Contract No. H2020 – 826098

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

D1.1 – Specification of evolved Wireless TCMS

Due date of deliverable: 31/12/2019

Actual submission date: 14/04/2020

Leader/Responsible of this Deliverable: Igor Lopez (CAF)

Reviewed: Y

Project funded from the European Union's Horizon 2020 research and innovation programme		
Dissemination Level		
PU	Public	X
CO	Confidential, restricted under conditions set out in Model Grant Agreement	

Start date: 01/10/2018

Duration: 30 months

Document status		
Revision	Date	Description
01	27/11/2018	First issue. Executive summary, Introduction and General architecture
02	27/06/2019	Contributions of sections 3.1, 3.2, 4.2, 5.2, 5.3, 6.1, 6.2, 6.3, 8
03	03/09/2019	Section 4.1 added. Updated sections 5, 6 and 8
04	22/11/2019	Doc template: corrected footer Abbreviations and Acronyms list: updated Section 3.2: corrected internal references according to CTA2-T1.1-I-BTD-008-04 Sections 6: updated accoding to CTA2-T1.1-I-BTD-030-09, added new references, corrected internal references
05	05/12/2019	Section 4.2.3: content added
06	06/12/2019	Updated according to CTA2-T1.1-R-SNF-061-01
07	08/12/2019	Section 5.2 and 5.3 added.
08	17/12/2019	Reviews to new contributions applied
09	20/12/2019	Whole Document review from CTA2 T1.1 members and Safe4RAIL-2 members
10	14/04/2020	Official Review Requests applied

Disclaimer
The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The content of this document reflects only the author`s view – the Joint Undertaking is not responsible for any use that may be made of the information it contains. The users use the information at their sole risk and liability.

ACKNOWLEDGEMENTS

This project has received funding from the Shift2Rail JU under the European Union’s Horizon 2020 research and innovation programme. Grant Agreement no. 826098.

REPORT CONTRIBUTORS

Name	Company	Details of Contribution
Igor Lopez	CAF	Excutive summary. section 1, section 2, section 3.1, section 4.1, section 5, section 8, document review
Imanol de Arriba	CAF	Section 3.1
Uwe Fuhr	BTG	Section 3.2, section 4.2, section 6, document review
Marvin Straub	BTG	Section 3.2, section 4.2, section 6, document review
Nerea Elorza	CAF	Section 8
Armin Heindel	SIE	Document review
Carolin Geitner	SIE	Section 3.3, section 4.3, section 7
Keno Buss	SIE	Section 3.3, section 4.3, section 7
Krishna Pandit	SIE	Annex B
Rainer Mattes	SIE	Section 9
Philippe Laporte	SNCF-M	Document review
François Charreyre	ALSTOM	Abbreviation and Acronyms, document review

EXECUTIVE SUMMARY

This deliverable provides the architecture and interface definition for the wireless networks within the Next Generation Train Control Network (NG-TCN). The advantages pursued with the inclusion of wireless technologies are twofold. On the one hand, the use of wireless communications aims to reduce costs. On the other hand, the adoption of wireless communications allows to introduce new railway functions such as the virtually coupled train operation.

The Wireless TCMS specification is divided in three main blocks; the Wireless Train Backbone (WLTB), the Wireless Consist Network (WLCN) and the alignment of train-to-ground (T2G) communciations defined in IEC 61375-2-6 with the Adaptable Communication System (ACS) defined in Shift2Rail TD2.1 [26]. The specification of these three blocks are derived from the Use Case collection summarized in CONNECTA D1.2 [01] and the High Level requirements listed in CONNECTA D1.5 [08]. While the WLTB and WLCN blocks will be carried out together with S2R OC Safe4RAIL-2 project, the third block will be specified in close relation to S2R CFM X2Rail-1 project.

In summary, the main achievements of this work are:

- Definition of the wireless network architecture for the WLTBN, following similar approaches in terms of diverse communication planes of the Next Generation Train Control Network (NG-TCN) architecture defined by CONNECTA D3.5 [06].
- Definition of the wireless train inauguration for the WLTBN in line with the new Safe Train Inauguration defined by CONNECTA D3.5 [06].
- Definition of the wireless network architecture for the WLCN.
- Safety analysis of the Wireless Train Inauguration in order to determine the achievable SIL level with the state-of-the-art market technology and to point out the evolution needed in order to achieve a SIL4 inauguration.
- Definition of adaptation to be made for the SDTv4 protocol defined by CONNECTA D3.5 [06] in order to be valid for wireless communications according to the EN 50159.
- Specification of the interface to be included in the IEC 61375-2-6 in order to allow the TCMS MCG to use the ACS.

The achievements of CONNECTA-2 T1.1 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.

ABBREVIATIONS AND ACRONYMS

3GGP	Third Generation Partnership Project
6LoWPAN	IPv6 over Low power Wireless Personal Area Network
ACS	Adaptable Communication System
AETBN	Adapted Ethernet Train Backbone Node
AETBN-RD	Adapted Ethernet Train Backbone Node Radio Device
AODV	Ad hoc On-Demand Distance Vector
ARP	Address Resolution Protocol
ARQ	Automatic Repeat reQuest
B.A.T.M.A.N.	Better Approach to Mobile Adhoc Networking
BER	Bit Error Rate
BPSK	Binary Phase-shift Keying
BSS	Basic Service Set
CAN	Controller Area Network
C2C	Consist-to-Consist
CCTV	Closed Circuit Television
CCU	Core Control Unit
CN	Consist Network
COS	Customer Oriented Service
COTS	Commerecial Of The Shelf
CRC	Cyclic redundancy Check
CS	Consist Switch
CSTINFO	Consist Information
CTA	Connecta
D2D	Device to Device
DC	Diagnostic Coverage

DHCP	Dynamic Host Configuration Protocol
DIR	Direction
DFS	Dynamic Frequency Selection
DL	Down Link
DNS	Domain Name System
DoS	Denial-of-service attack
DSSS	Direct-Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
EchoRing	Product name of a Reliable Realtime Radio Communication
ECN	Ethernet Consist Network
ECR	Ethernet Consist Ring
ECSC	ETB Control Service Client
ECSP	ETB Control Service Provider
ED	End Device
ED-S	End Device Safety
EMC	Electro-Magnetic Compatibility
eNodeB	evolved Node B (LTE base station)
ERP	Effective Radiated Power
ETB	Ethernet Train Backbone
ETBN	Ethernet Train Backbone Node
EUTRAN	Evolved Universal mobile telecommunications system Terrestrial Radio Access Network
FHSS	Frequency Hopping Spread Spectrum
FR	Foundational Requirement
GbE	Gigabit Ethernet
GNSS	Global Navigation Satellite System
GPS	Global Positioning System

GPRS	General Packet Radio Service
GSM-R	Global System for Mobile communication – Railways
HART	Highway Addressable Remote Transducer
HR-DSSS	High Rate Direct Sequence Spread Spectrum
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
HVAC	Heating Ventilation and Air-Conditioning
ICMP	Internet Control Message Protocol
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
IP	Internet Protocol (version 4)
IPv6	Internet Protocol (version 6)
ISM	Industrial, Scientific and Medical
IT	Information Technology
ITS	Intelligent Transport System
L2	Layer 2
LAN	Local Area Network
LLC	Logical Link Control
LLDP	Link Layer Discovery Protocol
LTE	Long Term Evolution
NG-TCN	Next Generation Train Communication Network
MAC	Media Access Control
MC	Multicast
MESH	Mesh networking synonym
MIB	Management Information Base

MIB2	Management Information Base version 2
MIMO	Multiple Input Multiple Output
MTBF	Mean Time Before Failure
N	RF Connector type N
NAS	Non-Access Stratum
ND	Network Device
NG-TCN	Next Generation Train Control Network
OFDM	Orthogonal Frequency Division Multiplexing
OFDMA	Orthogonal Frequency Division Multiple Access
OGM	Originator Message
OMTS	On-board Multimedia and Telematics
OLSR	Optimized Link State Routing Protocol
OOS	Operator Oriented Service
OPC-UA	Open Platform Communication-Unified Architecture
OS	Operating System
OSI	Open Systems Interconnection
OTA	Over The Air
PANA	Protocol for Carrying Authentication for Network Access
PC	Personal Computer
PD	Powered Device (PoE)
PDCP	Packet Data Convergence Protocol
PDU	Protocol Data Unit
PHY	Physical
PLC	Programmable Logic Controller
PoE	Power over Ethernet
PROFIBUS	Process Field Bus

PROFINET	Process Field Network
ProSe	Proximity Services
PSS	Product and Solution Security
QCI	QoS Class Identifier
QLF	RF Connector type QLF
QMA	RF Connector type QMA
QN	RF Connector type QN
QoS	Quality of Service
QPSK	Quadrature Phase-shift Keying
R2R	Roll2Rail
RADIUS	Remote Authentication Dial-In User Service
RAMS	Reliability – Availability – Maintainability – Safety
RD	Radio Device
RF	Radio Frequency
RFC	Request For Comments
RFID	Radio Frequency IDentification
RLC	Radio Link Control
R-NAT	Railway-Network Address Translation
RP-SMA	Reverse Polarity SMA connector
RPL	Routing Protocol for Low Power and Lossy Network
RRC	Radio Resource Control
S2R	Shift To Rail
S4R	Shift For Rail
SC-FDMA	Single Carrier Frequency Division Multiple Access
SDTv4	Safe Data Transmission version 4
SHARP	Synchronous and Hybrid Architecture for Real-Time Performance

SIL	Safety Integrity Level
SMA	Sub Miniature RF connector type A
SNR	Signal Noise Ratio
SNMP	Simple Network Management Protocol
SSID	Service Set Identifier
SSH	Secure SHell
TBN	Train Backbone Node
TCMS	Train Control Monitoring System
TCN	Train Communication Network
TCN-URI	Train Communication Network Uniform Resource Identifier
TCP	Transmission Control Protocol
TDMA	Time Division Multiple Access
TFFR	Tolerable Functional Failure Rate
TI	Train Inauguration
TLS	Transport Layer Security
TS	Technical Specification for (LTE/3GPP, 3gpp.org), format: TS xx.yyy
TND	Train Network Directory
TOPO	Topology
TRA	Threat and Risk Analysis
TRDP	Tra0069n Real Time Data Protocol
TRDP-MD	Train Real Time Data Protocol Message Data
TRDP-PD	Train Real Time Data Protocol Process Data
TSN	Time Sensitive Networking
TTDB	Train Topology Database
TTDP	Train Topology Discovery Protocol
UDP	User Datagram Protocol

UIC	Union internationale des chemins de fer
UE	User Equipment (LTE end device)
UL	Up Link
URLLC	Ultra-Reliable and Low Latency Communications
UWB	Ultra Wide Band
V2V	Vehicle to Vehicle
V2X	Vehicle to Everything
VID	VLAN Identifier
VLAN	Virtual Local Area Network
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network
WAP	Wireless Access Point
WCN	Wireless Consist Network
WED	Wireless End Device
WED-S	Safe Wireless End Device
Wi-Fi	Wireless Fidelity (Radio technology for wireless local area networks)
WIDS	Wireless Intrusion Detection System
WIPS	Wireless Intrusion Prevention System
WISA	Wireless Interface to Sensors and Actuators
WLAN	Wireless Local Area Network
WLCN	Wireless Consist Network
WLTB	Wireless Train Backbone
WLTBN	Wireless Train Backbone Node
WMN	Wireless MESH Network
WP	Workpackage
WSAN	Wireless Sensor and Actor

WTCMS	Wireless Train Control Monitoring System
WWW	World Wide Web

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

The CONNECTA-2 project brings clear contributions to the Shift2Rail general KPIs by increasing the capacity, increasing the reliability of the operation and the reduction of the LCC. This project is a continuation of CONNECTA project and covers the second phase of the TD1.2 as illustrated in Figure 1.

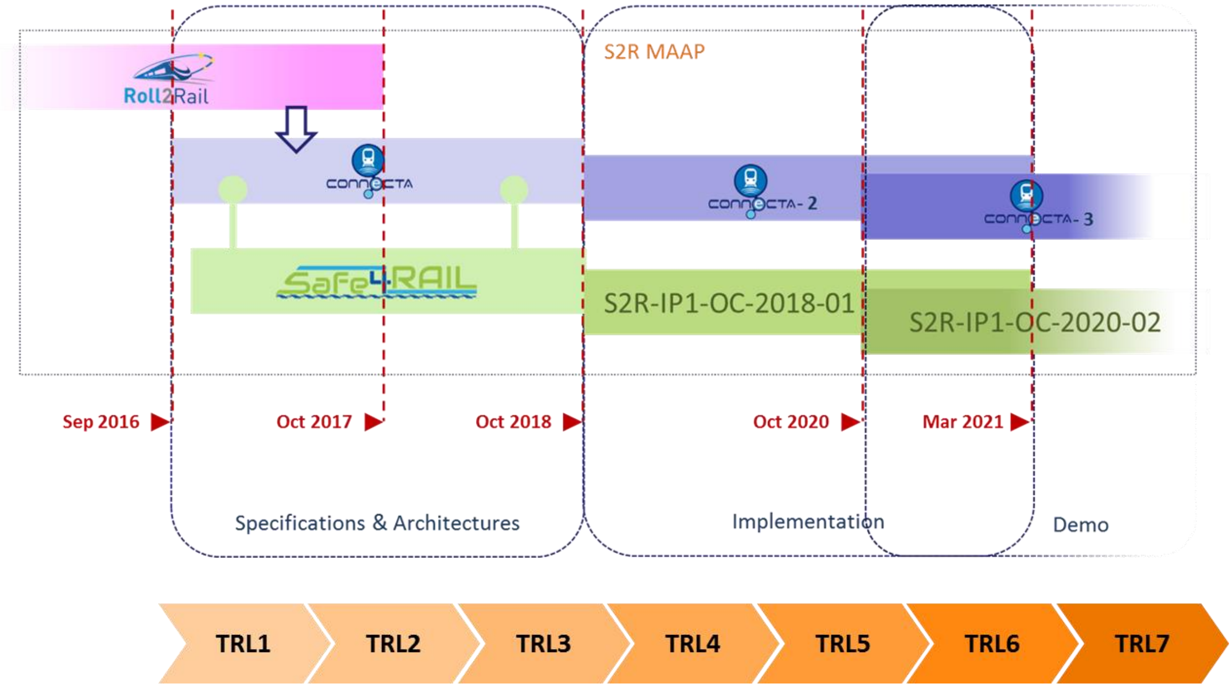


Figure 1: Positioning of the project

CONNECTA-2 project is structured in six technical work packages (WP). WP1 provides the specification and updated requirements definition for wireless TCMS, application profiles, Functional Distribution Framework and standardized DMI. WP2 contributes by deploying new train-to-ground services according to the IEC 61375-2-6, as well as deploying application profiles specified in CONNECTA and in WP1 of CONNECTA2. WP3 provides the technical specification and implementation of components for urban and regional lab demonstrators. WP4 continues the work of WP3 by defining the tests for both demonstrators. WP5 and WP6 implement and execute the tests defined by WP4 in urban and regional demonstrators respectively.

The main goals of this deliverable is to define the use cases and requirements for wireless TCMS, including the WLTB, the WLCN and the integration of the IEC 61375-2-6 MCG with the ACS defined by TD2.1. From this use cases and requirements, specified in sections 3 and 4 of this document, the detailed architectures and interface specifications are provided in sections 5, 6 and 7. Additionally, section 8 provides a new Wireless Train Inauguration to be applied over the WLTB. Last but not least, the adaptation to be made to the SDTv4 protocol to be used over wireless networks is presented in section 9.

The work for the definition of the Wireless TCMS does not start from scratch, by contrary, the work made by Roll2Rail and CONNECTA projects represent essential inputs to carry out this work.

Equally, the work covered by this deliverable will be aligned with other TDs and IPs as illustrated in Figure 2, mainly in the part of virtual coupling, cybersecurity, adaptable communications from IP2.

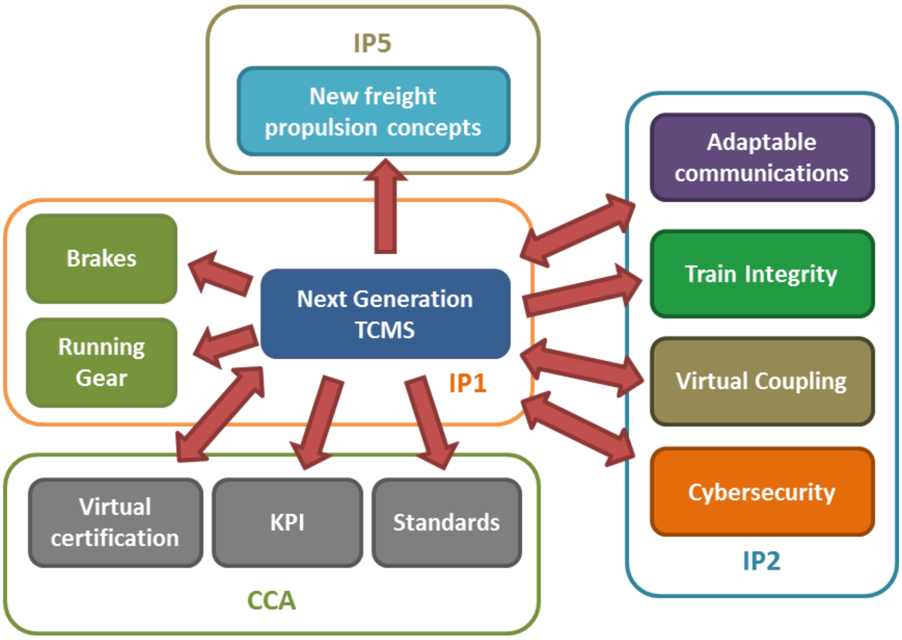


Figure 2: Interaction with other TDs and IPs

The specifications explained in this deliverable will be implemented in T2.1 (the new MCG-ACS interface), in T3.2 (the WLTB including the wireless inauguration) and in T3.4 (the WLCN) and validated in laboratory demonstrators.

2. GENERAL ARCHITECTURE OF THE WIRELESS TCMS

The WTCMS is designed to complement wired NG-TCN network in order to reduce cabling costs and ease the insertion of the WTCMS in existing fleet where the installation of new wiring is difficult or even impossible.

The WTCMS consists of two new wireless networks included in the NG-TCN; the WLTB, which work at train level; and the WLCN, which connects wireless end devices to the consist network. Figure 3 depicts the general architecture of the Wireless TCMS, which besides the WLTB and the WLCN, it also covers the integration of the MCG described in the IEC 61375-2-6 with the Adaptable Communication System deployed by S2R TD2.1.

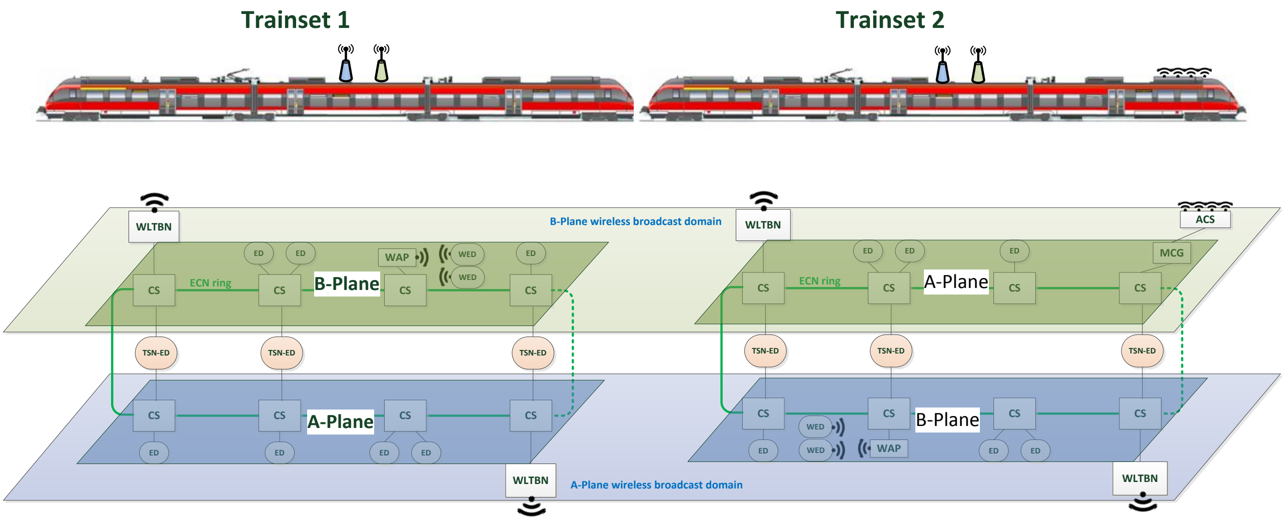


Figure 3: General architecture of the Wireless TCMS

This document takes the general architecture of the WTCMS and based of the general TCMS Use Cases, it defined a specific set of use cases for WTCMS in section 3. Linked to these use Cases, detailed requirements for the WTCMS are presented in section 4. Sections 5, 6 and 0 introduce a new specification of the WTCMS which covers the Use Cases and requirements previously mentioned.

3. USE CASES FOR WIRELESS TCMS

3.1 USE CASES FOR WIRELESS TRAIN BACKBONE

3.1.1 General

Based on the definition of user stories [01], use cases [01], and the functional based architecture **¡Error! No se encuentra el origen de la referencia.** defined in CONNECTA project, this section copes with the definition of use cases related to wireless technology (inter-consist). Wireless technology shall be used to consist-to-consist communication.

The main goal of this section is to define a specific set of requirements for WLTB that cover all possible generic Use Cases [01] where inter-consist wireless communications may be used.

While defining the use cases for the Wireless Train Backbone the following considerations have been taken into account:

- Wireless Train Backbone technology is intended to be used for inter-consist communication.
- Wireless Train Backbone technology is integrated into the TCMS network infrastructure (means: using the same consist-level wired infrastructure as TCMS devices), without influencing the TCMS data communication.
- Wireless Train Backbone Node is connected to the consist network via Ethernet.
- Wireless Train Backbone Nodes communicate with peer devices to interconnect different consist networks.
- Wireless Train Backbone uses the same wired NG-TCN network architecture and plane differentiation, being transparent for the end-devices.

From the list of use cases defined during CONNECTA project [01] & [03] it can be deduced that from the inter-consist wireless communication point of view, these use cases can be grouped in four main use cases with different requirements. These use case grouping comes from the type of function for which the data transmission will be carried out; therefore they fit with the function domain distributions, i.e. TCMS non-safety traffic, TCMS safety traffic, OOS traffic and the special case of train inauguration traffic. Table 1 summarizes these WLTB use cases.

Table 1: WLTB Use Cases

ID	Use Case	Actor / Actors
CTA2_D1.1_UC_1	TCMS safety	• passenger • train staff • maintenance staff • TCMS sensor • TCMS computing unit • rail vehicle manufacturer

CTA2_D1.1_UC_2	TCMS non-safety	• passenger • train staff • maintenance staff • TCMS sensor • TCMS computing unit • rail vehicle manufacturer
CTA2_D1.1_UC_3	OOS	• passenger • train staff
CTA2_D1.1_UC_4	Safe train inauguration	• TCMS computing unit • train staff

The use cases will be used to derive requirements for a wireless train backbone (WLTB) (section 4.1).

The use cases will be also used to specify a wireless train backbone (WLTB) (section 5.1).

3.1.2 Traceability of General Use Cases with WLTB Use Cases

As previously commented the set of use cases defined during CONNECTA project [01] can be linked with the WLTB Use Cases from the inter-consist wireless communication perspective. Table 2 provides the traceability of those general use cases defined in CONNECTA project and the four WLTB use cases defined in this document.

Table 2: Traceability of General Use Cases with WLTB Use Cases

WLTB Use Case ID	Use Case	General Use Case ID
CTA2_D1.1_UC_1	TCMS safety	CTA-D1.2-UC-6, CTA-D1.2-UC-14, CTA-D1.2-UC-20, CTA-D1.2-UC-21, CTA-D1.2-UC-22, CTA-D1.2-UC-24, CTA-D1.2-UC-27, CTA-D1.2-UC-28, CTA-D1.2-UC-29, CTA-D1.2-UC-31, CTA-D1.2-UC-39, CTA-D1.2-UC-90, CTA-D1.2-UC-91, CTA-D1.2-UC-92, CTA-D1.2-UC-93, CTA-D1.2-UC-94, CTA-D1.2-UC-96, CTA-D1.2-UC-97, CTA-D1.2-UC-98, CTA-D1.2-UC-99, CTA-D1.2-UC-100, CTA-D1.2-UC-101, CTA-D1.2-UC-102, CTA-D1.2-UC-103, CTA-D1.2-UC-104, CTA-D1.2-UC-105, CTA-D1.2-UC-106, CTA-D1.2-UC-107, CTA-D1.2-UC-108, CTA-D1.2-UC-109, CTA-D1.2-UC-110, CTA-D1.2-UC-111, CTA-D1.2-UC-112, CTA-D1.2-UC-113, CTA-D1.2-UC-114, CTA-D1.2-UC-115, CTA-D1.2-UC-116, CTA-D1.2-UC-117, CTA-D1.2-UC-118, CTA-D1.2-UC-119, CTA-D1.2-UC-120, CTA-D1.2-UC-122, CTA-D1.2-UC-123, CTA-D1.2-UC-132, CTA-D1.2-UC-133, CTA-D1.2-UC-134, CTA-D1.2-UC-135, CTA-D1.2-UC-136, CTA-D1.2-UC-143, CTA-D1.2-UC-144, CTA-D1.2-UC-145, CTA-D1.2-UC-146, CTA-D1.2-UC-186, CTA-D1.2-UC-187, CTA-D1.2-UC-188, CTA-D1.2-UC-189, CTA-D1.2-UC-190, CTA-D1.2-UC-191, CTA-D1.2-UC-192, CTA-D1.2-UC-193, CTA-D1.2-UC-194, CTA-D1.2-UC-195, CTA-D1.2-UC-196, CTA-D1.2-UC-197, CTA-D1.2-UC-198, CTA-D1.2-UC-199, CTA-D1.2-UC-200, CTA-D1.2-UC-201, CTA-D1.2-UC-202, CTA-D1.2-UC-203, CTA-D1.2-UC-204, CTA-D1.2-UC-205, CTA-D1.2-UC-206, CTA-D1.2-UC-207,

		CTA-D1.2-UC-208, CTA-D1.2-UC-209, CTA-D1.2-UC-210, CTA-D1.2-UC-211, CTA-D1.2-UC-212, CTA-D1.2-UC-213, CTA-D1.2-UC-231, CTA-D1.2-UC-232, CTA-D1.2-UC-233, CTA-D1.2-UC-234, CTA-D1.2-UC-235, CTA-D1.2-UC-354, CTA-D1.2-UC-355, CTA-D1.2-UC-359, CTA-D1.2-UC-363, CTA-D1.2-UC-364
CTA2_D1.1_UC_2	TCMS non-safety	CTA-D1.2-UC-1, CTA-D1.2-UC-2, CTA-D1.2-UC-3, CTA-D1.2-UC-4, CTA-D1.2-UC-5, CTA-D1.2-UC-11, CTA-D1.2-UC-12, CTA-D1.2-UC-13, CTA-D1.2-UC-18, CTA-D1.2-UC-19, CTA-D1.2-UC-23, CTA-D1.2-UC-25, CTA-D1.2-UC-26, CTA-D1.2-UC-32, CTA-D1.2-UC-33, CTA-D1.2-UC-34, CTA-D1.2-UC-35, CTA-D1.2-UC-36, CTA-D1.2-UC-37, CTA-D1.2-UC-38, CTA-D1.2-UC-40, CTA-D1.2-UC-41, CTA-D1.2-UC-42, CTA-D1.2-UC-43, CTA-D1.2-UC-44, CTA-D1.2-UC-45, CTA-D1.2-UC-46, CTA-D1.2-UC-47, CTA-D1.2-UC-54, CTA-D1.2-UC-55, CTA-D1.2-UC-56, CTA-D1.2-UC-57, CTA-D1.2-UC-58, CTA-D1.2-UC-59, CTA-D1.2-UC-60, CTA-D1.2-UC-61, CTA-D1.2-UC-62, CTA-D1.2-UC-63, CTA-D1.2-UC-64, CTA-D1.2-UC-65, CTA-D1.2-UC-66, CTA-D1.2-UC-67, CTA-D1.2-UC-68, CTA-D1.2-UC-69, CTA-D1.2-UC-70, CTA-D1.2-UC-71, CTA-D1.2-UC-72, CTA-D1.2-UC-73, CTA-D1.2-UC-74, CTA-D1.2-UC-75, CTA-D1.2-UC-76, CTA-D1.2-UC-77, CTA-D1.2-UC-78, CTA-D1.2-UC-79, CTA-D1.2-UC-80, CTA-D1.2-UC-81, CTA-D1.2-UC-82, CTA-D1.2-UC-83, CTA-D1.2-UC-84, CTA-D1.2-UC-85, CTA-D1.2-UC-86, CTA-D1.2-UC-87, CTA-D1.2-UC-88, CTA-D1.2-UC-89, CTA-D1.2-UC-124, CTA-D1.2-UC-125, CTA-D1.2-UC-126, CTA-D1.2-UC-127, CTA-D1.2-UC-128, CTA-D1.2-UC-129, CTA-D1.2-UC-130, CTA-D1.2-UC-131, CTA-D1.2-UC-137, CTA-D1.2-UC-138, CTA-D1.2-UC-139, CTA-D1.2-UC-140, CTA-D1.2-UC-141, CTA-D1.2-UC-142, CTA-D1.2-UC-147, CTA-D1.2-UC-148, CTA-D1.2-UC-149, CTA-D1.2-UC-150, CTA-D1.2-UC-151, CTA-D1.2-UC-152, CTA-D1.2-UC-153, CTA-D1.2-UC-154, CTA-D1.2-UC-155, CTA-D1.2-UC-156, CTA-D1.2-UC-157, CTA-D1.2-UC-158, CTA-D1.2-UC-159, CTA-D1.2-UC-160, CTA-D1.2-UC-161, CTA-D1.2-UC-162, CTA-D1.2-UC-163, CTA-D1.2-UC-164, CTA-D1.2-UC-165, CTA-D1.2-UC-166, CTA-D1.2-UC-167, CTA-D1.2-UC-168, CTA-D1.2-UC-169, CTA-D1.2-UC-170, CTA-D1.2-UC-171, CTA-D1.2-UC-172, CTA-D1.2-UC-173, CTA-D1.2-UC-174, CTA-D1.2-UC-175, CTA-D1.2-UC-176, CTA-D1.2-UC-178, CTA-D1.2-UC-179, CTA-D1.2-UC-180, CTA-D1.2-UC-181, CTA-D1.2-UC-182, CTA-D1.2-UC-183, CTA-D1.2-UC-184, CTA-D1.2-UC-185, CTA-D1.2-UC-214, CTA-D1.2-UC-215, CTA-D1.2-UC-216, CTA-D1.2-UC-217, CTA-D1.2-UC-218, CTA-D1.2-UC-219, CTA-D1.2-UC-220, CTA-D1.2-UC-221, CTA-D1.2-UC-222, CTA-D1.2-UC-223, CTA-D1.2-UC-224, CTA-D1.2-UC-225, CTA-D1.2-UC-226, CTA-D1.2-UC-227, CTA-D1.2-UC-228, CTA-D1.2-UC-229, CTA-D1.2-UC-230, CTA-D1.2-UC-240, CTA-D1.2-UC-241, CTA-D1.2-UC-242, CTA-D1.2-UC-243, CTA-D1.2-UC-244, CTA-D1.2-UC-245, CTA-D1.2-UC-246, CTA-D1.2-UC-247, CTA-D1.2-UC-278, CTA-D1.2-UC-279, CTA-D1.2-UC-280, CTA-D1.2-UC-281, CTA-D1.2-UC-282, CTA-D1.2-UC-283, CTA-D1.2-UC-284, CTA-D1.2-UC-318, CTA-D1.2-UC-319, CTA-D1.2-UC-320,

