to be developed in accordance to EN50128 SIL4.	Fulfilled. See 2.11
ID_30104	The relevant safety functions (Software) operating on ED-S has to fulfill the requirements of EN50128 and IEC61508 against random errors. (data corruption in memories, unexpected behaviour of COTS RTOS)	Fulfilled. See 2.11
ID_30105	A redundant HW-Structure of ED-S should be chosen for error-detection in each of the HW-Channel follow at least 1oo2 failsafe principle.	Fulfilled. See 2.11
ID_30106	The result of the train inauguration is needed for the detection of addressing errors in case of a safety relevant inter consist communication. Therefore the train inauguration and the storage of the result needs to be done in a safe manner	Fulfilled. See 2.11
ID_30108	For better Diagnostic Coverage (DC) in the case of an increasing bit error probability it could be useful to read some statistic information (for example CRC-Error) via SNMP. Therefore the switches should have implemented MIB2 and has to provide them via SNMP.	Fulfilled. See 2.11
ID_30109	network components which mimic failsafe telegrams are not allowed during failsafe operation.	Fulfilled. See 2.11
ID_60061	NG TCN shall provide following Security protections: 1) NG TCN shall Protect against malicious access to TCN resources 2) NG TCN shall ensure secure configuration of TCN resources 3) NG TCN shall Provide secure platform communication	Fulfilled. See 2.10

ID	Requirement Text	Implementation
	over all ED, ED-S 4) NG TCN shall Provide secure wireless train to ground communication 5) NG TCN shall Provide secure wireless intra consist communication	
ID_40070	Data traffic belonging to different security domains has to be separated in a way that it is equivalent to physical separation.	Fulfilled. See 2.10
ID_40071	All programmable devices (ED, ED-S and ND) connected to NG-TCN shall support logging of security events. Security events can be (list not exhaustive): - configuration change (including SW change) - unexpected incoming traffic (e.g. a tagged Ethernet frame ingressing with invalid VID) - device startup or reboot - unauthorized access attempt (e.g. service access with invalid credentials) - Link layer status change (up/down) - system time change	Fulfilled. See 3.5.7
ID_40073	The ETB consist interface shall be specified for data communication between Virtual Function Bus (all OSI communication layers except the application data itself) between ED/ED-S belonging to different consists.	Fulfilled. See 2.7
ID_40074	The specified ETB consist interface shall be proposed for standardization in IEC61375.	Fulfilled. See Annex D
ID_40075	For process data and message data exchange between: ED and ED or, ED-S and ED-S or, ED-S to ED ED to ED-S (without safety) belonging to different consists, the TRDP application layer protocol as specified in IEC61375-2-3 shall be used.	Fulfilled. See 3.5.2
ID_60048	5 Requirements for the lab demonstrator platform for proof-of-concept	Fulfilled. See Annex F
ID_60062	The demonstration platform shall be able to indicate the ability of NG TCN to implement the basic needs related at least to: 1) Clock synchronization needs. 2) Process synchronization needs. 3) Traffic shaping needs at least at switch level. 4) Real-time performance needs (closed loop latency measurement).	Fulfilled. See Annex F
ID_60063	The demonstration platform shall be realized by existing components. If specific components are required, the demonstration platform shall evaluate the related performances index with existing components and then an evaluation of the final result (result with specific components) shall be carried out by mean mathematical models	Fulfilled. See Annex F

ID	Requirement Text	Implementation
ID_60064	<p>The demonstration process shall be defined identifying at least following data.</p> <p>1) General info: date, place, operator, environmental conditions etc.</p> <p>2) Test environments set up, test conditions</p> <p>3) Devices under tests.</p> <p>4) Expected data and their acceptability range</p> <p>5) Measured data and precision.</p> <p>6) Acceptability criteria.</p>	Fulfilled. See Annex F
ID_60051	The NG-TCN shall provide a standard interface to simulate the TCMS by computer simulation	This requirement is not addressed by NG-TCN architecture. This in general is subject of CTA WP6.
ID_60052	The NG-TCN shall provide a standard interface to simulate the Signaling system	This requirement is not addressed by NG-TCN architecture. This in general is subject of CTA WP6.
ID_60053	The NG-TCN shall provide a standard interface to allow the simulation of ED devices.	This requirement is not addressed by NG-TCN architecture. This in general is subject of CTA WP6.
ID_60062	<p>All network devices implementing NG-TCN shall provide a standard interface based on SNMP to retrieve diagnostic information.</p> <p>NOTE: MIBs can be defined during architetture work</p>	Fulfilled. See 3.5.5
ID_60060	<p>ND and ED devices shall provide a standard diagnosis interface to TCN in order to enable the collection of standardized diagnosis data such as:</p> <p>1) Internal version of ND and ED.</p> <p>2) Internal status of ND and ED.</p> <p>3) Error and Warning of ND and ED.</p> <p>4) Logger specific data of ND and ED.</p> <p>The NG-TCN shall provide a standard maintenance interface to retrieve all the above diagnostic data of each ND and ED connected to TCN</p>	This requirement is not addressed by NG-TCN architecture..

D Annex – Input to standardization

D.1 Motivation and background

The architecture of the NG-TCN bases on the IEC61375 standard series. This standard series, which defines the Train Communication Network (TCN), was initiated in the beginning of the 90ties of the 20th century with the objective to define a communication network which establishes interoperability between train vehicles of different types and from different manufacturers. During the first wave of standardization (1991 – 1999), serial bus based technologies have been specified (WTB and MVB), which are until today still widely in use. In a second wave (2006 – 2015), a new network concept basing on Ethernet and IP technology has been introduced, leading to the definition of ETB and ECN as we know it today. Some of the new standard parts are even today not completed, like the conformance testing and the definition of application profiles. Other parts, like the train-to-wayside communication, require an overhaul to be practically usable.

The TCN standardization work of the second wave lies in the responsibility of the IEC Working Group 43 (WG43), where some of the participants in CONNECTA WP3 are member of. This circumstance facilitates the triggering of a third wave, which shall introduce the drive-by-data concepts into standardization. As for the standardization activities before, the objective is to ensure interoperability, which practically means that only those parts of the drive-by-data concept have to be considered that affect interoperability.

During the CONNECTA/Safe4Rail Advisory Board meeting held in June 2018, the question was raised how to initiate the drive-by-data standardization in the best manner. It was concluded that a simple amendment of existing standards will not be possible, because amendments are only possible in case of errors or unclarities. For significant technical changes a new revision of existing standard parts or even new standard parts have to be initiated. According to the process defined by IEC a New Work Item Proposal (NWIP) has to be submitted and has to be accepted by the IEC Technical Committee 9 (TC9). The standardization work itself can be done in the still active WG43.

The standardization process can be accelerated when, together with the NWIP, a draft version of the revised standard text is submitted. This draft version can then immediately be circulated as a committee draft (CD) of the standard. Subsequent steps are then CDV (Committee Draft for Vote), FDIS (Final Draft of International Standard) and IS (International Standard). When, as planned, the NWIP and the draft version are submitted in 2019 (supported by CONNECTA-2), a finalized standard can be released in 2022.

D.2 Proposed changes and extensions

Introducing Drive-by-Data concepts affects several TCN standard parts. Table 64 lists the affected standard parts and the related standard clauses.

Table 64: TCN Standard extensions

Standard part	Clause	Changes
IEC61375-1	5.2	Add ETB topology with separated ETB lines as an option
	5.2	Exclude new ETB topology from bypass
	5.6	Exclude new ETB topology from correction

Standard part	Clause	Changes
IEC61375-2-3	6.3	Add ECN topology with ring and dual homing
	4.3	Introduce ETB topology with separated ETB lines as an option
	5.6	Add specification of scheduled traffic over ETB
	6.6	Exclude “correction” for new ETB topology variant
	Annex A	Add specification of TSN-PD
	Annex B	Add specification of SDTv4
	Annex E	Add TTDB manager interface telegram that informs all ED in a consist about the local cstUUID value (see 3.5.5). This telegram should neither be SDTv2 nor SDTv4 protected.
	Annex F	Extend conformance test to scheduled traffic
IEC61375-2-5	4.2	Adding GbE transmission speed (1000BASE-T), interface and cable
	4.2	Adding 10GbE transmission speed, interface and cable as option
	4.2	Restrict bypass to ETB topology with aggregated ETB lines
	4.4	Introduce ETB topology with separated ETB lines as an option
	5	Add support of 802.1Qbv Time Aware Shaper
	5	Add new sub-clause about time synchronization
	5	Add new sub-clause about TSN
	5	Add new sub-clause about security on ETB level
	7	Add sub-clause about TSN-GW
	8	Add extension of TTDP protocol for ETB Topology variant with separated ETB lines
	8	Improve HELLO-frame checksum (see [05])
	8	Detection of duplicated MAC addresses in CT (see [05])
	8	Check for contradiction between parameter ‘egressDir’ in received HELLO-frames and direction derived from local CV (see [05]).
	11	Describe 802.1Qbv Time Aware Shaper
	11	New data class of scheduled process data
IEC61375-3-4	Annex A	Adapt for ETB Topology variant with separated ETB lines
	Annex C	Add support for ETB Topology variant with separated ETB lines
	4.2.3	Introduce TSN-aware ED as new ED class
	4.4	Add scheduled traffic as new service
	4.5	Introduce the A-Plane/B-Plane approach for scheduled traffic
	4.6	Add support of 802.1Qbv Time Aware Shaper
	4.9	Adding GbE transmission speed (1000BASE-T), interface and cable
	4.9	Adding 10GbE transmission speed, interface and cable as option
	4.9	Add support of time synchronization
	4.9	Add support of 802.1Qbv Time Aware Shaper
	4.10	Adding GbE transmission speed (1000BASE-T), interface and cable
	4.10	Add support of time synchronization
	4.10	Add support of 802.1Qbv Time Aware Shaper
	4	Add new sub-clause about TSN-GW
	4	Add new sub-clause about security

Standard part	Clause	Changes
IEC61375-2-8	All relevant clauses	Add conformance test for GbE transmission speed (1000BASE-T), interface and cable
		Add conformance test for 10GbE transmission speed, interface and cable
		Add conformance test for time synchronization
		Add conformance test for scheduled process data
		Add conformance test for extended TTDP

D.3 Other affected standards

Table 64 lists UNISID standards which are affected by NG-TCN.

Table 65: UNISIG Standard extensions

Standard part	Reference	Changes
Subset 119	E.2.3	should be reviewed to consider SDTv4
ERA_ERTMS_015560	E.2.5	should define as mandatory an internal functional interface between DMI and EVC following the physical approach considered by the ED-S architecture over NG-TCN
Subset 027	E.2.6	integration of ETCS onboard – JRU interface in the context of NG-TCN could be done considering JRU as a non-safety related ED
Subset 139	E.4.1	Consider ATO interfaces to vehicle functions over NG-TCN

E Annex – Reflection on Signalling subsystem integration

E.1 Signalling system

One aim of the NG-TCN is to support CONNECTA's KPIs (see [02]) which address the main goals of Shift2Rail:

Decreasing the life cycle cost of railway transports to 50%

Increasing railway capacity up to 100 %

Increasing reliability and punctuality up to 50%

This chapter is focused on the Integration of signalling system within the NG-TCN. In order to provide an end to end indication of integration effort, the fulfilment of NG-TCN respect to functional requirements of signalling system will be provided. If the signalling system defines a specific physical interface with some subsystem the gap will be highlighted in order to provide a summary of the gaps in the integration process.

E.2 Integration of ETCS Signalling components in NG TCN

Table 66: NG-TCN Signalling function requirements.

ID	Requirement Text (taken from [03])	Implementation
ID_60097	<p>This chapter is dedicated to the integration of ED-S implementing Signaling Functions (ED-S.SF) in the context of the NG-TCN. The NG-TCN shall provide the support to ED-S.SF in terms of communication needs in order to make the ED-S.SF able to perform their signaling functions.</p> <p>The ED-S.SF communication needs will be identified by means of Signaling Functions interface requirements as listed below.</p>	<p>The requirement is tagged as info only in the document [03], therefore it doesn't export any particular requirement to NG-TCN. Nevertheless, the info points out that the NG-TCN shall enable the Signaling Functions to be integrate in the new communication context.</p>
ID_60070	<p>Signaling System is an important part of any railway operations management system. In the past a number of different Signaling Systems have evolved in different countries at different times. These systems are incompatible and not interoperable with each other and are known as NTC (National train Control System).</p> <p>To overcome the above problem the ERTMS system has been developed in order to provide a standard Signaling system over all European Union.</p> <p>Signaling Metros traffic management systems are not standardized and they are known as ATC, CBTC etc. but all of these solutions are supplier dependent and often and ATO subsystem in integrated.</p>	<p>The requirement is tagged as info only in the document [03]. The info classifies the signaling system in two main groups: Standardized signaling systems, for example ERTMS, and non-standardized Signalling system.</p> <p>The NG-TCN should consider the integration of ERTMS as a standard solution. The integration of non-standard signaling system should be possible but specific project dependent.</p>
ID_60071	<p>Due to the nature of the required functions, the signaling system will have to be partly on the trackside and partly on board the trains.</p> <p>This defines two sub-systems, the on-board sub-system and the trackside sub-system.</p> <p>The on board sub-system has an interface with the vehicle therefore it has some relevance in the context of</p>	<p>The requirement is tagged as info only in the document [03]. The info identifies two entities for signaling systems: on board and trackside equipment. In the context of this document only ETCS onboard ED-S.SF</p>

ID	Requirement Text (taken from [03])	Implementation
	this document. For the reasons explained above, only ETCS on-board functions have been standardized so we will deal mainly with these functions.	devices have to be taken into account
ID_60072	NG-TCN shall allow ERTMS/ETCS on-board equipment to interface the NG-TCN in order to make the ERTMS/ETCS system able to perform its signaling functions according to the ETCS baseline specifications as defined by ERA in a list of mandatory subsets.	The requirement is tagged as Functional in the document [03]. E.2.1 reports more details about the fulfillment of this requirement.
ID_60072	NOTE 1: next to mandatory subset for ETCS a set of informative subset for ETCS are available at ERA website at link: List-of-supporting-informative-specifications---Set-of-specifications-2-.aspx">http://www.era.europa.eu/Core-Activities/ERTMS/Pages>List-of-supporting-informative-specifications---Set-of-specifications-2-.aspx NOTE 2: Some informative subsets could, by the time, become mandatory subsets: example SUBSET-119 (FFFIS train interface)	The requirement is tagged as info only in the document [03]. The info identifies the reference standards for the Signaling System.
ID_60074	NG-TCN is intended to allow ERTMS/ETCS on-board subsystem to access external interfaces of the ETCS system as defined in SUBSET-026-2 (System Requirements Specification) and hereafter represented in (Figure 6). On each external interface, the relative subset reference number is represented. More specific requirements on the interfaces can be found underneath.	The requirement is tagged as info only in the document [03] The info gives an overview to the signaling system which is better explained in E.2.2
ID_60076	NG-TCN shall enable ERTMS/ETCS on-board subsystem to interface the train according to SUBSET-034 (Train interface). The I/O information on Train Interface and the direction of the information is described in chapter 2 of SUBSET-034 (Train interface). NOTE 1: An informative standard SUBSET-119 (Train Interface FFFIS) on train interface has been delivered, the standard is pending to be approved as normative standard. The I/O signal between ERTMS/ETCS on-board subsystem and vehicle are defined in table 2.1 of SUBSET-119 (the list of I/O signals is reported in Figure 141). NOTE 2: An informative standard SUBSET-120 (FFFIS TI – Safety Analysis) on train interface safety analysis has been delivered , the standard is pending to be approved as normative standard.	The requirement is tagged as SIL>0 functional requirement in the document [03]. The requirement has been analyzed in E.2.3.

ID	Requirement Text (taken from [03])	Implementation
ID_60077	<p>The ERTMS/ETCS on-board subsystem connected to NG-TCN may interface to STM (Class B systems called also "legacy ATP") by a dedicated function (e.g. a gateway), which however is out of scope of this specification.</p> <p>NOTE 1: This interface is defined in:</p> <ul style="list-style-type: none"> 1) SUBSET-035 (Specific Transmission Module FFFIS) 2) SUBSET-056 (STM FFFIS Safe Time Layer) 3) SUBSET-057 (STM FFFIS Safe Link Layer) 4) SUBSET-058 (FFFIS STM Application Layer) <p>NOTE 2: In the above standards, the interface ERTMS/ETCS- STM, is a PROFIBUS interfaces.</p> <p>NOTE 3: The document ERA/TD/2011-11 (LIST OF CLASS B SYSTEMS) contains the list of train protection legacy systems (Class B systems) required in the Control-Command and Signaling TSI.</p> <p>NOTE 4 : Figure 7 shows the context of ETCS-STM interface, Table 11 of Annex C collects performance requirement of the interface.</p>	<p>The requirement is tagged as SILO functional requirement in the document [03]</p> <p>The requirement has been analyzed in E.2.4.</p>
ID_60079	<p>NG-TCN shall enable ERTMS/ETCS on-board subsystem to interface with the DMI (Driver machine Interface) according to ERA_ERTMS_015560 (ETCS DRIVER MACHINE INTERFACE).</p> <p>NOTE 1: An informative SUBSET-121 (DMI-EVC Interface FFFIS) has been delivered on DMI interface. The subset concerns the integration of Train Display System to integrate and ERTMS/ETCS subsystem display in one device.</p> <p>NOTE 2. Performance requirements between ERTMS/ETCS on-board subsystem and DMI are defined in Table10.1 SUBSET-121 (DMI-EVC Interface FFFIS). and in Table 10 of Annex C</p>	<p>The requirement is tagged as SILO functional requirement in the document [03].</p> <p>The requirement has been analyzed in E.2.5.</p>
ID_60080	<p>NG-TCN shall enable ERTMS/ETCS on-board subsystem to interface with the JRU according to SUBSET-027 (FIS Juridical Recording).</p> <p>NOTE: The interface between ERTMS/ETCS on-board subsystem and JRU ensures the recording of message and process data as defined in Table 13 Annex C (List of triggering events and related messages) of SUBSET-027.</p>	<p>The requirement is tagged as SILO functional requirement in the document [03].</p> <p>The requirement has been analyzed in E.2.6.</p>

ID	Requirement Text (taken from [03])	Implementation
ID_60081	<p>The NG-TCN shall coexist with G interface without interfering with each other. The operative conditions of G interfaces are standardized in SUBSET-100 (Interface 'G' Specification).</p> <p>NOTE: The interface ERTMS/ETCS on-board-Balise (Interface 'G') can be seen as an internal signaling system interfaces.(Figure 8)</p> <p>The NG-TCN should at least be compatible with this interface in the sense of the two systems can coexist under defined conditions without interfering with each other as to specified functions.</p>	<p>The requirement is tagged as SIL>0 functional requirement in the document [03].</p> <p>The requirement has been analyzed in E.2.7.</p>
ID_60083	<p>The NG-TCN shall coexist with Eurobalise interface without interfering with each other. The operative conditions of Eurobalise interface is standardized in SUBSET-036 (FFFIS for Eurobalise), see Figure 9.</p> <p>NOTE: The interface between ERTMS/ETCS on-board and Eurobalise can be seen as an internal signaling system interfaces.</p> <p>The NG-TCN should at least be compatible with this interface in the sense of the two systems can coexist under defined conditions without interfering with each other as to specified functions.</p>	<p>The requirement is tagged as SIL>0 functional requirement in the document [03].</p> <p>The requirement has been analyzed in E.2.8.</p>
ID_60085	<p>The NG-TCN shall coexist with Euroloop interface without interfering with each other. The operative conditions of Euroloop interface is standardized in SUBSET-044 (FFFIS for Euroloop).</p> <p>NOTE: The interface ERTMS/ETCS on-board -Euloop can be seen as an internal signaling system interfaces.</p> <p>The NG-TCN should at least be compatible with this interface in the sense of the two systems can coexist under defined conditions without interfering with each other as to specified functions.</p>	<p>The requirement is tagged as SIL>0 functional requirement in the document [03].</p> <p>The requirement has been analyzed in E.2.9.</p>
ID_60086	<p>The NG-TCN shall support the EuroRadio interface (train-to-ground communication specified in CONNECTA WP2). The operative conditions of EuroRadio interface are standardized in SUBSET-037 (EuroRadio FIS) and UIC document A11T 6001 (Radio Transmission FFFIS for EuroRadio), see Figure 10.</p> <p>NOTE: "support" can also mean "coexistence" for the case that a separate physical interface is used. In that case, the NG-TCN shall coexist with EuroRadio interface without interfering with each other.</p>	<p>The requirement is tagged as SIL>0 functional requirement in the document [03].</p> <p>The requirement has been analyzed in E.2.10.</p>
ID_60088	<p>The signaling system used for metro system are not standardized however some common standard are used as reference such as:</p> <ul style="list-style-type: none"> - IEEE Std 1474 Series for Communications Based Train Control (CBTC). - IEC 62290 Series for Urban Guided Transport Management and command/control Systems (UGTMS) 	<p>The requirement is tagged as info only in the document [03].</p> <p>The info identifies the available standards for Metro systems.</p>