		CTA-D1.2-UC-321, CTA-D1.2-UC-322, CTA-D1.2-UC-323, CTA-D1.2-UC-324, CTA-D1.2-UC-325, CTA-D1.2-UC-326, CTA-D1.2-UC-327, CTA-D1.2-UC-328, CTA-D1.2-UC-329, CTA-D1.2-UC-330, CTA-D1.2-UC-331, CTA-D1.2-UC-332, CTA-D1.2-UC-333, CTA-D1.2-UC-334, CTA-D1.2-UC-335, CTA-D1.2-UC-336, CTA-D1.2-UC-337, CTA-D1.2-UC-338, CTA-D1.2-UC-339, CTA-D1.2-UC-340, CTA-D1.2-UC-341, CTA-D1.2-UC-342, CTA-D1.2-UC-343, CTA-D1.2-UC-344, CTA-D1.2-UC-345, CTA-D1.2-UC-346, CTA-D1.2-UC-347, CTA-D1.2-UC-348, CTA-D1.2-UC-349, CTA-D1.2-UC-350, CTA-D1.2-UC-352, CTA-D1.2-UC-353, CTA-D1.2-UC-360
CTA2_D1.1_UC_3	OOS	CTA-D1.2-UC-248, CTA-D1.2-UC-249, CTA-D1.2-UC-250, CTA-D1.2-UC-251, CTA-D1.2-UC-252, CTA-D1.2-UC-253, CTA-D1.2-UC-254, CTA-D1.2-UC-255, CTA-D1.2-UC-256, CTA-D1.2-UC-257, CTA-D1.2-UC-258, CTA-D1.2-UC-259, CTA-D1.2-UC-260, CTA-D1.2-UC-261, CTA-D1.2-UC-262, CTA-D1.2-UC-263, CTA-D1.2-UC-264, CTA-D1.2-UC-265, CTA-D1.2-UC-266, CTA-D1.2-UC-267, CTA-D1.2-UC-268, CTA-D1.2-UC-269, CTA-D1.2-UC-270, CTA-D1.2-UC-271, CTA-D1.2-UC-272, CTA-D1.2-UC-273, CTA-D1.2-UC-274, CTA-D1.2-UC-275, CTA-D1.2-UC-276, CTA-D1.2-UC-277, CTA-D1.2-UC-285, CTA-D1.2-UC-286, CTA-D1.2-UC-287, CTA-D1.2-UC-288, CTA-D1.2-UC-289, CTA-D1.2-UC-290, CTA-D1.2-UC-291, CTA-D1.2-UC-292, CTA-D1.2-UC-295, CTA-D1.2-UC-296, CTA-D1.2-UC-299, CTA-D1.2-UC-300, CTA-D1.2-UC-304, CTA-D1.2-UC-305, CTA-D1.2-UC-307, CTA-D1.2-UC-311, CTA-D1.2-UC-313, CTA-D1.2-UC-315, CTA-D1.2-UC-356, CTA-D1.2-UC-357
CTA2_D1.1_UC_4	Safe train inauguration	CTA-D1.2-UC-7, CTA-D1.2-UC-8, CTA-D1.2-UC-9, CTA-D1.2-UC-10, CTA-D1.2-UC-30, CTA-D1.2-UC-48, CTA-D1.2-UC-49, CTA-D1.2-UC-50, CTA-D1.2-UC-51, CTA-D1.2-UC-95, CTA-D1.2-UC-236, CTA-D1.2-UC-237, CTA-D1.2-UC-238, CTA-D1.2-UC-239, CTA-D1.2-UC-351, CTA-D1.2-UC-358

3.1.3 Selected Use Cases to be tested in the Urban Demonstrator

After evaluating the use cases list defined during CONNECTA project [01] & [03], several use cases have been selected. The selection criterion for this set of use cases is the availability of such subsystems, e.g. HVAC subsystem or CCTV, in the urban demonstrator. The main goal with this selection criterion is the reusability of demonstrator subsystems for WLTB.

Table 3 lists the collection of selected use cases. The use of function domains will help afterwards to define specific network performance requirement for each group of functions.

Table 3: Use Cases for Wireless Train Backbone

Use Case ID	Name	Epic	Short Description	Severity	Function Domain
CTA-D1.2-UC-5	Climatise the passengers areas without active cab by driver	CTA-D1.2-EP-1 Climatise vehicle	The TCMS sends information in order to climatise the passengers' area of the train when there are passengers onboard and the driver's cab is not active. Ordered by the driver.	Medium	TCMS non-safety
CTA-D1.2-UC-8	Informing driver after decoupling	CTA-D1.2-EP-3 Create vehicle arrangement	The driver is informed that the train is usable after decoupling.	High	Safe train inauguration
CTA-D1.2-UC-9	Informing driver after coupling	CTA-D1.2-EP-3 Create vehicle arrangement	The driver is informed that the train is usable after coupling.	High	Safe train inauguration
CTA-D1.2-UC-20	Automatic management of train external lights when coupling	CTA-D1.2-EP-22 Integrate vehicle in the overall system rail	The external train lights are automatically managed when coupling so that the resulting train is in a safe mode.	High	TCMS safety
CTA-D1.2-UC-21	Automatic management of train external lights when decoupling	CTA-D1.2-EP-22 Integrate vehicle in the overall system rail	The external train lights are automatically managed when coupling so that the decoupled consists are in a safe mode.	High	TCMS safety
CTA-D1.2-UC-30	Ensure the train integrity	CTA-D1.2-EP-22 Integrate vehicle in the overall system rail	The TCMS surveys the integrity of the train so that no part of it is left on the track without control.	High	Safe train inauguration
CTA-D1.2-UC-39	Alert (alarm information) the driver	CTA-D1.2-EP-8 Monitor vehicle	The driver shall be aware of information concerning the train alerts or alarms so that he can decide which action shall be taken.	High	TCMS safety
CTA-D1.2-UC-50	Coupling	CTA-D1.2-EP-10 Operate vehicle	Two trains are coupled resulting in one train, ready for operation.	Medium	Safe train inauguration
CTA-D1.2-UC-51	Decoupling	CTA-D1.2-EP-10 Operate vehicle	A train consisting of two or more operational consists is operationally separated into two trains	Medium	Safe train inauguration
CTA-D1.2-UC-95	Perform coupling drive	CTA-D1.2-EP-9 Move vehicle	The driver wants to couple the consist to a consist awaiting coupling.	High	Safe train inauguration
CTA-D1.2-UC-130	Switch off passenger air conditioning in case of fire	CTA-D1.2-EP-4 Detect emergencies	The driver wants to switch off the passenger air conditioning in order to avoid spread of smoke.	High	TCMS non-safety
CTA-D1.2-UC-133	Detect insufficient air supply	CTA-D1.2-EP-4 Detect emergencies	The transportable staff detects insufficient air supply.		TCMS safety
CTA-D1.2-UC-214	Set cab climate	CTA-D1.2-EP-1 Climatise vehicle	The driver wants to set the cab climate (temperature, humidity and oxygen level).	Medium	TCMS non-safety

CTA-D1.2-UC-216	Request change of temperature	CTA-D1.2-EP-1 Climatise vehicle	The passenger wants to Change the temperature	High	TCMS non-safety
CTA-D1.2-UC-217	Adjust climate	CTA-D1.2-EP-1 Climatise vehicle	The Transportable Staff adjusts the temperature level in a coach.	Medium	TCMS non-safety
CTA-D1.2-UC-218	Monitor climate	CTA-D1.2-EP-1 Climatise vehicle	Transportable Staff wants to monitor the temperature, oxygen level and humidity in each coach.	Medium	TCMS non-safety
CTA-D1.2-UC-236	Shorten the train	CTA-D1.2-EP-3 Create vehicle arrangement	The driver wants to remove one or more consists.	Medium	Safe train inauguration
CTA-D1.2-UC-237	Train lengthening	CTA-D1.2-EP-3 Create vehicle arrangement	The driver wants to add one or more consists to the existing train	Medium	Safe train inauguration
CTA-D1.2-UC-238	Get arrangement information	CTA-D1.2-EP-3 Create vehicle arrangement	The driver wants to obtain Arrangement Information	High	Safe train inauguration
CTA-D1.2-UC-239	Monitor Arrangement	CTA-D1.2-EP-3 Create vehicle arrangement	The driver wants to monitor the arrangement and be notified of any changes in the arrangement	High	Safe train inauguration
CTA-D1.2-UC-299	Provide view of outside camera to driver	CTA-D1.2-EP-12 Passenger services	The driver wants to view the outside cameras.	Medium	OOS
CTA-D1.2-UC-320	Collect air conditioning maintenance data	CTA-D1.2-EP-8 Monitor vehicle	The railway undertaking collects air conditioning maintenance data to plan scheduled maintenance.	Medium	TCMS non-safety
CTA-D1.2-UC-322	Collect bogie maintenance data	CTA-D1.2-EP-8 Monitor vehicle	The railway undertaking collects bogie maintenance data to plan scheduled maintenance.	Medium	TCMS non-safety
CTA-D1.2-UC-324	Collect door maintenance data	CTA-D1.2-EP-8 Monitor vehicle	The railway undertaking collects door maintenance data to plan scheduled maintenance.	Medium	TCMS non-safety
CTA-D1.2-UC-335	Monitor interior air quality	CTA-D1.2-EP-8 Monitor vehicle	The railway undertaking monitors the interior air quality.	Medium	TCMS non-safety
CTA-D1.2-UC-338	Monitor passenger air conditioning	CTA-D1.2-EP-8 Monitor vehicle	The driver monitors the passenger air conditioning.	Medium	TCMS non-safety

3.2 Use Cases for Wireless Consist Network

3.2.1 General

Based on the definition of user stories [01], use cases [01], and the functional based architecture [02] defined in the CONNECTA project, this section copes with the definition of use cases related to wireless technology (intra consist). Wireless technology shall be used to connect wireless devices with the train network.

Focus of this contribution is the selection of relevant use cases of all domains, means TCMS, OOS, and COS. This also includes use cases which have a relation to safe data communication aspects. An evaluation of safety aspects (see section 9) will precise the usage of wireless technology in a train consist network.

3.2.2 Summary of top-level use cases

After evaluating the use cases list defined during CONNECTA project [03][04], several use cases are identified, having a potential relation to wireless communication in general. The criteria for selecting a use case as relevant are:

- an end device, which can be a wireless end device (WED), is connected to the train network
- the wireless end device (WED) is supposed to be onboard the train
- the wireless end device (WED) may be used to remotely control offered services (onboard and offboard)
- the wireless end device (WED) transmits/receives data to/from a service within the network (onboard and offboard); the data is not related to remote control purposes
- a device offering wireless access (WAP) is involved in the “Epic”, (e.g. providing status or statistic information)

The following Table 4 lists selected use cases in general. The table also maps these use cases to four predefined domains used in NG-TCN (refer CONNECTA D3.3 [05] and D3.5 [06]), enabling further analysis of wireless equipment (e.g. WAP) and related requirements regarding wireless device usage in the different domains as well as correct communication isolation between these domains (e.g. VLAN or firewall).

Table 4: Use Case Extract for Wireless TCMS

Use Case ID	Epic ID / name	Name	Short Description	Severety	NG-TCN Domain			
					TCMSs	TCMS	OOS	COS
CTA-D1.2-UC-4	CTA-D1.2-EP-1 Climatise vehicle	Climatise the passengers areas without active cab by maintenance staff	The TCMS sends information in order to climatise the passengers' area of the train when there are passengers onboard and the driver's cab is not active. Ordered by maintenance staff in a depot.	Medium		x	x	
CTA-D1.2-UC-6	CTA-D1.2-EP-2 Control doors	Automatic closing of the external doors	At standstill, the external doors are automatically closed after a given time, in order to minimize the climatisation effort.	Medium	x	x	x	
CTA-D1.2-UC-11	CTA-D1.2-EP-21 Light vehicle interior	Lighting the passengers areas without active cab by maintenance staff	The TCMS sends information in order to light the passengers' area of the train when there are passengers onboard and the driver's cab is not active. Ordered by maintenance staff in a depot.	Medium		x		
CTA-D1.2-UC-15	CTA-D1.2-EP-12 Passenger services	Internet access safety	The internet access system has no impact on the train safety.	High	x	x	x	x
CTA-D1.2-UC-16	CTA-D1.2-EP-12 Passenger services	Internet access security	The internet access system has no impact on the train IT Security	High		x	x	x
CTA-D1.2-UC-19	CTA-D1.2-EP-17 Surveil passenger area	Passenger Alarm System (PAS) survey maintenance	Maintenance staff is able to test the survey of the various passenger areas in order to remotely reset the Passenger Alarm Systems	High		x	x	

Use Case ID	Epic ID / name	Name	Short Description	Severety	NG-TCN Domain			
					TCMSs	TCMS	OOS	COS
CTA-D1.2-UC-25	CTA-D1.2-EP-22 Integrate vehicle in the overall system rail	Record train actions during journey	The actions related to train driving and the interaction of the train with the overall rail system (e.g. signalling) are recorded	High	x	x	x	
CTA-D1.2-UC-26	CTA-D1.2-EP-22 Integrate vehicle in the overall system rail	Record train actions during maintenance mode	The actions corresponding to train driving and the interaction of the train with the overall rail system (e.g. signalling) while the train is in maintenance mode are NOT recorded	High	x	x	x	
CTA-D1.2-UC-37	CTA-D1.2-EP-7 Maintain vehicle	Repair information transmission	The RU collects the information needed to repair the train so that the maintenance staff are ready when the train arrives at a workshop	Medium	x	x	x	x
CTA-D1.2-UC-40	CTA-D1.2-EP-8 Monitor vehicle	Alert (alarm information) the train staff	The train staff shall be aware of information concerning the train alerts or alarms so that he can decide which action shall be taken.	Medium		x	x	
CTA-D1.2-UC-43	CTA-D1.2-EP-8 Monitor vehicle	Train systems status communication for the driver	Many devices on the train are able to communicate their status so that the train global status is accurately known by the driver	High	x	x	x	x
CTA-D1.2-UC-45	CTA-D1.2-EP-8 Monitor vehicle	Train systems status communication for train staff	Many devices on the train are able to communicate their status so that the train global status is accurately known by the maintenance staff	High	x	x	x	x
CTA-D1.2-UC-71	CTA-D1.2-EP-20 Setup vehicle condition	Obtain maintenance information	The maintenance staff obtain State and Diagnostic information about the Train by using special interfaces.	High		x	x	
CTA-D1.2-UC-72	CTA-D1.2-EP-20 Setup vehicle condition	Setup maintenance information	The maintenance staff wants to set and reset Maintenance information.	High		x	x	
CTA-D1.2-UC-82	CTA-D1.2-EP-16 Superordinated control of vehicle	Configure ECU	The maintenance staff wants to configure the inside electronic control units (only allowed for SIL-0 train-IT).	High		x	x	x
CTA-D1.2-UC-83	CTA-D1.2-EP-16 Superordinated control of vehicle	Get data log	The maintenance staff want to get log data from current and previous operation cycles.	High		x	x	
CTA-D1.2-UC-84	CTA-D1.2-EP-16 Superordinated control of vehicle	Get data about level of the operating materials	The maintenance staff wants to get data.	High		x	x	
CTA-D1.2-UC-85	CTA-D1.2-EP-16 Superordinated control of vehicle	Get operating data	The maintenance staff want to get the train operating data.	High		x	x	

Use Case ID	**Epic ID / name**	**Name**	**Short Description**	**Severety**	**NG-TCN Domain**			
					TCMSs	TCMS	OOS	COS
CTA-D1.2-UC-86	CTA-D1.2-EP-16 Superordinated control of vehicle	Perform automatic brake test	The maintenance staff wants to perform an automated breake test via the remote communication system	High	x	x	x	
CTA-D1.2-UC-87	CTA-D1.2-EP-16 Superordinated control of vehicle	Reset data log	The maintenance staff want to reset and restart the data log.	High		x	x	
CTA-D1.2-UC-88	CTA-D1.2-EP-16 Superordinated control of vehicle	Retain train diagnostic data	The maintenance staff want to get the current content of diagnostic memory.	High		x	x	
CTA-D1.2-UC-89	CTA-D1.2-EP-16 Superordinated control of vehicle	Perform automatic diagnostic check of control units	The maintenance staff want to start some automatic checks of some electronic control units to get diagnostic information.	High	x	x	x	x
CTA-D1.2-UC-106	CTA-D1.2-EP-9 Move vehicle	Deactivate brakes	The maintenance staff wants to deactivate brakes.	Medium	x	x	x	
CTA-D1.2-UC-107	CTA-D1.2-EP-9 Move vehicle	Obtain brake maintenance information	The maintenance staff wants to obtain brake maintenance information.	High	x	x	x	
CTA-D1.2-UC-108	CTA-D1.2-EP-9 Move vehicle	Receive maintenance staff notification	The maintenance staff gets informed that a brake test has to be carried out.	High	x	x	x	
CTA-D1.2-UC-129	CTA-D1.2-EP-4 Detect emergencies	Provide surveillance of passenger area to driver	The driver surveils the passenger area.			x		
CTA-D1.2-UC-131	CTA-D1.2-EP-4 Detect emergencies	Notify the transportable staff about emergency situation	The transportable staff gets the instruction to check a potential emergency situation from the driver.	High		x		
CTA-D1.2-UC-139	CTA-D1.2-EP-13 Prevent emergencies	Check interior air pressure	The driver wants to check the interior air pressure.	High		x		
CTA-D1.2-UC-141	CTA-D1.2-EP-13 Prevent emergencies	Monitor interior train temperature	The transportable staff wants to monitor the interior train temperature.	High		x	x	
CTA-D1.2-UC-142	CTA-D1.2-EP-13 Prevent emergencies	Monitor motor and gears temperature	The driver wants to monitor the motor and gears temperature.	High		x		
CTA-D1.2-UC-145	CTA-D1.2-EP-13 Prevent emergencies	Notification about high carbon dioxide (CO2) level	The transportable staff wants to be notified about a low oxygen level in the train.	High		x	x	
CTA-D1.2-UC-146	CTA-D1.2-EP-13 Prevent emergencies	Notification about non-rotating wheels	The driver wants to be notified about non-rotating wheels of the train.	High		x		

Use Case ID	Epic ID / name	Name	Short Description	Severety	NG-TCN Domain			
					TCMSs	TCMS	OOS	COS
CTA-D1.2-UC-147	CTA-D1.2-EP-13 Prevent emergencies	Notify about low temperature	The transportable staff wants to be notified about low temperature in the train.	High		x	x	
CTA-D1.2-UC-148	CTA-D1.2-EP-13 Prevent emergencies	Notify about overheating	The Transportable Staff wants to be notified about overheating of the train.	High		x	x	
CTA-D1.2-UC-161	CTA-D1.2-EP-14 Provide information in case of emergency	Notify about activated emergency brake	The driver wants to be notified about an activated emergency brake.	High		x		
CTA-D1.2-UC-168	CTA-D1.2-EP-14 Provide information in case of emergency	Get emergency instructions from driver	The train staff wants to get emergency instructions of the driver using the communication system controlled by TCMS.	High		x	x	
CTA-D1.2-UC-169	CTA-D1.2-EP-14 Provide information in case of emergency	Issue Emergency instructions of transportable staff to passengers	The train staff wants issue emergency instructions to passengers using the emergency communication mechanism of TCMS.	High		x	x	
CTA-D1.2-UC-170	CTA-D1.2-EP-14 Provide information in case of emergency	Issue Emergency announcements of transportable staff to passengers	The train staff wants to issue emergency announcements using the emergency mechanism of TCMS.			x	x	
CTA-D1.2-UC-171	CTA-D1.2-EP-14 Provide information in case of emergency	Notify driver about operational hazards	The train staff wants to notify the driver about operational hazards using the emergency communication mechanism of TCMS.	High		x	x	
CTA-D1.2-UC-172	CTA-D1.2-EP-14 Provide information in case of emergency	Turn on/off automatic emergency announcements	The train staff wants to turn on/off automated announcements by using the announcement mechanism of TCMS.	Low		x	x	
CTA-D1.2-UC-173	CTA-D1.2-EP-14 Provide information in case of emergency	Receive emergency information	The transportable person wants to be informed appropriately (correct and current information, different languages, ...) about detected emergencies by using the emergency communication mechanism of TCMS.	High		x	x	x
CTA-D1.2-UC-174	CTA-D1.2-EP-14 Provide information in case of emergency	Display Location of emergency call to transportable staff	The Transportable Staff wants to know where an emergency call performed.	Medium		x	x	

Use Case ID	Epic ID / name	Name	Short Description	Severety	NG-TCN Domain			
					TCMSs	TCMS	OOS	COS
CTA-D1.2-UC-178	CTA-D1.2-EP-14 Provide information in case of emergency	Display activated emergency devices to transportable staff	The train staff wants to see where an emergency device (such as emergency brake request or emergency call,...) was activated.	Medium		x	x	
CTA-D1.2-UC-179	CTA-D1.2-EP-14 Provide information in case of emergency	Get event list	The Transportable Staff wants to know details, such as time, position, environmental data when an event happened.	Medium		x	x	
CTA-D1.2-UC-188	CTA-D1.2-EP-2 Control doors	Enter a cab	The driver wants to open the cab door.	High		x		
CTA-D1.2-UC-189	CTA-D1.2-EP-2 Control doors	Enter the locked train	The driver wants to unlock a door of a locked train.	Low		x		
CTA-D1.2-UC-193	CTA-D1.2-EP-2 Control doors	Lock the train	The driver wants to lock the train.	Medium		x		
CTA-D1.2-UC-199	CTA-D1.2-EP-2 Control doors	Obtain door maintenance information	The Maintenance staff wants to review the Door Maintenance Data	Medium		x	x	
CTA-D1.2-UC-202	CTA-D1.2-EP-2 Control doors	Notify on door malfunction	The train staff wants to be notified of door malfunctions and unexpected door openings.			x	x	
CTA-D1.2-UC-209	CTA-D1.2-EP-2 Control doors	Display notice of door malfunction	There is a door malfunction in the coach and is displayed on the coach door, so that the passenger is notified that the door cannot be used. (instead of paper)	Medium		x		
CTA-D1.2-UC-210	CTA-D1.2-EP-2 Control doors	Open a door	Transportable person wants the door to be opened	High		x		
CTA-D1.2-UC-213	CTA-D1.2-EP-2 Control doors	Enter the train for maintenance	Maintenance staff wants to enter a locked and stopped train for maintenance.			x	x	
CTA-D1.2-UC-217	CTA-D1.2-EP-1 Climatise vehicle	Adjust climate	The Transportable Staff adjusts the temperature level in a coach.	Medium		x	x	
CTA-D1.2-UC-218	CTA-D1.2-EP-1 Climatise vehicle	Monitor climate	Transportable Staff wants to monitor the temperature, oxygene level and humidity in each coach.	Medium		x	x	
CTA-D1.2-UC-219	CTA-D1.2-EP-1 Climatise vehicle	Notify climatization defect	Transportable Staff wants to be notified whenever there is a defect of air conditioning.	High		x	x	

Use Case ID	Epic ID / name	Name	Short Description	Severety	NG-TCN Domain			
					TCMSs	TCMS	OOS	COS
CTA-D1.2-UC-225	CTA-D1.2-EP-21 Light vehicle interior	Disable interior lights	Maintenance Staff wants to disable the interior lights in a coach to perform maintenance	Medium		x	x	
CTA-D1.2-UC-226	CTA-D1.2-EP-21 Light vehicle interior	Obtain interior lighting maintenance information	Maintenance Staff wants to obtain Interior Lighting Maintenance Information	Medium		x	x	
CTA-D1.2-UC-227	CTA-D1.2-EP-21 Light vehicle interior	Change interior lighting	Train Staff wants to change the interior lighting.	Medium		x	x	
CTA-D1.2-UC-228	CTA-D1.2-EP-21 Light vehicle interior	Notify transportable staff about light malfunction	Transportable Staff wants to be notified of all Light Malfunctions.	Medium		x	x	
CTA-D1.2-UC-229	CTA-D1.2-EP-21 Light vehicle interior	Set emergency light	Transportable Staff wants to switch on/off the emergency light.	High		x	x	
CTA-D1.2-UC-247	CTA-D1.2-EP-22 Integrate vehicle in the overall system rail	Update master data	Maintenance Staff wants to update train master data using the TCMS data update mechanism.	High		x	x	
CTA-D1.2-UC-252	CTA-D1.2-EP-15 Provide passenger information	Obtain system maintenance information of passenger information system	The Maintenance staff wants to obtain the Maintenance Information of the Passenger Information System.	Medium		x	x	
CTA-D1.2-UC-253	CTA-D1.2-EP-15 Provide passenger information	Adjust next stop information	Transportable Staff wants to adjust the next stop information.	Medium		x	x	
CTA-D1.2-UC-254	CTA-D1.2-EP-15 Provide passenger information	Make manual announcement of transportable staff	Transportable Staff wants to make a manual announcement.	Medium		x	x	
CTA-D1.2-UC-255	CTA-D1.2-EP-15 Provide passenger information	Set automatic display and announcements	The Train Staff wants to activate or deactivate the automatic display and announcement system.	Medium		x	x	
CTA-D1.2-UC-256	CTA-D1.2-EP-15 Provide passenger information	Setup passenger information system by transportable staff	Transportable Staff wants to setup the passenger information system.	Medium		x	x	
CTA-D1.2-UC-257	CTA-D1.2-EP-15 Provide passenger information	Setup seat reservations by transportable staff	The Train Staff wants to setup the seat reservation.	Medium		x	x	

Use Case ID	Epic ID / name	Name	Short Description	Severety	NG-TCN Domain			
					TCMSs	TCMS	OOS	COS
CTA-D1.2-UC-258	CTA-D1.2-EP-15 Provide passenger information	Notify of delay of current and connecting trains	Transportable Person wants to be notified automatically, if there is a change in delay of the current or any connecting trains.	Medium		x		x
CTA-D1.2-UC-259	CTA-D1.2-EP-15 Provide passenger information	Obtain alternative train information	Transportable Person wants to obtain train alternative information - for selected and connecting trains - including free seats on the alternatives.	Medium		x		x
CTA-D1.2-UC-260	CTA-D1.2-EP-15 Provide passenger information	Obtain available lavatory direction information	Transportable Person wants to obtain the information of the available lavatories.	Medium		x		x
CTA-D1.2-UC-261	CTA-D1.2-EP-15 Provide passenger information	Obtain delay of current and connecting trains	Transportable Person wants to obtain the delay and be informed about changes of connecting trains.	Medium		x		x
CTA-D1.2-UC-265	CTA-D1.2-EP-15 Provide passenger information	Obtain position and velocity information	Transportable Person wants to obtain the location and velocity of the train.	Medium		x		x
CTA-D1.2-UC-266	CTA-D1.2-EP-15 Provide passenger information	Obtain seat reservation information	Transportable Person wants to obtain seat reservation information to find their seat or assist other in finding their seat and to obtain guidance to available seats.	Medium		x		x
CTA-D1.2-UC-267	CTA-D1.2-EP-15 Provide passenger information	Obtain current location in train	Transportable Person wants to know its location on the train including consist and coach.	Medium		x		x
CTA-D1.2-UC-270	CTA-D1.2-EP-15 Provide passenger information	Test passenger information system	Maintenance staff wants to test all functions/mechanisms of the passenger information system.	Medium		x	x	
CTA-D1.2-UC-276	CTA-D1.2-EP-15 Provide passenger information	Make predefined announcement of transportable staff	Transportable Staff wants to make a predefined announcement with lowest priority.	Medium		x	x	
CTA-D1.2-UC-277	CTA-D1.2-EP-15 Provide passenger information	Display notice	The transportable Person gets information (e.g. car number, destination, class, available seats, ?) while standing outside of the train	Medium		x	x	x
CTA-D1.2-UC-280	CTA-D1.2-EP-17 Surveil passenger area	Notify transportable staff of surveillance event	Transportable Staff wants to be notified when an event is detected by passenger surveillance control on the train.	Medium		x	x	
CTA-D1.2-UC-281	CTA-D1.2-EP-17 Surveil passenger area	Provide surveillance of passenger area to transportable staff	Transportable Staff wants to monitor the passenger area.	Medium		x	x	

Use Case ID	Epic ID / name	Name	Short Description	Severety	NG-TCN Domain			
					TCMSs	TCMS	OOS	COS
CTA-D1.2-UC-282	CTA-D1.2-EP-17 Surveil passenger area	Test of passenger area surveillance	The maintenance staff wants to test the mechanisms/functions of the passenger area surveillance.	Medium		x	x	
CTA-D1.2-UC-283	CTA-D1.2-EP-17 Surveil passenger area	Notify railway undertaking of surveillance event	Railway undertaking wants to be notified when an event is detected by passenger surveillance control on the train.	Medium		x	x	
CTA-D1.2-UC-285	CTA-D1.2-EP-11 Passenger count	Obtain passenger count	System - TCMS wants to obtain the passenger count on the train.	Medium		x		
CTA-D1.2-UC-288	CTA-D1.2-EP-11 Passenger count	Obtain passenger counting maintenance data	The Maintenance staff wants to obtain the Passenger Counting System Maintenance Information.	Medium		x	x	
CTA-D1.2-UC-289	CTA-D1.2-EP-11 Passenger count	Notify transportable staff of passenger counting malfunction	Transportable Staff wants to be informed about any malfunction of passenger counting.	Medium		x	x	
CTA-D1.2-UC-290	CTA-D1.2-EP-11 Passenger count	Provide passenger count to transportable staff	Transportable Staff wants to obtain the passenger count on the train.	Medium		x	x	
CTA-D1.2-UC-292	CTA-D1.2-EP-11 Passenger count	Test passenger counting	The maintenance staff wants to test the mechanisms and functions of the passenger counting.	Medium		x		
CTA-D1.2-UC-300	CTA-D1.2-EP-12 Passenger services	Obtain passenger services maintenance data	The Maintenance staff wants to obtain the Passenger Services Maintenance Information.	Medium		x		
CTA-D1.2-UC-301	CTA-D1.2-EP-12 Passenger services	Access internet	Passenger wants to access the internet.	Medium				x
CTA-D1.2-UC-302	CTA-D1.2-EP-12 Passenger services	Access on-board entertainment	Passenger wants to access audio / video / game content on the train.	Medium				x
CTA-D1.2-UC-303	CTA-D1.2-EP-12 Passenger services	Adjust seat according to personal profile	Passenger wants to adjust its seat according to a stored profile.	Medium				x
CTA-D1.2-UC-304	CTA-D1.2-EP-12 Passenger services	Automatic validation of ticket	Passenger wants its ticket to be validated once seated.	Medium				x
CTA-D1.2-UC-305	CTA-D1.2-EP-12 Passenger services	Notify on invalid ticket for train	Passenger wants to be notified, if its ticket is invalid for this train.	Medium				x

Use Case ID	Epic ID / name	Name	Short Description	Severety	NG-TCN Domain			
					TCMSs	TCMS	OOS	COS
CTA-D1.2-UC-306	CTA-D1.2-EP-12 Passenger services	Obtain menu	Passenger wants to obtain the menu of food and beverage items available on board.	Medium				x
CTA-D1.2-UC-307	CTA-D1.2-EP-12 Passenger services	Purchase food and beverages	Passenger wants to purchase food and/or beverages for delivery to their seat.	Medium				x
CTA-D1.2-UC-309	CTA-D1.2-EP-12 Passenger services	Request assistance	Passenger wants to request assistance.	Medium			x	x
CTA-D1.2-UC-310	CTA-D1.2-EP-12 Passenger services	Provide view of outside camera to passengers	Passenger wants to view the outside cameras.	Medium		x		x
CTA-D1.2-UC-312	CTA-D1.2-EP-12 Passenger services	Notify of assistance request	Transportable Staff wants to be notified of when there is a request for assistance by a passenger.	Medium			x	x
CTA-D1.2-UC-313	CTA-D1.2-EP-12 Passenger services	Notify of lavatory malfunction	Transportable Staff wants to be notified in case of a lavatory malfunction.	Medium		x	x	
CTA-D1.2-UC-314	CTA-D1.2-EP-12 Passenger services	Notify of order for beverage and food	Transportable Staff wants to be notified when there is an order for food and/or beverages.	Medium			x	x
CTA-D1.2-UC-315	CTA-D1.2-EP-12 Passenger services	Test passenger services	The maintenance staff wants to test all passenger service functions.	Medium		x	x	x
CTA-D1.2-UC-316	CTA-D1.2-EP-12 Passenger services	Restaurant reservation	The passenger wants to make a seat reservation in the train restaurant.			x		x
CTA-D1.2-UC-317	CTA-D1.2-EP-12 Passenger services	Reserve seat	Passenger wants to make or change a seat reservation.	Medium		x		x
CTA-D1.2-UC-341	CTA-D1.2-EP-7 Maintain vehicle	Access maintenance data	The maintenance staff wants to access maintenance data of the train (doors, motors, wheels, clutches, ...).	Medium		x	x	
CTA-D1.2-UC-345	CTA-D1.2-EP-7 Maintain vehicle	Check passenger information system	The maintenance staff wants to check the functionality of the passenger information system.	Medium		x	x	
CTA-D1.2-UC-348	CTA-D1.2-EP-7 Maintain vehicle	Update software over the air (OTA)	The maintenance staff wants to update software of TCMS or some connected system OTA.	Medium	x	x	x	x
CTA-D1.2-UC-352	CTA-D1.2-EP-14 Provide information in case of emergency	Survey at a station by CCTV	The driver is able to have some visual information from the area where a Passanger Alarm System's handle has been activated when the train is stopped at a station.	High		x		

Use Case ID	Epic ID / name	Name	Short Description	Severety	NG-TCN Domain			
					TCMSs	TCMS	OOS	COS
CTA-D1.2-UC-353	CTA-D1.2-EP-14 Provide information in case of emergency	Survey out of a station by CCTV	The driver is able to have some visual information from the area where a Passanger Alarm System's handle has been activated when the train is outisde a station area.	High		x		

The list contains about 107 selected use cases of which are of different severity:

high	39
medium	61
low	2
undefined	5

3.2.3 Use Cases For Wireless Consist Network

General

The following sections are intended to translate the selected use case in Table 4 to functional use cases considering wireless technology, listed in Table 5.

In the scope of the project wireless technology means:

- wireless technology is intended to be used for intra-consist communication
- wireless technology is integrated into the TCMS network infrastructure (means: using the same wired infrastructure as TCMS devices), without influencing the TCMS data communication
- wireless end devices (WED) are connected to the train network via a wireless access point (WAP) offering appropriate access in a controlled manner (authentication, security)
- wireless end devices (WED) communicate with peer devices which are part of the train network infrastructure (transmit and receive data in general) offering data services/functions or information
- wireless end devices (WED) are using same network structure/infrastructure as devices which have a wired connection
- wireless end devices (WED) are devices belonging to different kind of actors (passenger, transportable staff, maintenance staff, rail vehicle manufacturer)

Later in the document, the use cases (Table 5) will be used to derive requirements for a wireless consist network (WLCN), see section 4.2.

And, the use cases will also be used to specify a wireless consist network (WLCN), see section 6.

Use Case List

Almost all uses cases listed in Table 4 can be simplified to a small number of use cases with respect to actors and related data services from technical point of view as listed in Table 5. Last column “NG-TCN Domain” maps in addition the use case to a related functional domain [05][06], while “RX” and “TX” indicate the associated domain and the communication directions.

Table 5: Use Cases simplified

ID	Use Case	Actor / Actors	NG-TCN Domain			
			TCMSs	TCMS	OOS	COS
CTA2_D1.1_UC_11	Connect a wireless end device to the TCMS network’s access point (fixed and moving end devices).	• passenger • train staff • maintenance staff • TCMS sensor • TCMS computing unit • rail vehicle manufacturer	-/-	RX/TX	RX/TX	-/RX
CTA2_D1.1_UC_12	Connect a safe wireless end device to the TCMS network’s access point (fixed end devices).	• TCMS computing unit	RX/TX	RX/TX	-/-	-/-
CTA2_D1.1_UC_13	A wireless end device exchanges data with services of the TCMS system (e.g. CCTV, HVAC, GPS, Diagnostic, Speed, ...).	• passenger • train staff • maintenance staff • TCMS sensor • TCMS computing unit • rail vehicle manufacturer	-/-	RX/TX	RX/TX	-/RX
CTA2_D1.1_UC_14	A wireless end device exchanges data with services in the WWW.	• passenger • train staff	-/-	-/-	RX/TX	RX/TX
CTA2_D1.1_UC_15	A wireless end device exchanges data with services on the train (e.g. restaurant, seat reservation, entertainment, climate).	• passenger • train staff	-/-	-/-	RX/TX	RX/TX
CTA2_D1.1_UC_16	A wireless end device exchanges data with services from operator's backend (e.g. ticket validation, special offers).	• passenger • train staff	-/-	-/-	RX/TX	RX/TX

3.2.4 Selected Use Cases for Regional Demonstrator

Some of the use cases presented in section 3.2.3 are selected to be demonstrated as part of the WP3 of CTA2 project. The selection criterion for this set of use cases is the availability of such subsystems, e.g. HVAC subsystem or CCTV, in the regional demonstrator. The main goal with this selection criterion is the reusability of demonstrator subsystems for WLCN.

Traceability of User Stories ⇔ Use Cases

A number of user stories are proposed to be realized as part of WP3. For transparent traceability, these user stories must be traceable to the related use cases defined in [03] and [04], as well as the IDs of the user stories defined in [01].

See Table 6 for a matrix depicting the relationships between these elements:

Table 6: Traceability of user story ⇔ use case ⇔ proposed use case for WP3

ID in [20]	User story	related use case(s) in [03]	related use case(s) in [04]	➔ Proposed UC
ID_10053	The train staff shall be aware of information concerning the train alerts or alarms so that he can decide which action shall be taken.	10041	CTA-D1.2-UC-40	CTA2_D1.1_UC_11 CTA2_D1.1_UC_12 CTA2_D1.1_UC_13
-	The Maintenance Staff wants to get data.	UC-1.2-013	CTA-D1.2-UC-84	CTA2_D1.1_UC_11 CTA2_D1.1_UC_12 CTA2_D1.1_UC_13
-	Transportable Staff wants to be notified when an event is detected by passenger surveillance control on the train.	UC-5.2-013	CTA-D1.2-UC-280	CTA2_D1.1_UC_11 CTA2_D1.1_UC_13
-	Passenger wants to request assistance.	UC-5.4-018	CTA-D1.2-UC-309	CTA2_D1.1_UC_11 CTA2_D1.1_UC_15
ID_00117	Passenger wants to view the outside cameras.	UC-5.4-019	CTA-D1.2-UC-310	CTA2_D1.1_UC_11 CTA2_D1.1_UC_15
ID_00223 ID_00231 ID_00233	The passenger wants to Change the temperature	UC-3.2-006	CTA-D1.2-UC-216	CTA2_D1.1_UC_11 CTA2_D1.1_UC_13 CTA2_D1.1_UC_15
ID_00053 ID_00054 ID_00055 ID_00056	The Transportable Staff adjusts the temperature level in a coach.	UC-3.2-007	CTA-D1.2-UC-217	CTA2_D1.1_UC_11 CTA2_D1.1_UC_13
ID_00024	Passenger wants to access the internet.	UC-5.4-009	CTA-D1.2-UC-301	CTA2_D1.1_UC_11 CTA2_D1.1_UC_14
-	Passenger wants to purchase food and/or beverages for delivery to their seat.	UC-5.4-015	CTA-D1.2-UC-307	CTA2_D1.1_UC_11 CTA2_D1.1_UC_15
ID_00138	Transportable Staff wants to be notified when there is an order for food and/or beverages.	UC-5.4-023	CTA-D1.2-UC-314	CTA2_D1.1_UC_11 CTA2_D1.1_UC_15

ID in [20]	User story	related use case(s) in [03]	related use case(s) in [04]	➔ Proposed UC
-	Passenger wants its ticket to be validated once seated.	UC-5.4-012	CTA-D1.2-UC-304	CTA2_D1.1_UC_11 CTA2_D1.1_UC_16
-	The maintenance staff wants to deactivate brakes.	UC-1.3-018	CTA-D1.2-UC-106	CTA2_D1.1_UC_11 CTA2_D1.1_UC_12 CTA2_D1.1_UC_13
-	The maintenance staff wants to update software of TCMS or some connected system OTA.	UC-6.2-008	CTA-D1.2-UC-348	CTA2_D1.1_UC_11 CTA2_D1.1_UC_12 CTA2_D1.1_UC_13

3.3 Use Cases for Train-to-ground communications over the Adaptable Communication System

This section contains the use cases for Train-to-ground (T2G) communication over the Adaptable Communication System (ACS) which is developed in X2Rail. To identify suitable use cases the modelled use cases from CONNECTA-1 [03] have been examined.

These use cases have been separated in two groups: "TCMS Use Cases" (relevant for revision of IEC 61375-2-6 [11]) and "Non-TCMS Use Cases" (other use cases, which need T2G communication infrastructure). For each use case it has been examined which data type needs to be delivered and which service from the IEC 61375-2-6 [37] can be used for that. Table 7 lists the "TCMS Use Cases" grouped by T2G Service.

Table 7: "TCMS Use Cases" grouped by data type and T2G service for realization

Data Type	T2G Service	Use Case ID
Process data	Train Telemetry Service	CTA-D1.2-UC-1, CTA-D1.2-UC-2, CTA-D1.2-UC-44, , CTA- CTA-D1.2-UC-287, CTA-D1.2-UC-294, CTA-D1.2-UC-295, CTA-D1.2-UC-296, CTA-D1.2-UC-297, CTA-D1.2-UC-332, CTA-D1.2-UC-333, CTA-D1.2-UC-334, CTA-D1.2-UC-335, CTA-D1.2-UC-336
Best effort data	File Transfer Service	CTA-D1.2-UC-37, D1.2-UC-71, CTA-D1.2-UC-72, CTA-D1.2-UC-79, CTA-D1.2-UC-80, CTA-D1.2-UC-82, CTA-D1.2-UC-83, CTA-D1.2-UC-88, CTA-D1.2-UC-107, CTA-D1.2-UC-199, CTA-D1.2-UC-226, CTA-D1.2-UC-247, CTA-D1.2-UC-248, CTA-D1.2-UC-250, CTA-D1.2-UC-252, CTA-D1.2-UC-268, CTA-D1.2-UC-269, CTA-D1.2-UC-279, CTA-D1.2-UC-288, CTA-D1.2-UC-319, CTA-D1.2-UC-320, CTA-D1.2-UC-321, CTA-D1.2-UC-322, CTA-D1.2-UC-323, CTA-D1.2-UC-324, CTA-D1.2-UC-325, CTA-D1.2-UC-326, CTA-D1.2-UC-341, CTA-D1.2-UC-342, CTA-D1.2-UC-348
Message Data	HTTP	CTA-D1.2-UC-73, CTA-D1.2-UC-74
Message Data	Train Information Service	CTA-D1.2-UC-38, CTA-D1.2-UC-242, CTA-D1.2-UC-246
Message Data	Train Location Service	CTA-D1.2-UC-181, CTA-D1.2-UC-331
Stream Data	not yet specified in IEC 61375-2-6	CTA-D1.2-UC-354, CTA-D1.2-UC-185, CTA-D1.2-UC-284

In Addition to that, further use cases for TCMS have been defined in CONNECTA-2. These use cases are listed in Table 8 and need final agreement in WP2. The data type for the listed use cases is process data which would be delivered via Train Telemetry Service.

Table 8: Additionally defined "TCMS Use Cases" for Train Telemetry Service

ID	Epic	Name	Short Description	Primary Actor	Trigger	Precondition	Result	Test case
CTA-D1.2-UC-XX1	CTA-D1.2-EP-8 Monitor vehicle	Alarm monitoring	The railway undertaking monitors variable groups related to existing alarms	RU	The TCMS monitors the alarms by using the Monitoring Mechanism of TCMS.	Alarms module and TCMS operable.	Alarms are monitored	Verifying that RU receive the variables related to an alarm
CTA-D1.2-UC-XX2	CTA-D1.2-EP-8 Monitor vehicle	Personalized alarm monitoring	The railway undertaking monitors personalized variable groups related to existing or personalized alarms	RU	The railway undertaking uses the control plane mechanism.	Remote communication is established, control plane mechanism is available and TCMS is operable.	Previously set of variables and alarms are monitored	Verifying that RU receive the set of variables specified on a given alarm
CTA-D1.2-UC-XX3	CTA-D1.2-EP-8 Monitor vehicle	Personalized variable monitoring	The railway undertaking monitors a set of personalized variables which can be set from a user interface	RU	The railway undertaking uses the control plane mechanism.	Remote communication is established, control plane mechanism is available and TCMS is operable.	Previously set of variables are monitored	Verifying that RU receive the set of variables defined
CTA-D1.2-UC-XX4	CTA-D1.2-EP-8 Monitor vehicle	Real time CBM	The railway undertaking defines a set of variables to apply an algorithm and develop CBM alarms in real time variables	RU	The railway undertaking uses the control plane mechanism.	Remote communication is established, control plane mechanism is available and TCMS is operable.	CBM alarm generated on ground	Verifying that RU receive the set of variables defined
CTA-D1.2-UC-XX5	CTA-D1.2-EP-8 Monitor vehicle	Remote HMI	The railway undertaking monitors the HMI and/or additional background	RU	The TCMS monitors the HMI by using the Monitoring Mechanism of	Remote communication is established, control plane	HMI is monitored	Verifying that RU receive HMI data.

			features		TCMS.	mechanism is available and TCMS is operable.		
CTA-D1.2-UC-XX6	CTA-D1.2-EP-8 Monitor vehicle	Operate Energy Measurement System Service	EN50463-4:2017 shall be able to use EN61375-2-6 to send data to energy metering server at ground side. Data exchange initiated mainly by train.	RU	DHS end device collects energy metering and sends data to a ground server	Energy Metering server on Internet.	Energy metering is available at ground side.	Check data reception at ground side
CTA-D1.2-UC-XX7	CTA-D1.2-EP-8 Monitor vehicle	Read Train Parameters	Maintainer would like to read the current value of a train function parameter . On demand or cyclically.	Maintenance staff	Ask the train to keep value			Check reading parameters
CTA-D1.2-UC-XX8	CTA-D1.2-EP-8 Monitor vehicle	Write Train Parameters	Maintainer would like to set the value of a train function parameter . On demand.	Maintenance staff	Ask the train to set value			Check writing parameters
CTA-D1.2-UC-XX9	CTA-D1.2-EP-8 Monitor vehicle	Read Ground Parameters	A train application would like to read the current value of a train mission parameter . On demand or cyclically.	RU, Driver, Staff	Ask the ground to read value			Check reading parameters
CTA-D1.2-UC-X10	CTA-D1.2-EP-8 Monitor vehicle	Write Ground Parameters	A train application would like to write the current value of a train mission parameter at ground side. On demand.	RU, Driver, Staff	Ask the ground to set value			Check writing parameters

Table 9 lists the “Non TCMS Use Cases” grouped by data type and service.

Table 9: “Non TCMS Use Cases” grouped by data type and service.

Data type	T2G Service	Use Case ID
Process data	Train Telemetry Service	CTA-D1.2-UC-154, CTA-D1.2-UC-156, CTA-D1.2-UC-286
Best effort data	File Transfer Service	CTA-D1.2-UC-84, CTA-D1.2-UC-85, CTA-D1.2-UC-152, CTA-D1.2-UC-153, CTA-D1.2-UC-258, CTA-D1.2-UC-259, CTA-D1.2-UC-261, CTA-D1.2-UC-263, CTA-D1.2-UC-293, CTA-D1.2-UC-300, CTA-D1.2-UC-327, CTA-D1.2-UC-328, CTA-D1.2-UC-329, CTA-D1.2-UC-330
Message Data	HTTP	CTA-D1.2-UC-86, CTA-D1.2-UC-87, CTA-D1.2-UC-89, CTA-D1.2-UC-108, CTA-D1.2-UC-109, CTA-D1.2-UC-138, CTA-D1.2-UC-151, CTA-D1.2-UC-155, CTA-D1.2-UC-180, CTA-D1.2-UC-289, CTA-D1.2-UC-291, CTA-D1.2-UC-304, CTA-D1.2-UC-305, CTA-D1.2-UC-317
	not yet specified in IEC 61375-2-6	CTA-D1.2-UC-76, CTA-D1.2-UC-77, CTA-D1.2-UC-78, CTA-D1.2-UC-81, CTA-D1.2-UC-240, CTA-D1.2-UC-243, CTA-D1.2-UC-244, CTA-D1.2-UC-245, CTA-D1.2-UC-249, CTA-D1.2-UC-272, CTA-D1.2-UC-273, CTA-D1.2-UC-274, CTA-D1.2-UC-275, CTA-D1.2-UC-283

The results from the tables above have been used to identify use cases which can be used for demonstration of the T2G communication over the ACS. For the regional demonstrator it was planned in WP3 to show the T2G communication via Telemetry Service. Therefore, a “TCMS Use Cases” from the category Train Telemetry Service was selected for demonstration of the communication over the ACS. As the HVAC functionality will be part of the regional demonstrator the use case CTA-D1.2-UC-335 “Monitor interior air quality” was chosen. The details are listed in Table 10.

Table 10: Selected use cases for demonstration of the T2G communication over ACS.

ID	Name	Short Description	Actor	Trigger	Precondition	Result	Test case
CTA-D1.2-UC-335	Monitor interior air quality	The railway undertaking monitors the interior air quality.	RU	The TCMS monitors the internal air quality by using the Monitoring Mechanism of TCMS.	HVAC and TCMS operable.	The internal air quality has been monitored by the TCMS.	Verifying that RU receive interior air quality data.

4. REQUIREMENTS FOR WIRELESS TCMS

4.1 Requirements for Wireless Train Backbone

This section is intended to collect requirements for the Wireless Train Backbone (WLTB) and more specifically for the Wireless Train Backbone Nodes (WLTBN). The approach is to extract relevant requirements from the top-level requirements list [08] and to detail the list by adding further requirements, be it functional and technical. The requirements are based on the Use cases introduced in section 3.1, on the functional based architecture [02] defined in the CONNECTA (CTA) project as well as in the Drive-by-Data architecture [06] and network requirements [07] defined in the same project.

4.1.1 Summary of top-level Requirements

The project CTA defined a set of top-level requirements [08]. These requirements were analysed in respect to wireless communication between consists. The following requirements have been selected as relevant for the WLTB, see Table 11:

Table 11: Selected Top-Level Requirements for Wireless TCMS

ID	Requirment	ReqType	Ref.-ID, Req.-Tool
CTA-D1.5-26	The wireless TCMS shall support wireless link between the consists of a train.	non-functional	ID_10001
CTA-D1.5-28	The wireless TCMS shall be maintainable during the whole lifetime of the train.	non-functional	ID_10003
CTA-D1.5-29	The wireless TCMS shall not have any EMC impact on the other components of the train according to EN 50121-3-2.	non-functional	ID_10004
CTA-D1.5-30	The wireless TCMS shall fulfil the laws guaranteeing against its impact on the staff and on the passengers.	non-functional	ID_10005
CTA-D1.5-31	The wireless TCMS shall fulfil a SIL convenient for the functions supported especially the brake functions.	non-functional	ID_10006
CTA-D1.5-32	The wireless TCMS shall be compatible with the supervision of the train integrity.	non-functional	ID_10008
CTA-D1.5-33 CTA-D1.5-34	The wireless TCMS shall be secured against the IT Security threats coming from outside the train for the risks identified in a cyber security risk analysis.	non-functional	ID_10009 ID_10010
CTA-D1.5-35	For a multi-consist train, the train operation shall be possible if one consist cannot be linked to the wireless TCMS.	non-functional	ID_10011
CTA-D1.5-36	The wireless TCMS shall be able to switch on and being operative in less than 90 s after it has been switched on by the driver.	functional	ID_10012
CTA-D1.5-37	The wireless TCMS shall be able to send status data to the train-to-ground interface.	functional	ID_10013

ID	Requirment	ReqType	Ref.-ID, Req.-Tool
CTA-D1.5-38	The wireless TCMS shall have no impact on the infrastructure (e.g. because of the EMC).	non-functional	ID_10014
CTA-D1.5-39	The bandwidth of the wireless TCMS shall not be used at more than 70 % of its maximum.	non-functional	ID_10015

Additionally, the requirements of the NG-TCN defined by CTA [06] has been analysed and the ones that may serve as a reference for WLTB specification have been summarised in the Table 12.

Table 12: Selected Requirements from NG-TCN

ID	Requirement	Ref.-ID, Req.-Tool[1]
CTA-D3.1-01	The next generation of TCMS shall support wired and wireless links between the consists of a train, and inside the consist, devices might be connected wired or wireless as well.	ID_60000
CTA-D3.1-02	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.	ID_60065
CTA-D3.1-03	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.	ID_60066
CTA-D3.1-04	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 behavior, demand-response-time, guaranteed bandwidth or jitter.	ID_60067
CTA-D3.1-05	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	ID_60068
CTA-D3.1-06	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	ID_40009
CTA-D3.1-07	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.	ID_40010
CTA-D3.1-08	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.	ID_40011
CTA-D3.1-09	The NG-TCN shall support the dynamic coupling or uncoupling of consists (train lengthening and train shortening) during service.	ID_40016

[1] Note that requirements 60000, 40011, 40025, 40026, 40050, 60096, 60010, 30000, 30007 are a summary of the corresponding set of requirements from **¡Error! No se encuentra el origen de la referencia.** and **¡Error! No se encuentra el origen de la referencia.**.

ID	Requirement	Ref.-ID, Req.-Tool[1]
CTA-D3.1-10	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.	ID_40017
CTA-D3.1-11	The IP-TCN shall support port based VLAN	ID_40022
CTA-D3.1-12	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.	ID_40023
CTA-D3.1-13	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.	ID_40024
CTA-D3.1-14	An ingressing tagged Ethernet frame with invalid VID shall be discarded.	ID_40025
CTA-D3.1-15	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	ID_40026
CTA-D3.1-16	NG-TCN shall support a precise time synchronization based on the protocol defined in IEEE 1588.	ID_40072
CTA-D3.1-17	TCN shall support a precise time synchronization within the network with a precision of ≤ 10 µs with a jitter of ± 1 µs (consist level) of ≤ 20 µs with a jitter of ± 2 µs (train level) NOTE: implies to use time-aware (IEEE 1588) switches	ID_40028
CTA-D3.1-18	Setup of synchronized clock after startup or network reconfiguration (e.g. inauguration) shall not take longer than 1.0s	ID_40070
CTA-D3.1-19	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	ID_40036
CTA-D3.1-20	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.	ID_40047
CTA-D3.1-21	Addressing on application layer shall use the TCN-URI schema defined in IEC61375-2-3.	ID_40048
CTA-D3.1-22	The TCN shall provide a service for dynamically assigning location specific IP addresses to end devices.	ID_40050
CTA-D3.1-23	The NG-TCN shall provide a DNS server (RFC 1034, RFC 1035) for resolving TCN-URI addresses (IEC61375-2-3) to IP addresses.	ID_40052
CTA-D3.1-24	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)	ID_40055
CTA-D3.1-25	The NG-TCN can provide a train topology database (TTDB) manager interface as specified in IEC61375-2-3 Annex E.	ID_40056
CTA-D3.1-26	The result of the train inauguration has to be published to those	ID_30107

ID	Requirement	Ref.-ID, Req.-Tool[1]
	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.	
CTA-D3.1-27	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.	ID_40059
CTA-D3.1-28	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.	ID_40060
CTA-D3.1-29	Train composition control shall only be granted to an authorized (dedicated) ED-S (or a redundant partner ED-S) in the consist.	ID_40061
CTA-D3.1-30	The NG-TCN can provide an ECSP interface for train composition control as specified in IEC61375-2-3 Annex E.	ID_40062
CTA-D3.1-31	The NG-TCN shall provide precise time information based on IEEE1588 to connected ED / ED-S.	ID_40076
CTA-D3.1-32	NG-TCN shall support the connection of ED-S implementing safety related function up to SIL 4.	ID_60004
CTA-D3.1-33	The NG-TCN subsystem provides the communication infrastructure used by end devices. Both, safety-related and non-safety-related equipment can be connected to the transmission system.	ID_60096
CTA-D3.1-34	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.2	ID_60010
CTA-D3.1-35	ED-S shall use at least a single-channel communication system. Redundancy may be used optionally for increased availability	ID_60012
CTA-D3.1-36	ED-S and ED communication shall be independent. However, ED-S and ED shall be able to use the same communication channel.	ID_60016
CTA-D3.1-37	Environmental conditions of NG-TCN shall be according to general railway requirements, mainly EN 50155, if there are no particular product standards.	ID_60035
CTA-D3.1-38	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.	ID_30100
CTA-D3.1-39	ED and ED-S connected to a NG NG-TCN may implement redundancy architecture to achieve the required reliability.	ID_60032
CTA-D3.1-40	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	ID_60033
CTA-D3.1-41	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.	ID_20000

[2] This means that the radio device should provide a cryptographic protection below the non-cryptographic safety code.