ID	Requirement Text (taken from [03])	Implementation
ID_60089	<p>NG-TCN shall be compatible with on board part of CBTC and UGTMS systems according to:</p> <ul style="list-style-type: none"> - IEEE Std 1474 Series for Communications Based Train Control (CBTC). - IEC 62290 Series for Urban Guided Transport Management and command/control Systems (UGTMS) <p>NOTE: This may be a subject of future investigations</p>	<p>Document [03] qualifies the requirements as functional.</p> <p>The requirement has been analyzed in E.3.1.</p>
ID_60090	<p>The railways have identified an opportunity to achieve improved capacity, on-time performance and make energy efficiency improvements through developing and implementing Automatic Train Operation (ATO). ATO is the sub-system which performs some or all of the functions of automatic speed regulation, accurate stopping, door opening and closing, performance level regulation, and other functions assigned to a train driver or train attendant.</p> <p>ATO is widely spread in Metro signaling systems, even if it is not a standardized subsystem.</p> <p>The integration of ATO with ERTMS system is an ongoing action on ERTMS USER group and a set of Specific UNISIG subset are planned.</p>	<p>The requirement is an info only in the document [03].</p> <p>The intent of info is to underline the advantage of ATO in the future signaling systems, therefore the NG-TCN architecture should take the need to support specific function (if any) coming from ATO into account.</p>
ID_60091	<p>The ATO over ETCS is an interoperable ATO that shall realize the benefits of ATO when applied to different railway infrastructures: urban, suburban, main line and high speed railways. The high level requirements of ATO over ETCS are collected in document EUG N. 13E137, the document is available at ERA Agency web site, link:</p> <p>http://www.era.europa.eu/Document-Register/Documents/ATO_Ops_Requirements_v1_7.pdf.</p>	<p>The requirement is an info only in the document [03].</p> <p>The intent of info is to introduce document EUG N. 13E137 [48] which contains the Operational Requirements of ATO over ERTMS.</p> <p>The document defines ATO as a non safety critical and interoperable component able to operate where the ETCS ATP guarantees the safety. NG-TCN should be able to provide the communication services needed for ATO</p>
ID_60092	<p>The ATO over ETCS system is based on two sub-systems: the ATP system and the ATO system, both ETCS and ATO include on-board and trackside constituents.</p> <p>ATO can only drive the train automatically in areas where ETCS is guaranteeing the safe movement of the train.</p> <p>ETCS supervises the train ensuring that speed and movement limits are observed and the train proceeds only when it is allowed by the trackside to do so.</p> <p>The ATO on-board automatically drives trains, through control of acceleration and braking, including but not limited to accurate stopping at specified stopping positions using operational data provided by a traffic management system (TMS) and infrastructure data provided by trackside equipment.</p>	<p>The requirement is an info only in the document [03].</p> <p>The intent of info is to introduce some specific ATO interfaces as defined in document EUG N. 13E137 [48].</p> <p>The ATO shall interface at least:</p> <ul style="list-style-type: none"> Traction and brake systems, DMI and ATP subsystem, Trackside subsystems PIS, passengers request and Fire alarm devices. <p>NG-TCN should be able to provide the communication services needed for ATO</p>

ID	Requirement Text (taken from [03])	Implementation
ID_60093	<p>ATO is not a safety critical system and therefore any identified safety requirements as a result of the ATO operational requirements will be assigned to other safety systems e.g. ETCS or Train Control Management Systems.</p>	<p>The requirement is an info only in the document [03]. The intent of info (coming from document EUG N. 13E137 [48]) is to introduce ATO as a non-safety critical ED which shall be under the control of a safety critical ED-S. ATO shall interact in a time critical way with traction subsystem. NG-TCN shall ensure the above needs.</p>
ID_60094	<p>NG-TCN shall be compatible with ATO to interface external subsystems according to the planned subset. NOTE1: The ATO SUBSET documents describing the external ATO Interfaces are ongoing in ERTMS USER GROUP, However a planned architecture is available in EUG document N. 13E137 (Figure 11) NOTE2: ATO-train interface has been planned in SUBSET 139.</p>	<p>The requirement is a SIL2 functional requirement in the document [03]. The requirement has been analyzed in E.4.1.</p>

E.2.1 ID_60072

This requirement ID_60072 expresses the general goal of NG-TCN to be able to interface on board signalling equipment. On the other hand, the onboard signalling system is composed of different equipment (ED in the context of NG-TCN) implementing different functions, most of them are already standardized for interoperability purpose. In particular, the European commission has delivered a Commission Regulation (EU) 2016/919 of 27 May 2016 regarding the (CCS TSI) technical specification for interoperability relating to the ‘control-command and signalling’ subsystems of the rail system in the European Union.

The CCS TSI 2016 (in Table 5.1 a, see Figure 131 and Figure 132) defines the basic interoperability constituents in the Control-Command and Signalling Subsystems for the Control-Command and Signalling On-board Subsystem. The interoperability of constituents is assured by fulfilment of mandatory requirement in TSI Table A.2.3 (see Figure 133, Figure 134, Figure 135, Figure 136, Figure 137) and TSI Table A.3 (see Figure 138).

Table 5.1.a
Basic interoperability constituents in the Control-Command and Signalling On-board Subsystem

1	2	3	4
N	Interoperability constituent IC	Characteristics	Specific requirements to be assessed by reference to Chapter 4
1	ETCS on-board	Reliability, Availability, Maintainability, Safety (RAMS)	4.2.1 4.5.1
		On-board ETCS functionality (excluding odometry)	4.2.2
		ETCS and GSM-R air gap interfaces	4.2.5
		— RBC (level 2 and level 3)	4.2.5.1
		— Radio in-fill unit (optional level 1)	4.2.5.1
		— Eurobalise air gap	4.2.5.2
		— Euroloop air gap (optional level 1)	4.2.5.3
		Interfaces	
		— STM (implementation of interface K optional)	4.2.6.1
		— GSM-R ETCS Data Only Radio	4.2.6.2
		— Odometry	4.2.6.3
		— Key management system	4.2.8
		— ETCS ID Management	4.2.9
		— ETCS Driver-Machine Interface	4.2.12
		— Train interface	4.2.2
		— On-board recording device	4.2.14
		Construction of equipment	4.2.16

Figure 131: Table 5.1 a as defined in CCS TSI 2016

1	2	3	4
N	Interoperability constituent IC	Characteristics	Specific requirements to be assessed by reference to Chapter 4
2	Odometry equipment	Reliability, Availability, Maintainability, Safety (RAMS)	4.2.1 4.5.1
		On-board ETCS functionality: only Odometry	4.2.2
		Interfaces — On-board ETCS	4.2.6.3
		Construction of equipment	4.2.16
3	Interface of External STM	Interfaces — On-board ETCS	4.2.6.1
4	GSM-R voice cab radio Note: SIM card, antenna, connecting cables and filters are not part of this interoperability constituent	Reliability, Availability, Maintainability, Safety (RAMS)	4.2.1 4.5.1
		Note: no requirement for safety	
		Basic communication functions	4.2.4.1
		Voice and operational communication applications	4.2.4.2
		Interfaces — GSM-R air gap — GSM-R Driver-Machine Interface	4.2.5.1 4.2.13
		Construction of equipment	4.2.16
5	GSM-R ETCS Data only Radio Note: SIM card, antenna, connecting cables and filters are not part of this interoperability constituent	Reliability, Availability, Maintainability, Safety (RAMS)	4.2.1 4.5.1
		Note: no requirement for safety	
		Basic communication functions	4.2.4.1
		ETCS data communication applications	4.2.4.3
		Interfaces — On-board ETCS — GSM-R air gap	4.2.6.2 4.2.5.1
		Construction of equipment	4.2.16
6	GSM-R SIM card Note: it is the responsibility of the GSM-R network operator to deliver to railway undertakings the SIM cards to be inserted in GSM-R terminal equipment	Basic communication functions	4.2.4.1
		Construction of equipment	4.2.16

Figure 132: Table 5.1 a as defined in CCS TSI 2016 (cont.)

Table A.2.3

List of mandatory specifications

Index No	Set of specifications # 3 (ETCS Baseline 3 Release 2 and GSM-R Baseline 1)			
	Reference	Name of Specification	Version	Notes
1	Intentionally deleted			
2	Intentionally deleted			
3	SUBSET-023	Glossary of Terms and Abbreviations	3.3.0	Note 14
4	SUBSET-026	System Requirements Specification	3.6.0	Note 14
5	SUBSET-027	FIS Juridical Recording	3.3.0	Note 14
6	ERA_ERTMS_015560	ETCS Driver-Machine interface	3.6.0	Note 14

Figure 133: Table A.2.3 as defined in CCS TSI 2016

Index No	Set of specifications # 3 (ETCS Baseline 3 Release 2 and GSM-R Baseline 1)			
	Reference	Name of Specification	Version	Notes
7	SUBSET-034	Train Interface FIS	3.2.0	
8	SUBSET-035	Specific Transmission Module FFHS	3.2.0	
9	SUBSET-036	FFHS for Eurobalise	3.1.0	
10	SUBSET-037	EuroRadio FIS	3.2.0	
11	SUBSET-038	Offline key management FIS	3.1.0	
12	SUBSET-039	FIS for the RBC/RBC handover	3.2.0	
13	SUBSET-040	Dimensioning and Engineering rules	3.4.0	
14	SUBSET-041	Performance Requirements for Interoperability	3.2.0	
15	Intentionally deleted			
16	SUBSET-044	FFHS for Euroloop	2.4.0	
17	Intentionally deleted			
18	Intentionally deleted			
19	SUBSET-047	Trackside-Trainborne FIS for Radio infill	3.0.0	
20	SUBSET-048	Trainborne FFHS for Radio infill	3.0.0	
21	Intentionally deleted			
22	Intentionally deleted			
23	SUBSET-054	Responsibilities and rules for the assignment of values to ETCS variables	3.0.0	
24	Intentionally deleted			
25	SUBSET-056	STM FFHS Safe time layer	3.0.0	
26	SUBSET-057	STM FFHS Safe link layer	3.1.0	
27	SUBSET-091	Safety Requirements for the Technical Interoperability of ETCS in Levels 1 and 2	3.6.0	Note 14
28	Intentionally deleted			
29	SUBSET-102	Test specification for interface 'K'	2.0.0	
30	Intentionally deleted			
31	Reserved SUBSET-094	Functional requirements for an on-board reference test facility		Note 13

Figure 134: Table A 2.3 as defined in CCS TSI 2016 (cont.)

Index No	Set of specifications # 3 (ETCS Baseline 3 Release 2 and GSM-R Baseline 1)			
	Reference	Name of Specification	Version	Notes
32	EIRENE FRS	GSM-R Functional requirements specification	8.0.0	Note 10
33	EIRENE SRS	GSM-R System requirements specification	16.0.0	Note 10
34	A11T6001	(MORANE) Radio Transmission FFHS for EuroRadio	13.0.0	
35	Intentionally deleted			
36 a	Intentionally deleted			
36 b	Intentionally deleted			
36 c	SUBSET-074-2	FFHS STM Test cases document	3.1.0	
37 a	Intentionally deleted			
37 b	Reserved SUBSET-076-5-2	Test cases related to features		Note 13
37 c	Reserved SUBSET-076-6-3	Test sequences		Note 13
37 d	Reserved SUBSET-076-7	Scope of the test specifications		Note 13
37 e	Intentionally deleted			
38	06E068	ETCS Marker-board definition	2.0	
39	SUBSET-092-1	ERTMS EuroRadio Conformance Requirements	3.1.0	
40	SUBSET-092-2	ERTMS EuroRadio test cases safety layer	3.1.0	
41	Intentionally deleted			
42	Intentionally deleted			
43	SUBSET 085	Test specification for Eurobalise FFHS	3.0.0	
44	Intentionally deleted			Note 9
45	SUBSET-101	Interface 'K' Specification	2.0.0	
46	SUBSET-100	Interface 'G' Specification	2.0.0	
47	Intentionally deleted			
48	Reserved	Test specification for mobile equipment: GSM-R		Note 4
49	SUBSET-059	Performance requirements for STM	3.1.0	
50	SUBSET-103	Test specification for Euroloop	1.1.0	
51	Intentionally deleted			

Figure 135: Table A 2.3 as defined in CCS TSI 2016 (cont.)

Index No	Set of specifications # 3 (ETCS Baseline 3 Release 2 and GSM-R Baseline 1)			
	Reference	Name of Specification	Version	Notes
52	SUBSET-058	FFFS STM Application layer	3.2.0	
53	Intentionally deleted			
54	Intentionally deleted			
55	Intentionally deleted			
56	Intentionally deleted			
57	Intentionally deleted			
58	Intentionally deleted			
59	Intentionally deleted			
60	SUBSET-104	ETCS System Version Management	3.3.0	
61	Intentionally deleted			
62	Intentionally deleted			
63	SUBSET-098	RBC-RBC Safe Communication Interface	3.0.0	
64	EN 301 515	Global System for Mobile Communication (GSM); Requirements for GSM operation on railways	2.3.0	Note 2
65	TS 102 281	Detailed requirements for GSM operation on railways	3.0.0	Note 3
66	TS 103 169	ASCI Options for Interoperability	1.1.1	
67	(MORANE) P 38 T 9001	FFFS for GSM-R SIM Cards	5.0	Note 10
68	ETSI TS 102 610	Railway Telecommunication: GSM; Usage of the UUIE for GSM operation on railways	1.3.0	
69	(MORANE) F 10 T 6002	FFFS for Confirmation of High Priority Calls	5.0	
70	(MORANE) F 12 T 6002	FIS for Confirmation of High Priority Calls	5.0	
71	(MORANE) E 10 T 6001	FFFS for Functional Addressing	4.1	
72	(MORANE) E 12 T 6001	FIS for Functional Addressing	5.1	
73	(MORANE) F 10 T 6001	FFFS for Location Dependent Addressing	4	
74	(MORANE) F 12 T 6001	FIS for Location Dependent Addressing	3	

Figure 136: Table A 2.3 as defined in CCS TSI 2016 (cont.)

Index No	Set of specifications # 3 (ETCS Baseline 3 Release 2 and GSM-R Baseline 1)			
	Reference	Name of Specification	Version	Notes
75	(MORANE) F 10 T 6003	FFFS for Presentation of Functional Numbers to Called and Calling Parties	4	
76	(MORANE) F 12 T 6003	FIS for Presentation of Functional Numbers to Called and Calling Parties	4	
77	ERA/ERTMS/033281	Interfaces between CCS trackside and other subsystems	3.0	Note 7
78	Intentionally deleted			Note 6
79	SUBSET-114	KMC-ETCS Entity Off-line KM FIS	1.0.0	
80	Intentionally deleted			Note 5
81	SUBSET-119	Train Interface FFHS		Note 12
82	SUBSET-120	FFHS TI — Safety Analysis		Note 12
83	SUBSET-137	On-line Key Management FFHS	1.0.0	

Note 1: only the functional description of information to be recorded is mandatory, not the technical characteristics of the interface

Note 2: the clauses of the specifications listed in point 2.1 of EN 301 515 which are referenced in Index 32 and Index 33 as 'MI' are mandatory.

Note 3: the change requests (CRs) listed in Tables 1 and 2 of TS 102 281 which affect clauses referenced in Index 32 and Index 33 as 'MI' are mandatory.

Note 4: Index 48 refers only to test cases for GSM-R mobile equipment. It is kept 'reserved' for the time being. The application guide will contain a catalogue of available harmonised test cases for the assessment of mobile equipment and networks, according to the steps indicated in point 6.1.2 of this TSI.

Note 5: the products which are on the market are already tailored to the needs of the RU related to GSM-R Driver-Machine Interface and fully interoperable so there is no need for a standard in the TSI CCS.

Note 6: information that was intended for Index 78 is now incorporated in Index 27 (SUBSET-091).

Note 7: this document is ETCS and GSM-R baseline independent.

Note 8: Intentionally deleted.

Note 9: ERA analysis showed there is no need for a mandatory specification for odometry interface.

Note 10: Only the (MI) requirements are mandated by TSI CCS.

Note 11: Intentionally deleted.

Note 12: Reference to these specifications will be published in the Application Guide, waiting for clarifications on the rolling stock side of the interface.

Note 13: Specifications to be set out in a technical opinion of the Agency.

Note 14: Additional information to be displayed in the Driver-Machine interface with the purposes of the drivers' ergonomics will be published by the Agency in a technical document (¹).

(¹) The Agency Technical Document developed in cooperation with the sector in line with the request of the Committee referred to in Article 29(1) of Directive 2008/57/EC defines the additional elements of information on the Driver-Machine Interface and identifies the changes in the relevant specification documents. The content of the Agency's technical document is consolidated with the other requirements relevant for the Driver-Machine Interface resulting in the updated documents in the Indices 3, 4, 5, 6 and 27.

Figure 137: Table A 2.3 as defined in CCS TSI 2016 (cont.)

Table A 3
List of mandatory standards

The standards listed in the table below shall be applied in the certification process, without prejudice for the provisions of Chapter 4 and Chapter 6 of this TSI.

No	Reference	Document name and comments	Version	Note
A1	EN 50126	Railway applications — The specification and demonstration of reliability, availability, maintainability and safety (RAMS)	1999	1
A2	EN 50128	Railway applications — Communication, signalling and processing systems — Software for railway control and protection systems	2001 or 2011	
A3	EN 50129	Railway applications — Communication, signalling and processing systems — Safety related electronic systems for signalling	2003	1
A4	EN 50159	Railway applications — Communication, signalling and processing systems	2010	1

Note 1: this standard is harmonised, see Commission communication in the framework of the implementation of the Directive 2008/57/EC of the European Parliament and of the Council of 17 June 2008 on the interoperability of the rail system within the Community (OJ C 345, 26.11.2013, p. 3), where also published editorial corrigenda are indicated.

Figure 138: Table A 3 as defined in CCS TSI 2016

From the above normative picture, it is evident that to integrate ERTMS on board signalling components as ED in the context on NG-TCN we have to face following conflicting needs.

1. NG-TCN goal to provide a new support to the communication of network ED, using new technical solutions.
2. The status of signalling component (potential ED) which shall be compliant to the above functional and sometimes physical standards.
3. All signalling mandatory standards and norms are antecedents to NG-TCN definition therefore the alignment is not guarantee and a standards gap is there.

In this paper the standards gap cannot be solved, the scope is to identify the gap, and proposing a possible technical solution if any is available.

E.2.2 ID_60074

The requirement is tagged as info only in the document CTA-T3.1-D-ANS-023-07, however, the Figure 139 identifies the ETCS On Board system (green part) with the main interfaces, which are standardized in the subset document, highlighted in the interface link. It is evident that each modification to a standardized interface shall involve an analysis/review to the relative Subset document in order to harmonize the new solution functional and physical interface.

The functional standard components and interface has been identified in CCS TSI 2016.

The physical implementation of “ETCS On-board” components (green part) are proprietary solutions even if some interfaces between components are defined at physical layer too (example the ETCS on board-STM is a Profibus link as defined in Subset 035).

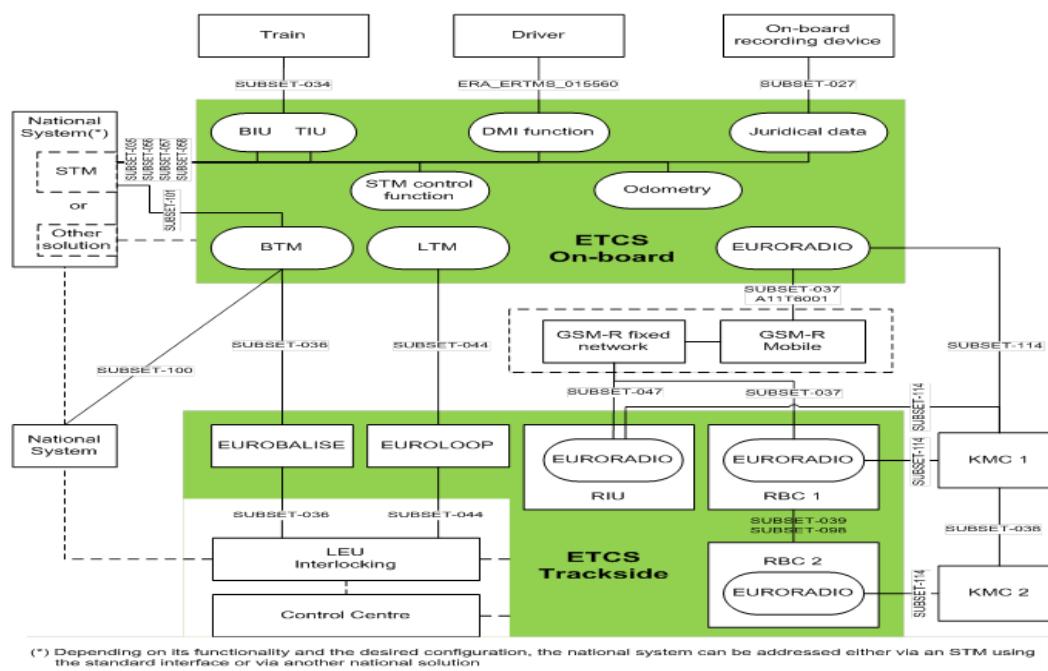


Figure 139 ERTMS/ETCS system and its interfaces

E.2.3 ID_60076

This requirement specifies the interface between the ERTMS/ETCS onboard equipment and the vehicle, in which the signalling equipment is installed. In the context of signalling system, the interface is historically called train interface and it is part of the ERTMS/ETCS architecture as defined in ID_60072.

The requirement is divided in two parts:

1. The mandatory functional part of interface is covered by the subset SUBSET-034
2. A not yet mandatory physical part of interface is covered by SUBSET-119.

Functional train interface SUBSET-034.

SUBSET-034 gives in its Table 1 (see Figure 140) the function information needed for train Interface and the direction of the information (Input / Output of the ERTMS/ETCS onboard).