ID	Requirement	Ref.-ID, Req.-Tool[1]
CTA-D3.1-42	This probability is measured with the failure rate ƛ, which is the inverse of the value of the mean time between failures (MTBF): MTBF = 1/ƛ	ID_20001
CTA-D3.1-43	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.	ID_20002
CTA-D3.1-44	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.	ID_20003
CTA-D3.1-45	The maximum failure rate of each function of the NG-TCN shall be: ƛ ≤ 10-7 failures/hour NOTE: only functions which may cause a service failure as defined in ID_20003 are affected	ID_20004
CTA-D3.1-46	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.	ID_20005
CTA-D3.1-47	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.	ID_40020
CTA-D3.1-48	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.	ID_30000
CTA-D3.1-49	Network Components only with reported MTBF by the supplier should be used in the network for a quantitatively calculation of the availability.	ID_30004
CTA-D3.1-50	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.	ID_30007
CTA-D3.1-51	The network quality should be traceable via standard tools and functions for providing early failure detection.	ID_30011
CTA-D3.1-52	It shall be possible to manufacture consists with identical NG-TCN configuration, except for the consist identifier which must be unique for each consist.	ID_40069
CTA-D3.1-53	SW executing safety related functions have to be developed in accordance to EN50128 SIL4.	ID_30103
CTA-D3.1-54	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	ID_30106
CTA-D3.1-55	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. Therefor the switches should have implemented MIB2 and has to provide them via SNMP.	ID_30108
CTA-D3.1-56	Network components which mimic failsafe telegrams are not allowed during failsafe operation.	ID_30109
CTA-D3.1-57	Applications using open transmission systems according to EN50159 to transfer messages between equipment are inherently vulnerable as unauthorized access cannot be excluded. Therefore, it is important to guarantee the integrity and authentication of	ID_60041

ID	Requirement	Ref.-ID, Req.-Tool[1]
	messages sent over a non-trusted transmission medium	
CTA-D3.1-58	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	ID_60061
CTA-D3.1-59	Data traffic belonging to different security domains has to be separated in a way that it is equivalent to physical separation.	ID_40070
CTA-D3.1-60	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.	ID_40073
CTA-D3.1-61	The specified ETB consist interface shall be proposed for standardization in IEC61375.	ID_40074
CTA-D3.1-62	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.	ID_40075
CTA-D3.1-63	NG-TCN shall at least support the following data rates for the ETB and the consist network as options: -1GbE -10GbE	ID_40042

4.1.2 Detailed Requirements for Wireless Train Backbone Node

4.1.3 General

This section provides the breakdown of the High level requirements specified by CONNECTA project. The set of requirements listed in [08] are divided in different categories depending on the function they shall fulfil. Although R2R and CONNECTA projects already pointed out that the LTE technology and its D2D/V2V operation mode were the most suitable technology for the Wireless Train Backbone, the requirements have been defined technology independent. The reason for that is twofold; on the one hand the Complementary Action should re-evaluate the current state-of-the-art in radio technologies and their roadmap to adopt the most suitable one with the horizon of 2021-2022 (High level Demonstrators); on the other hand, the specification shall be open enough to be adapted in the future to newer radio communication technology in order to overcome the different evolution pace between the telecommunication and railways technologies.

4.1.4 Terminology

The WLTBN mixes two domain knowledges which are the wireless radio technology and the Ethernet Train Backbone. In order to address properly the specification of the WLTBN, this node has been divided in two devices; one which covers all radio communication functionalities and their variants; and another which covers the train functionalities needed for the interconnection of different consists' ECNs according to the IEC 61375 standard series. Equally, this specification helps to differentiate effectively the function responsibility division between the Complementary Action (Safe4RAIL-2), i.e. radio communication experts, and the Call for Members (CONNECTA-2), i.e. TCMS experts. Figure 4 depicts an example of the function distribution between the two devices of the WLTBN

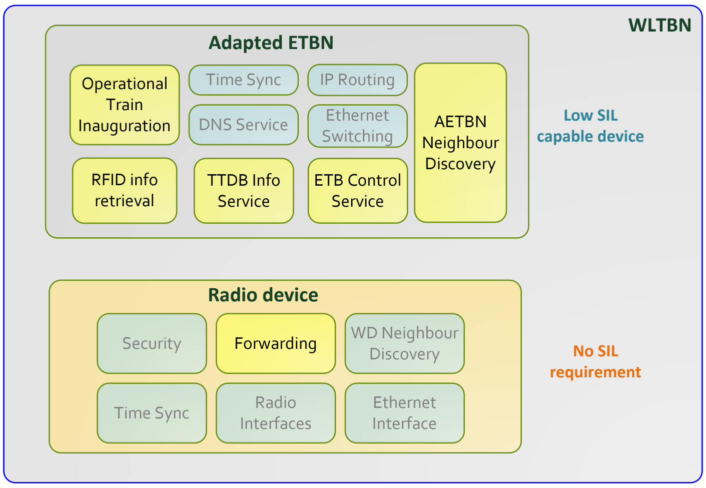


Figure 4: Example of functions division of the WLTBN[3]

4.1.5 Requirements

Table 13, Table 14, Table 15, Table 16, Table 17, Table 18, Table 19 and Table 20 list requirements which are to be considered in a Wireless Train Backbone. These requirements are on functional level and not specific to wireless technology.

Table 13: General Requirements for Wireless Train Backbone

ID	Requirement	High Level NG-TCN requirement reference
General		
CTA2-D1.1-1101	The WLTBN should be divided in two functional blocks: The WLTB radio functional block and the WLTB ETBN functional bock.	
CTA2-D1.1-1102	The WLTB radio device shall create a WLTB communication network between all WLTBN participating in the train composition.	CTA-D1.5-26 CTA-D3.1-01
CTA2-D1.1-1103	The WLTB radio device shall be able to communicate with other WLTBNs out of its radio coverage by implementing a multihop data forwarding protocol.	CTA-D1.5-35 CTA-D3.1-47

[3] Note that this is an example that could be used for the demonstrator in order to reuse existing ETBN with new radio device coming from the Complementary Action but the WLTBN may include all function in a single device.

ID	Requirement	High Level NG-TCN requirement reference
CTA2-D1.1-1104	The WLTB radio device shall reach at least the WLTBNs of two consist in each of its sides (front/rear), so that the WLTB is not completely lost when one consist cannot be linked.	CTA-D1.5-35
CTA2-D1.1-1105	The WLTBN shall implement the wireless safe train inauguration to compute the TTDB. The WLTBN shall maintain the discovery result in the Train topology database (TTDB) updated according to IEC 61375-2-3.	CTA-D3.1-10
CTA2-D1.1-1106	The WLTBN shall "forward/route the data between ECNs.	CTA-D3.1-06
CTA2-D1.1-1107	The WLTBN shall use a security layer which allows using the SDTv4 over wireless communications according to EN 50159.	CTA-D1.5-32 CTA-D3.1-02 CTA-D3.1-32 CTA-D3.1-34 CTA-D3.1-57
CTA2-D1.1-1108	The WLTBN shall be compliant with the IEC 62443.	CTA-D1.5-33 CTA-D1.5-34 CTA-D3.1-58 CTA-D3.1-59
CTA2-D1.1-1109	The WLTBN shall be able to switch on and being the WLTB operative in less than 90s after it has been switched on by the driver.	CTA-D1.5-36
CTA2-D1.1-1110	The WLTBN shall implement SNMP with specific MIB to indicate the folloging data updated to the current status: • Status of the device • Status of the radio link (e.g. SNR, BER) • Number of detected neighbours • List of neighbours (e.g. unique ID) • List of lost neighbours (i.e. since inauguration)	CTA-D1.5-37 CTA-D3.1-51 CTA-D3.1-55
CTA2-D1.1-1111	The bandwidth of the wireless TCMS shall not be used at more than 70 % of its maximum.	CTA-D1.5-39
CTA2-D1.1-1112	The WLTBN may implement redundancy architecture to achieve the required reliability[4] in accordance to NG-TCN.	CTA-D3.1-39 CTA-D3.1-48
CTA2-D1.1-1113	The WLTBN shall support all traffic data as defined in IEC 61375-1 tab 7: • Supervisory Data • Process Data • Message Data • Stream Data • Video • Voice • Best Effort Data	CTA-D3.1-40
CTA2-D1.1-1114	The WLTBN shall support TRDP traffic as specified in IEC61375-2-3.	CTA-D3.1-62

[4] 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. This probability for the WLTBN devices is measured with the failure rate λ, which is the inverse of the value of the mean time between failures (MTBF): MTBF = 1/λ.

ID	Requirement	High Level NG-TCN requirement reference
CTA2-D1.1-1115	The maximum failure rate of each function which may lead to service failures[5] shall be: $\lambda \leq 10^{-7}$ failures/hour	CTA-D3.1-44 CTA-D3.1-45
CTA2-D1.1-1116	The WLTBN devices providers shall report MTBF to be used in the network for a quantitatively calculation of the availability.	CTA-D3.1-48

Table 14: Environmental Requirements for Wireless Train Backbone

ID	Requirement	High Level NG-TCN requirement reference
Environment		
CTA2-D1.1-1201	The WLTBN shall comply with EN 50155:2017 class OT4, -40 °C to +70 °C.	CTA-D3.1-37
CTA2-D1.1-1202	The WTLBN shall comply with EN 50121-3-2:2015 and EN 50121-4:2016.	CTA-D1.5-29 CTA-D1.5-38
CTA2-D1.1-1203	The WTLBN shall comply with EN 50124-1:2017.	
CTA2-D1.1-1204	The WTLBN shall comply with EN 50125-1:2014.	
CTA2-D1.1-1205	The WTLBN Devices shall comply with EN 50125-3:2014 if signalling functions are integrated on TCMS network.	
CTA2-D1.1-1206	The WTLBN Devices shall comply with EN 45545-1:2013.	
CTA2-D1.1-1207	The WTLBN Devices shall comply with EN 45545-2:2013.	
CTA2-D1.1-1208	The WTLBN Devices shall comply with EN 45545-5:2013.	
CTA2-D1.1-1209	The WTLBN Devices shall comply with EN 50126-1:2017.	CTA-D3.1-05
CTA2-D1.1-1210	The WTLBN Devices shall comply with EN 50657:2017.	
CTA2-D1.1-1211	The WTLBN Devices shall comply with EN 50128:2011 if signalling functions are integrated on TCMS network.	
CTA2-D1.1-1212	The WTLBN Devices shall comply with EN 50129:2018.	
CTA2-D1.1-1213	The WTLBN Devices shall support input power voltage DC, and should support the range 24V-110V.	

[5] 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.

ID	Requirement	High Level NG-TCN requirement reference
CTA2-D1.1-1214	The WTLBN Devices may use M12 K-coded 5-pin male or M12 A-coded 4-pin male connector as the power connector.	
CTA2-D1.1-1215	Wireless TCMS devices shall fulfil the laws guaranteeing against its impact on the staff and on the passengers. Wireless TCMS devices shall be compliant with the European directive RED 2014/53/EU. Wireless TCMS devices shall be compliant with the norm EN 62311:2008.	CTA-D1.5-30

Table 15: Communication Requirements for Wireless Train Backbone

ID	Requirement	High Level NG-TCN requirement reference
Communication		
CTA2-D1.1-1301	Only WLTBN of the same WLTB should be able to communicate each other, excluding messages coming from other sources.	
CTA2-D1.1-1302	WLTBN shall be able to discover adjacent WLTBNs.	
CTA2-D1.1-1303	WLTBN of the same WLTB (i.e. excluding WLTBN from other train units) should be able to create a local forwarding table for the WLTBNs which are not reachable with a single hop.	
CTA2-D1.1-1304	Redundant WLTBN devices shall be able to work in different frequencies in order to avoid single point failures in a single band.	CTA-D3.1-48
CTA2-D1.1-1305	The WLTBN should be designed to allow frequency reutilization when possible.	
CTA2-D1.1-1306	The WLTBN shall ensure that the maximum time for the permitted interruption remains below 1.0s.	CTA-D3.1-50

Table 16: Configuration Requirements for Wireless Train Backbone

ID	Requirement	High Level NG-TCN requirement reference
Configuration		
CTA2-D1.1-1401	The WLTB radio shall be able to load a certificate or shared key for group authentication/authorization and secure data communication (related to CTA2-D1.1-1301).	
CTA2-D1.1-1402	Static IP addresses of the ETBN shall be set in the ECN interface.	
CTA2-D1.1-1403	When DHCP is available for dynamic IP addressing and the ECSP is located within the ETBN, the DHCP server shall be configured.	
CTA2-D1.1-1404	When ECSP is located within the ETBN, the static consist information shall be configured.	

ID	Requirement	High Level NG-TCN requirement reference
CTA2-D1.1-1405	ETB Inauguration (TTDP) settings: Settings required for the ETBN to conduct ETB inauguration according to IEC 61375-2-5.	
CTA2-D1.1-1406	Settings required for the ETBN to act as firewall.	

Table 17: Logging Requirements for Wireless Train Backbone

ID	Requirement	High Level NG-TCN requirement reference
Logging		
CTA2-D1.1-1501	The WLTBN shall support logging of OS related events.	
CTA2-D1.1-1502	The WLTBN shall support logging of neighbour discovery processes.	
CTA2-D1.1-1503	The WLTBN shall support logging of failure authentication/authorization attempts in neighbour discovery processes.	

Table 18: Network Requirements for Wireless Train Backbone

ID	Requirement	High Level NG-TCN requirement reference
Network		
CTA2-D1.1-1701	The WLTBN AETBN shall act as a router between ECN and WLTB for unicast and multicast IP packets including network address translation.	CTA-D3.1-06
CTA2-D1.1-1702	The WLTBN Radio device shall act as an OSI L2 bridge between the WLTB and the WLTBN AETBN.	CTA-D3.1-06 CTA-D3.1-08
CTA2-D1.1-1703	The WLTBN shall support IP as defined in RFC 791.	CTA-D3.1-07
CTA2-D1.1-1704	The WLTBN shall support ARP as defined in RFC 826.	
CTA2-D1.1-1705	The WLTBN shall support UDP as defined in RFC 768.	
CTA2-D1.1-1706	The WLTBN shall support TCP as defined in RFC 793.	
CTA2-D1.1-1707	The WLTBN shall support ICMP as defined in RFC 792.	
CTA2-D1.1-1708	The WLTBN shall support IGMP Message Format as defined in RFC 3376 Clause 4.	

ID	Requirement	High Level NG-TCN requirement reference
CTA2-D1.1-1709	The WLTBN shall support IGMP Router Filter-Mode as defined in RFC 3376 Clause 6.2.1.	
CTA2-D1.1-1710	The WLTBN shall support IGMP Querier Election as defined in RFC 3376 Clause 6.6.2.	
CTA2-D1.1-1711	The WLTBN shall support IGMP Interoperation With Older Versions of IGMP as defined in RFC 3376 Clause 7.	
CTA2-D1.1-1712	The WLTBN shall support IGMP Query Interval setting as defined in RFC3376 Clause 8.14.2.	
CTA2-D1.1-1713	The WLTBN may support IGMP snooping, prevent hosts on a local network from receiving traffic for a multicast group they have not explicitly joined.	
CTA2-D1.1-1714	The WLTBN should support a DHCP server	CTA-D3.1-07
CTA2-D1.1-1715	The WLTBN shall support DHCP server to provide IPv4[6] address allocation as defined in RFC 2131 Clause 3.	CTA-D3.1-07
CTA2-D1.1-1716	The WLTBN may support DHCP server to provide Router Option as defined in RFC 2132 Clause 3.5.	
CTA2-D1.1-1717	The WLTBN shall support DHCP server to provide Domain Name Server option as defined in RFC 2132 Clause 3.8.	
CTA2-D1.1-1718	The WLTBN shall support DHCP server to provide IP Address Lease Time option as defined in RFC 2132 Clause 9.2.	
CTA2-D1.1-1719	The WLTBN shall support DHCP server to provide TFTP Server Name option as defined in RFC 2132 Clause 9.4.	
CTA2-D1.1-1720	The WLTBN shall support DHCP server to provide Bootfile Name option as defined in RFC 2132 Clause 9.5.	
CTA2-D1.1-1721	The WLTBN may support DHCP server to provide Client-identifier option as defined in RFC 2132 Clause 9.14.	
CTA2-D1.1-1722	The WLTBN may support DHCP server to provide Relay-agent information - Server operation as defined in RFC 3046.	
CTA2-D1.1-1723	The WLTBN shall support SNMP	
CTA2-D1.1-1724	The WLTBN shall support IEC 61375-2-5 MIB to meet requirements which is defined in ETBN inauguration sheet	

[6] For the Wireless TCMS, as well as for the NG-TCMS, IPv4 has taken as a reference protocol. The selection of this network layer protocol instead of IPv6 has been made due to different reasons. First of all, currently the consist-level and train-level IP address mapping is handled by a well-known system based on the operation train inauguration defined in the standard IEC 61375-2-5, which will be kept. Second, the transition to IPv6 would require the update of all on-board subsystems. Last but not least, the main advantage of IPv6 is the bigger address space which allows providing a unique public address to any device, allowing it to be reached through the internet. However, this approach goes in opposition to the TCMS T2G architecture, in which the single entrance to on-board TCMS service is the MCG.

ID	Requirement	High Level NG-TCN requirement reference
CTA2-D1.1-1725	The WLTBN shall support IEC 61375-2-3 MIB to meet requirements which is defined in ETBN Service sheet	
CTA2-D1.1-1726	Addressing on network layer shall use the IP address schema defined in IEC 61375-2-5 (inter-consist) and IEC 61375-3-4 (intra-consist) in case IPv4 is deployed.	CTA-D3.1-20
CTA2-D1.1-1727	WLTB should allow the network performances summarized in Annex A.	CTA-D3.1-63
CTA2-D1.1-1728		

Table 19: Time Requirements for Wireless Train Backbone

ID	Requirement	High Level NG-TCN requirement reference
Time		
CTA2-D1.1-1801	The WLTBN shall support precise time synchronization based on GNSS/Ground Infrastructure.	
CTA2-D1.1-1802	The WLTBN of the leading consist should be able to act as a clock reference for the rest of WLTB devices.	
CTA2-D1.1-1803	The WLTB radio device shall be able to propagate clock synchronization to the ECN via IEEE 1588 with a precision of ≤ 10 µs with a jitter of ± 1 µs (consist level) of ≤ 20 µs with a jitter of ± 2 µs (train level) Note: The suitability of these accuracy values will be evaluated by Safe4RAIL-2 T2.6 and the results will be publicly available in Safe4RAIL-2 D2.4.	CTA-D3.1-16 CTA-D3.1-17 CTA-D3.1-31
CTA2-D1.1-1804	Setup of synchronized clock after startup or network reconfiguration (e.g. inauguration) shall not take longer than 1.0s	CTA-D3.1-18

Table 20: Inauguration Requirements for Wireless Train Backbone

ID	Requirement	High Level NG-TCN requirement reference
Inauguration		
CTA2-D1.1-1901	The WLTBN shall be able to compute the TTDB.	
CTA2-D1.1-1902	WLTBN shall compute the Train Network Directory with TFFR of less than 10^{-6}/h to achieve safety integrity level SIL2. Note: Current specification of Train Network Directory computation in IEC 61375-2-5 is assumed to be sufficient for SIL 2.	CTA-D1.5-31 CTA-D3.1-03 CTA-D3.1-05 CTA-D3.1-02

ID	Requirement	High Level NG-TCN requirement reference
CTA2-D1.1-1903	The WLTBN shall provide TTDB information to TI validator via TTDB manager interface defined in IEC 61375-2-3, and shall transfer data via safe data transmission protocol (e.g. SDTv2).	CTA-D3.1-24 CTA-D3.1-25 CTA-D3.1-30 CTA-D3.1-54 CTA-D3.1-02 CTA-D3.1-26
CTA2-D1.1-1904	The WLTBN shall provide a user service to set/reset the local vehicle to/from status "leading" as it is specified in IEC61375-2-3.	CTA-D3.1-27
CTA2-D1.1-1905	The WLTBN shall provide a user service to inhibit a train inauguration. In case train inaugurations are inhibited, no new train network directory shall be computed.	CTA-D3.1-28

4.2 Requirements for Wireless Consist Network

This section is intended to collect requirements for a Wireless Consist Network (WCN). The approach is to extract relevant requirements from the top-level requirements list [08] and to detail the list by adding further requirements, be it functional and technical. The requirements are based on the definition of user stories [01], use cases [01], and the functional based architecture [02] defined in the CONNECTA (CTA) project.

4.2.1 Summary of top-level Requirements

The previous project CTA defined a set of top-level requirements [08]. These requirements were analysed in respect to wireless communication (inside a consist / intra-consist). The following requirements have been selected as relevant for the wireless consist network, see Table 21:

Table 21: Selected Top-Level Requirements for Wireless TCMS

ID	Requirment	ReqType	Ref.-ID, Req.-Tool
CTA-D1.5-27	The wireless TCMS shall support wireless links inside the consist making up the train.	non-functional	ID_10002
CTA-D1.5-28	The wireless TCMS shall be maintainable during the whole lifetime of the train.	non-functional	ID_10003
CTA-D1.5-29	The wireless TCMS shall not have any EMC impact on the other components of the train according to EN 50121-3-2.	non-functional	ID_10004
CTA-D1.5-30	The wireless TCMS shall fulfil the laws guaranteeing against its impact on the staff and on the passengers.	non-functional	ID_10005
CTA-D1.5-31	The wireless TCMS shall fulfil a SIL convenient for the functions supported especially the brake functions.	non-functional	ID_10006
CTA-D1.5-32	The wireless TCMS shall be compatible with the supervision of the train integrity.	non-functional	ID_10008
CTA-D1.5-33 CTA-D1.5-34	The wireless TCMS shall be secured against the IT Security threats coming from outside the train for the risks identified in a cyber security risk analysis.	non-functional	ID_10009 ID_10010
CTA-D1.5-36	The wireless TCMS shall be able to switch on and being operative in less than 90 s after it has been switched on by the driver.	functional	ID_10012
CTA-D1.5-37	The wireless TCMS shall be able to send status data to the train-to-ground interface.	functional	ID_10013
CTA-D1.5-38	The wireless TCMS shall have no impact on the infrastructure (e.g. because of the EMC).	non-functional	ID_10014
CTA-D1.5-39	The bandwidth of the wireless TCMS shall not be used at more than 70 % of its maximum.	non-functional	ID_10015

4.2.2 Detailed Requirements for Wireless Consist Network

In Roll2Rail (R2R) project WP2 T2.5 the general wireless communication architecture was proposed for insides consist communication, see [09], chapter 4. The conclusion favoured WLAN technology according to either IEEE 802.11g/h/n or IEEE 802.11ac. Which one to use, mainly depends on the needed bandwidth. The needed bandwidth, in turn, depends on the vehicle functions of the different domains.

The scope of this document is the TCMS domain. According to [09], a bandwidth of 10Mbit/s is estimated for this domain. Thus, WLAN according IEEE 802.11n or even IEEE 802.11g would be sufficient. But, having in mind, that newer/faster technology is already available and having in mind to use wireless technology also in the OOS domain, it makes sense to choose IEEE 802.11ac (with higher data rate) for both domains.

On the other hand, limiting the technology to IEEE 802.11 only, would exclude technical aspects, which were evaluated and additionally defined in CTA project. Related to wireless consist network, one of the interesting features is the time sensitive networking (TSN), enabling reliable and safe network communication between end devices and between safe end devices. Using TSN based on IEEE 802.1Q or IEEE 802.1AS in a wireless environment is not yet possible with access points based on IEEE 802.11. Other technologies are to be considered instead, e.g. LTE 5G, but this would be very costly for intra-consist communication purposes. With help of the requirements in Table 22 a complementary action in Safe4RAIL-2 project will evaluate which technology to choose.

Terminology

For common understanding some definitions are set. Since different abbreviations were used in the previous projects (Roll2Rail and CONNECTA) a mapping is provided to ease the common understanding. The following terms are defined:

WED: Wireless End Device is an active end device, using a wireless network interface to exchange data within the TCMS network. Synonyms: WLED

WAP: Wireless Access Point is an active network device, using a wireless network interface to offer access to the TCMS network. Synonyms: AP

Requirements

Table 22 lists requirements which shall be considered in a wireless TCMS consist network. These requirements are on functional level and specific to wireless technology. Each requirement has a “Type”, defining whether it is optional (“O”) or mandatory (“M”). The “Comment” column may state additional text for better understanding.

Table 22: Requirements for Wireless TCMS

ID	Requirment	Type	Comment
CTA2-D1.1-01	The TCMS network shall use WAP to provide access for WED.	M	
CTA2-D1.1-02	The TCMS network shall provide access for static WED.	M	Fixed mounted devices.
CTA2-D1.1-03	The TCMS network shall provide access for WED in motion.	M	Moving devices, like SMART devices or PCs; moving relative to the train and consist Remark: IEEE 802.11r, fast BSS transition; KRACK

ID	Requirment	Type	Comment
CTA2-D1.1-04	The TCMS network shall provide access for WED in motion in trains of multiple consists.	M	Rooming function for EDs in motion.
CTA2-D1.1-05	The TCMS network shall provide redundant access for WED.	O	e.g. same SSID, WAP building an ESS (extended service set) → one WED must be able to reach all WAP devices of the redundant system
CTA2-D1.1-06	A WED shall operate on a well-defined wireless communication standard.	M	IEEE 802.11n, 2,4/5GHz IEEE 802.11a, 5GHz IEEE 802.11ac, 5GHz IEEE 802.11ax, 1..6GHz LTE 5G
CTA2-D1.1-07	A WED shall be able to participate in the TSN.	O	The end device shall support time critical data communication (e.g. using 802.11ax or LTE).
CTA2-D1.1-08	A WAP shall operate on a well-defined wireless communication standard.	M	IEEE 802.11n, 2,4/5GHz IEEE 802.11a, 5GHz IEEE 802.11ac, 5GHz IEEE 802.11ax, 1..6GHz LTE 5G
CTA2-D1.1-09	A WAP shall be able to participate in the TSN.	O	The access point shall support time critical data communication (e.g. using 802.11ax or LTE).
CTA2-D1.1-10	A WAP shall be able to operate on a well-defined wired communication standard.	M	IEEE 802.3; wired connection to a distribution system, e.g. TCMS, if needed; also due to maintenance and configuration purposes
CTA2-D1.1-11	A WED shall operate on a well-defined wired communication standard.	O	IEEE 802.3; due to maintenance and configuration purposes
CTA2-D1.1-12	The TCMS network shall provide a controlled access for WED.	O	MAC Filtering, whitelisting allowed end devices.
CTA2-D1.1-13	The TCMS consist network shall provide a secured access for WED in the same consist.	M	IEEE 802.11i WPA2 (AES/TKIP), IEEE 802.11-2016 WPA3 (OWE) IEEE 802.1X RADIUS IEEE 802.11w protected MGMT frames
CTA2-D1.1-14	The WAP shall exchange communication data between the wired and wireless networks.	M	Routing
CTA2-D1.1-15	Data exchanged between the wired and wireless networks shall be controllable with traffic filters.	M	Firewall
CTA2-D1.1-16	The TCMS network shall assign appropriate IP-address to WED.	O	DHCP

ID	Requirment	Type	Comment
CTA2-D1.1-17	The wireless TCMS network shall enable intra consist data communication between connected WED.	M	
CTA2-D1.1-18	The WAP shall be able to control/scale the bandwidth usage of the wireless TCMS network.	M	Max. 70% of its capabilities.
CTA2-D1.1-19	The wireless technology shall be able to support an even distribution of WED.	O	Client balancing. Spread WED over available WAPs
CTA2-D1.1-20	Data traffic belonging to different domains (e.g. TCMS or OOS) shall be separated by using different SSIDs.	M	Virtual SSID are allowed.
CTA2-D1.1-21	Data traffic belonging to different domains (e.g. TCMS or OOS) shall be separated by using VLAN technique.	M	
CTA2-D1.1-22	The wireless technology shall be scalable in terms of max. number of connectable WED.	M	
CTA2-D1.1-23	The wireless technology shall be scalable in terms of spatial conditions.	M	Radio spread, car body conditions, passengers, antenna types
CTA2-D1.1-24	A WAP, which is part of wireless TCMS network, is connected to a ring switch of the ECR (Ethernet Consist Ring).	M	
CTA2-D1.1-25	A WAP, which is part of wireless TCMS network, is integrated in a ring switch of the ECR (Ethernet Consist Ring).	O	RS and WAP are housed in the same hardware device
CTA2-D1.1-26	A WAP, which is part of wireless TCMS network, is integrated in an ETBN.	O	TS and WAP are housed in the same hardware device
CTA2-D1.1-27	A WAP, which is part of wireless TCMS network, is integrated in an WLBN.	O	WLBN and WAP are housed in the same hardware device
CTA2-D1.1-28	The WAP shall support mechanisms to minimize communication delay and jitter for time critical applications, ensuring predicable behaviour.	M	IEEE 802.11e WMM Scheduled Access or WMM QoS; WMM: Wireless Multi Media
CTA2-D1.1-29	The WED shall support mechanisms to minimize communication delay and jitter for time critical applications, ensuring predicable behaviour.	M	IEEE 802.11e WMM Scheduled Access or WMM QoS; WMM: Wireless Multi Media
CTA2-D1.1-30	The WAP shall be able to establish a wireless distribution system without using the ECN/ECR.	O	IEEE 802.11s MESH (in MAC Layer) Future use. At least the WAP HW shall be prepared.
CTA2-D1.1-31	The WAP shall support TSN.	O	IEEE 802.1Q IEEE 802.1AS Future use. At least the WAP HW shall be prepared.
CTA2-D1.1-32	The WAP shall provide a static configuration interface for the wireless technology.	M	e.g. USB config plug, config key

ID	Requirment	Type	Comment
CTA2-D1.1-33	The WAP shall provide a dynamic configuration interface for the wireless technology.	M	e.g. SNMP
CTA2-D1.1-34	The WAP shall provide a control interface, to control the wireless technology.	M	request an action (e.g. via SNMP)
CTA2-D1.1-35	The WAP shall provide a status interface, to get information from the wireless technology.	M	get status information (e.g. via SNMP)
CTA2-D1.1-36	The WED shall provide a static configuration interface for the wireless technology.	M	e.g. internal memory, USB config plug
CTA2-D1.1-37	The WED shall provide a control interface, to control the wireless technology.	O	request an action (e.g. via SNMP)
CTA2-D1.1-38	The WED shall provide a status interface, to get information from the wireless technology.	M	request an action; get status information (e.g. via SNMP)
CTA2-D1.1-39	The configuration of a WAP shall be stored in a file.	M	
CTA2-D1.1-40	The configuration of a WED shall be stored in a file.	M	
CTA2-D1.1-41	A WAP device shall support logging of OS related events.	M	local or remote syslog
CTA2-D1.1-42	A WAP device shall support logging of connection requests.	O	granted and denied connection attempts
CTA2-D1.1-43	A WAP device shall support logging of disconnection requests.	O	
CTA2-D1.1-44	A WAP shall synchronize with the time base in the TCMS network.	M	
CTA2-D1.1-45	A WED shall synchronize with the time base in the TCMS network.	M	
CTA2-D1.1-46	The TCMS network shall support the integration of devices providing WIPS.	O	WIPS: Wireless Intrusion Prevention System; a network device that monitors the radio spectrum for the presence of unauthorized APs; part of WIDS (Wireless Intrusion Detection System)

4.2.3 Requirement Traceability Matrix

This chapter contains a table which offers traceability between the top-level requirements in chapter 4.2.1 (Table 21) and the requirements in chapter 4.2.2 (Table 22).