Chapter	Name	Reference in SRS [1]	Input / Output
2.2.1	Sleeping	4.4.6 / 4.6.3	Input
2.2.2	Passive shunting	4.4.20 / 4.6.3	Input
2.2.3	Non-Leading	4.4.15 / 4.6.3	Input
2.2.4	Isolation	4.4.3.1.1	Output
2.3.1	Service brake command	3.13.2.2.7	Output
2.3.2	Brake pressure	3.13.2.2.7 / A.3.10	Input
2.3.3	Emergency brake command	3.13.10 / 3.14.1 / 4.4.4 / 4.4.5 / 4.4.13	Output
2.3.4	Special brake inhibit	3.12.1	Output
2.3.6	Special brake status	3.13	Input
2.3.7	Additional brake status	3.13	Input
2.4.1	Change of traction system	3.12.1	Output
2.4.2	Pantograph	3.12.1	Output
2.4.4	Air tightness	3.12.1	Output
2.4.6	Passenger Door	3.12.1	Output
2.4.7	Main Power Switch	3.12.1	Output
2.4.9	Traction Cut Off	3.13.2.2.8	Output
2.4.10	Change of allowed current consumption	3.12.1	Output
2.5.1	Cab Status	4.6.3	Input
2.5.2	Direction Controller	3.14.2 / 5.13.1.4	Input

Figure 140 Table 1 of train Interface function.

Physical train interface SUBSET-119.

The physical implementation of train interface isn't yet a mandatory standard and it is defined over informative subset SUBSET-119, which forecasts a wired interface called serial interface and a bus interface called serial interface.

Figure 141 gives an overview of which information shall be transmitted via the serial or parallel interface (marked with "M" for mandatory) and which can be transmitted via the parallel interface (marked with 'O' for optional).

No	Functional I/O as per [7]	Source	Parallel interface	Serial interface
1	Sleeping	TR	O	M
2	Passive Shunting	TR	O	M
3	Non-Leading	TR	O	M
4	Isolation	OBUs	M	-
5	Service Brake Command	OBUs	O	M
6	Brake pressure	TR	-	M
7	Emergency brake Command	OBUs	M	M
10	Regenerative Brake Inhibit (to be harmonized)	OBUs	to be harmonized	to be harmonized
11	Magnetic Shoe Brake Inhibit (to be harmonized)	OBUs	to be harmonized	to be harmonized
12	Eddy Current Brakes for Service Brake Inhibit (to be harmonized)	OBUs	to be harmonized	to be harmonized
13	Eddy Current Brakes for Emergency Brake Inhibit (to be harmonized)	OBUs	to be harmonized	to be harmonized
14	Special Brake Inhibit – STM Orders	OBUs	O	M
15	Special Brake Status	TR	O	M
16	Additional Brake Status	TR	O	M
17	Change of Traction System (to be harmonized)	OBUs	to be harmonized	to be harmonized
18	Pantograph – Trackside orders (to be harmonized)	OBUs	to be harmonized	to be harmonized
19	Pantograph – STM orders	OBUs	O	M
20	Air Tightness – Trackside orders (to be harmonised)	OBUs	to be harmonized	to be harmonized
21	Air Tightness – STM orders	OBUs	O	M
223	Passenger door (to be harmonised)	OBUs	to be harmonized	to be harmonized
23	Main Power Switch – trackside orders (to be harmonised)	OBUs	to be harmonized	to be harmonized
24	Main Power Switch – STM orders	OBUs	O	M
25	Change of allowed current consumption (to be harmonised)	OBUs	to be harmonized	to be harmonized
26	Traction Cut-Off	OBUs	M	M
27	Cab Status	TR	O	M
28	Direction Controller	TR	O	M
29	Train Integrity (to be harmonized)	TR	to be harmonized	to be harmonized
30	Traction Status	TR	O	M
32	Type of Train Data Entry	TR	O	M
33	Train Data Information (to be harmonized)	TR	to be harmonized	to be harmonized
34	National System Isolation	TR	O	M

Figure 141 I/O functionality forecast for train interface.

Physical train interface SUBSET-119: Parallel interface.

To implement the parallel interface, SUBSET-119 defines an architecture based on ECN connecting OBU with TCMS (Figure 142).

The architecture allows the transmission of both non-safety related and safety related information using SDT as defined in [18].

The usage of SDT over MVB is illustrated in .

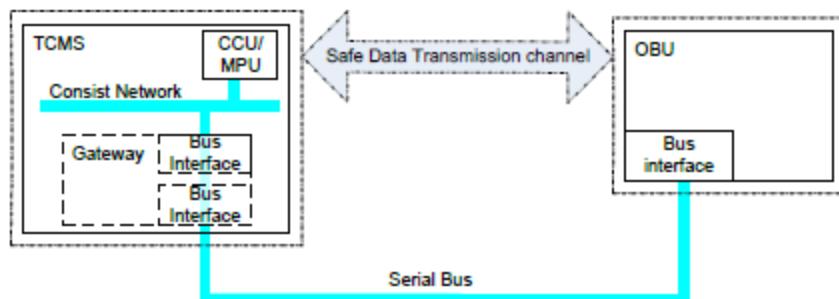


Figure 4-2 Architecture b)

Figure 142 Architecture for bus interface regarding Onboard I/O.

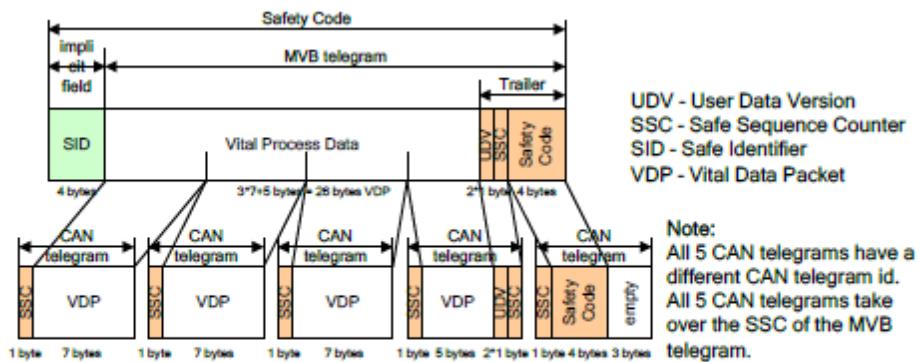


Figure 4-3 Safe Data Transmission via CAN

Figure 143 SDT as referred in Subset 119.

Conclusion:

The train interface implements the I/O between ETCS onboard subsystem and the Vehicle the interface as given in SUBSET-119 is quite suitable to be integrated in the context of NG-TCN, following gap should be covered.

1. SUBSET-119 should be review in order to consider SDTv4.

2. Safe data transmission channel should be implemented by protocol SDTv4, therefore OBU should manage a "SDTv4 channel" versus an I/O Server module which has in charge the collection of all required functional information regarding the interface.
3. Subset 119 considers the use of both links (wired and bus) marked both mandatory in (Figure 141). To overcome the point, the solution could be one or both of following.
 - a. A proper safety analysis should be performed on the new architecture interfaces (NG-TCN –OBU), to verify Emergency brake can triggered by on board respecting the SIL4 requirement.
 - b. NG-TCN should enable the use of wired interface regarding the emergency brake (not referred).

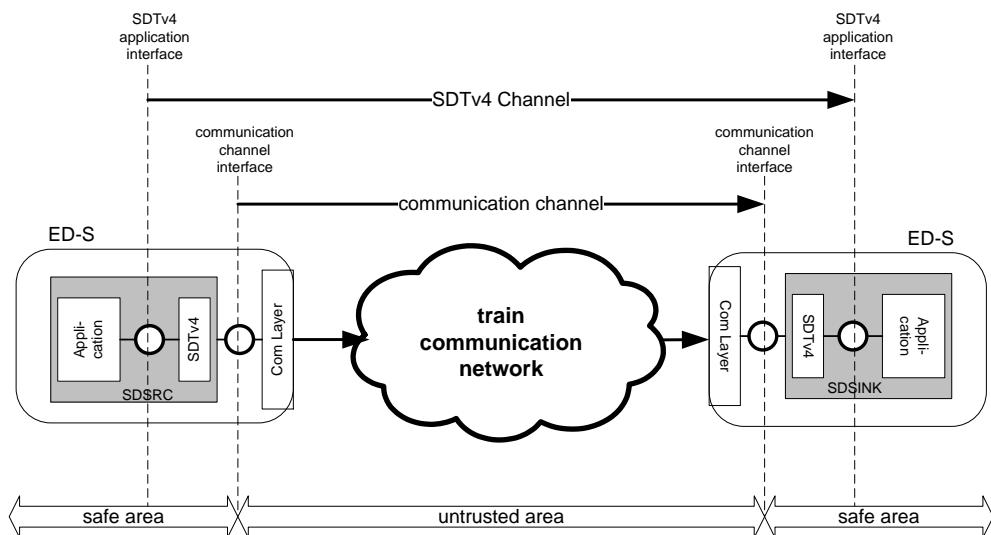


Figure 144 Parallel I/O in the context of NG-TCN.

E.2.4 ID_60077

The requirement is related to the integration between ERTMS/ETCS on-board subsystem and STM using the services of NG-TCN. The interfaces is defined by mean following UNISIG standards:

1. SUBSET-035 (Specific Transmission Module FFFIS)
2. SUBSET-056 (STM FFFIS Safe Time Layer)
3. SUBSET-057 (STM FFFIS Safe Link Layer)
4. SUBSET-058 (FFFIS STM Application Layer)

Subset 035 imposes PROFIBUS as Physical Link of the interface between, ERTMS/ETCS - STM therefore following solutions seems reasonable:

1. Keep the interface ERTMS/ETCS-STM outside NG-TCN, it means dedicated link should forecast for the two component ETCS and STM. As a mitigation it should be noted that the two equipment often are in the same cabinet, therefore the cabling should be an "internal cabling"

2. Use a Profibus-Ethernet Gateway able to interface the two entities on the NG-TCN ad follow. The solution has to be investigate seems cost expensive and need to be investigate regarding the RAM index of available gateway.
3. Modify ERTMS-STM standards, it take long time and doesn't assure retro-compatibility.

Rationale:

Solution 1 seems the more suitable even if it does not meet NG-TCN architecture, but the wiring will be limited to interconnect Devices on the “same subsystem”, often installed in the same cabinet.

E.2.5 ID_60079

This requirement is related to an internal interface of ERTMS/ETCS onboard between EVC (European vital computer) usually installed in the leading consist, and the DMI module installed on the driver cab.

The ERA_ERTMS_015560 standard cover the interface between the DMI and the Driver (what DMI should display), the internal interface EVC-DMI is OEM dependent.

From a practical point of view, typically EVC is installed in a rack somewhere in the leading consist instead the DMI shall be installed on the driver desk, therefore both components could take advantage from NG-TCN that enable the mutual interconnection, however following process should be followed:

1. UNISIG should define as mandatory an internal functional interface between DMI and EVC following the physical approach considered by ED-S architecture over NG-TCN.
2. An FMEA safety analysis should be done on the new internal interface EVC-DMI to demonstrate it is compatible with existing THR target.
3. After the previous two points have been clearly solved, a possible technical solution could be impended using SDTV4 protocol as depicted in Figure 145.
4. If FMEA safety analysis could demonstrate the SDTV4 is not needed, SDTv2 protocol could be used as the interface is an ETCS on Board internal interface.

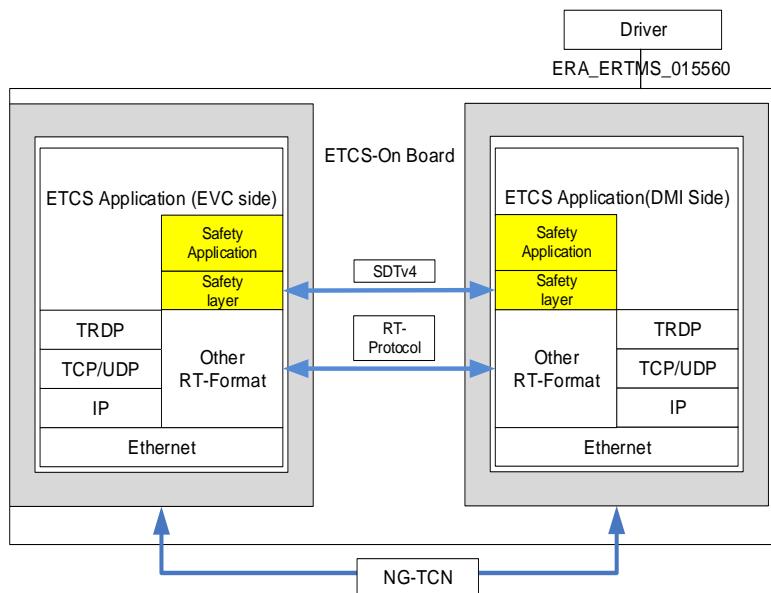


Figure 145 Possible DMI integration on NG-TCN

E.2.6 ID_60080

This requirement is related to an external interface between ERTMS/ETCS onboard and JRU (juridical recorder).

Subset 027 is a Functional definition of the interface ETCS onboard – JRU. The physical interfaces ETCS onboard – JRU is not yet standardized, the required SIL in the link is not defined. Taking advantage of the above considerations, the integration of ETCS onboard –JRU interface in the context of NG-TCN could be done considering JRU as a non-safety related ED. Due to the A-B-Plane architecture, JRU end devices should evaluate eventually duplicated packet.

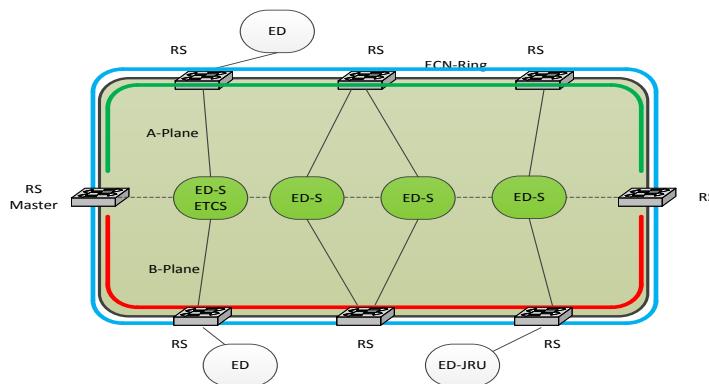


Figure 146 ETCS-JRU interface over NG-TCN.

E.2.7 ID_60081

The requirement is referred to the air gap, Interface 'G', between the Balise and the combination of the On-board Transmission Equipment and the KER STM of the related national Balise Transmission Systems using the same frequency ranges as Eurobalise.

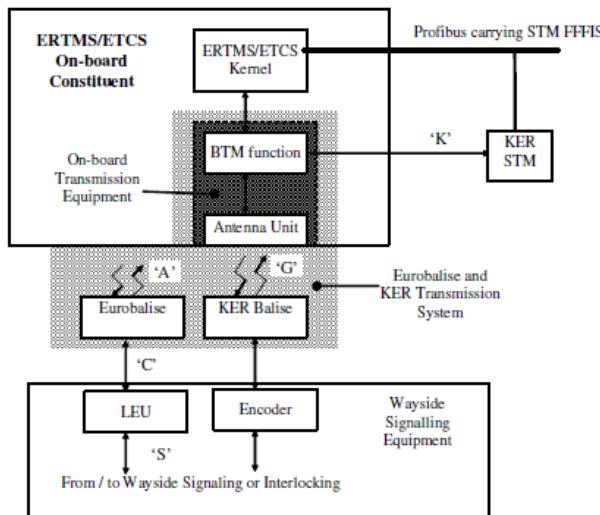


Figure 1: General Architecture

Figure 147 Balise -BTM Antenna-interface

The 'G' interface is specified in SUBSET 100, and it is not functionally connected to NG-TCN. The requirement is at system compatibility level and express the general need for NG-TCN and G interface to do not interfere each other from an EMC point of view.

In particular, The Up-link signal of 'G' interface complies with in-band emission levels as specified in the standard EN 50121-2. The in-band frequency range for Up-link transmission is from 3.8 MHz to 5.2 MHz. Down link of 'G' interfaces is comply with following mask

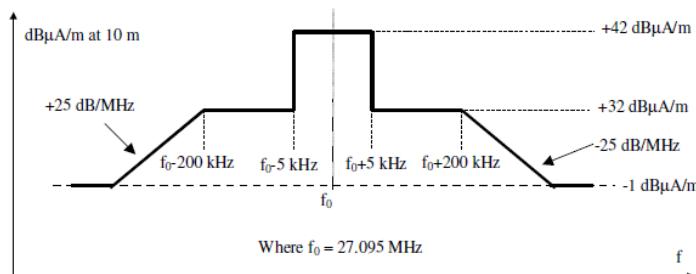


Figure 20: Tele-powering frequency mask

Figure 148 Down link emission Mask.

NG-TCN network devices shall comply with the applicable items of table 9 in clause 8 of EN 50121-3-2, but this requirement does not apply for the frequency band 2.5 MHz to 6.0 MHz, nor for the frequency range ± 1.52 MHz centred on the Tele-powering carrier frequency. Therefore NG-TCN should take care with the emission in 2.5 MHz to 6.0 MHz bands.

E.2.8 ID_60083

The requirement is referred to the air gap, Interface 'A', between the Euro Balise and The On-board Transmission Equipment communicates with the ERTMS/ETCS Kernel. The interface is defined in SUBSET 036.

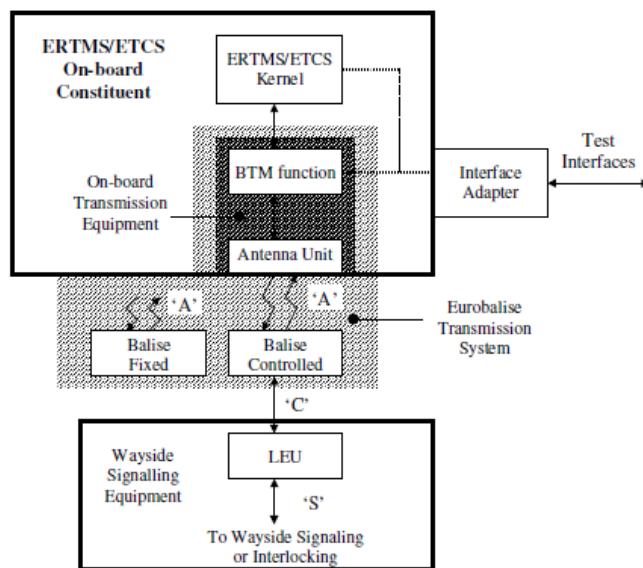


Figure 1: Eurobalise Transmission System, Interfaces

Figure 149 "A" Interface

"A" interface is not directly connected to NG-TCN therefore it should be assured only the environmental compatibility regarding the EMC aspect. Subset 030 defines Noise for "A" interface following signal, with the value in table. "A" withstand to the maximum noise here identified, therefore the requirement for NG-TCN is to do not exceed maximum noise on A interface.

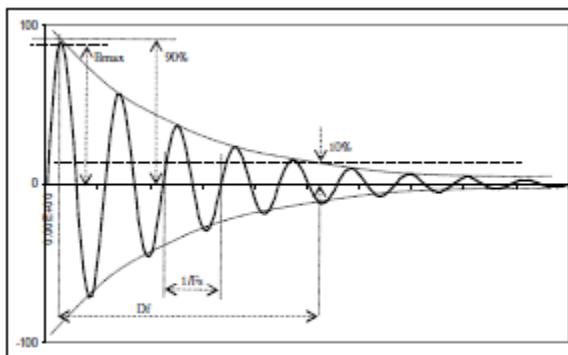


Figure 52: Shape of the Damped Interference Signal

Figure 150 Noise for "A" Interface

6.7.4.2 Limits

Damped oscillation noise:

Decaying Factor [cycles]	Repetition Rate [kHz]	Self Frequency [MHz]	Class H Field Strength, Bmax [dB μ A/m]	Class M Field Strength, Bmax [dB μ A/m]
5	1.5	1.0	95	87
5	1.5	2.5	83	80
5	1.5	3.9	70	65
5	1.5	4.5	70	65
5	1.5	6.0	74	74
5	5.0	3.9	70	65
5	5.0	4.5	70	65
5	15	1.0	95	87
5	15	2.5	83	80
5	15	3.9	70	65
5	15	4.5	70	65
5	15	6.0	74	74
30	1.5	1.0	95	87
30	1.5	2.5	83	80
30	1.5	3.9	67	60
30	1.5	4.5	67	60
30	1.5	6.0	74	74
30	5.0	3.9	67	60
30	5.0	4.5	67	60
30	15	1.0	95	87
30	15	2.5	83	80
30	15	3.9	67	60
30	15	4.5	67	60
30	15	6.0	74	74

Table 22: Field Strength Limits for Damped Oscillations

CW noise:

Frequency [MHz]	Field Strength, RMS [dB μ A/m]
1.0	100
2.5	83
3.9	49
4.5	49
6.0	74

Table 23: Field Strength Limits for CW Noise

Test methods, test procedures, and test tools shall be as defined in UNISIG SUBSET-116.

Figure 151 Limit of Noise on “A” Interface

E.2.9 ID_60085

The requirement is referred to the air gap, Interface ‘A’, between the Euro loop and The On-board Transmission Equipment communicates with the ERTMS/ETCS Kernel. The interface is defined in SUBSET 044.

Figure 5-2 identifies all interfaces of the ELS.

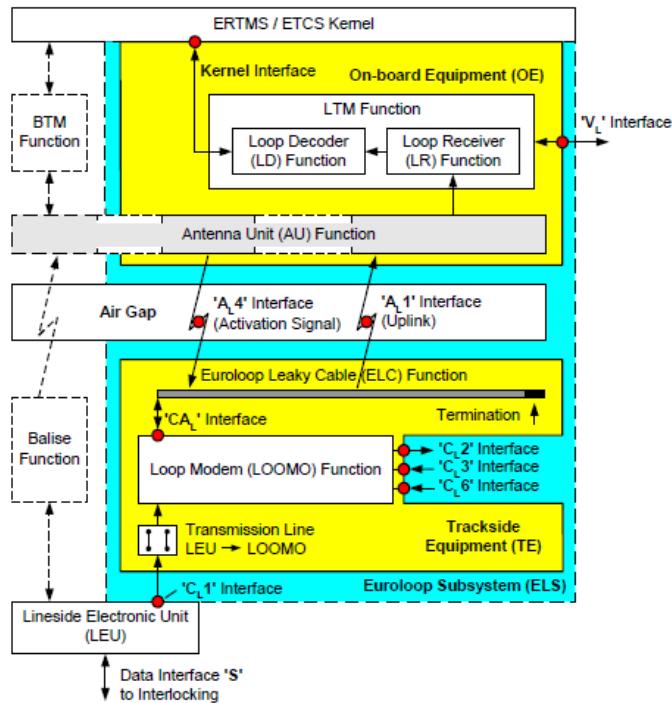


Figure 152 Euro loop interface

Subset 044 at 7.11.2.2.1 demands to the specific application the proof of EMC compatibility between Vehicle and Euroloop air gap:

"No harmonised standards exist to date on this kind of susceptibility issue. Therefore, each supplier of On-board Equipment shall responsibly define suitable models representing worst case susceptibility conditions and modes (with reference to the recalled ones) that may be possible within the range of application cases of his commercial interest. The definition of the noise environment and the suitability of the elaborated models are a matter of shared responsibility between suppliers of On-board Equipment, rolling stock devices, and infrastructure devices"

In order to avoid EMI issues, NG-TCN Devices should emitting as less as possible in the euro loop spectrum (Figure 153)

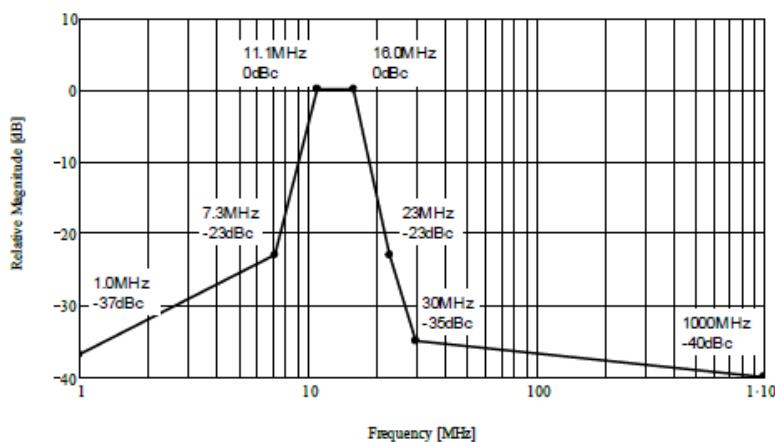


Figure 6-17: Spectrum Mask of Euroloop Up-link Signal

Figure 153 Euro Loop Spectrum mask.

E.2.10 ID_60086

The requirement is related to Euroradio interface which is an interface internal to ERTMS system defined in SUBSET 037 and in the document A11T 6001.

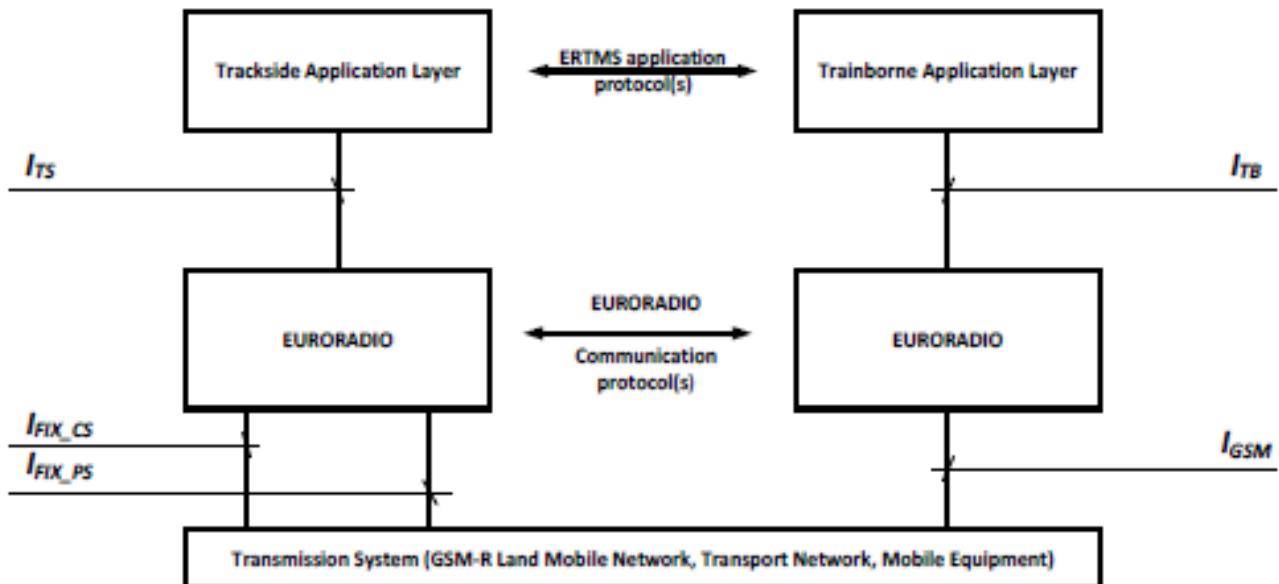


Figure 1-1 Euro Radio Interfaces

Figure 154 Euro radio interface

The requirement expresses the need for the interface to be functionally compatible in the context of NG-TCN that should not damage the RAMS parameter of Euro radio interface, including EMC effect and QoS parameters.

E.3 Integration of Metro Signalling components in NG-TCN

E.3.1 ID_60089

Metro systems CBTC and “traditional Metro” are not in deep standardized as ERTMS system because the interoperability isn’t an issue. Many functional interfaces between On Board part of the signalling system, the vehicle and trackside are system provider and project dependent, therefore a general approach is more difficult.

However, the basics components of the on-board part of system are very close to ATP needs of ERTMS (already investigated) plus specific needs to fulfil the ATO needs which are investigate in the next chapter

Based on that, specific requirements are exported to ED devices or solved in the context of specific project.

E.4 Integration of ATO components in NG-TCN

E.4.1 ID_60094

The requirement is related to the SUBSET 139 that define a standardised ATO-OB / vehicle interface at functional level to support ATO over ERTMS. SUBSET 139 is not yet delivered however some guideline could be taken.

Following ATO-Train interface are considered.

1. ATO interface with Propulsion (Traction / Dynamic Brake) Control -
2. ATO interface with Door Control
3. ATO interface with Emergency brake
4. ATO interface with Odometry.

Even if an FMEA analysis on the interface ATO-Vehicle is not yet available, the required SIL at most should be 2.

Supposing valid the above assumption, the integration of ED-ATO with a generic train interface Server ED could be done using SDTv2 as defined in 61375-2-3 annex B which guarantee a SIL2.

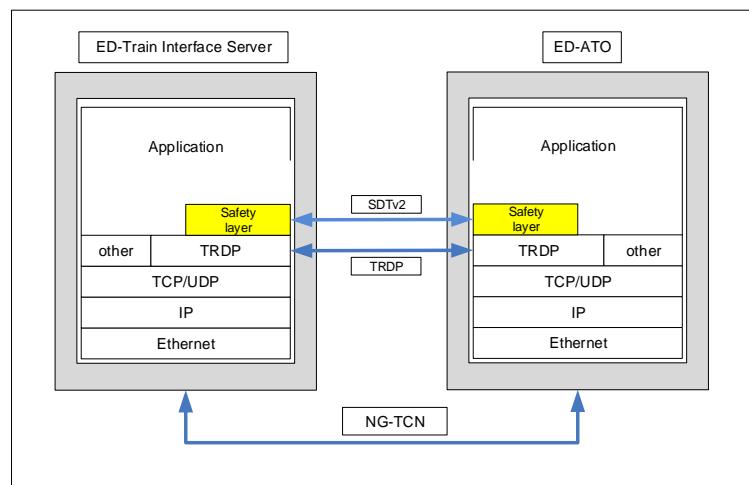


Figure 155 ATO integration over NG-TCN

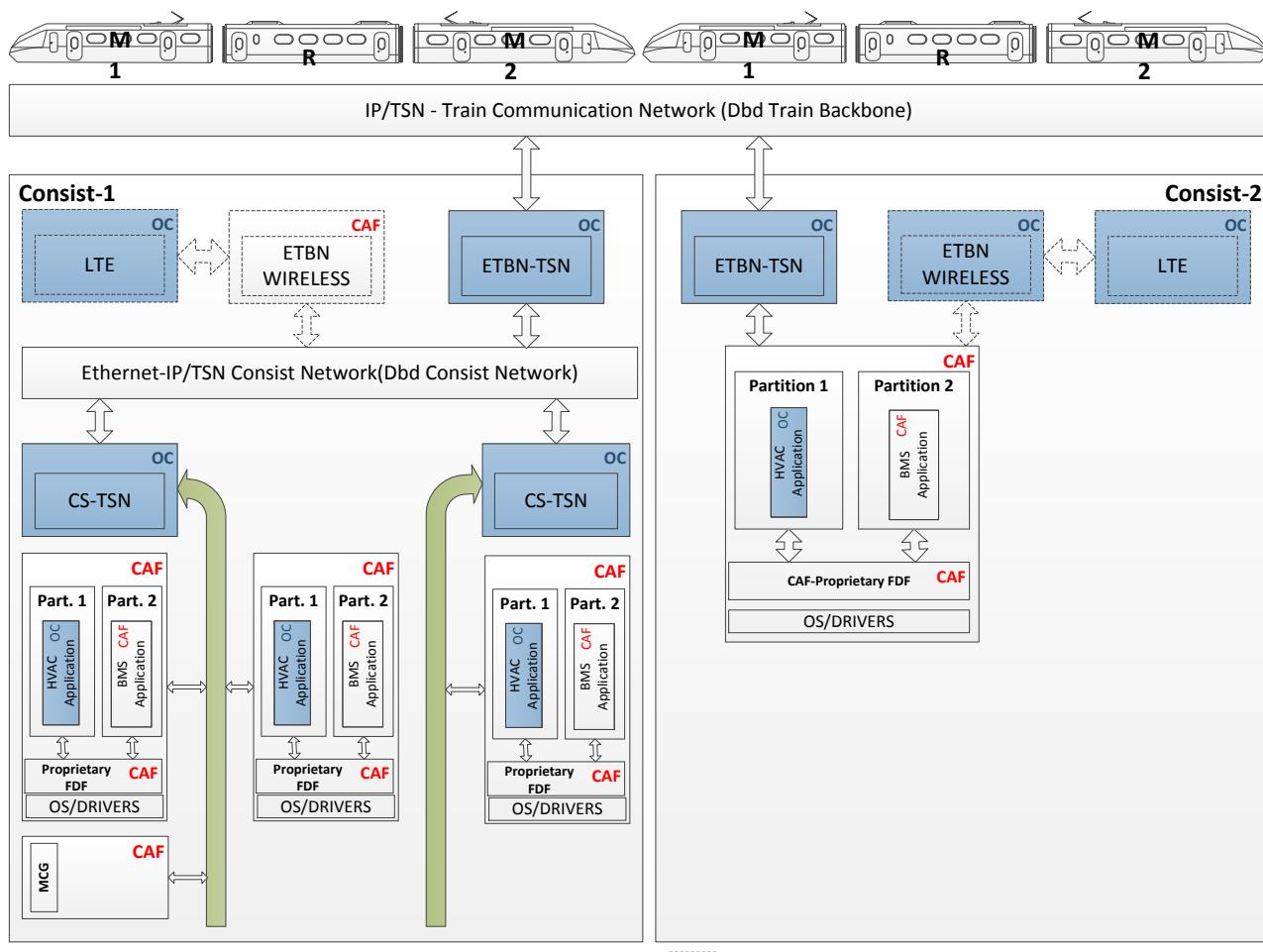
F Annex – Proposal for a proof-of-concept test setup

The objective of this deliverable was to specify the NG-TCN “Drive-by-Data” architecture and to define all technical features to an extend (TRL 3) that prototyping and testing of appropriate components will be possible. A summary of the components and the expected component capabilities has already been given in Annex A.

In a next step, which is planned to be executed within CONNECTA-2, component prototypes shall be developed and tested in a lab test set-up to achieve a TRL 4. A proposal of the NG-TCN proof-of-concept setup was already elaborated for the CONNECTA-2 project proposal, and a summary of this proposal in relationship to NG-TCN will be presented within this Annex.

For the purpose of proof-of-concept two laboratory demonstrators are planned, one for an urban and one for a regional train application.

The urban laboratory demonstrator (Figure 156) provides two consists equipped with NG-TCN, but in parallel also demonstrates the feasibility of a wireless train backbone (WLTB) as it was specified during the course of the Roll2Rail lighthouse project.



OC: Open Call S2R-OC-IP1-01-2018
Ddb: Drive by Data
FDF: Functional Distribution Framework
BMS: Bogie Monitoring System
MCG: Mobile Communication Gateway
HVAC: Heating, Ventilating, and Air Conditioning
TSN: Time Sensitive Networking

IP: Internet Protocol
CS: Consist Switch
ETBN: Ethernet Train Backbone Node
LTE: Long-Term Evolution
OS: Operating System
Part: Partition

Scenario for Wireless Communication
OC Device/Application Development

Figure 156: CONNECTA-2 Urban Demonstrator

The regional laboratory demonstrator (Figure 157) couples three consists equipped with NG-TCN. Focus of the demonstration is the proof of interoperability, for which reason each consist is provided by a different project participant and also equipment inside consists can be from different project participants.

In addition, WLAN Aps are connected to the ECN to provide wireless communication to selected WLED.

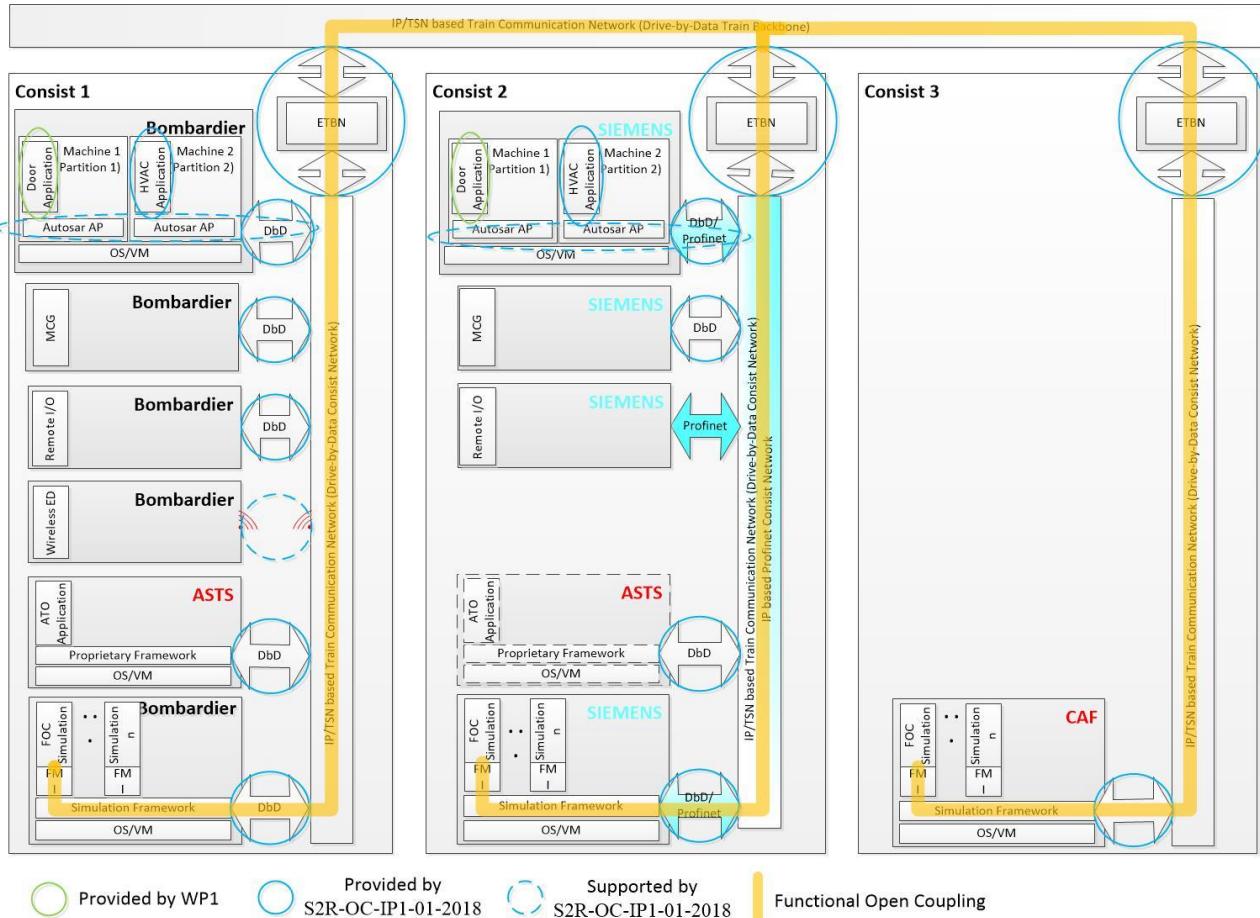


Figure 157: CONNECTA-2 Regional Demonstrator

G Annex – Analysis of Consist Internal ETB Topologies

G.1 Objective

The analysis of inner-consist network topologies aims to identify inner-consist network (ETB) topologies which are optimal with respect to lowest cost and highest reliability, but respecting the safety targets. As cost and reliability are often opposing the best compromise should be identified. This analysis is based on the characteristic properties of the topology variant and on the defined use cases.

G.2 Use cases

The analysis will be done on the base of three characteristic use cases, which are:

- a) Passenger train consisting of loco-hauled passenger coaches

In a passenger train each car typically corresponds to one consist (see UIC Leaflet 556 [32]). The train is kept in service even when there is a powerless passenger coach (e.g. caused by defective battery charger).

- b) Train consisting of 2-car trainsets (“married pairs”, example Chicago Transit Authority train)

Train service with a powerless trainset is not tolerated.

- c) Train consisting of 8-car consists (example ICE3 high-speed train)

Train service with a powerless consist is not accepted, but train service with one powerless car might be tolerated dependant on the car type. However, those consists typically have a sophisticated power and battery supply management which makes power outages of complete consists quite unrealistic.

The basic characteristics of these use cases are given in Table 67:

Table 67: Use cases

Characteristic Consist Type	Number of cars	No of consists	Car length [m]	Consist length [m]	Train length [m]	ETB line length [m]¹⁾
UC1: Loco hauled passenger train	16	16	26	26	416	624
UC2: Married pair	16	8	20	40	320	480
UC3: 8-car trainset	16	2	25	200	400	600

1) Assumed cable length in consist is 1.5 times consist length.

G.3 Transmission medium

The choice of the transmission medium has an influence on the topology, and the analysis shall therefore be done for a copper transmission medium (as it is used today) and for an optical transmission medium.

Replacing the well-known copper wiring with optical wiring has two major consequences:

For optical ETB it is suggested to use MMF because MMF is cheaper and much easier to handle in the field than SMF. With MMF, distances up to 550m (GbE), 300m (10GbE over OM3 MMF) or 400m (10GbE over OM4 MMF) can theoretically be realized³¹. As a consequence, those distances would significantly reduce the number of required ETB repeaters on ETB. For the subsequent analysis, a conservative distance of 300m is assumed.

An ETB bypass function requires also a different technology in case of optical wiring. In principle, there are optical switches (relays) available, and some Ethernet switch suppliers are offering “optical bypass relays” as independent devices. The suitability of those technologies for railway application with respect to reliability and cost is presently an open question and requires further investigations.

³¹ In reality, the distance might be lower due to additional attenuation introduced by intermediate connectors.

G.4 Inner-consist Architecture Variants

The basic characteristics of the different ETB topology variants, also reflected to the different use cases, are listed in Table 68.

Table 68: ETB topology variants characteristics (related to one consist)

Variant Aspect	Detail	A	B	C	D₁	D₂	E
Feature	General	ETB lines aggregate d; ETB and ECN physically separated	ETB lines aggregate d; ETB and ECN physically separated	ETB and ECN on same physical wire, separated by VLAN/Virtual Link	ETB lines separated ; ETB and ECN physically separated	ETB lines separated ; ETB and ECN physically separated	ETB lines separated ; ETB and ECN on same wire, separated by VLAN/Virtual Link.
	ETB Bypass required	Yes	Yes	No ¹⁾	No	Yes	No
Topology	Number of inter-consist Ethernet links	2	2	2	2	2	2
	number of inter-vehicle Ethernet links	4	4	2	4	4	2
	number of ETBN	1	2	2	2	2	2
	Number of ETB repeater in 1-car consist (UC1) using copper or optical medium	0	0	0	0	0	0
	number of ETB Ethernet segments in 1-car consist (UC1) using copper or optical medium	4	6	4	4	4	4
	Number of ETB repeater in married pair (UC2) using copper medium ^{3) 7)}	1	0	0	0	2	0
	number of ETB Ethernet	6	6	4	4	6	4

Variant Aspect	Detail	A	B	C	D₁	D₂	E
	segments in married pair (UC2) using copper medium						
	Number of ETB repeater in 8-car consist (UC3) using copper medium ^{3) 7)}	5	4	0 ²⁾	4	10	0 ²⁾
	number of ETB Ethernet segments in 8-car consist (UC3) using copper medium	14	14	4	8	14	4
	Number of ETB repeater in married pair (UC2) using optical medium ^{3) 7)}	0	0	0	0	0	0
	number of ETB Ethernet segments in married pair (UC2) using optical medium	4	6	4	4	4	4
	Number of ETB repeater in 8-car consist (UC3) using optical medium ^{3) 4) 6) 7)}	1	0	0 ²⁾	0	2	0 ²⁾
	number of ETB Ethernet segments in 8-car consist (UC3) using optical medium	6	6	4	2	6	4
Failure effect	Effect of single ETBN or ETB	Loss of ETBN isolates CN;	TSN timing needs	Loss of ETBN interrupts ETB	No (one line interrupted)	No (TSN timing needs)	No

Variant Aspect	Detail	A	B	C	D₁	D₂	E
	repeater failure	TSN timing needs reschedule	reschedule			reschedule (on one line)	
	Effect of single ETB Ethernet link/connecto r failure	No	No	No	No	No	No
	Effect of double ETB Ethernet link/connecto r failure affecting Line A and Line B at different locations	No	No	No	Interrupts ETB	Interrupts ETB	Interrupts ETB
	Effect of powerless car/consist	No	No	Interrupts ETB	Interrupts ETB	No	Interrupts ETB
Fire/Vandalism protection	Effect of one ETBN or one ETB repeater in ETB path destroyed by fire or by vandalism	Interrupts ETB	Interrupts ETB	Interrupts ETB	No	No	No
ECN/ETB Independence	Possibility of mutual interference	No	No	Yes	No	No	yes
Protocol complexity ⁵⁾	Train inauguration synchronization (“reconciliation”) between ETB line A and ETB line B necessary?	No	No	No	Yes	Yes	Yes

Annotations:

- 1) A ETB bypass makes no sense in this topology
- 2) The CS take the role of ETB repeaters
- 3) Assumed cable length of 1.5 times consist length.
- 4) With MMF category ≥ OM3

- 5) Protocol complexity has an effect on non-recurring costs
- 6) Assumption is that an optical Ethernet segment can extend to 300m (compared to 100m in case of copper)
- 7) Ethernet signals must be repeated at about half the length of an Ethernet segment (50m copper, 150m fiber) to cope with a failed component bypassing the signal.