Table 23: Traceability Matrix

Top-Level ID	Requirment	Ref.-ID, Req.-Tool	Req. Wireless Consist Network ID

Top-Level ID	Requirment	Ref.-ID, Req.-Tool	Req. Wireless Consist Network ID
CTA-D1.5-27	The wireless TCMS shall support wireless links inside the consist making up the train.	ID_10002	CTA2-D1.1-01, CTA2-D1.1-02, CTA2-D1.1-03, CTA2-D1.1-04, CTA2-D1.1-05, CTA2-D1.1-14, CTA2-D1.1-16, CTA2-D1.1-17, CTA2-D1.1-20, CTA2-D1.1-21, CTA2-D1.1-22, CTA2-D1.1-23, CTA2-D1.1-24, CTA2-D1.1-25, CTA2-D1.1-26, CTA2-D1.1-27, CTA2-D1.1-30, CTA2-D1.1-44, CTA2-D1.1-45
CTA-D1.5-28	The wireless TCMS shall be maintainable during the whole lifetime of the train.	ID_10003	CTA2-D1.1-10, CTA2-D1.1-11, CTA2-D1.1-32, CTA2-D1.1-33, CTA2-D1.1-34, CTA2-D1.1-36, CTA2-D1.1-37, CTA2-D1.1-39, CTA2-D1.1-40, CTA2-D1.1-41, CTA2-D1.1-42, CTA2-D1.1-43
CTA-D1.5-29	The wireless TCMS shall not have any EMC impact on the other components of the train according to EN 50121-3-2.	ID_10004	CTA2-D1.1-06, CTA2-D1.1-08
CTA-D1.5-30	The wireless TCMS shall fulfil the laws guaranteeing against its impact on the staff and on the passengers.	ID_10005	CTA2-D1.1-06, CTA2-D1.1-08
CTA-D1.5-31	The wireless TCMS shall fulfil a SIL convenient for the functions supported especially the brake functions.	ID_10006	CTA2-D1.1-07, CTA2-D1.1-09, CTA2-D1.1-28, CTA2-D1.1-29, CTA2-D1.1-31
CTA-D1.5-32	The wireless TCMS shall be compatible with the supervision of the train integrity.	ID_10008	CTA2-D1.1-35, CTA2-D1.1-38, CTA2-D1.1-41, CTA2-D1.1-42, CTA2-D1.1-43, CTA2-D1.1-44
CTA-D1.5-33 CTA-D1.5-34	The wireless TCMS shall be secured against the IT Security threats coming from outside the train for the risks identified in a cyber security risk analysis.	ID_10009 ID_10010	CTA2-D1.1-12, CTA2-D1.1-13, CTA2-D1.1-15, CTA2-D1.1-46
CTA-D1.5-36	The wireless TCMS shall be able to switch on and being operative in less than 90 s after it has been switched on by the driver.	ID_10012	
CTA-D1.5-37	The wireless TCMS shall be able to send status data to the train-to-ground interface.	ID_10013	CTA2-D1.1-35, CTA2-D1.1-38
CTA-D1.5-38	The wireless TCMS shall have no impact on the infrastructure (e.g. because of the EMC).	ID_10014	CTA2-D1.1-06, CTA2-D1.1-08
CTA-D1.5-39	The bandwidth of the wireless TCMS shall not be used at more than 70 % of its maximum.	ID_10015	CTA2-D1.1-18, CTA2-D1.1-19

4.3 Requirements for Train-to-ground communications over the Adaptable Communication System

In order to be used as a communication channel for the Train-to-Ground communications according to IEC 61375-2-6:2018 standard the Adaptable Communication System (ACS) needs to satisfy the requirements listed in Table 24.

Table 24: Requirements on the Adaptable Communication System (ACS) for the Train-to-Ground communications according to IEC 61375-2-6:2018 standard

Req-ID	Description
CTA2-ACS-REQ-01	The ACS must support the Ethernet standards IEEE 802.3 for Gigabit Ethernet and beyond.
CTA2-ACS-REQ-02	The ACS must support network communication over the Internet Protocol version 4 (IPv4).
CTA2-ACS-REQ-03	The ACS must support network communication over the Internet Protocol version 6 (IPv6).
CTA2-ACS-REQ-04	The ACS must support both modes of disclosing physical communication channels towards the MCG: 1. All physical channels appear as a single channel. ACS provides an interface, where QoS requirements on the communication service can be dynamically defined by the MCG (including a high-level distribution strategy of bandwidth aggregation and improved reliability). 2. For failover capabilities, all physical links shall be directly accessible to the MCG.
CTA2-ACS-REQ-05	The ACS must provide appropriate interfaces for the MCG [38] to receive real-time feedback whether QoS requirements are met or violated and to receive notification upon establishment or loss of communication. The information provided by the interface shall include the number and kind of provided physical wireless links and quality information for diagnostic purposes. This shall include: 1. Polling of the information 2. Notification on change and 3. Cyclic information (adaptable cycle times)
CTA2-ACS-REQ-06	The ACS must provide suitable interfaces for the MCG [38] to enable and disable each provided physical wireless link. Reasoning: Need for active management of links due to limitation of free quota for wireless connections (4G/5G).

5. DETAILED SPECIFICATION OF THE WIRELESS TRAIN BACKBONE

The Wireless Train Backbone aims to remove the wiring used currently in train-level networks. The WLTB specification shall be able to work with legacy consist networks as well as with the NG-TCN defined in CTA D3.5 [06] and illustrated Figure 5. The presence of WLTB instead of ETB shall be transparent for end-device, acting for the consist network as a legacy ETBN.

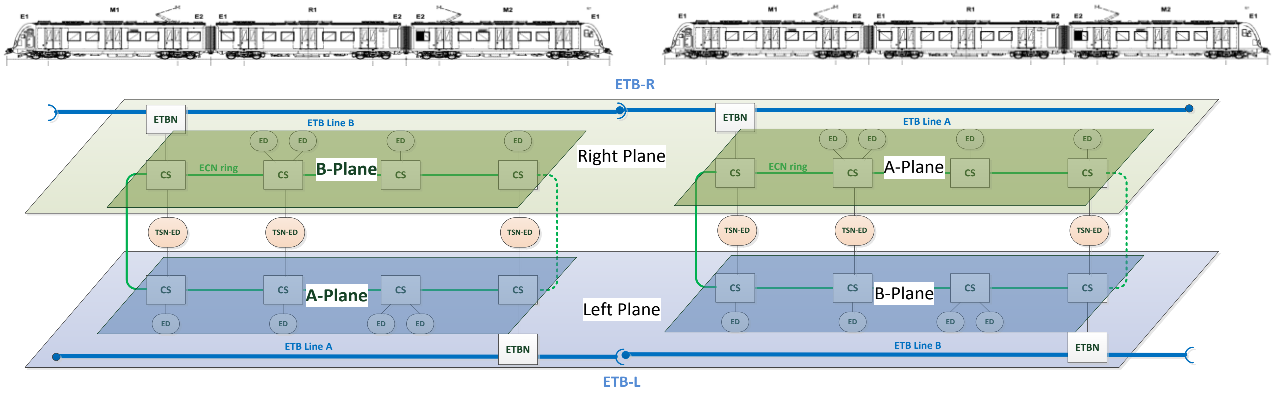


Figure 5: NG-TCN architecture

5.1.1 Prerequisites

Some requirements presented in section 4.1 introduce constraints for the design of the architecture of the Wireless Train Backbone. On the one hand, the latency should not exceed the maximum latency of three times the cycle time of the train functions. On the other hand, the WLTB should cover the reference train unit of the UIC 556 which may be composed of up to 22 vehicles and up to 32 train bus nodes with a maximum cable bus length of 850m [15].

Currently, two kind of train compositions are commonly in operation:

- Type A: a train unit with several single vehicle consists;
- Typer B: a train unit with 2-3 consists composed of 6-8 vehicles.

From the WLTB point of view, these two type of train units introduce different constraints. While Type A may require a radio technology capable to interconnect up to 32 nodes without mutual interferences, Type B may require lower number of nodes (i.e. two per consist).

5.1.2 Alternative topologies for WLTB architecture

In this section, different tentative topologies for the WLTB architecture are analysed, taking as a reference not only the requirements presented in section 4.1, but also the prerequisites explained in section 5.1.1.

Variant 1: Linear topology

The first alternative for the evolved WLTB is the linear topology. This architecture follows the same communication principle of the existing wired ETB where each consist can only communicate directly to its neighbours, communicating with the rest of consists through one of its neighbours (DIR1 neighbour or DIR2 neighbour). In order to create a linear topology for the WLTB it must be ensured that each consist side can only communicate with its direct neighbour. This can be ensured using directive antennas, association filtering, and/or dedicated frequencies, being these frequencies reusable by the alternation of frequencies along the composition (e.g. f_1-f_2-f_1-f_2-f_1).

The easiest way to create this topology is the substitution of the ETB lines by wireless links connected to existing ETBN.

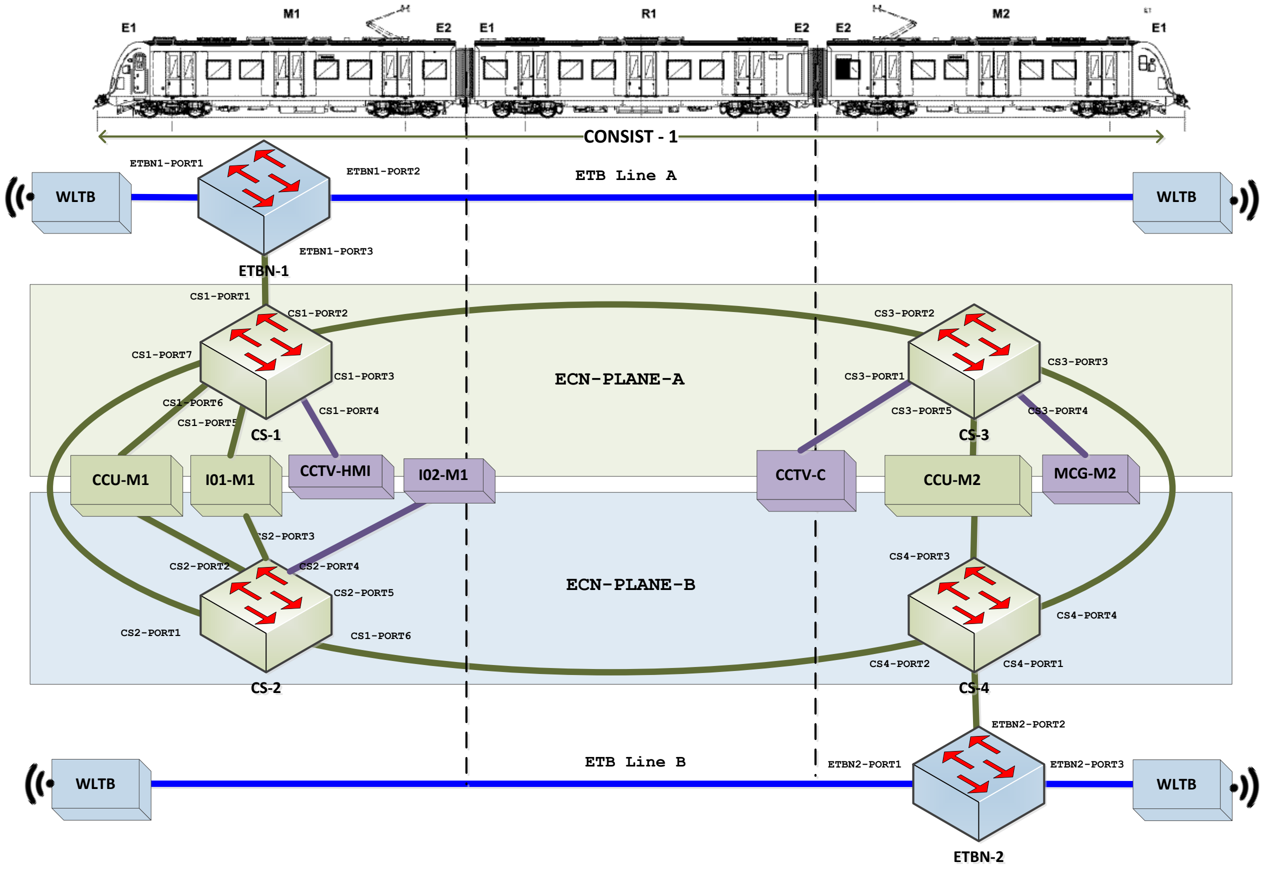


Figure 6: Linear topology[7]

One of the main advantages of this topology for the Wireless Train Backbone is the reuse of existing equipment in the market, being also applicable the existing train inauguration protocol. Moreover, if the wireless tunnels may be able to provide the same characteristics of the wiring proposed for the NG-TCN, the safe train inauguration should in principle be applicable to this topology.

The main disadvantage is the latency produced by this kind of topology. In effect, for train compositions with more than two consists, data packets must be forwarded by intermediates consists producing an additive delay in each hop. Therefore, in a composition with multiple hops to achieve destination and considering the minimum forwarding time for these wireless equipment could be around 1ms, the maximum number of consists to be supported by TCMS according to the IEC 61375[8] and maximum latency for time-critical functions could not be fulfilled together. The minimal latency that may be achieved with this topology can be expressed as the sum of the additive latency produced by the forwarding of ETB and WLTBN in each hop:

$$L = \sum L_{ETB} + L_{WLTB}$$

[7] Note that the Plan A/B division at ECN level is illustrative and out-of-the-scope of the definition of WLTB.

[8] The IEC 61375 defines a maximum of 32 consists (one ETBN in each consist).

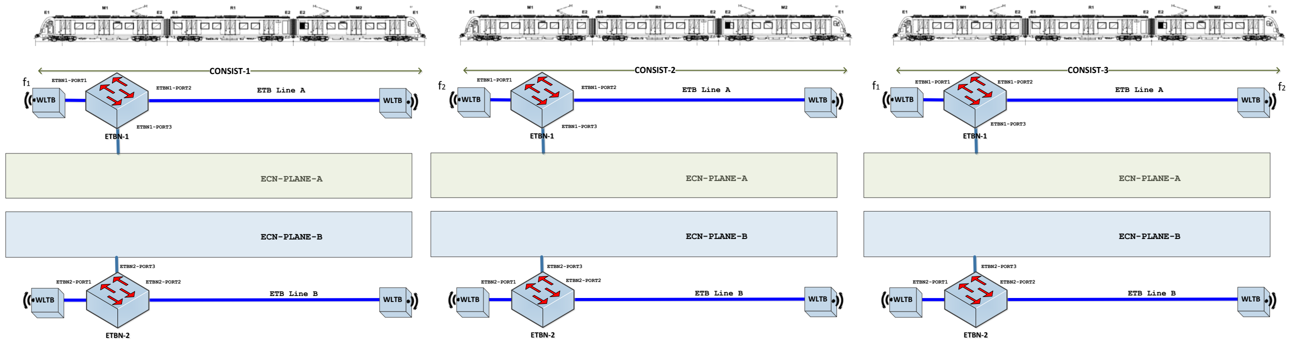


Figure 7: Linear topology (three consists example)

Moreover, this topology does not produce significant wiring redunction. In fact, it only substitutes the physical connectors by radio links, keeping the rest of the wiring for the train bus.

Variant 2a: Mesh topology

The second alternative for the WLTB architecture is based on a mesh topology in which all nodes of the wireless network can directly reach each other. Comparing to the linear topology, all consists can be reached in a single hop, therefore the end-to-end transmission delay will be significantly lower in compositions with a high amount of consists. However, this capability to directly reach all nodes implies that the total composition length is limited by the transmission/reception range of a node. This constraint could make difficult to reach train lengths of 850m [15]. The main limitations in this sense come from the maximum transmission power fixed by national regulatory authorities and the fading produced by railway environments, since CONNECTA D2.4 [16] demonstrated that the effective range in railway environments is less than 500m. Furthermore, fading may create lack of communication availability in certain situations reducing the reliability and availability of the system.

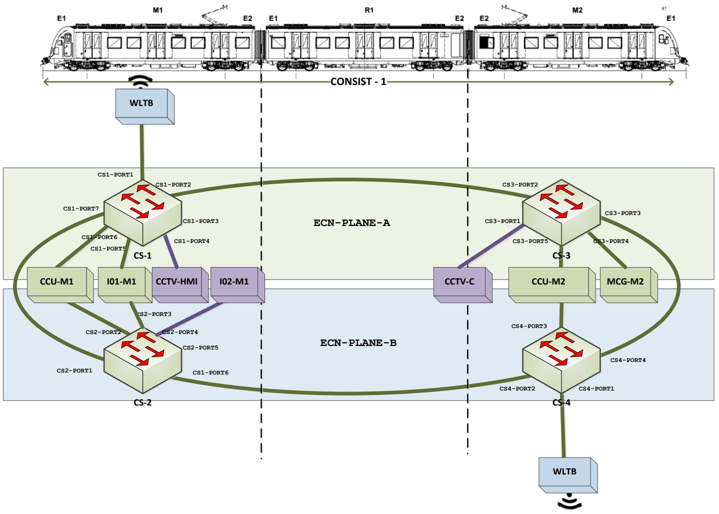


Figure 8: Mesh topology

Another significant drawback of this architecture is the incompatibility with the current train inauguration procedure. In fact, the nature of wireless medium, where all nodes are able to communicate directly with the rest and not only with the adjacent neighbours, avoids the use of a discovery protocol based on TTDP HELLO frames.

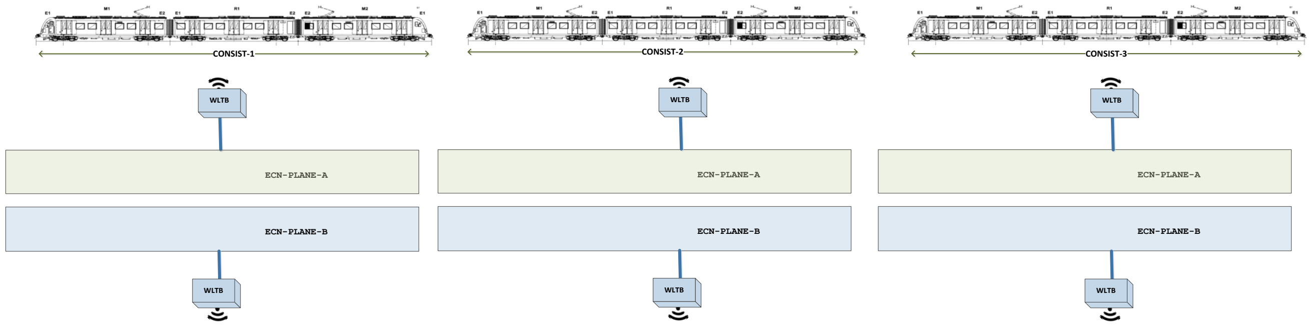


Figure 9: Mesh topology (three consists example)

Variant 2b: Mesh topology

This variant of mesh topology overcomes the problems to fulfil the train length of 850m and provides higher robustness against fading. In this variant not all consist communicate each other in a single hop, therefore when one consist wants to communicate with other consist out of its coverage, it transmits the data packet to its neighbours and these neighbours forwards the packet until it achieves its destination as depicted in Figure 10. Since all nodes do not communicate each other directly, the available spectrum may be divided in frequency blocks that may be reused along the train composition, providing higher spectrum efficiency while reducing interferences.

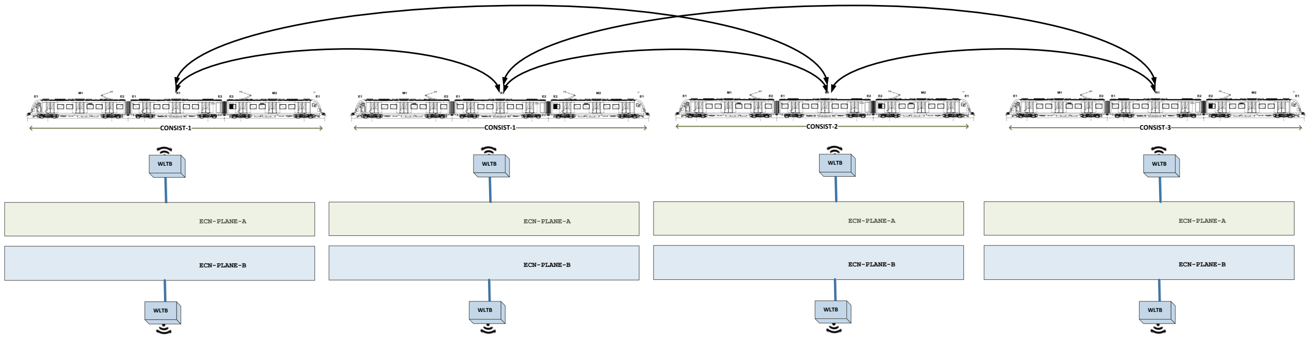


Figure 10: Mesh topology with multihop packet forwarding

In terms of delay, this architecture will introduce higher delay than the Variant 2a but significant less than the Variant 1, being a good trade-off between both approaches and allowing using the same architecture for both train unit types described in section 5.1.1.

The main drawback of this variant comparing to variant 2a is the complexity of introducing a forwarding/routing protocols needed to carry out the packet forwarding for nodes out of direct coverage. This protocol should prevent uncontrolled broadcast storms that could end in a complete loss of connectivity.

Conclusions

The Variant 1 is the most direct evolution from current ETB architecture. It allows removing the physical connectors between coupled consists, but it keeps the majority of the wiring. Additionally, it introduces an incremental latency per forwarding, preventing to use it in Type A train units.

The Variant 2a removes the latency problem of Variant 1 and removes completely the wiring of the train bus. However, it requires 850m-long radio range which is unrealistic in train-to-train communications.

The Variant 2b reduces the latency problem of Variant 1 to an acceptable delay. In this architecture, if each WLTBN has 250m-long range it may require 3 intermediate hops to reach the maximum allowed train length of 800m, which would be potentially far below of the maximum latency (e.g. 3 times 20ms of cycle time).

All in all, the most appropriate architecture for the WLTB seems to be the Variant 2b, since it covers all the needs covered by IEC 61375-1 and UIC 556 [15] without latency penalty. However, a new inauguration procedure will have to be defined for the WLTB.

5.1.3 Wireless Train backbone Node architecture

As it is illustrated in Figure 11, the WLTB shall be integrated in the NG-TCN in a transparent way for the ED and ED-S. As it is proposed for the NG-TCN for the ETB, the WLTB is duplicated in order to get better RAM values by redundancy. This redundancy is handled the same way as in wired NG-TCN, in fact one internal part of the WLTBN is an Adapted ETBN which acts for the ECN as a regular ETBN but adapting the inauguration procedure.

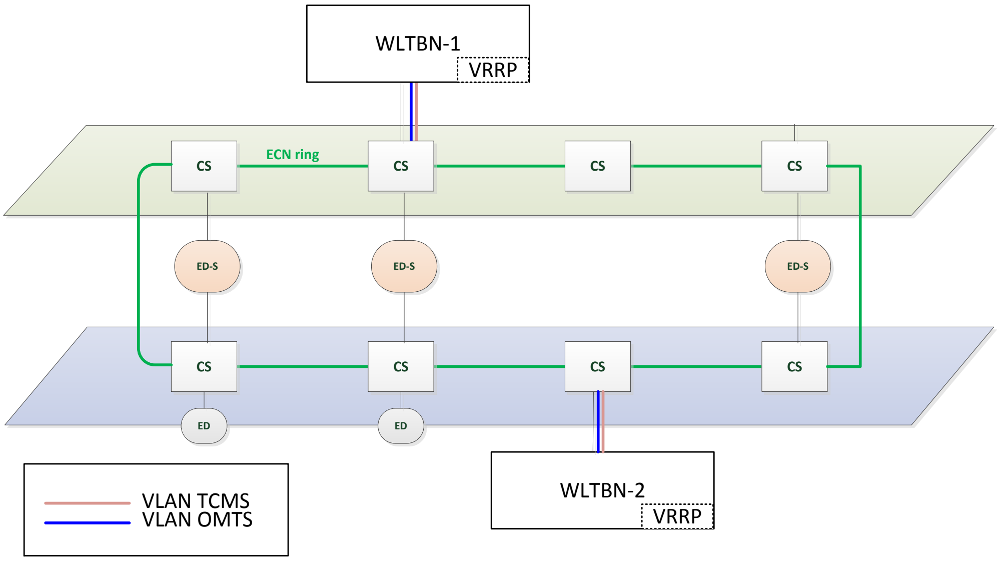


Figure 11: NG-TCN with WLTB

The following list defines the general functions to be covered by the WLTBN:

- The WLTBN should have a mechanism to discover adjacent WLTBNs.

- Only WLTBN participating in the same WLTB of the train composition should be able to communicate each other, excluding messages coming from other train units or other WLTB.
- The WLTBN participating in the WLTB should be able to create a local forwarding/routing table for the WLTBN which is not achievable with a single hop.
- The WLTBN should be able to exchange data with other WLTBN participating in the WLTB.
- The WLTBN should be able to carry out the Train Inauguration procedure resulting on a TTDB with low SIL level (e.g. SIL2).
- The WLTBN should integrate an ETB control service.
- The WLTBN should be able to transfer the TTDB safely to the CCU.

The WLTB consists of two functional blocks that can be placed in a single device or in different devices: an Adapted ETBN (AETBN) and the Radio Devices (RD). Figure 12 depicts the internal architecture of the WLTBN. In this figure there are two logical connections, orange and blue, which represents two connections for TCMS and OMTS domain respectively. These logical connections may be established with physical ports or with different VLANs, depending if the radio interfaces work in different devices or in a single one. In case this is made using VLANs, the VLANs used for TCMS and OMTS may be used. This radio split between TCMS and OMTS provides enough flexibility to overcome one of the problems detected in CONNECTA project's field tests which demonstrated that deterministic traffic cannot cover the data rate required by OMTS, but non-deterministic radio technologies, such as 802.11, can do it.

The main objective of this functional split is twofold. On the one hand, it allows locating railway-specific technologies and procedures, such as inauguration, in the Adapted ETBN, while connectivity functions can be served by COTS radio devices. On the other hand, this differentiation prevents to mix different lifecycles and evolution paces of telecommunication and railway industries.