From these characteristics, we can draw first conclusions:

- Variant A has a cost advantage in small consists (1 car), because only one ETBN is needed and minimal number of ETB Ethernet links.
- Variant B corresponds to the architecture defined in IEC 61375-2-5.
- Variant C is susceptible to single point of failure and offers no further advantages, so this variant will not be further considered.
- Variant D₁ differs from D₂ only in its inability to deal with powerless consists, but avoids a ETB bypass and has therefore an advantage. This variant is interesting for consists in trains which need not to be operable with a powerless coach/consist.
- Variant E has some technical drawbacks (e.g. lowered reliability) compared to other variants, especially variants B and D, but provides a cost-efficient solution because it doesn't require ETB bypass and ETB repeater devices. Variant E resembles variant D₁ from a functional point of view because the only difference is that the physical ETB lines of Variant D₁ are replaced by virtual ETB lines (VLAN). This variant might be applied in trains where (recurring) costs are sensitive and reliability requirements are not that strong. For the purpose of this analysis this variant will not be further considered.

The following sub-chapter will restrict for the Variants A, B, D₁ and D₂.

G.5 Cost impact

To estimate the impact on cost and to provide a ranking for the different topology variants, the following assumptions are made:

- Recurring costs (costs for each manufactured vehicle) are mainly determined by the cost for installation, which increases with the number of Ethernet links, and the number and cost of devices. The device cost depends on the functionality:
 - Cost drivers in network devices are bypass relays, switch cores and power supply.
 - Cost level of ETBR devices depends on design. Can be low (just Ethernet Phys + simple power supply) or high (diagnosable ETBR with bypass). For this cost impact estimation, it is assumed that cost for one ETBN supporting two Ethernet lines (used in variants A and B) is lower than the sum of one ETBN and one ETBR, both supporting only one Ethernet line, but with bypass (variant D₂).
 - Components for variant D₁ and D₂ support only 1 ETB line, so are cheaper than components used for variants A and B.

- Components for variant D₁ are cheapest because no bypass is required³².
- Non-recurring cost are mainly determined by the development and homologation effort.

a) Cost in case of copper transmission medium

The device quantities for the different topology variants and use cases are listed in Table 68. When comparing these, one can see that Variant D₂ requires in general more active components (ETBN, ETBR) than Variant A, B and D₁. Of course, D₂ components are more cost efficient because only one ETB line needs to be handled, which means half the number of ETB bypass relays. But the expectation is that those cost savings will not compensate the additional cost created by additional devices. Quantities for B and D₁ are equal, so D₁ has a cost advantage because it doesn't need a bypass.

As an example, a cost ranking for UC3 (8-car consist) is given in Table 69.

Table 69: Cost ranking (copper based ETB, 8-car consist)

Variant Aspect	Detail	A	B	D₁	D₂
Cost (ranking, 1 = best)	Recurring (HW) ¹⁾	1 Only one ETBN plus ETB repeaters	3 Same number of component than Variant D ₁ .	2 No ETB bypass required	4 Highest number of components
	Non-recurring	1	2	3	4

b) Cost in case of optical transmission medium

The device quantities for the different topology variants and use cases are listed in Table 68. As for the copper case, D₁ is more cost efficient than B because D₁ components don't require a bypass. Cost for an optical bypass are assumed high, so D₁ is rated better than A.

As an example, a cost ranking for UC3 (8-car consist) is given in Table 70.

Table 70: Cost ranking (optical based ETB, 8-car consist)

Variant Aspect	Detail	A	B	D₁	D₂
Cost (ranking, 1 = best)	Recurring (HW) ¹⁾	2 Requires optical bypass	3 Same number of component than Variant D ₁ , but with optical bypass	1	4 Highest number of components

³² Additional cost introduced by optional PoE are not considered here.

Variant Aspect	Detail	A	B	D₁	D₂
	Non-recurring 2)	1	2	3	4

As a preliminary conclusion, it can be stated that variants A and B (which are using the same component designs) can be expected lower priced than D₂ if powerless consists shall be supported. If powerless consists are tolerated, variant D₁ will be better despite the higher non-recurring cost.

G.6 Reliability

Communication system reliability defines the ability of the communication network inside the consist to transfer data both within the consist (intra-consist) and between consists (inter-consist). The communication reliability is quantified by the rate (failure per time) that a (single) failure causes the loss of one or both abilities.

The communication system reliability is mainly determined by the material reliability of the involved active and passive components (Ethernet links, connectors, CS, ETBN, ETBR) and by the level of installed redundancy (functional reliability).

Concerning the communication system reliability, [05] came to the following conclusions:

a) Material reliability

The Material Reliability refers to the inherent reliability of the system. It is calculated by summing the material reliability figures of each of the components of the network. In the Material reliability all the failures that lead to a maintenance action (repair) are considered, including those that do not affect the service or function.

The material reliability value of topology B and D₁ are almost the same for all the use cases. The reliability value of the variant D₁ is a little higher because the active devices do not have bypass and there are less intra-consist connectors. Topology A can be considered slightly better than B because there is only one ETBN per consist. Topology D₂ is worst because of the high number of needed network components.

Table 71: Material reliability ranking (copper based ETB, 8-car consist)

Variant Aspect	Detail	A	B	D₁	D₂
Reliability (ranking, 1 = best)		2	3	1	4 Most components

b) Functional reliability

The functional reliability considers the rate of service failures, which are related to the two functions of the ETB:

- Train inauguration (determine train composition)
- Data transport between consists

Service failure means a failure which impairs or degrades the service. Examples are incomplete train inauguration (e.g. undetected consists) or unreliable data communication (e.g. high frame error rate, addressing errors, unreachable end devices).

The service failure rate is determined by executing a failure analysis (FMECA) and using RBD or FTA to obtain the functional reliability values (see [05]).

The service failure rate is mainly influenced by the level of installed redundancy. As can be seen from the ranking in Table 72, variant A is worst because a single fault may degrade the train inauguration and reachability of end devices. Variants B is worse than D₁ and D₂, and D₂ does not bring any benefit regarding reliability compared to D₁. See [05] for details.

Table 72: Functional Reliability ranking (copper based ETB, 8-car consist)

Variant Aspect	Detail	A	B	D₁	D₂
Reliability (ranking, 1 = best)		4 single fault (ETBN)	3	1	2

G.7 Safety

G.7.1 Functional safety

For functional safety, the question is to which extend the ETB topology variants support the two safety functions “safe train inauguration” and “safe data transmission”.

It can be stated in general that safe data transmission does not rely on the black communication channel (which ETB belongs to) and that for that reason no impact on safety by using different topology variants exists. There might be impact on reliability, but not safety.

There are however differences for the safe train inauguration, as the detailed safety analysis in [05] revealed. Actually, 3.2.10 defines two inauguration protocol variants, one (centralized inauguration)

suitable for ETB topology variant B and D, and the other (parallel inauguration) for ETB topology variant D only. In the parallel inauguration, both ETB lines A and B are inaugurated separately, and the most complete line is taken for operation. In this way, the parallel inauguration improves reliability, but not safety³³. From a safety perspective, this is equivalent to a centralized inauguration, which as well must tolerate the absence of a redundant ETB line. What makes the difference between the two ETB topology variants is the ability of variant D to support the detection of specific failure modes (see [05]):

- ETB topology variant D makes an independent consist orientation check without additional equipment (like train lines) possible.
- ETB topology variant D₁ is safe, in combination with train end detection, in detecting the presence of powerless intermediate consists³⁴.

G.7.2 Fire protection

Besides the mentioned functional safety related differences, there is also an advantage of ETB topology variant D with respect to fire protection due to the completely separated ETB lines. To keep train running capabilities in case of fire on board of rolling stock, EN 50553 [16] sets out requirements especially for the case of locally confined fires (type 2 fires), caused for example by luggage fires or arson. Due to the spatial separation of the two ETB lines (which of course have to comply to EN 50553), the risk of a complete ETB outage is extremely low because the probability that both ETBN or both ETB lines are destroyed by a locally confined fire is negligible.

G.7.3 Safety ranking

The leads to the following safety ranking (Table 73):

Table 73: Safety ranking

Variant Aspect	Detail	A	B	D ₁	D ₂
Safety (ranking, 1 = best)		4	3	1	2

G.8 Functional aspects

Besides cost, reliability and safety there are also functional aspects to be considered:

- Variants A and B is less suitable for TSN scheduled traffic because a failure of one ETBN (or ETBR, design dependent) may require a rescheduling on ETB level.

³³ Safety would be increased when the inauguration results of ETB line A and ETB line B are compared, and a safe state is entered in case of a discrepancy. This however would significantly reduce the availability of the ETB.

³⁴ Powerless intermediate consists are not detectable during inauguration in ETB topology variant B

- Continuation of the A-Plane/B-Plane concept on ETB level is simpler implementable in variants D₁ and D₂.
- Train inauguration function implementation in variants D₁ and D₂ is more complex and involves ECN communication.
- Variant D₁ works well with optical media because there is no bypass required
- GbE link up/down times are greater ($\approx 1.0\text{s}$) than for 100FDX ($\approx 0.1\text{s}$ with fast link), which leads to an ETB outage for variants A and B when bypass is activated.

Because these functional aspects are difficult to quantify, a rating is not made.

G.9 Powerless Consist

It has been said before that powerless consists can be tolerated when a bypass function is available as it is the case for topology variant B. This statement needs to be relativized.

The concept of “bypassing” was introduced with the WTB technology (IEC61375-2-1) for the purpose to bypass powerless coaches in locomotive hauled passenger trains. Because WTB defines a bus technology for data transmission over a serial line supporting a line length of 960m without repeater, there was practically no limit for the bypassing length. So, it even works in a train where all middle coaches are unpowered and only the end vehicles (e.g. locomotive and steering car) are communicating.

When ETB was introduced as replacement of WTB, the topology (2 aggregated train backbone lines) and bypass concept was adopted from WTB (see IEC61375-2-5). Ethernet however has a link limit of 100m (copper) or 300m (optical), which restricts the length of bypassed powerless consists. For copper medium, the consist length that can be bypassed is about 30m. This means that only the special case of one coach being one consist can be supported which is less than WTB supports, independent from the topology variant!

NOTE With optical media or with the aid of PoE (feeding the edge ETBNs in the consist) this consist length limit could be extended (optical media: to about 100m, PoE: to about 66m).

Another problem with powerless consists is the necessity for a train inauguration correction function as defined in IEC61375-2-3. Because sequence information is safety related, this correction function must also be safely implemented. Furthermore, the information about the location of vehicles to be inserted must be available. In trains with driver it is the driver's responsibility to take care about, but what about driverless trains?

In the case a consist loses power during operation, some safety critical functions like for instance the brake system might be affected. According to TSI LOC&PAS sub-chapter 4.2.4.2.1, it is requested that the control line (which are the ECN and ETB in our case) run continuously, and in case of an inadvertent disruption (loss of integrity, line de-energized) of the control line brakes shall be activated on all vehicles of the train. Because a powerless consist disrupts ETB communication in ETB topology Variant D₁, the loss of integrity is detectable by all brake systems not affected by the power loss. However, also brake systems belonging to the powerless consist are requested to react, for which a technical solution like a local energy supply might be foreseen.

G.10 Conclusions

The analysis performed in this sub-chapter aimed to identify the topology variant which provides the best compromise between cost, reliability, safety and functionality.

The diagram shown in Figure 158 summarizes the ratings made in the previous sub-chapters. According to this diagram, variant D₁ is rated best followed by variant B.

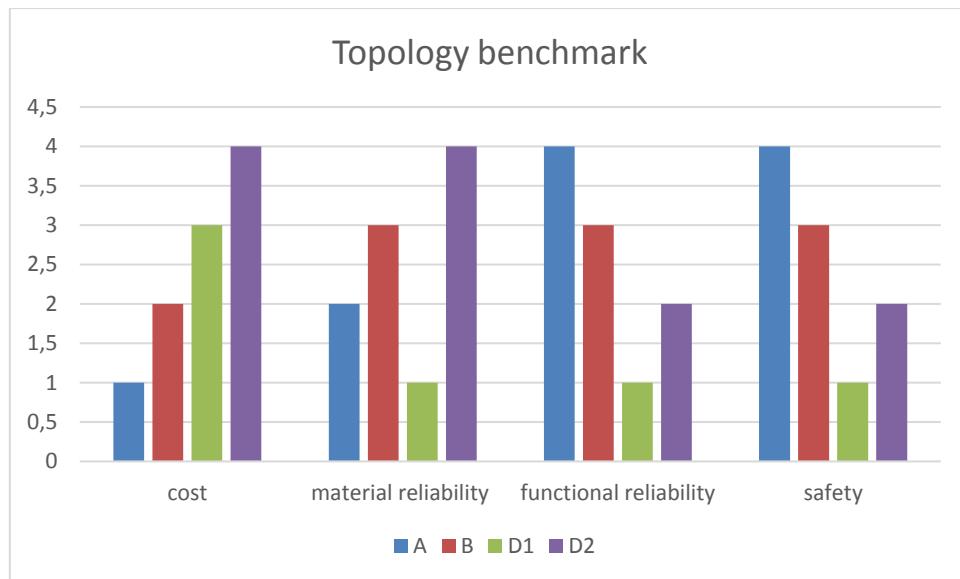


Figure 158: Topology variant benchmark

For a better understanding, the specific pros and cons of variant B and variant D₁ are summarized in Table 74.

Table 74: ETB topology variants B and D₁ – Pros and Cons

Aspect	B		D ₁	
	PRO	CON	PRO	CON
Reliability		Worse functional reliability	Better functional reliability	
		Activating or deactivating bypass requires a new link-up lasting about 1.0 s for GbE and interrupting ETB data traffic	ETBN failure causing a new link-up affects only one ETB line. No interruption of TSN data traffic.	
Functional Safety		Requires separate train lines for independent orientation check	Inherent independent orientation check	
		Powerless intermediate consist are not detectable	Detection of powerless intermediate consist	
		Train inauguration correction function needed	No need of train inauguration correction function	
Fire protection³⁵		Fire destroying one ETBN not tolerated (violates EN 50553) ³⁾	Fire destroying one ETBN tolerated (supports EN 50553) ³⁾	
Cost		Higher cost because of additional ETB interfaces and bypass	Lower cost due to single ETB line and no bypass	
Usability	Supports powerless coaches (consists with one vehicle)			No support of powerless coaches
Support optical media		Optical bypass required	No bypass required	
Support high transmission rate \geq 10GbE		Bypass suitable for high frequencies required	No bypass required	
TSN Support		A single failure may require a re-scheduling of data traffic leading to temporary traffic interruption	Single failure has no impact on data traffic	
		Higher number of ETB hops increases latency time	Lower number of ETB hops reduces overall latency time	
Standardization	Already specified in IEC61375			Needs to be introduced in IEC61375
Backward compatibility²⁾	Restricted ¹⁾ backward compatibility to existing IEC compliant ETB implementations			Not backward compatible to existing IEC compliant ETB implementations

Annotations:

- ¹⁾ Only if SIL4 capable train inauguration protocol can be kept compatible to existing inauguration protocol.
- ²⁾ When using application profiles defined in CONNECTA WP4 backward compatibility to existing train fleets is not given.
- ³⁾ Relevant standard for fire protection is EN50553, which itself is referenced in TSI SRT (safety in railway tunnels), and therefore becomes mandatory for TSI SRT compliant implementations.

The support of powerless consists is key for Loco hauled passenger trains, where each car is a consist. This ability of variant B (or A), and the fact that variant B is already specified in IEC 61375-2-5, make variant B indispensable for a NG-TCN solution.

On the other hand, variant D₁ demonstrates its strength when it comes to safety and reliability, and because both are key aspects of CONNECTA, D₁ is finally the better solution.

From a standardization point of view, D₁ could be introduced as an option besides variant B for train applications which require a high safety integrity. This would mainly affect the IEC61375-2-5 standard. The coexistence of variants B and D₁ makes it possible to address the complete range of train application and to select the optimal topology variant for a specific application. A possible mapping between train applications and topology variants is shown in Table 75.

Table 75: ETB Topology variants – characteristics and applications

ETB Topology Variant	Characteristics	Application
B (A)	Double, aggregated ETB line Bypass function in all ETBN/ETBR At least one ETBN per consist	Loco hauled passenger trains Trains requiring backward compatibility Legacy trains
D ₁	Separated ETB lines, related to consist sides A and B. No bypass Two ETBN per consist	Train with larger units (e.g. Trams, Metros, Regional, HST) which cannot operate with powerless consists

³⁵ Relevant standard for fire protection is EN50553, which itself is referenced in TSI SRT (safety in railway tunnels), and therefore becomes mandatory for TSI SRT compliant implementations.

H Annex – Security zones and conduits

The following tables list the characteristics of all defined security zones and conduits.

Table 76: Definition of Common Zones

GZ01	Zone Name	ETBN
	Zone group	-
	Zoning requirements applied (ref.:[22])	ZCR 3.2
	Logical boundary	This zone comprises the functionality of the Ethernet Train Backbone Node (ETBN). The main functions of ETBN are train backbone inauguration according IEC61375-2-3 and IEC61375-2-5 resulting in the building of train network directory, data exchange over the train backbone and the provision of train network directory data for the construction of Train Topology Database (TTDB).
	Physical boundary	ETBN is located in locked cabinets or in cable conduits (Ethernet cable) only accessible by maintenance staff.
	Safety designation	Safety related with respect to train inauguration function. Non-safety related with respect to data exchange between ECN and ETB.
	Logical access points	ETB Ethernet interface ports ECN Ethernet interface ports ETB ED Ethernet interface ports Local service Ethernet interface port
	Physical access points	ETBN located in locked cabinets only accessible to authorized personnel.
	Data flows	IP packets addressing devices in other consists routed (OSI Layer 3) from ECN to ETB and vice versa (unicast and multicast); no filtering (firewall) foreseen. IP packets addressing devices in other consists bridged (OSI Layer 2) from ETB-ED to ETB and vice versa (unicast and multicast).
	Connected zones or conduits	Conduit ETBN_TCMS_Consist_R Conduit ETBN_TCMS_Consist_S Conduit ETBN_OOS Conduit Ethernet_Train_Backbone
	Assets	ETBN
	SL-T	{1, 1, 1, 1, 1, 1}
	Applicable security countermeasures	Security event detection
	Assumptions and external dependencies	-
GZ02	Zone Name	MAR
	Zone group	-
	Zoning requirements applied (ref.:[22])	ZCR 3.6
	Logical boundary	The zone comprises the assets which ensure secure communication between train and ground systems.
	Physical boundary	Devices of this zone are in locked cabinets or in cable conduits (Ethernet cable) only accessible by maintenance staff.
	Safety designation	Non-safety critical
	Logical access points	ECN Ethernet interface port Antennas
	Physical access points	Devices are located in locked cabinets only accessible to authorized personnel.
	Data flows	Exchange of non-safety critical data like diagnostic or telemetric information
	Connected zones or conduits	Conduit MAR_TCMS Conduit MAR_OOS Conduit GCC_MAR (out of scope)
	Assets	MAR, MCG Category 1

	SL-T	Out of scope
	Applicable security countermeasures	Out of scope
	Assumptions and external dependencies	-
<hr/>		
GZ03	Zone Name	Local_Maintenance
	Zone group	-
	Zoning requirements applied (ref.:[22])	ZCR 3.4
	Logical boundary	The zone comprises the devices with maintenance applications that are directly connected (i.e. a dedicated physical interface is assigned to this connection) to respective TCMS devices.
	Physical boundary	Service device (PC, laptop, etc.) owned and supervised by maintainer
	Safety designation	Safety-related (EN50657 tool classes 2 and 3)
	Logical access points	Physical interface (e.g. Ethernet port or USB port) for connecting to a service port of a TCMS device and establishing a secured communication to the device.
	Physical access points	Service device only accessible to authorized maintenance staff
	Data flows	Reading of diagnostic information Reading and writing configuration parameters Download of software
	Connected zones or conduits	Conduit LM_TCMS_Safety
	Assets	Service device (authenticated)
	SL-T	Out of scope
	Applicable security countermeasures	Out of scope
	Assumptions and external dependencies	With respect to the SuC the devices of this zone are considered as external entities. They are supposed to be connected temporally.
<hr/>		
GZ04	Zone Name	Onboard_Remote_Maintenance
	Zone group	-
	Zoning requirements applied (ref.:[22])	ZCR 3.4
	Logical boundary	The zone comprises the devices with maintenance applications that are connected to respective TCMS or OOS devices via on-board NG-TCN network. Compared to local maintenance the remote maintenance requires the access to the NG-TCN network.
	Physical boundary	Service device (PC, laptop, etc.) owned and supervised by maintainer
	Safety designation	Not safety related. Remote maintenance is not allowed for the devices of TCMS_Const_Safety zone.
	Logical access points	Physical (e.g. Ethernet port or USB port) or wireless (WLAN) interface for connecting to ECN and establishing a secured communication to the device.
	Physical access points	Service device only accessible to authorized maintenance staff
	Data flows	Reading of diagnostic information (OOS and TCMS regular devices only) Reading and writing configuration parameters (OOS and TCMS regular devices only) Download of software (OOS and TCMS regular devices only)
	Connected zones or conduits	Conduit RM_TCMS_R Conduit RM_OOS_Wired Conduit RM_OOS_Wireless
	Assets	Service device (authenticated), Measurement device (e.g. protocol analyser)
	SL-T	Out of scope
	Applicable security countermeasures	Out of scope
	Assumptions and external dependencies	With respect to the SuC the devices of this zone are considered as external entities. They are supposed to be connected temporally.

GZ05	Zone Name	COS
	Zone group	-
	Zoning requirements applied (ref.:[22])	ZCR 3.2, ZCR 3.4, ZCR 3.5, ZCR 3.6
	Logical boundary	The zone groups devices that carry functions assigned to the COS domain and that are located in the same consist, possibly distributed over several cars. It can be assumed that this zone comprises a WLAN system operating for access by passengers.
	Physical boundary	No physical boundary due to passenger access.
	Safety designation	Not safety related.
	Logical access points	Physical (e.g. Ethernet port) or wireless (WLAN) interface for connecting to COS network.
	Physical access points	Not applicable due to passenger access.
	Data flows	Unrestricted data exchange
	Connected zones or conduits	Conduit COS_OOS
	Assets	Wired and/or wireless end devices that carry functions assigned to the COS domain, passenger owned wireless devices, passive and active network components constituting the network segment assigned to this zone.
	SL-T	{0, 0, 0, 0, 0, 0}
	Applicable security countermeasures	None
	Assumptions and external dependencies	With respect to the SuC the devices of this zone are considered as external entities. Partly they are supposed to be connected temporally.
GZ06	Zone Name	Ground
	Zone group	-
	Zoning requirements applied (ref.:[22])	ZCR 3.5, ZCR 3.6
	Logical boundary	The zone comprises ground applications (remote clients) communicating with train on-board devices through Ground Communication Gateway (GCG) and the GCG itself.
	Physical boundary	No physical boundary due to wireless network.
	Safety designation	Not safety related.
	Logical access points	Mobile network like LTE or GSM.
	Physical access points	Not applicable due to wireless network.
	Data flows	Exchange of non-safety critical data like diagnostic or telemetric information
	Connected zones or conduits	Conduit GCG_MAR
	Assets	Ground Communication Gateway (GCG) and remote clients
	SL-T	Out of scope
	Applicable security countermeasures	Out of scope
	Assumptions and external dependencies	With respect to the SuC the devices of this zone are considered as external entities.

Table 77: Definition of Common Conduits

GC01	Conduit Name	Ethernet_Train_Backbone
	Zone group	-
	Zoning requirements applied (ref.:[22])	-
	Logical boundary	ETB spanning over complete train with all its network devices (switches, repeaters, connectors, cables, couplers). Interfaces are the IP router interface of ETBN to ECN and the ETB-ED interfaces.

	Physical boundary	Assets of this conduit are mainly in locked cabinets or in cable conduits (Ethernet cable) only accessible by maintenance staff. However, the coupler provides on the outside of the consist an interface to the ETB (for interconnection) which is in general more difficult to physically secure and therefore a weak point.
	Safety designation	Safety related with respect to data exchange between devices in zone TCMS_Constit_Safety of different consists as well as train inauguration function. Non-safety related with respect to data exchange between devices in other zones of different consists.
	Logical access points	Physical (e.g. Ethernet port) interface for connecting network devices on ETB (switches and repeaters).
	Physical access points	Assets are mainly located in locked cabinets only accessible to authorized personnel. However, the coupler provides on the outside of the consist an access point.
	Data flows	Exchange of safety and non-safety critical train-wide data.
	Connected zones or conduits	Zone ETBN
	Assets	Passive and active network components constituting the wired network segment assigned to this conduit.
	SL-T	{1, 1, 1, 1, 1, 1, 1}
	Applicable security countermeasures	None
	Assumptions and external dependencies	-
GC02	Conduit Name	GCG_MAR
	Zone group	-
	Zoning requirements applied (ref.: [22])	-
	Logical boundary	The conduit interconnects the zone Ground and zone MAR that contains MCG devices with different categories.
	Physical boundary	Out of scope
	Safety designation	Out of scope
	Logical access points	Out of scope
	Physical access points	Out of scope
	Data flows	Out of scope
	Connected zones or conduits	Zone Ground Zone MAR
	Assets	Out of scope
	SL-T	Out of scope
	Applicable security countermeasures	Out of scope
	Assumptions and external dependencies	-

Table 78: Definition of TCMS Zone Groups

TG01	Zone Group Name	TCMS
	Zoning requirements applied (ref.: [22])	ZCR 3.1; ZCR 3.2; ZCR 3.7; ZCR 3.8
	Characteristics	The zone groups devices (end devices and network devices) onboard train that carry functions assigned to the TCMS domain. The zone is a dynamic one, meaning that the types and number of assets can change in dependence on train composition.
TG02	Zone Group Name	TCMS_Constit
	Parent Zone	TCMS

	Zoning requirements applied (ref.:[22])	ZCR 3.2
	Characteristics	The zone groups devices that carry functions assigned to the TCMS domain and that are located in a single consist. The zone is a static one.

Table 79: Definition of TCMS Zones

TZ01	Zone Name	TCMS_Consist_Safety
	Zone group	TCMS_Consist
	Zoning requirements applied (ref.:[22])	ZCR 3.3, ZCR 3.8
	Logical boundary	The zone groups devices that carry safety-related functions assigned to the TCMS domain and that are located in a single consist, possibly distributed over several cars.
	Physical boundary	Devices of this zone are in locked cabinets or in cable conduits (Ethernet cable) only accessible by maintenance staff.
	Safety designation	Safety critical
	Logical access points	Network shared with zone TCMS_Consist-Regular (ECN). Remote maintenance is not allowed for the devices of this zone. The direct connection to the zone MAR for the train to ground communication is not allowed.
	Physical access points	Devices are located in locked cabinets only accessible to authorized personnel.
	Data flows	Exchange of safety related data only using VDP (IEC61375-2-3).
	Connected zones or conduits	The zone directly interacts with the TCMS_Consist-Regular and Local_Maintenance zones. The devices of this zone communicate with the devices located in TCMS_Consist_Safety zones of other consists via train backbone represented to them as the ETBN zone which they interact with via the ETBN_TCMS_Consist_S conduit.
	Assets	Wired end devices that carry safety-related functions, passive and active network components constituting the wired consist network segment assigned to this zone. NOTE The relation to TTDB, DNS should be primarily addressed in safety analysis.
	SL-T	{4, 1, 1, 1, 1, 1, 1}
	Applicable security countermeasures	Security event detection
	Assumptions and external dependencies	-
TZ02	Zone Name	TCMS_Consist-Regular
	Zone group	TCMS_Consist
	Zoning requirements applied (ref.:[22])	ZCR 3.3
	Logical boundary	The zone groups devices that carry non-safety-related functions assigned to the TCMS domain and that are located in a single consist, possibly distributed over several cars.
	Physical boundary	Devices of this zone are in locked cabinets or in cable conduits (Ethernet cable) only accessible by maintenance staff.
	Safety designation	Non-safety critical
	Logical access points	Network shared with zone TCMS_Consist_Safety (ECN).
	Physical access points	Devices are located in locked cabinets only accessible to authorized personnel.
	Data flows	Exchange of non-safety critical data using TRDP (IEC61375-2-3).
	Connected zones or conduits	The zone directly interacts with the TCMS_Consist_Safety, OOS_Consist_Wired, MAR and Onboard_Remote_Maintenance zones. The devices of this zone communicate with the devices located in TCMS_Consist-Regular zones of other consists via train backbone represented to them as the ETBN zone which they interact with via the ETBN_TCMS_Consist_R conduit.
	Assets	Wired end devices that carry non-safety critical functions, passive and active network components constituting the wired consist network segment assigned to this zone.
	SL-T	{3, 1, 1, 1, 1, 1, 1}

	Applicable security countermeasures	Security event detection
	Assumptions and external dependencies	-

Table 80: Definition of TCMS Conduits

TC01	Conduit Name	TCMS_Consist_Regular_Safety
	Zone group	TCMS_Consist
	Zoning requirements applied (ref.:[22])	ZCR 3.3
	Logical boundary	The conduit connects the zone TCMS_Consist_Safety with the zone TCMS_Consist-Regular in the same consist.
	Physical boundary	Assets of this conduit are in locked cabinets or in cable conduits (Ethernet cable) only accessible by maintenance staff.
	Safety designation	Safety critical
	Logical access points	Network shared with zone TCMS_Consist_Safety and zone TCMS_Consist-Regular..
	Physical access points	Assets are located in locked cabinets only accessible to authorized personnel.
	Data flows	Exchange of non-safety critical data using TRDP (IEC61375-2-3).
	Connected zones or conduits	Zone TCMS_Consist_Safety Zone TCMS_Consist-Regular
	Assets	Passive and active network components constituting the wired consist network segment assigned to this conduit.
	SL-T	{1, 1, 1, 1, 1, 1}
	Applicable security countermeasures	Firewalls, Security event detection
	Assumptions and external dependencies	
TC02	Conduit Name	ETBN_TCMS_Consist_R
	Zone group	TCMS
	Zoning requirements applied (ref.:[22])	-
	Logical boundary	The conduit connects the zone ETBN with the zone TCMS_Consist-Regular in the same consist.
	Physical boundary	Assets of this conduit are in locked cabinets or in cable conduits (Ethernet cable) only accessible by maintenance staff.
	Safety designation	Non-safety critical
	Logical access points	Physical (e.g. Ethernet port) interface for connecting the ETBN to ECN.
	Physical access points	Assets are located in locked cabinets only accessible to authorized personnel.
	Data flows	Exchange of non-safety critical train-wide data using TRDP (IEC61375-2-3).
	Connected zones or conduits	Zone ETBN Zone TCMS_Consist-Regular
	Assets	Passive and active network components constituting the wired consist network segment assigned to this conduit.
	SL-T	{4, 4, 1, 1, 4, 1, 1}
	Applicable security countermeasures	Firewalls, Security event detection
	Assumptions and external dependencies	-
TC03	Conduit Name	ETBN_TCMS_Consist_S
	Zone group	TCMS

	Zoning requirements applied (ref.:[22])	-
	Logical boundary	The conduit connects the zone ETBN with the zone TCMS_Consist_Safety in the same consist.
	Physical boundary	Assets of this conduit are in locked cabinets or in cable conduits (Ethernet cable) only accessible by maintenance staff.
	Safety designation	Safety critical
	Logical access points	Physical (e.g. Ethernet port) interface for connecting the ETBN to ECN.
	Physical access points	Assets are located in locked cabinets only accessible to authorized personnel.
	Data flows	Exchange of safety related train-wide data only using VDP (IEC61375-2-3).
	Connected zones or conduits	Zone ETBN Zone TCMS_Consist_Safety
	Assets	Passive and active network components constituting the wired consist network segment assigned to this conduit.
	SL-T	{4, 4, 1, 1, 4, 1, 1}
	Applicable security countermeasures	Firewalls, Security event detection
	Assumptions and external dependencies	-
TC04	Conduit Name	MAR_TCMS
	Zone group	TCMS
	Zoning requirements applied (ref.:[22])	-
	Logical boundary	The conduit connects the zone MAR with the zone TCMS_Consist-Regular in the same consist.
	Physical boundary	Assets of this conduit are in locked cabinets or in cable conduits (Ethernet cable) only accessible by maintenance staff.
	Safety designation	Non-safety critical
	Logical access points	Physical (e.g. Ethernet port) interface for connecting the MAR to ECN.
	Physical access points	Assets are located in locked cabinets only accessible to authorized personnel.
	Data flows	Exchange of non-safety critical data like diagnostic or telemetric information
	Connected zones or conduits	Zone MAR Zone TCMS_Consist-Regular
	Assets	Passive and active network components constituting the wired consist network segment assigned to this conduit.
	SL-T	{4, 4, 1, 1, 4, 1, 1}
	Applicable security countermeasures	Firewalls, Security event detection
	Assumptions and external dependencies	-
TC05	Conduit Name	RM_TCMS-Regular
	Zone group	TCMS
	Zoning requirements applied (ref.:[22])	-
	Logical boundary	The conduit interconnects the end devices of the TCMS_Consist-Regular zone with the maintenance tool via NG-TCN. Contrary to local maintenance the remote maintenance requires the access to the NG-TCN
	Physical boundary	Assets of this conduit are in locked sockets or in cable conduits (Ethernet cable) only accessible by maintenance staff.
	Safety designation	Non-safety critical
	Logical access points	Physical (e.g. Ethernet port) interface for connecting a service device to ECN.

	Physical access points	Assets are located in locked sockets (normally in driver cab) only accessible to authorized personnel.
	Data flows	Reading of diagnostic information Reading and writing configuration parameters Download of software
	Connected zones or conduits	Zone Onboard_Remote_Maintenance Zone TCMS_Consist_Regular
	Assets	Passive and active network components constituting the wired consist network segment assigned to this conduit.
	SL-T	{4, 4, 1, 1, 4, 1, 1}
	Applicable security countermeasures	Firewalls, Security event detection, Network access control
	Assumptions and external dependencies	-
TC06	Conduit Name	LM_TCMS_Safety
	Zone group	TCMS
	Zoning requirements applied (ref.:[22])	-
	Logical boundary	The conduit directly interconnects the end device located in the TCMS_Consist_Safety zone and the maintenance tool via dedicated interface of the end device.
	Physical boundary	Assets are only connected on demand (in case of maintenance access) to end devices located in locked cabinets.
	Safety designation	Safety critical
	Logical access points	Physical (e.g. Ethernet or serial port) interface for connecting a service device to end device.
	Physical access points	Assets are only connected on demand.
	Data flows	Dependent on end device.
	Connected zones or conduits	Zone TCMS_Consist_Safety Zone Local_Maintenance
	Assets	Passive or active components like service cables.
	SL-T	{4, 4, 1, 1, 4, 1, 1}
	Applicable security countermeasures	No recommendation because dependence on end device.
	Assumptions and external dependencies	-
TC07	Conduit Name	OOS_TCMS
	Zone group	TCMS
	Zoning requirements applied (ref.:[22])	-
	Logical boundary	The conduit interconnects the TCMS_Consist-Regular and the OOS_Consist zones in the same consist.
	Physical boundary	Assets of this conduit are in locked cabinets only accessible by maintenance staff.
	Safety designation	Non-safety critical
	Logical access points	Virtual interfaces inside GW devices
	Physical access points	Assets are located in locked cabinets only accessible to authorized personnel.
	Data flows	Exchange of non-safety critical data using TRDP (IEC61375-2-3).
	Connected zones or conduits	Zone OOS_Consist_Wired Zone TCMS_Consist-Regular
	Assets	Active network components with GW functionality.
	SL-T	{4, 4, 1, 1, 4, 1, 1}
	Applicable security countermeasures	Firewalls, Security event detection

	Assumptions and external dependencies	-

Table 81: Definition of OOS Zone Groups

OG01	Zone Group Name	OOS
	Zoning requirements applied (ref.:[22])	ZCR 3.1; ZCR 3.2; ZCR 3.7; ZCR 3.8
	Characteristics	The zone groups devices (end devices and network devices) onboard train that carry functions assigned to the OOS domain. The zone is a dynamic one, meaning that the types and number of assets can change in dependence on train composition.
OG02	Zone Group Name	OOS_Consist
	Parent Zone	OOS
	Zoning requirements applied (ref.:[22])	ZCR 3.2
	Characteristics	The zone groups devices that carry functions assigned to the OOS domain and that are located in a single consist. The zone is a static one.

Table 82: Definition of OOS Zones

OZ01	Zone Name	OOS_Consist_Wired
	Zone group	OOS_Consist
	Zoning requirements applied (ref.:[22])	ZCR 3.2
	Logical boundary	The zone groups devices that carry functions assigned to the OOS domain and that are located in the same consist, possibly distributed over several cars. The devices of this zone are connected to the wired part of the consist network.
	Physical boundary	Devices of this zone are in locked cabinets or in cable conduits (Ethernet cable) only accessible by maintenance staff. In addition, devices can also be located in public like PIS displays or CCTV cameras.
	Safety designation	Non-safety critical
	Logical access points	Network infrastructure is shared with consist network of zones in group TCMS but need to be logically separated with for example VLANs.
	Physical access points	Devices are located in locked cabinets only accessible to authorized personnel or located in public.
	Data flows	Exchange of non-safety critical data using TRDP (IEC61375-2-3) as well as OOS specific data like video streams.
	Connected zones or conduits	The zone directly interacts with the TCMS_Consist-Regular, OOS_Consist_Wireless, MAR and Onboard_Remote_Maintenance zones. The devices of this zone communicate with the devices located in OOS_Consist_Wired zones of other consists via train backbone represented to them as the ETBN zone which they interact with via the ETBN_OOS conduit.
	Assets	Wired end devices that carry functions assigned to the OOS domain, passive and active network components constituting the wired consist network segment assigned to this zone.
	SL-T	{2, 1, 1, 1, 1, 1, 1}
	Applicable security countermeasures	Security event detection, Encryption, Network access control
	Assumptions and external dependencies	-
OZ02	Zone Name	OOS_Consist_Wireless
	Zone group	OOS_Consist
	Zoning requirements applied (ref.:[22])	ZCR 3.5

	Logical boundary	The zone comprises a WLAN/WPAN system operating within one consist. The zone incorporates the wireless devices that carry functions assigned to the OOS domain.
	Physical boundary	No physical boundary due to wireless network.
	Safety designation	Non-safety critical.
	Logical access points	Wireless (WLAN) interface for connecting to OOS network.
	Physical access points	Not applicable due to wireless network.
	Data flows	Exchange of non-safety critical data using TRDP (IEC61375-2-3) as well as OOS specific data like video streams.
	Connected zones or conduits	Conduit OOS_Wireless
	Assets	Wireless end devices that carry functions assigned to the OOS domain, passive and active network components constituting the wireless consist network segment assigned to this zone.
	SL-T	Out of scope
	Applicable security countermeasures	Out of scope
	Assumptions and external dependencies	-

Table 83: Definition of OOS Conduits

OC01	Conduit Name	RM_OOS_Wired
	Zone group	OOS
	Zoning requirements applied (ref.:[22])	-
	Logical boundary	The conduit interconnects the end devices of the OOS_Consist_Wired zone with the maintenance tool via NG-TCN. Contrary to local maintenance the remote maintenance requires the access to the NG-TCN
	Physical boundary	Assets of this conduit are in locked sockets or in cable conduits (Ethernet cable) only accessible by maintenance staff.
	Safety designation	Non-safety critical
	Logical access points	Physical (e.g. Ethernet port) interface for connecting a service device to ECN.
	Physical access points	Assets are located in locked sockets (normally in driver cab) only accessible to authorized personnel.
	Data flows	Reading of diagnostic information Reading and writing configuration parameters Download of software
	Connected zones or conduits	Zone Onboard_Remote_Maintenance Zone OOS_Consist_Wired
	Assets	Passive and active network components constituting the wired consist network segment assigned to this conduit.
	SL-T	{2, 2, 1, 1, 2, 1, 1}
	Applicable security countermeasures	Firewalls, Security event detection, Network access control
	Assumptions and external dependencies	-

OC02	Conduit Name	RM_OOS_Wireless
	Zone group	OOS
	Zoning requirements applied (ref.:[22])	-
	Logical boundary	The conduit interconnects the end devices of the OOS_Consist_Wireless zone with the maintenance tool via WLAN of OOS. Contrary to local maintenance the remote maintenance requires the access to the WLAN of OOS.
	Physical boundary	Out of scope

	Safety designation	Non-safety critical
	Logical access points	Wireless (WLAN) interface for connecting a service device to network.
	Physical access points	Out of scope
	Data flows	Out of scope
	Connected zones or conduits	Zone Onboard_Remote_Maintenance Zone OOS_Consist_Wireless
	Assets	Passive and active network components constituting the wireless consist network segment assigned to this conduit.
	SL-T	Out of scope
	Applicable security countermeasures	Out of scope
	Assumptions and external dependencies	-
<hr/>		
OC03	Conduit Name	ETBN_OOS
	Zone group	OOS
	Zoning requirements applied (ref.:[22])	-
	Logical boundary	The conduit connects the zone ETBN with the zone OOS_Consist_Wired in the same consist.
	Physical boundary	Assets of this conduit are in locked cabinets or in cable conduits (Ethernet cable) only accessible by maintenance staff.
	Safety designation	Non-safety critical
	Logical access points	Physical (e.g. Ethernet port) interface for connecting the ETBN to ECN.
	Physical access points	Assets are located in locked cabinets only accessible to authorized personnel.
	Data flows	Exchange of non-safety critical train-wide data using TRDP (IEC61375-2-3) as well as OOS specific data like video streams.
	Connected zones or conduits	Zone ETBN Zone OOS_Consist_Wired
	Assets	Passive and active network components constituting the wired consist network segment assigned to this conduit.
	SL-T	{2, 2, 1, 1, 2, 1, 1}
	Applicable security countermeasures	Firewalls, Security event detection
	Assumptions and external dependencies	-
<hr/>		
OC04	Conduit Name	MAR_OOS
	Zone group	OOS
	Zoning requirements applied (ref.:[22])	-
	Logical boundary	The conduit connects the zone MAR with the zone OOS_Consist_Wired in the same consist.
	Physical boundary	Assets of this conduit are in locked cabinets or in cable conduits (Ethernet cable) only accessible by maintenance staff.
	Safety designation	Non-safety critical
	Logical access points	Physical (e.g. Ethernet port) interface for connecting the MAR to ECN.
	Physical access points	Assets are located in locked cabinets only accessible to authorized personnel.
	Data flows	Exchange of non-safety critical data like diagnostic information or video streams
	Connected zones or conduits	Zone MAR Zone OOS_Consist_Wired
	Assets	Passive and active network components constituting the wired consist network segment assigned to this conduit.