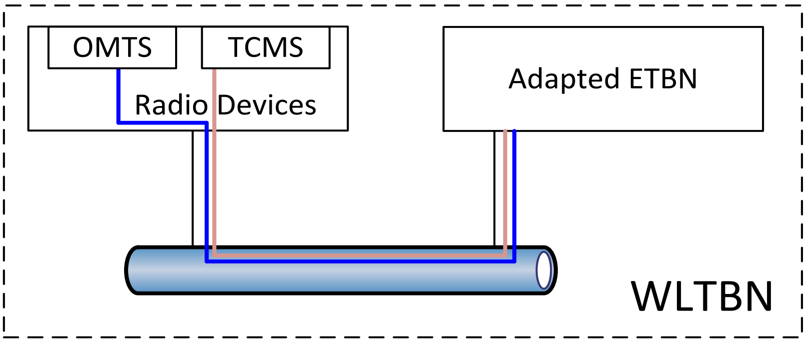


Figure 12: WLTBN internal architecture

From the logical train backbone perspective, this split in two networks, one for TCMS and another for OMTS, will be handled by having a WLTBN ID=0 for TCMS and WLTB ID=1 for OMTS (equivalent to ETB ID of the current standard IEC 61375-2-3. However, it is worth noting that the wireless safe train inauguration shall only take place on TCMS logical WLTB, i.e. WLTB ID=0, and other WLTB ID shall follow the computed result from TCMS logical WLTB's TTDB.

Function distribution

The functionalities of the WLTBN are divided between the RD and the AETBN.

Radio Devices (RD)

- The RD should have a mechanism to discover adjacent WLTBNs.
- Only RD participating in the same WLTB of the train composition should be able to communicate each other, excluding messages coming from other train units or other WLTB.
- The RD participating in the WLTB should be able to create a local forwarding/routing table for the WLTBN which is not achievable with a single hop.
- The RD should be able to exchange data with other WLTBN participating in the WLTB.
- CyberSecure network association
- CyberSecure data delivery

Adapted ETBN (AETBN)

- The AETBN should have a mechanism to discover adjacent WLTBNs.
- The AETBN should be able to exchange data with other WLTBN participating in the WLTB.
- The AETBN should be able to carry out the Train Inauguration procedure resulting on a TTDB with low SIL level (e.g. SIL2).
- The AETBN should integrate an ETB control service.
- The AETBN should be able to transfer the TTDB safely to the CCU[9].
- Safe Data Transmission
- Safe TTDB calculation

[9] To be agreed if this is needed in CTA2:WP3 "Safe Train Inauguration"

5.2 STATE OF THE ART IN WIRELESS COMMUNICATION FOR WLTB

This section aims to provide an analysis of the current state-of-the-art regarding the radio communications that has been identified as candidates for the WLTB. Furthermore, since the WLTB topology is based on mesh network with multihop forwarding capability, different potential candidate routing/forwarding protocols have been also identified.

5.2.1 Technology selection criteria

While evaluating the suitability of technologies to be adopted by the WLTB different indicators based on the requirements defined in section 4.1 have been used. On the one hand, the expected network performance in both domains at the train-level network has been considered. On the other hand, their suitability for the WLTB proposed architecture has been taken into account.

Table 25 shows the expected network performance identified by Roll2Rail project for the WLTB based on the current network uses, as well as the network performance expected by the NG-TCN. It is worth noting that the minimum requirements to be fulfilled are the ones which match with the current use. However, the requirements integrated by the NG-TCN are also considered in order to keep the functional compatibility of WLTB with the NG-TCN. Nevertheless, the data rates and latencies for NG-TCN are illustrative for future radio technologies since the specified values are not achievable by the current state-of-the-art.

From Table 25 it can be deduced that the radio technology to be adopted for the TCMS domain, with the current use, has an aggregated data rate requirements of 43 Mbit/s (30 Mbit/s / 70%)[10] with cycle times equal or higher than 20 ms and latencies equal or higher than 60 ms. Moreover, currently no TSN features are covered so the radio technology shall not have to cover this functionalities. Equally, for the OMTS domain, with the current use, has an aggregated data rate requirements of 50 Mbit/s (35.2 Mbit/s / 70%) with latencies equal or higher than 100 ms.

For future integration of the WLTB in the NG-TCN the requirements in terms of data rate, TSN features, latency and jitter are much more demanding. From Table 25 it can be deduced that the radio technology to be adopted for the TCMS domain, fully compatible with NG-TCN, has an aggregated data rate requirement of 240 Mbit/s[11] with cycle times equal or higher than 1 ms, latencies equal or higher than 15.92 ms and a jitter equal or higher than ± 1%. Equally, for the OMTS domain, there is an aggregated data rate requirement of 269.2 Mbit/s with latencies equal or higher than 100 ms. Additionally, the TCMS domain, according to NG-TCN requirements, shall have TSN features, meaning that the radio technology shall be deterministic, synchronized with a protocol compatible to IEEE 802.1AS-rev and able to handle traffic priorities in a compatible way to IEEE802.1Qav and IEEE802.1Qbv.

[10] This calculation is based on the CTA-D1.5-39 requirement defined in the section **¡Error! No se encuentra el origen de la referencia.**.

[11] The NG-TCN requirements already cover implicitly the CTA-D1.5-39 requirement defined in the section **¡Error! No se encuentra el origen de la referencia.** since it covers the future use.

Regarding the suitability for the proposed architecture the following requirements can be exported: equal or higher than 250 meters transmission range, mesh capabilities, group communication, frequency reuse capability and protection against EMIs.

Table 25: Train Network Performance Values (Sources: Roll2Rail Deliverable 2.1 and CONNECTA Deliverable 3.1)

SCOPE	DATA CLASS		DATA SIZE (octets)	DATA RATE NEED		CYCLE TIME		LATENCY [1]		JITTER	
				Current Use [2]	NG-TCN	Current Use [2]	NG-TCN	Current Use [2]	NG-TCN	Current Use [2]	NG-TCN
TCMS	Process Data	time sensitive	≤ 1432 [acc. IEC61375-2-3]	N/A	≤ 100Mbit/s	N/A	≥ 1 ms	N/A	$T_L = \sum T_{Sn}$ (Example: n=128 → T_L = 15.92ms)	N/A	± 1%
		normal	≤ 1432 [acc. IEC61375-2-3]	10Mbit/s	≤ 100Mbit/s	20ms	≥ 10 ms	Between 3CycleTime and 7CycleTime	$T_L = 2*\sum T_{Sn}$	N/A	± 50%
	Message Data		≤ 65388 [acc. IEC61375-2-3]	10Mbit/s	≤ 10Mbit/s	N/A	N/A	250ms	≤ 500 ms	N/A	Not relevant
	Supervisory Data		Not relevant	10 Mbit/s	≤ 10Mbit/s	Not relevant	50ms	250ms	$T_L = 2*\sum T_{Sn}$	N/A	Like process data (normal)
OMTS	Streaming Data	Audio	N/A	≤ 3.2 Mbit/s (100 Kbit/s audio channel, one per consist)		N/A	N/A	≤ 100 ms		N/A	For synchronized A/V Stream: ≤ 80ms difference (lipsynch); minimal jitter
		Video	N/A	≤ 32 Mbit/s 1 Mbit/s video stream [no needs for HD]	≤ 256 Mbit/s (one stream rear-/side-/internal view per consist 8Mbit/s video stream [HD])	N/A	N/A	≤ 500 ms	≤ 100 ms		
	BestEffort Data		≤ 4 GB	Not relevant	≥ 10Mbit/s	N/A	N/A	Not relevant		Not relevant	Not relevant

[1] Latency time TL in switched networks is a function of the number of switch hops (= n) and of the amount of interfering traffic, which is a quantity that can only be described by statistical methods. The values of this table are extracted from the calculations made for wired NG-TCN.

[2] Values obtained from industrial experience among Roll2Rail project members.

5.2.2 Wireless Access Technologies under evaluation

Within the radio technology evaluation for the WLTB, currently available (along the CONNECTA-2 project timing) five technologies have been evaluated, as well as two technologies that are being specified nowadays and could provide a significant improvement to the WLTB. Table 26 summarizes the analysis of these technologies made in collaboration with Safe4RAIL-2. The following output can be pointed out for the following technologies:

1. **LTE-V2X:** This technology makes use of the new Sidelink (SL) introduced by LTE ProSe in 3GPP release 12 and allows the direct communication between UEs in the vehicular scenario. LTE-V2X, defined in the 3GPP release 14 describes two operation modes; the mode 3 in which the eNodeB of the LTE network makes the radio resource scheduling for the SL; and the mode 4 (ad-hoc) in which the UE implements a Listen-before-Talk and Semi-persistent scheduling. This technology allows up to 27 Mbps data rate and 50-100ms latency, therefore it does not fulfil the requirements for the TCMS domains, neither for OMTS domain. By contrary, it fulfils the transmission range requirements and the possibility of working in mode3 and mode 4 allows its use in busy scenarios, i.e. busy junctions, train stations or depots, with a radio scheduling provided by the LTE network and therefore having a collision-free deterministic performance.

2. **ITS-G5:** This technology provides similar functionalities than LTE V2X but over Wi-Fi (similar to IEEE 802.11p), allowing device-to-device communications for transport domain. It has been promoted by the ETSI and has its equivalence for USA, DSRC. It also provides a data-rate up to 27 Mbps, but comparing to LTE-V2X it gets latencies from 1-20 ms. However, unlike LTE-V2X, ITS-G5 does not provide any mode with a radio scheduling that may allow deterministic behaviour.

3. **Wi-Fi:** This well-known technology is specified by IEEE 802.11 series. The data-rate and latency varies depending on the version implemented in the physical layer, e.g. 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, or 802.11ax. Generally it allows data-rates up to 2.4 Gbps and latencies from 1-20 ms. It has no deterministic behaviour and it may provide device-to-device communication implementing the 802.1s which modifies the MAC layer.

4. **VLC:** Visible Light Communication is a wireless communication system in which the signal is produced by light emitting diode (LED). According to the analysis made by Safe4RAIL-2 D2.2 this technology may achieve data-rates up to 60 Mbps, latencies from 20-40 ms and transmission range up to 20 m. However, recent studies presented in the WCRR2019 [27] saw data-rates up to 100 Mbps using this technologies in the couplers, this is in scenarios with very short distances.

5. **BLE:** Bluetooth Low Energy (BLE) was introduced in 2006 in order to reduce the energy consumption of Bluetooth. Among other modifications, this technology removes the Master-Slave pairing of Bluetooth and substitutes it by a new “advertising channel” which in fact allows its use in mesh and multi-hop scenarios. This technology only achieves up to 2 Mbps data-rate and latencies from 50-100 ms. However, it provides high robustness due to the frequency hopping implemented by default and it provides deterministic behaviour.

6. **IEEE 802.11BD:** This technology is being specified as an evolution of IEEE 802.11p and it integrates all the improvements available in IEEE 802.11ax. This technology provides much higher data-rate and although it still does not provide deterministic behaviour it may provide it if the recently started studies regarding the compatibility of IEEE TSN and IEEE 802.11 succeed. It provides mmWave support and therefore possibility to have strong directional beamforming increasing the protection against EMIs.

7. **NR V2X:** This technology is the evolution of LTE V2X technology which profits of 5G features, this is Ultra Reliable Low Latency and high data rate. At the timing of writing this deliverables the final data-rates and latencies provided by NR V2X are not clear but considering it will work over 5G the data rate may arrive up to Gbps and latencies between 1-20 ms. Additionally, will provide different operation modes, multicast/group support in one of them and mmWave support.

From the previous analysis it can be concluded that none of the existing radio technologies satisfy completely the TCMS domain. By contrary, the requirements of OMTS domain may be satisfied in theory by IEEE 802.11s. In the future, once the specification is finished (probably by the end of 2019) and first devices commercially available appear (expected to 2025), NR V2X seems to be the most appropriate technology to satisfy the WLTB requirements. On the one hand, the different operation modes allow the integration with 5G networks, relaying on the scheduling assisted by the network in scenarios, where many nodes may be transmitting and competing for the radio resources. On the other hand, the trend in the railway domain towards the adoption of 5G technology fits perfectly in order to use the same technologies for train-to-ground, train-to-train and eventually train-to-vehicle/pedestrians.

Since the NR V2X is not available currently and will not be available within the time frame of Shift2Rail, CONNECTA-2 will investigate, together with Safe4RAIL-2, the adoption of LTE V2X with improved functionalities coming from LTE D2D, such as Service Discovery (in order to discover UEs corresponding to the same train composition), Group Communications (in order to discard communications from other train compositions), all of them expected to be part of NR V2X. Additionally, the protocol stack will be modified in order to add multi-hop forwarding support. These investigations will help to evaluate the functional suitability of NR V2X although the performance would not be evaluated yet.

Table 26: Wireless Technology Comparison for the WLTB radio (source Safe4RAIL-2 Deliverable 2.2)

		WIRELESS TECHNOLOGIES						
REQUIREMENTS		***LTE-V2X***	***ITS-G5***	***Wi-Fi***	***VLC***	***BLE***	***DOT11BD***	***NR V2X***
Max. Bit rate	100 Mbps per traffic type	27 Mbps	27 Mbps	(1) <2.4 Gbps (2) <6.5Gbps (mmWave)	LED dependent up (2Mbps-60Mbps)	up to 2Mbps	*estimation*: (1) <2-3Gbps (2) <20Gbps	*estimation:* (1) <2-3Gbps (2) <20Gbps
Max. Latency	16-500ms	50-100ms	1-20ms	(1) 1 - 20ms (2) 5-250ms	20-40ms	50ms-1000ms	*estimation*: (1) 1 - 20ms (2) 5-250ms	*estimation:* *prob. 1 - 20ms*
Medium Access	Deterministic	Mode 3: Deterministic ; Mode 4 Non-Deterministic	Non-Deterministic	Non-Deterministic	Non-Deterministic	Deterministic	Non-Deterministic	Non-Deterministic & Deterministic
Communication Range	up to 820m	300m-1000m	300m-1000m	(1) > 200m (2) < 2m	5m-20m	50m-200m	*estimation:* <1000m	*estimation:* <1000m
Group Communication	Multicast/Group	-	-	(2) DOT11y	-	Clustering	Multicast/groupcast	clustering (mode 2(d))
Mesh Capabilities	up to 32 nodes	-	Geonet/1609.3	DOT11s	-	inter-cluster	Geonet/1609.3	-
Freq. reuse	1 / car	2-3	-	ISM, mmWave	Directional	ISM	Carrier aggregation (Mx10Mhz)	mmWave
Protect. against interferences	-	-	-	(1) DSSS+Freq Hopping (2) BeamForming	Beam Forming	Freq. Hopping	BeamForming	BeamForming

Note 1: General assumptions for each technology (frequency band, environment (LOS/NLOS), evaluation methodology,..) are described in the cited papers.

Note 2: Performance of VLC technologies are assumed in a vehicular context and strongly depend on the receiver LED and modulation.

Note 3: The required WLTB communication range includes optional multi-hop forwarding.

5.2.3 Routing/Forwarding protocols under evaluation

The ad-hoc routing and forwarding protocols can be divided in two groups: stateless and state-full protocols.

The protocols of the first group have no knowledge about the network and it has to find the route to destination every time that they do have to send a message. This kind of behaviour is highly suitable for networks where the nodes change continuously their position or where they just add and quit from the network randomly. This is the case of automotive scenario in which the cars to be connect to may change from one message delivery to the next one. However, this behaviour is obviously extremely inefficient since it has a significant penalty in terms of transmission delay and communication channel use efficiency.

By contrary, the stateful protocols keep the notion of the network and they care to update the network state periodically. This is, with these protocols a node knows how to reach the destination before starting sending the message and it knows that the network will remain as it is unless the state is updated. This kind of protocols are the most suitable for the WLTB because although there is a mobile ad-hoc scenario, the nodes involved in the WLTB remain in the same relative position with respect of their neighbour nodes until the train composition changes. Within the existing stateful Ad-Hoc protocols, the following have been evaluated:

- **Optimized Link State Routing (OLSR):** This protocol is widely used in ad-hoc networks. The main disadvantage is that it is a routing protocol working in OSI L3. This limit the reuse of many inauguration functions existing in ETBNs where the topology frames are shared in OSI L2 and the IP addressing is the result of the Operational Train Inauguration.

- **Hybrid Wireless Mesh Protocol (HWMP or IEEE 802.11s):** This protocol is an amendment to Wi-Fi, where Wi-Fi Access Point/Mobile Node have the capabilities to provide OSI L2 multi-hop networking between each other. It is similar to OSLR but adapted to handle MAC addresses instead of IP addresses and operating on a wireless OSI L2 link.

- **Better Approach To Mobile Ad-hoc Networking (B.A.T.M.A.N.):** This protocol takes also many concepts from OLSR. However, comparing to OLSR, it only keeps the state information over 1-hop only instead of the whole network. Moreover, comparing to OLSR it works in OSI L2.

- **Advanced On-Demand Distance Vector (AODV):** The AODV protocol is also a well-known multi-hop routing protocol. It is the routing protocol used in Zigbee. Unlike OLSR, AODV only build multi-hop routes on-demand, minimizing the overhead to maintain the overall state at the cost of a route establishment delay.

From the evaluated candidates, the most suitable protocols are B.A.T.M.A.N and HWMP. Regarding the literature, the first one obtains better performance so it has been selected for WLTB. However, within CONNECTA-2 laboratory tests of B.A.T.M.A.N and HWMP will be implemented and compared in the OMTS domain due to the relatively easy of integration of both of them over Wi-Fi.

5.3 Interface specification for WLTB

5.3.1 General

According to the architecture described in section 5.1.3, the WLTBN is connected to the Consist Network via Ethernet wired connection and to other consists (i.e. to other WLTBNs) using a wireless connection. The interfaces of the WLTBN are depicted in Figure 13.

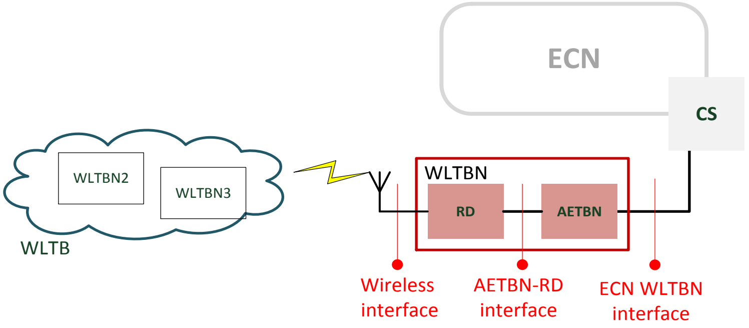


Figure 13: WLTBN interfaces

In many aspects the WLTBN can be seen as an evolution of the IEC 61375-2-5 2014 in which the ETBN is adapted in order to be compatible with a wireless interface to connect with other consists. This wireless interface is a new feature, which has not yet been defined in the IEC 61375 standard.

5.3.2 Inter-consist TCMS interface between radio devices

This interface is a radio link between the RD of one consist and the RD of other consist for TCMS domain. This interface is based on LTE-V2X nowadays and tentatively it will have to be upgrade to 5G NR V2X once it is fully available. The interface used in the demonstrator has been defined with the tight collaboration of Safe4RAIL-2 project and includes additional functionalities on top of LTE-V2X.

The main characteristics of this interface are listed in Table 27

Table 27: Characteristics of Inter-consist radio interface for TCMS domain

OSI Layer	Interface features
1 and 2	Radio link according to LTE-V2X (3GPP release 14)
2	Wireless L2 forwarding protocols • B.A.T.M.A.N-adv Wireless security based on secure password-based authentication and key establishment protocol Simultaneous Authentication of Equals (SAE), RFC 7664.

Physical Layer

Frequency

At the time of writing this document it is not clear which frequency band could be available for the WLTB. On the one hand, this system may use ISM bands, however this may involve interferences with other system. Considering the TCMS domain is used to exchange information between train control systems, some of them safety critical, these interference would imply operational availability problems. On the other hand, dedicated band may be used, but nowadays no band has been reserved for this system. Tentatively, and always depending on national regulation and operator willingness to use these bands for this system, the following band could be under the scope in Europe:

- ITS non-safety band 5.855-5.885GHz
- ITS safety band 5.905-5.925GHz dedicated to safety urban rail applications
- Current GSM-R bands
- Future NR V2X bands
- Future new FRCMS bands

Transmission power

According to the distance between the communication partners, the transmission power may be adjusted, providing that the values requested to obey the local regulations are not exceeded. Moreover, depending on the frequency band used and the country in which it is used, the maximum transmission power varies.

According to the ETSI Harmonized Standard EN 302 663, any transmitter for ITS operations in 5.9GHz, any tx device must follow the radiation and spectrum specifications of the ETSI Harmonized Standard EN 302 571.

Additionally, the maximum transmit power is fixed as in Figure 14. The 3GPP LTE V2X rel. 14 shall follow these regulations.

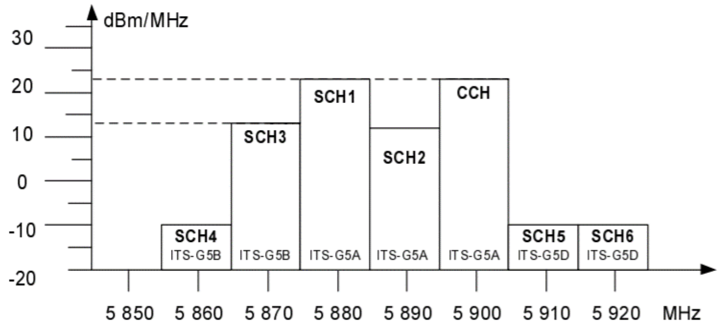
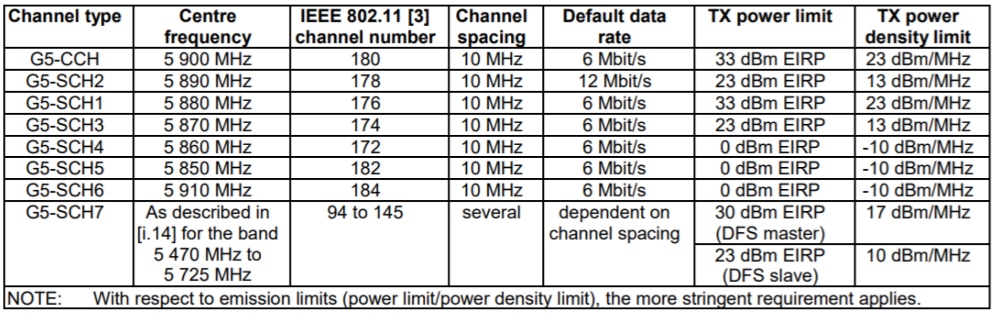


Figure 14: Transmit Power Density Limits ITS channel (source: ETSI EN 302 663)

Considering the WLTB operating on ITS frequency bands, the maximum Transmit limit will be set either as 33dBm EIRP or 23dBm EIRP. However, considering the WLTB operating in mesh topologies, the effective transmit power will be adjusted to maximize the frequency reuse.

Modulation

According to EN 302 663, the default modulation for ITS band (see Figure 15) is 6Mbps, except for the SCH2 having 12Mpbs (considering a reduced Tx power and very short transmit range). The 3GPP LTE V2X rel. 14 reaches 6Mbps for the MCS 6 QPSK ½ (0.48). Considering that LTE-V2X operates in broadcast without HARQ, and considering WLTB will not have a service overlay, the default modulation will be used.



Channel type	Centre frequency	IEEE 802.11 [3] channel number	Channel spacing	Default data rate	TX power limit	TX power density limit
G5-CCH	5 900 MHz	180	10 MHz	6 Mbit/s	33 dBm EIRP	23 dBm/MHz
G5-SCH2	5 890 MHz	178	10 MHz	12 Mbit/s	23 dBm EIRP	13 dBm/MHz
G5-SCH1	5 880 MHz	176	10 MHz	6 Mbit/s	33 dBm EIRP	23 dBm/MHz
G5-SCH3	5 870 MHz	174	10 MHz	6 Mbit/s	23 dBm EIRP	13 dBm/MHz
G5-SCH4	5 860 MHz	172	10 MHz	6 Mbit/s	0 dBm EIRP	-10 dBm/MHz
G5-SCH5	5 850 MHz	182	10 MHz	6 Mbit/s	0 dBm EIRP	-10 dBm/MHz
G5-SCH6	5 910 MHz	184	10 MHz	6 Mbit/s	0 dBm EIRP	-10 dBm/MHz
G5-SCH7	As described in [i.14] for the band 5 470 MHz to 5 725 MHz	94 to 145	several	dependent on channel spacing	30 dBm EIRP (DFS master)	17 dBm/MHz
					23 dBm EIRP (DFS slave)	10 dBm/MHz
NOTE: With respect to emission limits (power limit/power density limit), the more stringent requirement applies.						

Figure 15: European Channel Allocations for ITS

Antenna

In order to guarantee the communication performances, the specifications of the antenna should support MIMO for the used radio bands. The antenna shall be approved according to railway standards (EN 50155, EN 45545-2 and EN 50125-3) and IP 66/ IP 67.

The maximum allowed radiated power depends on the used frequency range and shall conform to local regulations. In Europe, 33dBm EIRP will be used for CCH and SCH1, and 23dBm EIRP for SCH2 as defined by EN 302 663.

These values of the overall radiation power shall not be exceeded by the gain of the antenna.

Hardware Sensitivity level and out-of-band emissions:

For radio hardware operating at ITS frequency band, the specifications of the Harmonized Standard EN 302 571 must be enforced. The LTE V2X hardware used for the demonstrator follow these requirements. In particular, a minimum sensitivity limit of -82dBm will be set.

Antenna Cables

In order to guarantee the communication performances, the specifications of the antenna cables shall have an impedance of 50 Ohm and be usable for the LTE (3GPP) frequency bands.

Connectors

Common connectors for antennas shall be used. This includes the following types:

- SMA, RP-SMA
- QMA
- N
- QN (QLF)

Data Link Layer

ARQ

ARQ will not be used for the WLTB (LTE V2X rel. 14 does not support it).

PDU (Frame format)

The PDU will consist of the LTE V2X header encapsulating the WLTB L2 packet. According to LTE V2X specifications for MCS 6, subchannels are multiple of 190 Bytes. Accordingly, WLTB L2 PDUs will have to be padded to match a multiple of 190 Bytes.

MAC Addressing

48 bits MAC addresses will be used. The WLTB Radio device MAC address will be built from the LTE V2X NIC.

L2 forwarding protocol

Packet forwarding will be performed by B.A.T.M.A.N. Advanced (operating in L2). B.A.T.M.A.N will transmit OriGinator Message (OGM) in order to allow WLTB nodes to be discovered by other WLTB nodes. OGM may be relayed over multiple hops. In order to mitigate channel overflowing and traffic congestions, OGM relaying will be limited to the expected number of consists.

According to B.A.T.M.A.N internal rules, a packet will be forwarded to the best mesh 1-hop relay for the target destination WLTB node. In addition to OGM, other link quality management packets will be used to provide additional link quality information.

QoS (Priorities)

LTE V2X uses 8 ProSe (Proximity Services) Per Packet Priorities (PPPP), the lowest PPPP being the most urgent, while the highest PPPP being the less critical. Ethernet also uses 8 priority levels. Accordingly, a one-to-one mapping between L2 prioritization and the LTE V2X PPPP will be applied.

Clock synchronization

The WLTB Radio Device will have its own clock synchronization mechanism, independently to the AETBN.

Under UTRAN coverage, the eNodeB will provide clock synchronization for the WLTB RD (LTE V2X mode 3). In off-network scenario (LTE V2X mode 4), WLTB RD will synchronize among each other. Synchronization among WLTB RD will be provided by LTE V2X specific signals. WLTB RD will try to select a SyncRef UE. If none is found, it will become the SyncRef UE. The SyncRef UE will send a LTE V2X specific signal 'SLSS' over the LTE V2X sidelink broadcast channel. Any WLTB RD not having themselves a SyncRef UE will adopt the timing indicated in the SLSS message of the SyncRef UE.

Considering that LTE V2X SyncRef UEs are selected mostly considering wireless link reliability, it is unlikely that the WLTB RD being the SyncRef UE would also be the AETBN synchronization entity. Accordingly, both synchronization systems should be kept separately.

Traffic scheduling – Media Access Control

3GPP LTE V2X (rel. 14) in mode 4 is based on a Listen-Before-Talk MAC scheduling. WLTB RD shall first listen and measure the Reference Signal Received Power (RSRP) on the wireless channel. As depicted in Figure 19, a WLTB RD must first sense the wireless channel for a 1 second sensing period, and then it will select wireless resources within a 100ms selection window. A WLTB RD may only select wireless resources within that window having a RSRP lower than a target threshold. Accordingly, near-far problems may cause packet collisions between different WLTB RD.