	SL-T	{2, 2, 1, 1, 2, 1, 1}
	Applicable security countermeasures	Firewalls, Security event detection
	Assumptions and external dependencies	-
<hr/>		
OC05	Conduit Name	OOS_Wireless
	Zone group	OOS
	Zoning requirements applied (ref.:[22])	-
	Logical boundary	The conduit connects the zone OOS_Consist_Wireless with the zone OOS_Consist_Wired in the same consist.
	Physical boundary	Assets of this conduit are in locked cabinets or in cable conduits (Ethernet cable) only accessible by maintenance staff.
	Safety designation	Non-safety critical
	Logical access points	Physical (e.g. Ethernet port) interface for connecting the AP to ECN.
	Physical access points	Assets are located in locked cabinets only accessible to authorized personnel.
	Data flows	Exchange of non-safety critical data using TRDP (IEC61375-2-3) as well as OOS specific data like video streams.
	Connected zones or conduits	Zone OOS_Consist_Wireless Zone OOS_Consist_Wired
	Assets	Passive and active network components constituting the wired consist network segment assigned to this conduit.
	SL-T	{1, 1, 1, 1, 1, 1, 1}
	Applicable security countermeasures	Firewalls, Security event detection
	Assumptions and external dependencies	-
<hr/>		
OC06	Conduit Name	COS_OOS
	Zone group	OOS
	Zoning requirements applied (ref.:[22])	-
	Logical boundary	The conduit connects the zone COS with the OOS_Consist zones in the same consist.
	Physical boundary	Assets of this conduit are in locked cabinets only accessible by maintenance staff.
	Safety designation	Non-safety critical
	Logical access points	Virtual interfaces inside GW devices
	Physical access points	Assets are located in locked cabinets only accessible to authorized personnel.
	Data flows	Non-safety critical data like telemetric information only in direction of COS (data diode)
	Connected zones or conduits	Zone COS Zone OOS_Consist_Wired
	Assets	Active network components with GW functionality.
	SL-T	{2, 2, 1, 1, 2, 1, 1}
	Applicable security countermeasures	Firewalls, Security event detection
	Assumptions and external dependencies	-

I Annex – ETB Bypass (for legacy applications)

I.1 General

In ETB topology variant B the redundant ETB nodes are connected in series. To achieve a good system availability each ETB node should be able to feed through traffic between Directions 1 and 2 with a high dependability. Therefore, a bypass relay mechanism as shown in Figure 159 is used. If the relays are not energized (special case: power loss) the node galvanically feeds through the signals between direction 1 and 2. If the relays are energized the Dir1 and Dir2 connections are attached to ports of the switch core and normal operation is achieved. The practical implementation uses RF (high frequency and balanced line) relays with DPDT contacts (two mechanically coupled SPDT switches for switching one balanced signal pair). For 100BASE-TX 4 such relays are required per redundant line (as shown in Figure 159), that is 8 relays in total. For 1000BASE-T (see Figure 160), which is the proposed technology for the future ETB, the total number of relays doubles to 16.

Due to the high number of relay contacts involved, a relay circuit malfunction may lead to a high number of different incorrect contact combinations.

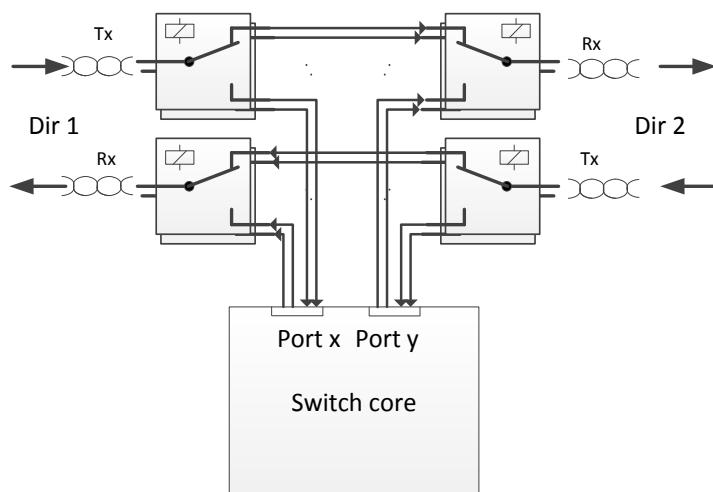


Figure 159:Bypass Relays, 100BASE-TX, one redundant line shown

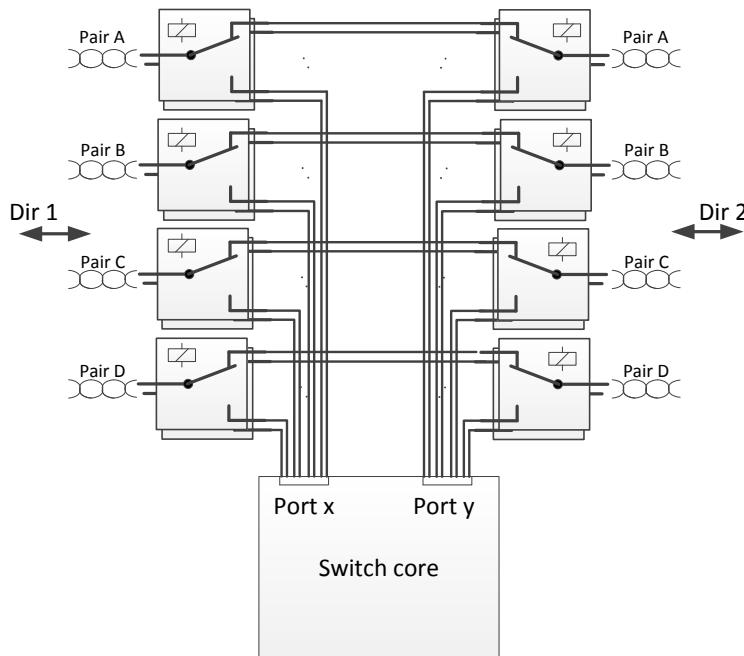


Figure 160:Bypass Relays, 1000BASE-T , one redundant line shown

I.2 Bypass relay circuit

Principally each SPDT contact can be switched to either of the 2 taps or being open (due to contact malfunction). With 32 SPDT contacts inside an ETBN that leads to $3^{32} = 1.9 \times 10^{15}$ combinations, with only 2 of the combinations being valid (all the relays either activated or not).

A single failure in the bypass circuit shall not render the complete system useless. This is established by using redundant ETB lines. The line redundancy won't help if the erroneous line is not correctly identified. Reliable detection of a relay fault is therefore a critical sub function of the bypass relay circuit.

I.2.1 Bypass relay failure modes (single relay)

Table 84 lists the potential single relay failure modes.

Table 84: Relay failure modes

Relay Failure	Possible Cause	Relative Probability
Both SPDT contacts in one relay stuck in the non-energized position	Defect of coil, control or wiring. Mechanical defect	Highest
Both SPDT contacts in one relay stuck in the energized position	Defect of control, mechanical defect.	High
Contact open	Wear of individual contact. Typically only one or few contacts are effected.	Medium to low
Within a single relay the two SPDT contacts are switched differently	Mechanical defect	Very low.

I.2.2 Common mode faults

Common mode failures, where a single failure leads to multiple relays switching wrong are easily introduced by the necessity to connect all relay coils in series or in parallel or a combination of both. On one hand common mode faults are principally undesirable. In the context of the bypass relay circuit, intentionally allowing for it and grouping relays (e.g. by putting relay coils in series) reduces the probability of arbitrary single relay faults, which might be harder to detect and to cope with than a failure of a group of relays.

I.2.3 Physical layer 1000BASE-T versus 100BASE-TX

The traditional 100BASE-TX Ethernet physical layer [29], clause 25, (which was used so far for the ETB) uses two wire pairs, carrying one data direction per pair (Figure 161). Relay failure of a pair of relays used for conveying the same differential pair cause a failure scenario, which cannot be trivially detected by just looking at the link status. See example in Figure 162: two of the relays of the middle ETBN are switched to the wrong position. Still all three ETBNs have a “link-up” indication on their ETB ports. The situation is still detectable by evaluating the received TOPO and HELLO frames, which will not lead to a valid inauguration. The situation is also detectable by evaluating the redundant link and detecting a discrepancy with the received HELLO frames there.

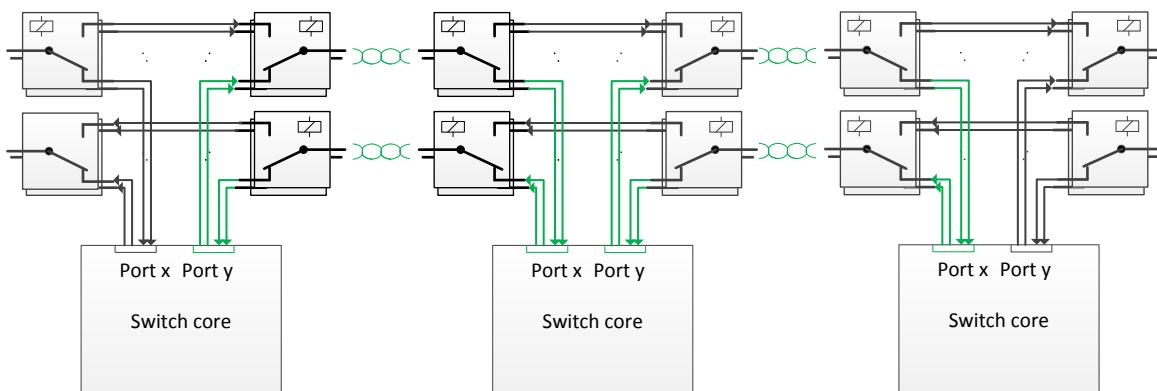


Figure 161: 3 ETBNs, normal operational mode (100BASE-TX), one redundant line shown

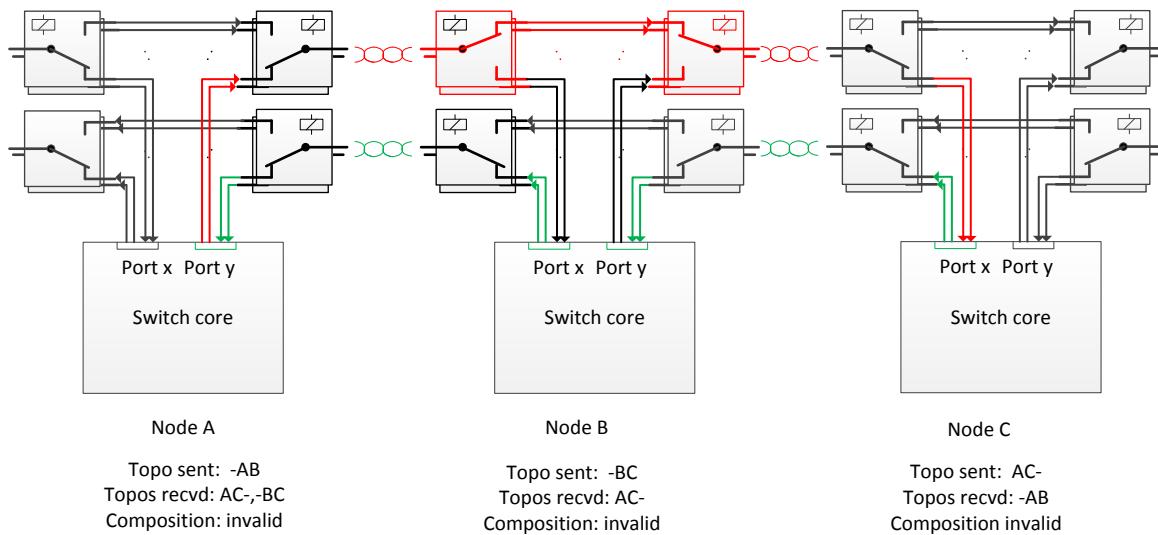


Figure 162: 3 ETBNs, bypass relay failure (100BASE-TX), one redundant line shown

Using 1000BASE-T Ethernet [29], clause 40, greatly simplifies the detection of a contact fault. The 1000BASE-T physical layer uses all 4 wire pairs in parallel and bi-directionally. If the wire pairs are not terminated to the same port no valid code bit stream will be detected and no link indication signalled. That is a single or multiple contact faults always lead to an easily detectable link down.

I.3 Line redundancy

The ETB supports two individual redundant links using link aggregation (see Figure 163). Link aggregation assumes that both lines originate from the same ETBN. Considering a possible common mode failure of the bypass circuit a scenario as shown in Figure 164 is feasible, where the lines originate from different ETBNs. This is an undesirable scenario as it is not easily decidable from line redundancy point of view which line to choose.

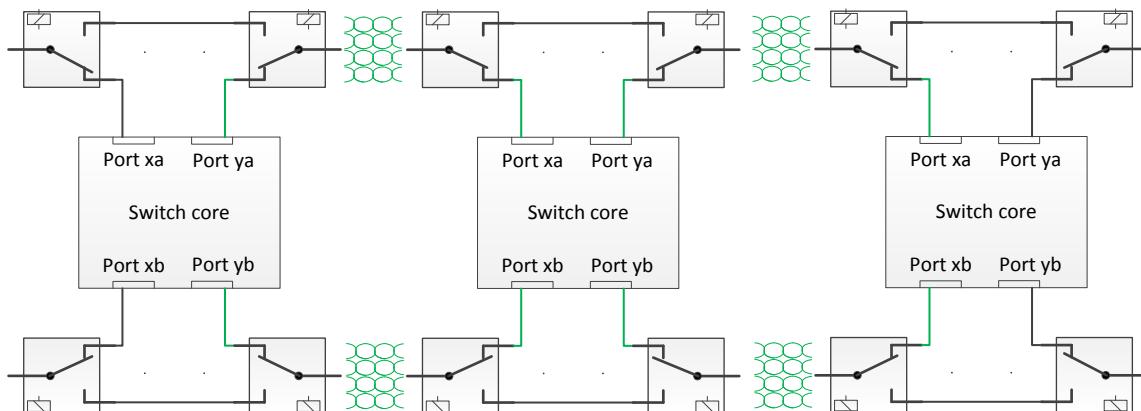


Figure 163: 3 ETBNs, normal operation, redundant line

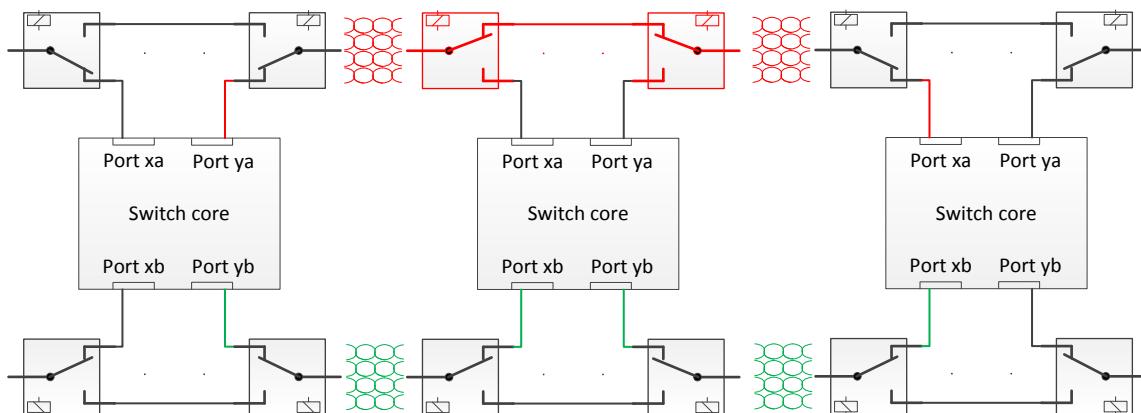


Figure 164: 3 ETBNs, failure in middle ETBN

I.4 Relay Control to Optimize Detectability and Availability

Table 85 summarizes design goals for the ETB relay bypass system. There are 4 relay groups with 4 relays each (one relay per wire pair) as shown in Figure 165. Each group is associated with one ETB port.

The first goal is to reduce the probability of common mode failures affecting both redundant lines (independence of groups Dir1A/Diir2A relative to Dir1B/Dir2B). The second goal is to reduce the probability of common mode failures affecting groups Dir1 relative to Dir2 on the same redundant line. In effect the control and power supply of all 4 groups shall be reasonably independent. An individual check that a relay group is energized or not (e.g. by current sense) is required to detect the degradation of the system before a double fault can materialize.

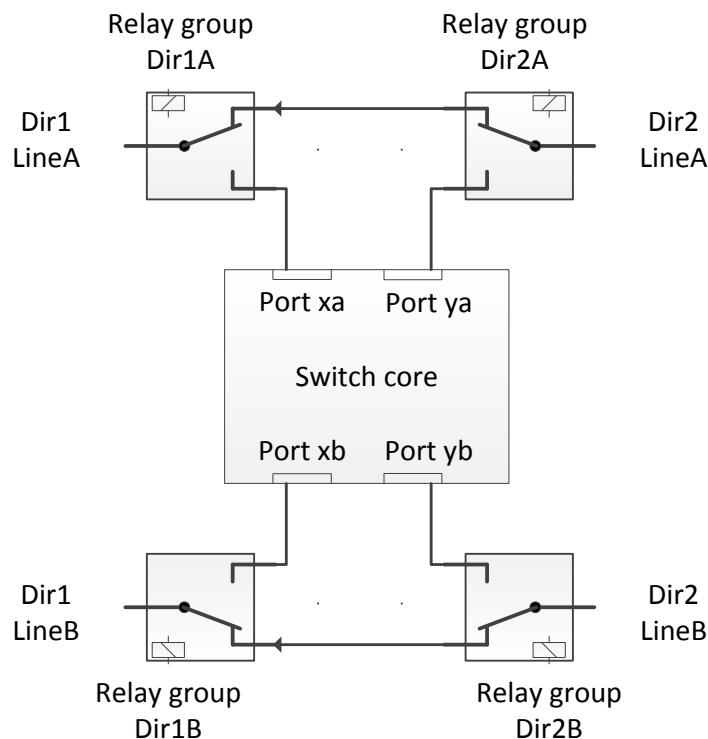


Figure 165: Bypass relays 4 groups with 4 relays each

Table 85: Failure modes and mitigations, Variant B ETB bypass

Design Goal	Possible Implementation	Comment
Single relay failure shall not cause malfunction.	1000BASE-T can easily cope with single relay failures. Single relay failure prevent link up.	Detected by “no link” status. Only works for 1000BASE-T.
Avoid scenario where only one redundant line is bypassed (as in Figure 164).	Independent power supply and control of the 4 relay groups connected to ETB ports.	Read back of relay status (current sense) for diagnostics desirably to detect continuous degradation.
Keep redundant lines independent.	Independent power supply and control of the relays belonging to either redundant line.	Already covered by above mitigation.
Prevent undetected isolation of ETBN due to relay circuit fault.	Read back relay status (current sense).	Maintaining redundancy requires diagnostics.

J Analysis of single points of failure

This annex revises the analysis of the single points of failure of the network done in T3.3 (see [05]) to check if any of them is not covered by the NG-TCN architecture. This analysis is only done for the D₁ ETB topology variant.

In general, there were 3 types of failure that with a single error could lead to the unavailability of the train:

- Persistent errors in synchronization frames in the "master ETBN". Here it was supposed that there was only one active master clock, only in one of the ETB lines and that this was the one that disseminated the time to the other line. Thus, it was supposed that if there was a persistent error in the master ETBN, none of the lines would be synchronized. Anyway, it was assumed that there would be a "degraded mode" that could somehow mitigate this.

Now, we have discarded the "degraded mode", but the concept is different as we assume that there are redundant clocks in both ETB lines. So these errors would still be mitigable.

- It was supposed that there could exist critical data for availability, but which is not safety related data so the SDT is not used, could be transmitted as TSN (in both lines). In the worst case, when the wrong frame is arrived first and is not discarded as the error is not detectable, it was supposed that the train could go to an unavailable state. Nevertheless, it was assumed as well that if the data is considered critical, necessary mechanisms could be applied at application level to detect those errors. This assumption is still valid.
- And finally the errors in inauguration frames. Here the problem was with the errors that are persistent. With the different mitigations proposed in the new inauguration mechanisms, the errors could be detected, but it was assumed that if the errors persist, the inauguration could not be finalized.

The doubt here is if it is always possible to detect where these errors (Master ETBN, Slave ETBN, Repeaters, cables) are located and if it is possible to finalize the inauguration not taking into account the related element.

The table we did in the FMECA in D3.3 has been copied (Table 86) and a new column to analyse it with the "last concept" of the architecture has been added. Here one can see all the errors analysed. The ones in green are the ones that were already assumed as mitigable, and the ones in white are the ones that we were not sure if they were mitigable.

The main doubt is the one previously stated about the persistent errors in inauguration frames. If these are mitigable (not sure if all of them would be), it can be said that ID_30000 (in chapter 2.11) can be fulfilled.

Table 86: Revision of single points of failure analysis

COMPONENT NETWORK	ID FAILURE MODE	FURTHER MITIGATION MEASURE	NEW REVISION for T3.5
Master ETBN	ID_3007 Transient loss of TSN sync frames through the corresponding line of the master ETBN	In case this failure mode occurs, the network would go to asynchronous mode and in order not to loss critical data, a degraded mode could be defined. In this degraded mode, the rest of the traffic is cut passing only the critical data (S4R proposal). This or another possible mitigation shall be analysed in D3.5	It is supposed that this would was mitigated with the degraded mode. Although we do not assume the degraded mode now, as the synchronization of the other line would happen although there is an error in the "master ETBN" the synchronization will not be lost in the other line (previously it was supposed that the master clock would exist only in the master ETBN). So this single point of failure could be mitigated.
Master ETBN	ID_3008A Inauguration data frame transmitted from the corresponding switch port (master ETBN) is corrupted (persistent)	Not for now.	Mitigations where already proposed. - <i>Direction check with the egressDir</i> . - <i>Improve CRC of HELLO frames</i> . - <i>Plausibility check of CSTINFO</i> . But then it was supposed that the corruption was detected and an invalid inauguration will occur. In this case, would it be possible to detect which ETBN is the corrupted one and discard that from the inauguration?
Master ETBN	ID_3010A TSN ETB data frame transmitted from the corresponding switch port is corrupted (persistent)	It could be analysed which mitigation measure could be applied for the non-safety but critical data to detect the wrong message and discard it, so the frame of the other plane would be processed correctly.	Here it was supposed that critical data for availability, but which is not safety-related so the SDT is not used, could be transmitted as TSN (both lines). In the worst case, when the wrong frame is arrived first and is not discarded as the error is not detected, it was supposed that the train could go to an unavailable state. Anyway, it is supposed that if the data is considered critical, necessary mechanisms could be applied at application level to detect the errors.
Master ETBN	ID_3010B TSN ETB data frame transmitted from the corresponding switch port is corrupted (sporadic)	It could be analysed which mitigation measure could be applied for the non-safety but critical data to detect the wrong message and discard it, so the frame of the other plane would be processed correctly.	Here it was supposed that critical data for availability, but which is not safety-related so the SDT is not used, could be transmitted as TSN (both lines). In the worst case, when the wrong frame is arrived first and is not discarded as the error is not detected, it was supposed that the train could go to an unavailable state. Anyway, it is supposed that if the data is considered critical, necessary mechanisms could be applied at application level to detect the errors.
Master ETBN	ID_3011A TSN sync frame transmitted from the corresponding switch port is corrupted (persistent)	In case this failure mode occurs, the network would go to asynchronous mode and in order not to loss critical data, a degraded mode could be defined. In this degraded mode, the rest of the traffic is cut passing only the critical data (S4R proposal). This or another possible mitigation shall be analysed in D3.5	Similar to ID_3007. It is assumed could be mitigated if there are redundant master clocks.
Master ETBN	ID_3016 TSN sync frames transmitted from the corresponding switch port with an unacceptable delay	In case this failure mode occurs, the network would go to asynchronous mode and in order not to loss critical data, a degraded mode could be defined. In this degraded mode, the rest of the traffic is cut passing only the critical data (S4R proposal). This or another possible mitigation shall be analysed in D3.5	Similar to ID_3007. It is assumed could be mitigated if there are redundant master clocks.
Master ETBN	ID_3021A A TSN sync frame is transmitted from the wrong port of the switch. (persistent)	In case this failure mode occurs, the network would go to asynchronous mode and in order not to loss critical data, a degraded mode could be defined. In this degraded mode, the rest of the traffic is cut passing only the critical data (S4R proposal). This or another possible mitigation shall be analysed in D3.5	Similar to ID_3007. It is assumed could be mitigated if there are redundant master clocks.

COMPONENT NETWORK	ID FAILURE MODE	FURTHER MITIGATION MEASURE	NEW REVISION for T3.5
Master ETBN	ID_3023A A inauguration data frame egresses from the switch port in a wrong order. (persistent)	Not for now.	It has been supposed that error is detectable with the respective sequence counters of the inauguration frames. But that if the error persists, a correct inauguration would not be possible. Would it be possible to detect where is the error and discard the corresponding ETBN to finalize the inauguration?
Master ETBN	ID_3025A A TSN ETB data frame egresses from the switch port in a wrong order. (persistent)	It could be analysed which mitigation measure could be applied for the non-safety but critical data to detect the wrong message and discard it, so the frame of the other plane would be processed correctly.	Similar to ID_3010A. It is assumed could be mitigated with mechanisms at application level in critical but non-safety related applications.
Master ETBN	ID_3026A A TSN sync frame egresses from the switch port in a wrong order. (persistent)	In case this failure mode occurs, the network would go to asynchronous mode and in order not to loss critical data, a degraded mode could be defined. In this degraded mode, the rest of the traffic is cut passing only the critical data (S4R proposal). This or another possible mitigation shall be analysed in D3.5	Similar to ID_3007. It is assumed could be mitigated if there are redundant master clocks.
Master ETBN	ID_3028A A inauguration data frame is sent replicated from the switch port. (persistent)	Not for now.	Similar to ID_3023A. It has been supposed that error is detectable with the respective sequence counters of the inauguration frames. But that if the error persists, a correct inauguration would not be possible. Would it be possible to detect where is the error and discard the corresponding ETBN to finalize the inauguration?
Master ETBN	ID_3030A A TSN ETB data frame is sent replicated from the switch port. (persistent)	It could be analysed which mitigation measure could be applied for the non-safety but critical data to detect the wrong message and discard it, so the frame of the other plane would be processed correctly.	Similar to ID_3010A. It is assumed could be mitigated with mechanisms at application level in critical but non-safety related applications.
Master ETBN	ID_3030B A TSN ETB data frame is sent replicated from the switch port. (sporadic)	It could be analysed which mitigation measure could be applied for the non-safety but critical data to detect the wrong message and discard it, so the frame of the other plane would be processed correctly.	Similar to ID_3010A. It is assumed could be mitigated with mechanisms at application level in critical but non-safety related applications.
Master ETBN	ID_3031A A TSN sync frame is sent replicated from the switch port. (persistent)	In case this failure mode occurs, the network would go to asynchronous mode and in order not to loss critical data, a degraded mode could be defined. In this degraded mode, the rest of the traffic is cut passing only the critical data (S4R proposal). This or another possible mitigation shall be analysed in D3.5	Similar to ID_3007. It is assumed could be mitigated if there are redundant master clocks.
Slave ETBN	ID_3041A Inauguration data frame transmitted from the corresponding switch port is corrupted (persistent)	Not for now.	Same as in Master ETBN.

COMPONENT NETWORK	ID FAILURE MODE	FURTHER MITIGATION MEASURE	NEW REVISION for T3.5
Slave ETBN	ID_3043A TSN ETB data frame transmitted from the corresponding switch port is corrupted (persistent)	It could be analysed which mitigation measure could be applied for the non-safety but critical data to detect the wrong message and discard it, so the frame of the other plane would be processed correctly.	Same as in Master ETBN.
Slave ETBN	ID_3043B TSN ETB data frame transmitted from the corresponding switch port is corrupted (sporadic)	It could be analysed which mitigation measure could be applied for the non-safety but critical data to detect the wrong message and discard it, so the frame of the other plane would be processed correctly.	Same as in Master ETBN.
Slave ETBN	ID_3056A A inauguration data frame egresses from the switch port in a wrong order. (persistent)	Not for now.	Same as in Master ETBN.
Slave ETBN	ID_3058A TSN ETB data frame egresses from the switch port in a wrong order.(persistent)	It could be analysed which mitigation measure could be applied for the non-safety but critical data to detect the wrong message and discard it, so the frame of the other plane would be processed correctly.	Same as in Master ETBN.
Slave ETBN	ID_3061A A inauguration data frame is sent replicated from the switch port. (persistent)	Not for now.	Same as in Master ETBN.
Slave ETBN	ID_3063A TSN ETB data frame is sent replicated from the switch port. (persistent)	It could be analysed which mitigation measure could be applied for the non-safety but critical data to detect the wrong message and discard it, so the frame of the other plane would be processed correctly.	Same as in Master ETBN.
Slave ETBN	ID_3063B TSN ETB data frame is sent replicated from the switch port. (persistent)	It could be analysed which mitigation measure could be applied for the non-safety but critical data to detect the wrong message and discard it, so the frame of the other plane would be processed correctly.	Same as in Master ETBN.
Master Repeater	ID_3073 Transient loss of TSN sync frames through the corresponding line.	In case this failure mode occurs, the network would go to asynchronous mode and in order not to loss critical data, a degraded mode could be defined. In this degraded mode, the rest of the traffic is cut passing only the critical data (S4R proposal). This or another possible mitigation shall be analysed in D3.5	Same as in Master ETBN.
Master Repeater	ID_3074A Inauguration data frame transmitted from the corresponding repeater port is	Not for now.	Same as in Master ETBN.

COMPONENT NETWORK	ID FAILURE MODE	FURTHER MITIGATION MEASURE	NEW REVISION for T3.5
	corrupted (persistent)		
Master Repeater	ID_3076A TSN ETB data frame transmitted from the corresponding repeater port is corrupted (persistent)	It could be analysed which mitigation measure could be applied for the non-safety but critical data to detect the wrong message and discard it, so the frame of the other plane would be processed correctly.	Same as in Master ETBN.
Master Repeater	ID_3076B TSN ETB data frame transmitted from the corresponding repeater port is corrupted (sporadic)	It could be analysed which mitigation measure could be applied for the non-safety but critical data to detect the wrong message and discard it, so the frame of the other plane would be processed correctly.	Same as in Master ETBN.
Master Repeater	ID_3077A TSN sync frame transmitted from the corresponding repeater port is corrupted (permanent)	In case this failure mode occurs, the network would go to asynchronous mode and in order not to loss critical data, a degraded mode could be defined. In this degraded mode, the rest of the traffic is cut passing only the critical data (S4R proposal). This or another possible mitigation shall be analysed in D3.5	Same as in Master ETBN.
Master Repeater	ID_3082 TSN sync frames transmitted from the corresponding repeater port with an unacceptable delay	In case this failure mode occurs, the network would go to asynchronous mode and in order not to loss critical data, a degraded mode could be defined. In this degraded mode, the rest of the traffic is cut passing only the critical data (S4R proposal). This or another possible mitigation shall be analysed in D3.5	Same as in Master ETBN.
Master Repeater	ID_3087A A TSN sync frame is transmitted from the wrong port of the repeater. (persistent)	In case this failure mode occurs, the network would go to asynchronous mode and in order not to loss critical data, a degraded mode could be defined. In this degraded mode, the rest of the traffic is cut passing only the critical data (S4R proposal). This or another possible mitigation shall be analysed in D3.5	Same as in Master ETBN.
Master Repeater	ID_3089A A inauguration data frame egresses from the repeater port in a wrong order. (persistent)	Not for now.	Same as in Master ETBN.
Master Repeater	ID_3091A A TSN ETB data frame egresses from the repeater port in a wrong order. (persistent)	It could be analysed which mitigation measure could be applied for the non-safety but critical data to detect the wrong message and discard it, so the frame of the other plane would be processed correctly.	Same as in Master ETBN.

COMPONENT NETWORK	ID FAILURE MODE	FURTHER MITIGATION MEASURE	NEW REVISION for T3.5
Master Repeater	ID_3092A A TSN sync frame egresses from the repeater port in a wrong order. (persistent)	In case this failure mode occurs, the network would go to asynchronous mode and in order not to loss critical data, a degraded mode could be defined. In this degraded mode, the rest of the traffic is cut passing only the critical data (S4R proposal). This or another possible mitigation shall be analysed in D3.5	Same as in Master ETBN.
Master Repeater	ID_3094A A inauguration data frame is sent replicated from the repeater port. (persistent)	Not for now.	Same as in Master ETBN.
Master Repeater	ID_3096A A TSN ETB data frame is sent replicated from the repeater port. (persistent)	It could be analysed which mitigation measure could be applied for the non-safety but critical data to detect the wrong message and discard it, so the frame of the other plane would be processed correctly.	Same as in Master ETBN.
Master Repeater	ID_3096B A TSN ETB data frame is sent replicated from the repeater port. (sporadic)	It could be analysed which mitigation measure could be applied for the non-safety but critical data to detect the wrong message and discard it, so the frame of the other plane would be processed correctly.	Same as in Master ETBN.
Master Repeater	ID_3097A A TSN sync frame is sent replicated from the repeater port. (persistent)	In case this failure mode occurs, the network would go to asynchronous mode and in order not to loss critical data, a degraded mode could be defined. In this degraded mode, the rest of the traffic is cut passing only the critical data (S4R proposal). This or another possible mitigation shall be analysed in D3.5	Same as in Master ETBN.
Slave Repeater	ID_3106A Inauguration data frame transmitted from the corresponding repeater port is corrupted (persistent)	Not for now.	Same as in Master ETBN.
Slave Repeater	ID_3108A TSN ETB data frame transmitted from the corresponding repeater port is corrupted (persistent)	It could be analysed which mitigation measure could be applied for the non-safety but critical data to detect the wrong message and discard it, so the frame of the other plane would be processed correctly.	Same as in Master ETBN.
Slave Repeater	ID_3108B TSN ETB data frame transmitted from the corresponding repeater port is corrupted (sporadic)	It could be analysed which mitigation measure could be applied for the non-safety but critical data to detect the wrong message and discard it, so the frame of the other plane would be processed correctly.	Same as in Master ETBN.
Slave Repeater	ID_3121A A inauguration data frame egresses from the repeater	Not for now.	Same as in Master ETBN.

COMPONENT NETWORK	ID FAILURE MODE	FURTHER MITIGATION MEASURE	NEW REVISION for T3.5
	port in a wrong order. (persistent)		
Slave Repeater	ID_3123A A TSN ETB data frame egresses from the repeater port in a wrong order. (persistent)	It could be analysed which mitigation measure could be applied for the non-safety but critical data to detect the wrong message and discard it, so the frame of the other plane would be processed correctly.	Same as in Master ETBN.
Slave Repeater	ID_3126A A inauguration data frame is sent replicated from the repeater port. (persistent)	Not for now.	Same as in Master ETBN.
Slave Repeater	ID_3128A A TSN ETB data frame is sent replicated from the repeater port. (persistent)	It could be analysed which mitigation measure could be applied for the non-safety but critical data to detect the wrong message and discard it, so the frame of the other plane would be processed correctly.	Same as in Master ETBN.
Slave Repeater	ID_3128B A TSN ETB data frame is sent replicated from the repeater port. (sporadic)	It could be analysed which mitigation measure could be applied for the non-safety but critical data to detect the wrong message and discard it, so the frame of the other plane would be processed correctly.	Same as in Master ETBN.
Line Master	ID_3132 Data corrupted/erroneous output	Not for now.	Worst case, for inauguration persistent error. In this case is it possible to discard it? As the error is not in the node but in the cable.
Line Slave	ID_3135 Data corrupted/erroneous output	Not for now.	Worst case, for inauguration persistent error. In this case is it possible to discard it? As the error is not in the node but in the cable.

REFERENCES

- [01] Shift2Rail Grant Agreement; Number 730539; 2016
- [02] CONNECTA D1.5 – High Level requirements; CTA-T1.5-D-SNF-004
- [03] CONNECTA D3.1 – Requirement Specification; CTA-T3.1-D-ANS-023
- [04] CONNECTA D3.2 – Technology Evaluation Report; CTA-T3.2-D-BTD-003
- [05] CONNECTA D3.3 – Report on RAMS and Security Analysis; CTA-T3.3-D-CAF-006
- [06] CONNECTA D3.4 – Report on Safety Approval Concept; CTA-T3.4-D-SIE-003
- [07] CONNECTA D4.4 – Report on technology evaluation for application distribution
- [08] Roll2Rail D2.4 – RAMS and Security Analysis Report; R2R-T2.4-D-CAF-012-14
- [09] Roll2Rail D2.5 – Architecture for the Train and Consist Wireless Network; R2R-T2.5-D-BTD-003
- [10] Safe4Rail D1.6 – Network Design Methodology and (Re)-Configuration; 2018-04.
- [11] EN 50155 – Railway applications - Rolling stock – Electronic equipment; 2017
- [12] EN 50121-3-2 – Railway applications – Electromagnetic compatibility – Part 3-2: Rolling stock – Apparatus; 2016
- [13] EN 50126-1 – Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 1: Generic RAMS Process; 2017
- [14] FprEN 50126-2 – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 2: Systems Approach to Safety; 2017
- [15] EN 60706-5 – Maintainability of equipment – Part 5: Testability and diagnostic testing (IEC 60706-5); 2007
- [16] EN 50553 – Requirements for running capability in case of fire on board of rolling stock; 2016
- [17] IEC/EN 61375-1 – Train Communication Network – General Architecture; 2011
- [18] IEC/EN 61375-2-3 – Train Communication Network – Communication Profile; 2015
- [19] IEC/EN 61375-2-5 – Train Communication Network – Ethernet Train Backbone; 2014
- [20] IEC/EN 61375-3-4 – Train Communication Network – Ethernet Consist Network; 2014
- [21] IEC 61784-3-3 : 2016 Industrial communication networks – Profiles – Part 3-3: Functional safety fieldbuses – Additional specifications for CPF 3
- [22] IEC 62442-3-2 – Security Risk Assessment, System Partitioning and Security Levels; Draft7 2017
- [23] IEEE P802.1Q-REV/D1.3 – Bridges and Bridged Networks
- [24] IEEE P802.1Qci/D2.1 – Per-Stream Filtering and Policing
- [25] IEEE P802.1Qch/D2.2 – Cyclic Queuing and Forwarding
- [26] IEEE P802.1Qcr/D0.5 – Asynchronous Traffic Shaping
- [27] IEEE P802.1AS-Rev/D4.5 – Timing and Synchronization for Time-Sensitive Applications
- [28] IEEE P802.1CB/D2.8 – Frame Replication and Elimination for Reliability
- [29] IEEE 802.3-2012, IEEE Standard for Ethernet
- [30] IEEE 802.1D – Media Access Control Bridges; 2004
- [31] IEEE 802.AX – Link Aggregation; 2008

- [32] UIC Code 556 – Information transmission in the train (train bus); 5th Edition 2009
- [33] UIC Code 558 – Remote Control and Data Cable, 1st Edition 1996
- [34] Measurement of Switching Latency in High Data Rate Ethernet Networks; ELEKTRONIKA IR ELEKTROTECHNIKA, ISSN 1392-1215, VOL. 21, NO. 3, 2015
- [35] TRDP over TSN; SAFE4RAIL Report ICT-730830
- [36] <http://www.meo/etc.upt.ro/materii/cursuri/ISMT/3.pdf>
- [37] <http://www.fujitsu.com/downloads/TEL/fnc/pdfservices/ethernet-prerequisite.pdf>
- [38] <https://www.ccontrols.com/pdf/ExtV1N3.pdf>
- [39] <http://intronetworks.cs.luc.edu/current/ComputerNetworks.pdf>
- [40] <https://www.hpe.com/de/de/networking.html>
- [41] <https://www.lifewire.com/internet-network-key-concepts-4102693>
- [42] <https://tools.ietf.org/html/rfc3748>
- [43] http://h22208.www2.hpe.com/eginfolib/networking/docs/switches/5130ei/5200-3946_security_cg/content/485048058.html
- [44] http://h22208.www2.hpe.com/eginfolib/networking/docs/switches/5130ei/5200-3946_security_cg/content/485048059.html
- [45] http://h22208.www2.hpe.com/eginfolib/networking/docs/switches/5130ei/5200-3946_security_cg/content/485048060.html
- [46] https://www.cisco.com/c/en/us/td/docs/routers/crs/software/crs_r4-2/system_management/configuration/guide/b_sysman_cg42crs/b_sysman_cg42crs_chapter_01100.pdf
- [47] <https://tools.ietf.org/html/rfc2284>
- [48] ATO over ETCS Operational Requirements; EUG Reference: 13E137; 2016
- [49] http://www.wikiwand.com/en/10_Gigabit_Ethernet
- [50] <http://www.fiberopticshare.com/10gb-ethernet-copper-optical-fiber.html>
- [51] “10 Things to Know Before Deploying 10 Gigabit Ethernet” “Netgear Whitepaper : <http://www.hptctoday.com/best-practices/10-things-to-know-before-deploying-10-gigabit-ethernet/>
- [52] An Introduction to Computer Networks; Release 1.9.10, February 19, 2018; Peter L Dordal
- [53] https://en.wikipedia.org/wiki/Simple_Network_Management_Protocol
- [54] SIMATIC NET – Network management; Diagnostics and configuration with SNMP; Diagnostic Manual, 09/2017, C79000-G8976-C357-02
- [55] <https://www.pcb.its.dot.gov/standardstraining/mod19/sup/m19sup.html>
- [56] http://telescript.denayer.wenk.be/~hcr/cn/idoceo/udp_snmp.html
- [57] Koopmann P. (2002), “32-Bit Cyclic Redundancy Codes for Internet Applications”, DSN '02 Proceedings of the 2002 International Conference on Dependable Systems and Networks Pages 459-472
- [58] www.hirschmann.com © 2014, Belden Inc. Media redundancy concepts | WP1003HE_INIT_HIR_1014_E_EMEA
- [59] Hubert Kirrmann – Fault tolerant computing in industrial automation (http://lamspeople.epfl.ch/kirrmann/Pubs/FT_Tutorial_HK_050418.pdf)

- [60] https://www.cisco.com/c/en/us/td/docs/switches/connectedgrid/cg-switch-sw-master/software/configuration/guide/mrp/b_mrp_ie.html
- [61] www.hirschmann.com WP00027 TSN – Time Sensitive Networking