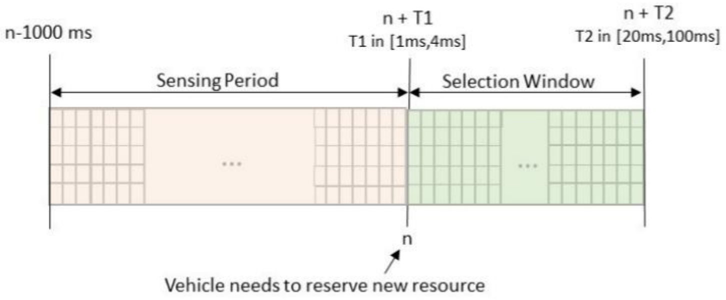


Figure 16: LTE V2X sensing and resource selection procedure

The LTE V2X (rel. 14) in mode 4 uses a Semi-Persistent Scheduling approach particularly tailored for periodic type communications. Resources may be reserved for 1, 3, 5, and 7 potential transmissions, before a LBT reselection must be performed. However, SPS on a LBT strategy may also increase potential collisions over multiple transmissions unless a LBT reselection is performed.

Train backbone topology discovery

The Train backbone topology will be discovered through the B.A.T.M.A.N. L2 Mesh protocol relying on broadcast originator messages (OGM).

Security aspects

3GPP LTE V2X does not provide any form of security, and relies on higher layers for securing the WLTB link. Accordingly, the WLTB link will protected by the Secure Password-based Authentication and Key Establishment protocol Simultaneous Authentication of Equals (SAE), according to RFC 7664.

5.3.3 Inter-consist OMTS interface between radio devices

This interface is a radio link between the RD of one consist and the RD of other consist for OMTS domain. This interface is based on Wi-Fi and more specifically in IEEE 802.11s.

The main characteristics of this interface are listed in Table 27

Table 28: Characteristics of Inter-consist radio interface for OMTS domain

OSI Layer	Interface features
1 and 2	Radio link according to IEEE 802.11 a/b/g/n/ac/ax (Wi-Fi, 2.4/5 GHz)
2	Wireless security based on secure password-based authentication and key establishment protocol Simultaneous Authentication of Equals (SAE), RFC 7664. Wireless L2 forwarding protocols • B.A.T.M.A.N-adv • HWMP

Physical Layer

The Physical Layer of a RD for OMTS domain shall conform to IEEE 802.11 a/b/g. Recommended is a conformance to IEEE 802.11 n/ac/ax which supports MIMO.

Transmission power

According to the distance between the communication partners, the transmission power may be adjusted, providing that the values requested to obey the local regulations are not exceeded.

For Wi-Fi an emission power of 100 mW is identified [17].

Frequency

In order to avoid interference between WLTB OMTS domain and other external communications using the same ISM band, RD will provide several alternative radio frequencies. Table 33 lists channels and frequencies used by this domain. In case that the frequencies are conflicting with the regulations of the radio administration authority, the operator applies for alternative frequencies compliant with such regulations.

Modulation

The modulation of the radio depends on the used protocol. Refer to Table 33 for the different Wi-Fi modulations.

Antenna

In order to guarantee the communication performances, the specifications of the antenna should support MIMO, 2,4 GHz band and 5 GHz band. The antenna shall be approved according to railway standards (EN 50155, EN 45545-2 and EN 50125-3) and IP 66/ IP 67.

The maximum allowed radiated power depends on the used frequency range and shall conform to local regulations.

These values of the overall radiation power shall not be exceeded by the gain of the antenna.

Antenna Cables

In order to guarantee the communication performances, the specifications of the antenna cables shall have an impedance of 50 Ohm and be usable for the Wi-Fi frequencies.

Connectors

Common connectors for antennas shall be used. This includes the following types:

- SMA, RP-SMA
- QMA
- N
- QN (QLF)

Data Link Layer

A RD of OTMS domain may support the MAC modification according to IEEE 802.11s. This device shall also support security based on secure password-based authentication and key establishment protocol Simultaneous Authentication of Equals (SAE) defined in the RFC 7664.

5.3.4 Interface between Adapted ETBN and Radio Devices

Physical Layer

The physical layer is in accordance to the IEC 61375-2-5:2014 Table 3.

Security aspects

The AETBN, the RD and their cabling shall be in protected locked cabinets that cannot be accessed by not authorized person. Unused AETBN ports shall be disabled to prevent from unforeseen connections.

Data Link Layer

The physical layer is in accordance to the IEC 61375-2-5:2014 Table 4.

5.3.5 Interface between Adapted ETBN and consist network

Physical Layer

The physical layer is in accordance with the IEC 61375-3-4:2014 Subclause 4.9.4. To increase the bandwidth the standard allows using 1000BASE-T. However, the standard does not provide more precise information on protocols, cables, and connectors. The missing information is added in this document.

Security aspects

The AETBN, the RD and their cabling shall be in protected locked cabinets that cannot be accessed by not authorized person. Unused AETBN ports shall be disabled to prevent from unforeseen connections.

Data Link Layer

The data link layer is in accordance with the IEC 61375-3-4:2014 Subclause 4.9.5.2, 4.10.3 respectively.

Redundancy management

AETBN should be compliant with VRRPv3 in order to handle WLTBN redundancy.

Network Layer

IP addressing

The AETBN has at least two interfaces, one connected to the RD which has a train-level IP address and another connected to the ECN, which has an ECN IP address. Both IP addresses shall be unique in WLTB and ECN respectively. For the WLTB addressing the scheme described in IEC 61375-2-5 for ETB will be used, while for ECN the IEC 61375-3-4 will be used.

Railway-Network Address Translation (R-NAT)

IP addresses must be unique within an ECN, however, different ECNs may use the same address space. In order to have a unique IP addresses, ECN range addresses are translated to train range addresses when transmitting over the WLTB using the R-NAT. The algorithm for this translation is specified in IEC 61375-3-4. As the train wide addressing may change after inauguration, the ETBN shall be automatically reconfigured after inauguration process.

IP to MAC address resolution

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

IP routing

The AETBN shall handle the IP routing between ETB and ECN. The routing process differs slightly between IP unicast routing and IP multicast routing. While unicast traffic is translated using R-NAT, in multicast traffic destination addresses are not translated but each AETBN shall configure for all train-wide multicast groups the related consist local source devices.

ICMP

ICMP as defined in IETF RFC 792 shall be supported.

Transport Layer

At transport layer TCP and UDP shall be supported. While TRDP PD will use UDP, TRDP MD may use UDP or TCP.

Application Layer

The following function shall be supported by AETBN as service provided to the ECN:

- ETB Inauguration:
    - Discover the ETB topology and generate the train network directory (TND).
    - Inhibit train inauguration on demand.
    - Indicate train lengthening/shortening.
- Operational Train Inauguration:
    - Compute the TTDB after train composition change or after train leadership change.
- TTDB Info service:
    - Provide ED interface for retrieving TTDB information.
- ETB Control Service as specified in IEC 61375-2-3:
    - Provide ED interface for informing about AETBN state, set/reset leading, inhibition, train composition confirmation/correction and sleep control.
- TND Info Service:
    - Provide ED interface for retrieving TND information as specified in IEC61375-2-5.
- DNS server interface (Standard & TCN):
    - Provide mapping between TCN-URI and IP address.

5.4 Implementation requirements for Wireless Train Backbone Node

This section introduces the low level requirements needed for WLTBN implementation. These requirements are the breakdown of the requirements described in section 4.1.5, taking into account the detailed specification of the Wireless Train Backbone done in section 5. Since the set of requirements have been elaborated in narrow collaboration with Sfae4Rail-2 project, each CTA2 requirement ID has been linked to its corresponding S4R2 requirement ID [20].

5.4.1 Implementation requirements for Adapted ETBN

The implementation requirements needed for the AETBN deployment and been used in the CONNECTA-2 urban demonstrator are listed in Table 29.

Table 29: Implementation requirements for the AETBN

Req ID	Description	S4R2 Req ID [20]
CTA2_AETBN_001	The AETBN should provide at least 3 Ethernet ports following IEEE 802.3 with · 2 ports GbE for WLTB connection · 1 port GbE for ECN connection Note: 100Mbps may be sufficient for WLTB connection	DBD_ND_001
CTA2_AETBN_002	The WLTBN ports shall support the reception and transmission of Ethernet frames in accordance to IEEE 802.3	DBD_ND_002
CTA2_AETBN_003	The AETBN shall support adding, recognizing, interpreting, and removing VLAN tags as defined in IEEE 802.1Q.	DBD_ND_006
CTA2_AETBN_004	The AETBN shall provide 8 output queues per port, each allocated to one traffic class 1..8.	DBD_ND_007
CTA2_AETBN_005	The AETBN shall support strict priority-based transmission selection algorithm (IEEE 802.1Q)	DBD_ND_008
CTA2_AETBN_006	The AETBN shall act as a router between ECN and WLTB for unicast and multicast IP packets including network address translation	DBD_ND_012
CTA2_AETBN_007	The AETBN shall support the Internet protocol suite including · IP (RFC 791) · ARP (RFC 826) · UDP (RFC 768) · TCP (RFC 793) · ICMP (RFC 792)	DBD_ND_013
CTA2_AETBN_008	The AETBN shall support TRDP according IEC 61375-2-3	DBD_ND_014
CTA2_AETBN_009	The AETBN shall support SDTv2 according IEC 61375-2-3	DBD_ND_015
CTA2_AETBN_010	The AETBN shall provide train backbone topology discovery according IEC 61375-2-5 with modifications defined in section 8.	DBD_ND_016
CTA2_AETBN_011	The AETBN shall provide train composition discovery according IEC 61375-2-3 with modifications defined in section 8.	DBD_ND_017

Req ID	Description	S4R2 Req ID [20]
CTA2_AETBN_012	The AETBN may support sleep mode according IEC 61375-2-3	DBD_ND_018
CTA2_AETBN_013	The AETBN shall implement an ECSP according IEC 61375-2-3 with modifications defined in section 8.	DBD_ND_019
CTA2_AETBN_014	The AETBN shall implement a TTDB which is managed by a TTDB Manager function	DBD_ND_020
CTA2_AETBN_015	The AETBN shall support resolving TCN-URI addresses (IEC 61375-2-3) to IP addresses	DBD_ND_021
CTA2_AETBN_016	The AETBN shall provide service interfaces according IEC 61375-2-3 annex E: · ECSP interface · TTDB manager interface (ECSP and ED) · DNS server interface (Standard & TCN) · ETBN control interface Note: In order to be able to retrieve the TTDB from one WLTBN to another, as explained in section 8.	DBD_ND_022
CTA2_AETBN_017	The AETBN shall support IGMP snooping	DBD_ND_023
CTA2_AETBN_018	The AETBN should support a DHCP server	DBD_ND_024
CTA2_AETBN_019	The AETBN shall support SNMP.	DBD_ND_025
CTA2_AETBN_020	The AETBN may provide an authentication server (IEEE 802.1x).	DBD_ND_026
CTA2_AETBN_021	The AETBN shall support detection and reporting of security events	DBD_ND_027
CTA2_AETBN_022	The AETBN shall support device redundancy with switch-over time of ≤ 0.8 s.	DBD_ND_028
CTA2_AETBN_023	Each WLTB shall be scalable up to 32 AETBN (64 in total in 2xWLTB).	DBD_ND_029
CTA2_AETBN_024	The wireless safe train inauguration should have 2 physical WLTBs for availability reasons.	WLTB-AETBN-001
CTA2_AETBN_025	Each ECN shall be connected to two WLTB via two AETBNs.	DBD_ND_030
CTA2_AETBN_026	One AETBN shall connect ECN to one physical WLTB. Note: Each AETBN is connected to one of the two physical WLTBs and to ECN.	DBD_ND_031
CTA2_AETBN_027	NG TCN shall transfer non-TSN data between ECNs on one physical WLTB. Note: Link aggregation is not used.	DBD_ND_032
CTA2_AETBN_028	The 2 physical WLTBs shall inaugurate separately and each of the physical WLTB shall compute its own TTDB	WLTB-AETBN-002

Req ID	Description	S4R2 Req ID [20]
CTA2_AETBN_029	After the inauguration is done, by comparing the two TTDBs from each physical WLTB, a common TTDB will be computed and provided to CCU Note. Theoretically, the TTDBs would be the same if no failure occurs	WLTB-AETBN-003
CTA2_AETBN_030	One physical WLTB shall be able to run different train application on different logical WLTBs, and each of the logical WLTB shall use different WLTB ID e.g. Physical WLTB 0 with 2 logical WLTBs with TCMS (ID 0) and OMTS (ID 1) Physical WLTB 1 also with 2 logical WLTBs with TCMS (ID 0) and OMTS (ID 1)	WLTB-AETBN-004
CTA2_AETBN_031	The wireless safe train inauguration shall only take place on TCMS logical WLTB (WLTB ID 0 of physical WLTB 0 and 1), other train subsystems run on different logical WLTB shall follow the computed result from TCMS TTDB	WLTB-AETBN-005
CTA2_AETBN_032	If any AETBN failures on the WLTB is detected by the master AETBN, it shall become backup AETBN and shift the master role to the backup AETBN. Note: The failure could be detected by TOPO frame timeout, and it is covered in IEC 61375-2-5. However, in order to fulfill 200ms link failover time, the TOPO frames timeouts have been adapted in section 8. Therefore, it is only needed to shift the master role from the master to backup AETBN	WLTB-AETBN-006
CTA2_AETBN_033	Train Inauguration shall be safety-related function of safety integrity level (SIL) 2.	DBD_ND_051
CTA2_AETBN_034	Train inauguration function shall perform ETB topology discovery and Operational Train Inauguration.	DBD_ND_052
CTA2_AETBN_035	AETBN shall use TTDP protocol specified in IEC 61375-2-5 for ETB topology discovery with the improvements for NG-TCN topology Wireless Inauguration topology (see section section 8).	DBD_ND_053
CTA2_AETBN_036	The AETBN shall be able to retrieve up-to-date neighbour consist information listed below from the RFID transponders installed at the frontend and backend of the consist • the consist identifier (consist id) of the local consist • the direction information (end in direction 1 or end in direction 2) of the local consist • the identifier of the WLTB and WLTBN o WLTB ID (this ID must be unique) o WLTBN ID (these IDs must be unique), the adapted ETBN MAC address will be taken.	WLTB-AETBN-007
CTA2_AETBN_037	The AETBN shall communicate with the RFID transponders via SIL 2 safety communication	WLTB-AETBN-008
CTA2_AETBN_038	The AETBN shall refer to the result of TOPOLOGY frame for discovery of neighbour aliveness instead of using TTDP HELLO frames	WLTB-AETBN-009

Req ID	Description	S4R2 Req ID [20]
CTA2_AETBN_039	AETBN shall transmit TTDP protocol TOPOLOGY frames in WLTB	DBD_ND_060
CTA2_AETBN_040	AETBN shall receive TOPOLOGY frames from all other AETBNs on the same physical WLTB.	DBD_ND_061
CTA2_AETBN_041	The AETBN shall build the connectivity vector (partial view) by using the information retrieved from RFID transponder	WLTB-AETBN-011
CTA2_AETBN_042	AETBN shall use received TOPOLOGY frames to calculate Train Network Directory as specified in IEC 61375-2-5.	DBD_ND_062
CTA2_AETBN_043	AETBN shall compute the Train Network Directory with tolerable functional failure rate (TFFR) of less than 10^-6/h to achieve safety integrity level SIL2. Note: Current specification of Train Network Directory computation in IEC 61375-2-5 is assumed to be sufficient for SIL 2.	DBD_ND_063
CTA2_AETBN_044	The AETBN shall adopt the new TOPOLOGY frame structure defined in section 8.	WLTB-AETBN-012
CTA2_AETBN_045	The AETBN shall transmit TOPOLOGY frames via SIL 2 safety communication	WLTB-AETBN-013
CTA2_AETBN_046	If selected wireless forwarding / routing protocol works in L3, the AETBN shall encapsulate the TOPOLOGY frame in an IP package and send it using a multicast IP address Note: Not recommended due to IP addressing problems before inauguration.	WLTB-AETBN-014
CTA2_AETBN_047	The AETBN shall provide TTDB information to TI validator via TTDB manager interface defined in IEC 61375-2-3, and shall transfer data via safe data transmission protocol (e.g. SDTv2).	DBD_ND_064
CTA2_AETBN_048	The AETBN shall support up to 32 logical ECNs in each consist	DBD_ND_066
CTA2_AETBN_049	The AETBN shall support local subnet addressing defined in IEC 61375-2-5 chapter 6.4.2 on ECN side.	DBD_ND_067
CTA2_AETBN_050	The AETBN shall support WLTB ID 0 and WLTB ID 1.	DBD_ND_068
CTA2_AETBN_051	The AETBN of each physical WLTB shall be able to exchange consist information with all AETBNs on the same physical WLTB	DBD_ND_201
CTA2_AETBN_052	The AETBN of each physical WLTB shall be responsible to send and receive the CSTINFO telegrams class 1. on the same physical WLTB	DBD_ND_202
CTA2_AETBN_053	The AETBN may support closed train - CSTINFO telegram class 2 and class 3	DBD_ND_203
CTA2_AETBN_054	The AETBN shall provide a safe storage for TTDB, which is a repository for all the information related to the actual train composition and the actual AETB state	DBD_ND_204

Req ID	Description	S4R2 Req ID [20]
	- Consist information - Train network directory - Train directory - Operational train directory	
CTA2_AETBN_055	The TTDB shall be maintained by a TTDB Manager function, and it shall always keep the TTDB up-to-date	DBD_ND_205
CTA2_AETBN_056	The AETBN may support TTDB for multiple logical WLTB	DBD_ND_206
CTA2_AETBN_057	The AETBN shall support computation of the train directory	DBD_ND_207
CTA2_AETBN_058	If train inaugurations are not inhibited, the AETBN shall (re-)compute the train directory each time there is a change of the etbTopoCnt.	DBD_ND_208
CTA2_AETBN_059	The AETBN shall support DNS server for resolving TCN-URI host part to IP addresses with the aid of the TCN-DNS as defined in IEC 61375-2-3 Clause 5.4.2	DBD_ND_209
CTA2_AETBN_060	The AETBN shall map TCN-URI to IP multicast group addresses in accordance to the IP addressing scheme defined in IEC 61375-2-3 Clause 5.4.5.2	DBD_ND_210
CTA2_AETBN_061	The AETBN shall map TCN-URI to IP addresses in accordance to the IP addressing scheme defined in IEC 61375-2-5 Clause 6.4	DBD_ND_211
CTA2_AETBN_062	The AETBN shall provide DNS server service for TCN URI scheme defined in IEC 61375-2-3 Clause 5.4.4	DBD_ND_212
CTA2_AETBN_063	The AETBN shall implement the standard DNS protocols as specified in RFC 1034 and RFC 1035	DBD_ND_213
CTA2_AETBN_064	The AETBN shall support TRDP DNS server interface according to IEC 61375-2-3 annex E	DBD_ND_214
CTA2_AETBN_065	The AETBN shall only provide ETB control service on the operational network (WLTB 0)	DBD_ND_215
CTA2_AETBN_066	The AETBN shall support ECSP election mechanism to select the master AETBN, the other AETBN becomes backup AETBN	DBD_ND_407
CTA2_AETBN_067	A failure of the ECSC shall be detected latest after a time of T_{ECSC_fail} = 5,0 s	DBD_ND_217
CTA2_AETBN_068	If a failure is detected, the ECSP shall react as defined for the individual AETB control service functions.	DBD_ND_218
CTA2_AETBN_069	The AETBN shall be responsible to send and receive safe ETBCTRL telegram on the same physical WLTB cyclically using SDTv2 as defined in IEC 61375-2-3 Clause 6.4	DBD_ND_219
CTA2_AETBN_070	In case of multiple logical WLTBs, ETBCTRL telegrams shall only be exchanged on the operational network (ETB0 of each physical WLTB).	DBD_ND_220

Req ID	Description	S4R2 Req ID [20]
CTA2_AETBN_071	The AETBN shall collect ETBCTRL telegrams received from all ECSPs on the same physical WLTB, including the own ECSP as well as the remote ECSPs	DBD_ND_221
CTA2_AETBN_072	The AETBN shall support computation of the operational train directory	DBD_ND_222
CTA2_AETBN_073	The AETBN shall compute a new operational train directory each time there is a change of - Train Directory - Collection of ETBCTRL telegrams received from all ECSPs	DBD_ND_223
CTA2_AETBN_074	The AETBN shall support leading function to elect one of the vehicles within the train to become the leading vehicle	DBD_ND_224
CTA2_AETBN_075	The AETBN shall be able to detect leading conflict	DBD_ND_225
CTA2_AETBN_076	The AETBN shall be able to indicate leading conflict to the ECSC latest 1.0s after detection	DBD_ND_226
CTA2_AETBN_077	The AETBN shall follow the rules to determine the operational directions defined in IEC 61375-2-3 Clause 4.2.4.3	DBD_ND_227
CTA2_AETBN_078	The AETBN may support function sleep mode	DBD_ND_228
CTA2_AETBN_079	The AETBN shall enter sleep mode if there is a request from all consists, and leave if there are demands from at least one consist	DBD_ND_229
CTA2_AETBN_080	The AETBN shall provide ECSP interface according to IEC 61375-2-3 annex E	DBD_ND_230
CTA2_AETBN_081	The AETBN shall provide TTDB manager interface (client and server side) according to IEC 61375-2-3 annex E and modifications specified in section 8 of this document.	DBD_ND_231
CTA2_AETBN_082	The AETBN shall preform as ED in TTDB manager interface to retrieve the TTDB from paired AETBN of the same consist.	WLTB-AETBN-015
CTA2_AETBN_083	The AETBN TTDB manager shall support a new specific telegram using non-safe data communication for providing own cstUUID value within the consist	DBD_ND_232
CTA2_AETBN_084	The AETBN may provide ETBN control interface according IEC 61375-2-3 annex E	DBD_ND_233
CTA2_AETBN_085	The AETBN shall send TRDP process data telegrams with IEEE 802.1p traffic priority class 3	DBD_ND_234
CTA2_AETBN_086	The AETBN shall send TRDP message data telegrams with IEEE 802.1p traffic priority class 2	DBD_ND_235
CTA2_AETBN_087	The AETBN shall support the safe ECSP status telegram transmission using SDTv2	DBD_ND_236

Req ID	Description	S4R2 Req ID [20]
CTA2_AETBN_088	The AETBN shall support the safe TTDB information telegram transmission using SDTv2	DBD_ND_237
CTA2_AETBN_089	The AETBN shall support the safe ETBCTRL telegram transmission using SDTv2	DBD_ND_238
CTA2_AETBN_090	The AETBN shall be able to receive safe ECSP control telegram using SDTv2	DBD_ND_239
CTA2_AETBN_091	The AETBN shall support adding, recognizing, interpreting, and removing VLAN tags as defined in IEEE 802.1Q.	DBD_ND_285
CTA2_AETBN_092	The AETBN shall support strict priority-based transmission selection algorithm (IEEE 802.1Q)	DBD_ND_286
CTA2_AETBN_093	The AETBN may support credit-based shaper algorithm (IEEE 802.1Q)	DBD_ND_287
CTA2_AETBN_094	AETBN shall support at least 8 egress queues.	DBD_ND_289
CTA2_AETBN_095	The AETBNs within a consist shall use VRRPv3 over the ECN to select a master router for routing unicast traffic between ECN and ETB.	DBD_ND_405
CTA2_AETBN_096	The AETBN which is currently selected master by the VRRP shall also be responsible for routing multicast traffic between ECN and ETB.	DBD_ND_406
CTA2_AETBN_097	After the inauguration is done, the master AETBN shall be responsible for retrieving the TTDB from the backup AETBN including the information below via TTDB manager interface defined in IEC 61375-2-3 - Consist information - Train network directory	WLTB-AETBN-016
CTA2_AETBN_098	The master AETBN shall compute a common and complete TTDB by comparing the TTDBs from different physical WLTBs, and obtaining the corresponding information of the missing consist	WLTB-AETBN-017
CTA2_AETBN_099	The master AETBN shall be responsible of providing the common TTDB information to CCU if the common TTDB is computed successfully without contradiction	WLTB-AETBN-018
CTA2_AETBN_100	The master AETBN shall notify the result of the computation to backup AETBN, and also share the complete TTDB if it is computed successfully without contradiction	WLTB-AETBN-019
CTA2_AETBN_101	The master and backup AETBN shall exchange the TTDB information and computation result via a dedicated VLAN	WLTB-AETBN-020
CTA2_AETBN_102	Both active and backup AETBN shall provide ETB control service. Note: The ECSC in the CCU shall send separate ECSP control telegrams to both master and backup AETBN.	WLTB-AETBN-021
CTA2_AETBN_103	The AETBN shall support device redundancy with switch-over time of ≤ 0.8 s.	DBD_ND_408

Req ID	Description	S4R2 Req ID [20]
CTA2_AETBN_104	The AETBN shall support push communication pattern to transmit PD-PDUs cyclically	DBD_ND_513
CTA2_AETBN_105	The AETBN shall support pull communication pattern to transmit PD-PDUs on request	DBD_ND_514
CTA2_AETBN_106	The AETBN shall use an IP unicast address for addressing a known process data subscriber/publisher.	DBD_ND_515
CTA2_AETBN_107	The AETBN shall use an IP multicast address for addressing groups of known process data subscribers/publishers (e.g. redundancy groups).	DBD_ND_516
CTA2_AETBN_108	The AETBN shall use an IP multicast address for addressing unknown process data subscribers/publishers.	DBD_ND_517
CTA2_AETBN_109	The AETBN shall send process data telegram according to the PD-PDU structure defined in IEC 61375-2-3 annex A.6.5	DBD_ND_518
CTA2_AETBN_110	The AETBN shall support TRDP PD redundancy groups	DBD_ND_519
CTA2_AETBN_111	The AETBN shall follow the PD protocol state machine defined in IEC 61375-2-3 annex A.6.8	DBD_ND_520
CTA2_AETBN_112	If the AETBN support pushed PD-PDU, it shall apply a traffic shaping mechanism for equal distribution of the PD-PDU's over the time	DBD_ND_521
CTA2_AETBN_113	The TRDP message data packet size shall be limited to 64 Kbytes	DBD_ND_522
CTA2_AETBN_114	The AETBN shall support MD push and pull communication pattern	DBD_ND_523
CTA2_AETBN_115	The AETBN shall support the following message data transfer options a) request without reply ('notification') b) request with reply but without confirmation c) request with reply and confirmation	DBD_ND_524
CTA2_AETBN_116	As a message data caller, the AETBN shall use an IP unicast address or an IP multicast address for addressing known replier(s)	DBD_ND_525
CTA2_AETBN_117	As a message data caller, the AETBN shall use an IP multicast address for addressing unknown repliers.	DBD_ND_526
CTA2_AETBN_118	As a message data caller, the AETBN may use an IP multicast address for addressing a known replier redundancy group.	DBD_ND_527
CTA2_AETBN_119	As a message data replier, the AETBN shall respond to the caller's unicast address.	DBD_ND_528
CTA2_AETBN_120	The AETBN shall send message data telegram according to the MD-PDU structure defined in IEC 61375-2-3 annex A.7.5	DBD_ND_529
CTA2_AETBN_121	The AETBN shall support the filtering rules according to IEC 61375-2-3 annex A.7.6.3	DBD_ND_530
CTA2_AETBN_122	The AETBN shall follow the MD protocol state machine defined in IEC 61375-2-3 annex A.7.8	DBD_ND_531
CTA2_AETBN_123	As a message data caller, the AETBN shall close an existing TCP connection (active end) in the following cases: • A signal that the TCP connection will be closed has been received. • TRDP shut down or re-initialization. • A timeout occurred because the TCP connection has not been used for a defined time.	DBD_ND_532
CTA2_AETBN_124	As a message data replier, the AETBN shall use the TCP connection opened by the caller.	DBD_ND_533

Req ID	Description	S4R2 Req ID [20]
CTA2_AETBN_125	As a message data replier, the AETBN shall close an existing TCP connection (passive end) in the following cases: • A signal that the TCP connection will be closed has been received. • TRDP shut down or re-initialization. • Another TCP connection was opened from the same caller device and the old connection is not used anymore for a defined time.	DBD_ND_534
CTA2_AETBN_126	The AETBN may support MD echo function	DBD_ND_535
CTA2_AETBN_127	The AETBN shall provide topography counter check specified in IEC 61375-2-3 annex A.6.7 and A 7.7	DBD_ND_536
CTA2_AETBN_128	If the topography counter check fails before sending a telegram, the AETBN shall not send the telegram	DBD_ND_537
CTA2_AETBN_129	If the topography counter check fails after receiving a telegram, the AETBN shall not accept the telegram	DBD_ND_538
CTA2_AETBN_130	If the TRDP configuration is not supported, the AETBN shall support the default TRDP configuration value as in IEC 61375-2-3 annex C	DBD_ND_539
CTA2_AETBN_131	The AETBN shall send out TTDB status telegram periodically	DBD_ND_601
CTA2_AETBN_132	The AETBN shall provide TTDB information on request	DBD_ND_602
CTA2_AETBN_133	The AETBN may support TRDP echo function	DBD_ND_603
CTA2_AETBN_134	The AETBN shall send out ECSP status telegram to ECSC periodically	DBD_ND_604
CTA2_AETBN_135	The AETBN shall send out ETBN status telegram periodically with multicast destination address	DBD_ND_605
CTA2_AETBN_136	The AETBN shall support SNMP.	DBD_ND_621
CTA2_AETBN_137	The AETBN shall be capable of exchanging SNMP messages security.	DBD_ND_622
CTA2_AETBN_138	It shall be possible to read out Ethernet port operational status via SNMP	DBD_ND_623
CTA2_AETBN_139	It shall be possible to get an SNMP Notification (Trap/Notify/Report) when an Ethernet port changes state.	DBD_ND_624
CTA2_AETBN_140	AETBN shall provide packet error counters via SNMP to facilitate better Diagnostic Coverage (DC) in the case of an increasing bit error probability.	DBD_ND_625
CTA2_AETBN_141	It shall be possible to use SNMP to read out ingress and egress packet statistics to facilitate monitoring of packet loss rate.	DBD_ND_626
CTA2_AETBN_142	IP Address: Static IP addresses of the switches shall be set.	DBD_ND_651
CTA2_AETBN_143	DHCP Server: When DHCP is available for dynamic IP addressing and the ECSP is located within the AETBN, the DHCP server shall be configured.	DBD_ND_652
CTA2_AETBN_144	Port settings: Port assignment and ingress and egress policing configuration shall be set.	DBD_ND_653
CTA2_AETBN_145	Static consist information: When ECSP is located within the AETBN, the static consist information as detailed in IEC61375-2-3 shall be configured.	DBD_ND_657

Req ID	Description	S4R2 Req ID [20]
CTA2_AETBN_146	Settings required for the AETBN to conduct wireless inauguration according to IEC 61375-2-5 and section 8 of this document.	DBD_ND_659
CTA2_AETBN_147	Settings required for the AETBN to act as redundant router for traffic on ECN and WLTB.	DBD_ND_660
CTA2_AETBN_148	Settings required for the AETBN to act as firewall.	DBD_ND_661
CTA2_AETBN_149	The AETBN should use Ethernet M12 X-coded 8-pin female connector for Gigabit Ethernet port according to IEC 61076-2-109. Note: For 100Mbps A-coded 4-pin would be sufficient.	DBD_ND_702
CTA2_AETBN_150	The AETBN shall be at least an IP30 class device	DBD_ND_703
CTA2_AETBN_151	The AETBN should support wall or rack mounting for installation	DBD_ND_704
CTA2_AETBN_152	The AETBN shall provide a console for maintenance / debugging	DBD_ND_705
CTA2_AETBN_153	The AETBN may provide a reset function to reset the user configurations	DBD_ND_706
CTA2_AETBN_154	The AETBN may provide an out-of-band Ethernet port for maintenance	DBD_ND_707
CTA2_AETBN_155	The AETBN may provide system indicators, at least ok and sum of error indication	DBD_ND_708
CTA2_AETBN_156	The AETBN may provide port status indicators (link, traffic, blocked)	DBD_ND_709
CTA2_AETBN_157	The AETBN shall support input power voltage 24V, and should support the range 24V-110V.	DBD_ND_710
CTA2_AETBN_158	The AETBN may use M12 K-coded 5-pin male or M12 A-coded 4-pin male connector as the power connector.	DBD_ND_711
CTA2_AETBN_159	The power consumption of the AETBN should not exceed 30W (non-PoE)	DBD_ND_712
CTA2_AETBN_160	The AETBN shall comply with EN 50155:2017 class OT4, -40 °C to +70 °C	DBD_ND_721
CTA2_AETBN_161	The AETBN shall comply with EN 50121-3-2:2015	DBD_ND_722
CTA2_AETBN_162	The AETBN shall comply with EN 50124-1:2017	DBD_ND_723
CTA2_AETBN_163	The AETBN shall comply with EN 50125-1:2014	DBD_ND_724
CTA2_AETBN_164	The AETBN shall comply with EN 50125-3:2014 if signalling functions are integrated on TCMS network	DBD_ND_725
CTA2_AETBN_165	The AETBN shall comply with EN 45545-1:2013	DBD_ND_726
CTA2_AETBN_166	The AETBN shall comply with EN 45545-2:2013	DBD_ND_727
CTA2_AETBN_167	The AETBN shall comply with EN 45545-5:2013	DBD_ND_728
CTA2_AETBN_168	The AETBN shall comply with EN 50126-1:2017	DBD_ND_729
CTA2_AETBN_169	The AETBN shall comply with EN 50657:2017	DBD_ND_730
CTA2_AETBN_170	The AETBN shall comply with EN 50128:2011 if signalling functions are integrated on TCMS network	DBD_ND_731

Req ID	Description	S4R2 Req ID [20]
CTA2_AETBN_171	The AETBN shall comply with EN 50129:2018	DBD_ND_732
CTA2_AETBN_172	AETBN may be capable of acting as IEEE 802.1x Authentication Server (RADIUS)	DBD_ND_803
CTA2_AETBN_173	If AETBN supports IEEE 802.1X Authentication Server, it shall support EAP method(s) supporting derivation of master key derivation for MACsec.	DBD_ND_805
CTA2_AETBN_174	AETBN shall provide a network-based firewall service	DBD_ND_806
CTA2_AETBN_175	It 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) and TRDP ComId	DBD_ND_807
CTA2_AETBN_176	AETBN shall support HTTPS for secure file transfer	DBD_ND_808
CTA2_AETBN_177	AETBN shall support SSH for secure login	DBD_ND_809
CTA2_AETBN_178	AETBN shall support syslog for logging if security related events	DBD_ND_810
CTA2_AETBN_179	The AETBN shall support detection and reporting of security events	DBD_ND_811
CTA2_AETBN_180	Login Successful If a user logs in, the concerned device creates a log message including the user name.	DBD_ND_812
CTA2_AETBN_181	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.	DBD_ND_813
CTA2_AETBN_182	Account modification A network device generates an audit log message whenever any of the following events occur: - Creation of a new user account - Deletion of a user account - Modification of the privilege level, or group membership, of a user account	DBD_ND_814
CTA2_AETBN_183	Privilege escalation A network device generates an audit log message whenever any of the following events occurs: - A user spawns a shell, terminal or other application or command using different user credentials than his own (e.g. uses sudo) - A user changes his effective user credentials, group membership, privilege level, or similar credentials (e.g. uses su).	DBD_ND_815
CTA2_AETBN_184	Credential modification A network device generates an audit log message whenever any of the following events occurs: - 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	DBD_ND_816
CTA2_AETBN_185	Firewall activation When the firewall is taken up during system operation, the	DBD_ND_817

Req ID	Description	S4R2 Req ID [20]
	concerned device generates firewall log messages.	
CTA2_AETBN_186	Firewall deactivation When the firewall is taken down during system operation, the concerned device generates firewall log messages.	DBD_ND_818
CTA2_AETBN_187	Firewall reconfiguration When the firewall is reconfigured, reinitialized, or reloaded at runtime, the concerned reconfiguration device generates firewall log messages.	DBD_ND_819
CTA2_AETBN_188	Unexpected incoming traffic When unexpected traffic is received on the external interface, the concerned device generates a firewall log message. Note: The firewalls are configured via a white list. All traffic not included in the white list is unexpected. This applies only to the internal firewall between network zones.	DBD_ND_820
CTA2_AETBN_189	System service startup A device sends this message whenever a security-related system service is started.	DBD_ND_821
CTA2_AETBN_190	System service shutdown A device sends this message whenever a security-related system service gets shut down.	DBD_ND_822
CTA2_AETBN_191	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.	DBD_ND_823
CTA2_AETBN_192	System reboot (i.e. the system re-initializes itself by reboot command, reload configuration, watchdog etc.) A device sends this log message whenever the system gets rebooted, including a reboot reason/trigger.	DBD_ND_824
CTA2_AETBN_193	System shutdown (i.e. the system is powered off either safely or unexpectedly) A device sends this log message whenever the system gets shut down.	DBD_ND_825
CTA2_AETBN_194	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.	DBD_ND_826
CTA2_AETBN_195	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.	DBD_ND_827
CTA2_AETBN_196	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.	DBD_ND_828
CTA2_AETBN_197	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.	DBD_ND_831
CTA2_AETBN_198	Physical or link layer up Network devices generate a log message whenever a connection to an externally accessible device is established on	DBD_ND_832

Req ID	Description	S4R2 Req ID [20]
	the physical or link layer. This only applies to the originator device to which the externally accessible device is directly connected.	
CTA2_AETBN_199	Messages dropped Devices may generate a log 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.	DBD_ND_833
CTA2_AETBN_200	Wireless TCMS devices shall fulfil the laws guaranteeing against its impact on the staff and on the passengers. Wireless TCMS devices shall be compliant with the European directive RED 2014/53/EU. Wireless TCMS devices shall be compliant with the norm EN 62311:2008.	N/A

6. DETAILED SPECIFICATION OF THE WIRELESS CONSIST NETWORK

This chapter copes with the specification of a wireless consist network, which shall be part of the train communication network in general.

Chapter 6.1 presents the results of the complementary action [17] within the Safe4RAIL-2 project, which evaluated different wireless technologies.

Based on these results, chapter 6.2 presents possible architectures to implement a wireless consist network. Starting with a simple approach by just adding wireless access points (WAP) to a wired Ethernet Consist Ring (ECR) enabling integration of wireless end devices (WED) and closing with an architecture reflecting also requirements for the next generation train network (NG-TCN), supporting Time Sensitive Networking (TSN) enabling “drive-by-data” [07]. Chapter 6.2 also specifies RAMS aspects, devices quantities, as well as time synchronisation, security and TSN aspects.

Chapter 6.3 describes the interfaces of a wireless consist network and used protocols.

During the specification work some design constraints appeared and are mentioned in chapter 0.

6.1 State of the art in wireless communication for WLCN

6.1.1 Technology

The selection of a suitable technology for radio-based data transmission depends on several factors. On the one hand there are norms and standards to meet and on the other hand a robust and reliable data transmission is desired. Several technologies are available for selection and are suitable for a wide range of applications (e.g. sensor technology, visualisation, control). It may make sense to use different technologies for different purposes. Based on the requirements 4.2, several technologies were preselected, refer to Table 30. In a complementary action [17] within the Safe4RAIL-2 project, these technologies were evaluated regarding main requirements 4.2 and previous project results from R2R [18] in detail and mainly regarding the following key figures:

- bit rate & latency
- medium access
- communication range
- max number of nodes
- robustness / interference immunity
- TSN roadmap

The following comparison, Table 30, is a compressed presentation of the detailed analysis [17], showing the different technology key figures, separated by currently available and future technologies:

Table 30: Comparison of wireless technologies for WCLN

		CURRENT WIRELESS TECHNOLOGIES							FUTURE WIRELESS TECHNOLOGIES			
REQUIREMENTS		***LTE***	***ZigBee***	***Wireless HART***	***UWB***	***Wi-Fi***	***ECHORING***	***WSAN/ WISA***	***SHARP***	***5G***	***WirelessHP***	***Wi-Fi 6***
Max. Bit rate	~ 100 Mbps per traffic type	50 Mbps (UL) 150 Mbps (DL)	250 kbps	250 kbps	27 Mbps	1.73 Gbps	10 kbps (9 nodes) 1 Mbps (5 nodes) 5 Mbps (2 nodes)	4 x 1 Mbps (UL); 1 Mbps (DL)	54 Mbps	620 Mbps (UL) 578 Mbps (DL)	480 Mbps	4.8 Gbps
Max. Latency	4 – 250 ms	50 – 300 ms [e]	> 80 ms (25-50 nodes)	15 – 60 ms (50-100 nodes)	N/A[d]	1 - 20 ms	1 – 10 ms (6 – 9 nodes) 1 – 200 ms (11 nodes)	5 ms (typ.)	550 µs	10 – 300 ms	N/A[d]	N/A[d]
Medium Access	Deterministic	yes	no	yes	no	no	yes	yes	yes	yes	N/A[d]	no
Communi-cation Range	30 m (1 car)	400 m[a]	100 m[a]	100 m[a]	20m[a]	200 m[a]	30 m[b]	50 m[a]	200 m[a]	400 m[a]	25 m	200 m[a]
Max. number of nodes	40 nodes / car	200 / cell	65000	Hundreds	N/A[d]	Hundreds	11 (simulated)	120	20	200/cell	N/A[d]	N/A[d]
Protection against inter-ferences	-	dedicated band + MRO[c]	DSSS	DSSS + Freq. Hopping	Wideband Trans-mission	IEEE 802.11s: DFS (5 GHz)	Freq. Hopping + Cooperative ARQ + Evolved Failure Tolerance Mechanisms + Adaptation of Error Handling Strategy	FDD + Freq. Hopping	No	Dedicated Band + MRO[c]	No	BSS Coloring
TSN	Supports TSN (in roadmap)	no	no	no	no	no	no	no	yes	no	no	no

[a] Estimated from transmitter output power, receiver sensitivity, and intra-consist path loss model [18]

[b] Measured value

[c] Mobility Robustness Optimization

[d] N/A: Not Available

[e] The upper-bound latencies depend on non-deterministic delay at application level

The technology evaluation [17] concludes with the following summary:

For Table 30 a subset of the lower layer requirements (MAC and PHY layer) has been used. For currently available wireless technologies, the results indicate that there is no single technology that covers all the requirements of the WLCN. The following analysis can be made on both current and future wireless technologies:

1. LTE provides a deterministic medium access and supports a wide range of data rate requirements, although it only covers the traffic types which are under 100 Mbps. On the other hand, it does not meet the low latencies of 4 ms and 8 ms required by Process Data and Supervisory Data.

2. ZigBee and WirelessHART do not cover any of the bit rate requirements of the WLCN. Regarding latencies, ZigBee covers all requirements except Process Data and Supervisory Data, and WirelessHART presents a huge latency in comparison with the rest of technologies and does not cover any of the latency requirements of the WLCN. As a summary, neither ZigBee nor WirelessHART can be considered as suitable wireless technologies for the WLCN.

3. UWB does not meet the high throughput values required by Process Data and Video Streaming in the WLCN. On the other hand, it does not have a deterministic medium access, and it is designed for short indoor coverage (room-coverage), as it is mainly used in ranging applications. Therefore, it cannot be considered as an option for the WLCN.

4. Wi-Fi is able to achieve the high data rates and low latencies required by all types of traffic, but its medium access technique is non-deterministic.

5. ECHORING provides low latency values, but only for small networks (i.e. 6-9 nodes), and the obtained bit rates are only suitable for Audio Streaming applications. On the other hand, the low number of nodes is a limiting factor for this technology.

6. WISA is a suitable technology in terms of deterministic medium access and low latencies (only Time Sensitive Process Data cannot be covered). However, due to its low data rate (1 Mbps) it is not applicable for the WLCN. On the other hand, only outdated references have been found in literature.

7. SHARP[12] presents extremely low latencies (below 1 ms) with a medium bit rate and a hybrid medium access (deterministic and non-deterministic). It presents also compatibility with IEEE 802.11g and TSN synchronization. However, the number of nodes is not enough for the WLCN.

8. 5G improves the features of its predecessor (LTE) by increasing the bit rate and covering all WLCN traffic types and reducing latencies down to 10 ms. This minimum latency value is theoretical, and it should be checked against real implementations of 5G devices, especially to check the impact of the software dependency of the protocol.

[12] SHARP is an IKERLAN's proprietary technology [39].

9. WirelessHP presents optimal PHY features in terms of data rate, covering all traffic types required in the WLCN (except Video Streaming). However, the MAC layer has not been implemented yet, so it cannot be fully evaluated in terms of latency. On the other hand, only software implementations of WirelessHP have been found in literature.

10. Wi-Fi 6 provides very high data rates which cover the requirements of WLCN. No latency figures have been found in literature, but it is expected to overperform the low latencies provided by IEEE 802.11ac. However, the medium access layer is still non-deterministic.

Therefore, the following recommendations can be made for the WLCN:

1. ZigBee, WirelessHART and UWB are unsuitable technologies for the WLCN. WirelessHP cannot be used either, due to the lack of a MAC layer implementation.

2. ECHORING could be used for low-latency traffic, but WLCN data rate requirements should be relaxed. In addition, several ECHORING networks should be deployed to cover all nodes in the WLCN.

3. WISA could fit in the same category as ECHORING, but it should be further checked with ABB due to the lack of recent updates on this technology.

4. Wi-Fi could be used for non-critical and high-data-rate WLCN traffic, such as Audio/Video Data Streaming and Best Effort Data, as it is a high performance and non-deterministic technology. In order to use Wi-Fi for critical traffic, a deterministic MAC layer should be added, as has been done in SHARP.

5. LTE, in spite of providing a deterministic access, does not provide enough data rate for Streaming Data traffic, and it does not provide sufficiently low latency for Process Data and Supervisory Data traffic in the WLCN. 5G could be explored as an alternative, but further experimentation would be required to confirm the specified latency values.

As a conclusion, in order to cover all TCMS traffics in the WLCN, a combination of the existing wireless technologies would be the most valid approach. To cover Process Data a very low deterministic latency is required but currently available technologies don't fulfil this. Wi-Fi can meet the required times but can't guarantee them. With this in mind, time critical Process and Supervisory Data can't be covered with current wireless technologies. In the future SHARP can be a solution.

6.1.2 Selection

So, there is not only one wireless technology that could be used in all areas of TCMS. It makes more sense to choose the appropriate technology in terms of function, purpose, communication parameters and cost of a device (e.g. actor, sensor, small and big display, control unit, and smart device).

This specification therefore follows the approach of integrating different technologies into the TCMS network. In general, a wireless network is usually based on an access point (WAP) and the connecting terminals (WED). While terminal devices usually support only one technology, there are access points in which several technologies are installed simultaneously. These devices are often based on a modular approach. In the following chapters WAP and WED are further described.

In principal, the WAP and WED hardware shall match railway, radio, and IT security standards.

6.1.3 WAP device

As depicted in Figure 17, the WAP devices consists of two main interfaces from networking point of view; first, the cable interface and second, the radio interface. Typically, these interfaces are put in one housing.

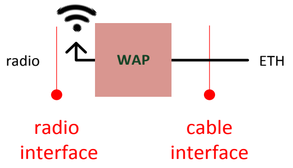


Figure 17: WAP device, overview network interfaces

The interfaces are specified in chapter 6.3.

Regarding the main network functions of the WAP, this device can be simplified as shown in Figure 18.

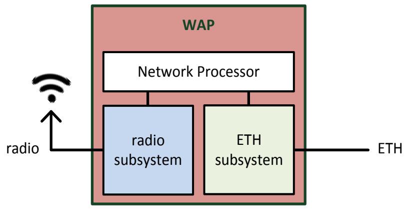


Figure 18: WAP device, simplified block diagram

When using multiple radio technologies (radio subsystem A and B), then the WAP can be depicted as shown in Figure 19.

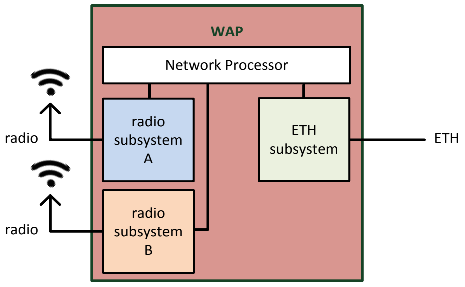


Figure 19: WAP device, multiple radio technologies, single LAN subsystem

As further extension level, multiple radio subsystems (radio subsystem A and B) are mapped to different LAN subsystems (A and B) as shown in Figure 20.

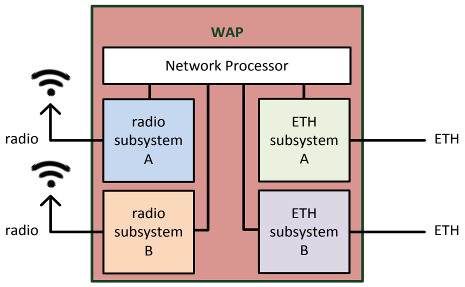


Figure 20: WAP device, multiple radio technologies, multiple LAN subsystems

The cable-based interface used by the LAN subsystem shall be according to IEEE 802.3 (e.g. 100BASE-TX or 1000BASE-T Ethernet) to establish a possible connection to the ECN, which in turn is constituting the interface to the TCMS network, offering access to services in the distribution system.

The radio subsystems can be different, e.g. operating according to IEEE 802.11 or IEEE 802.15.4. A radio subsystem operating on LTE would be possible as well.

The network processing unit manages the data exchange between the different subsystems, by using switching or routing mechanisms and based on the WAP configuration settings.

Due to the wireless domain peculiarities a WAP devices shall grant access to local WED only; local means: WED is in the same consist as WAP.

6.1.4 WED device

The WED device usually connects to a peer WAP to gain access to the network and the offered services (located in the distribution system). The wireless technology as well as radio band must match with the peer WAP-band to establish a proper connection. Due to the wireless domain peculiarities WED devices shall connect to local WAP only; local means: WAP is in the same consist as WED.

Within the scope of this specification, a WED is a device which has hardware corresponding to its function (e.g. camera, display, actuator, or sensor) and uses a wireless interface for communication purposes, both combined in one housing, see Figure 21. An external antenna may be a feasible option.

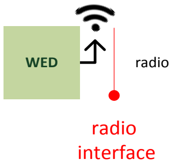


Figure 21: WED device, overview network interface

The interface is specified in chapter 6.3.

Regarding the main network functions of the WED, this device can be simplified as shown in Figure 22.

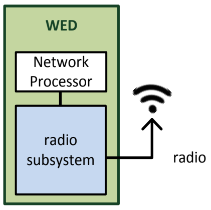


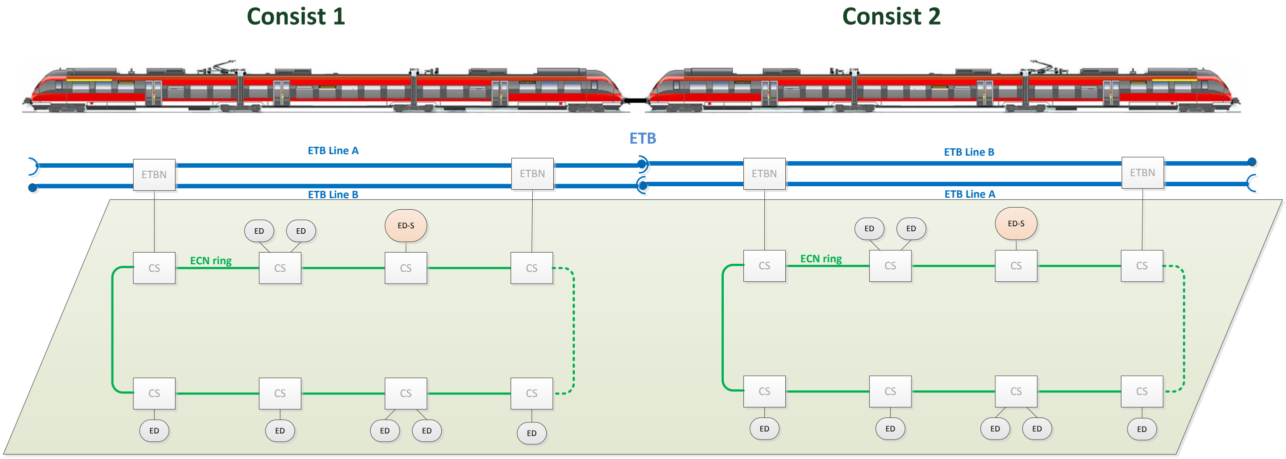
Figure 22: WED device, simplified block diagram

This specification does not cope with the consideration of connecting already established wired devices (TCMS devices) to the wireless network by means of a converter (e.g. media changer from LAN to WLAN and vice versa). The reason for this is that such a converter offers only less possibilities for controlling or configuring data communication (e.g. latency and data rate).

6.2 Specification for Wireless Consist Network

6.2.1 General

A conventionally Ethernet consists network (according to IEC 61375-2-5 and -3-4) is usually a composition of managed Ethernet switches which are connected in a structured way using wires, see Figure 23. These managed switches are called Consist Switches (CS) and constitute the Ethernet Consist Network (ECN). In addition, CS devices provide access for end devices, like control units, displays or any kind of computer, to the ECN, enabling end-to-end communication between the devices. In the case, that a train wide communication is needed, then train backbone nodes (TBN) are integrated into the ECN. The TBN devices are in turn connected to the train wide network, the Ethernet Train Backbone (ETB). The used network technology is typically equipped with appropriate mechanisms, interfaces and protocols, providing a robust and reliable distribution system for the connected end devices. Typically, end devices are assigned to dedicated vehicle functions (including non-safe, safe, non-time critical and time critical function) which in turn are controlled by the main vehicle application.



CS	Consist Ethernet Switch
ECN	Ethernet Consist Network
ED	End Device
ED-S	Safety critical ED
ETB	Ethernet Train Backbone
ETBN	Ethernet Train Backbone Node

Figure 23: Overview wired consist network

The CONNECTA-2 project and the previous projects Roll2Rail and CONNECTA aim to define a next generation communication network (NG-TCN), overcoming drawbacks of today's network architectures. Figure 24 depicts the general architecture of a train communication network as it was defined in the CONNECTA project [07].

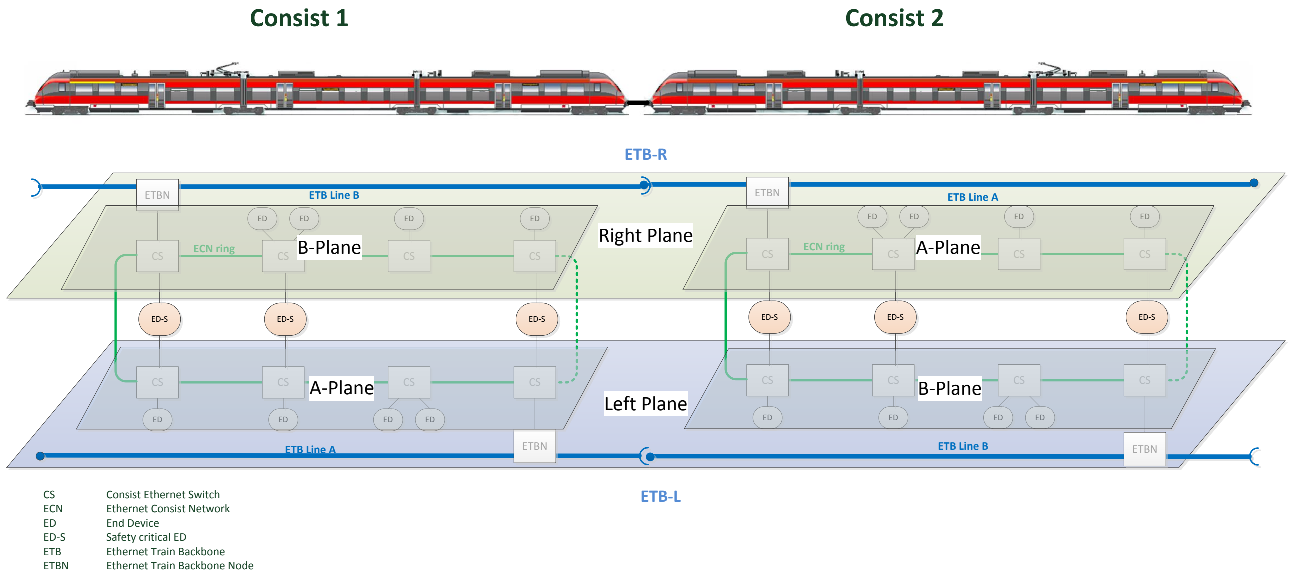


Figure 24: Overview wired NG-TCN consist network

In the above shown architectures examples (Figure 23 and Figure 24), network devices are exclusively interconnected with Ethernet cables. Different to that, a wireless network basically is a network set up by using radio technology to communicate among computers and other network devices.

So, what does wireless technology mean for implementation in the consist network? Several approaches are imaginable, as the application of the wireless technology extends from converting vehicles (retrofitting) to completely new ones.

In terms of wireless consist, two main approaches are considerable:

1) Mixed approach:

   a) The existing cable-based ECN is extended by wireless technology. A device operating as Wireless Access Point (WAP) is connected to the CS and offers access to the ECN via radio to devices operating as wireless end device (WED).

   b) Same as a), but wireless technology is integrated in CS device.

2) Pure Wireless approach:

   The ECN is replaced by a wireless technology, offering a pure wireless consist network (WCN). This means that CS devices are replaced by WAP devices. WAP devices also include an interface to the train backbone. This approach is also known as wireless MESH network (WMN) in non-railway network structures. Like the ECN ring structure, a virtual consist network structure (e.g. a ring topology) is established via radio links and appropriate protocols.

As for the wired network, also in the wireless network appropriate functions and services must be provided, ensuring a secure and reliable data communication.

6.2.2 Architectures

In the following, three possible architecture of a wireless consist are presented:

- Wired ECN extended by WAP/WED (regular) Variant A
- Wired ECN extended by WAP/WED (safe & TSN) Variant B
- Wireless CN build up by WAP/WED (safe & TSN) Variant C

It is assumed, that the train backbone is wired and according to the definitions made in the CONNECTA project [07].

In the following architectural figures, a wired ETB with wired ETBNs is drawn. This is due to the parallel development (WLTB and WLCN) and can be accepted in so far as the WLTBN - composed of a radio unit and an adapted ETBN (AETBN) - is having a similar structure (see Figure 11 and Figure 12 in section 5.1.3 and behaves the same from the point of view of the WLCN.

1st architecture (variant A) shows the integration of wireless technology by adding radio-based network to the existing consist network.

2nd architecture (variant B) is the same but taking the requirements for safe communication and TSN into account.

And 3rd architecture (variant C) proposes a completely wireless consist network.

Wired ECN extended by WAP/WED (regular) – Variant A

Figure 25 depicts wired ECN ring structure, which is build up with two CS devices, one in each plane. Conventionally, wired end devices (ED) are connected to the CS devices. In turn, CS devices are connected to ETB lines, enabling train wide communication. The wireless technology is simply added to the existing network structure. Wireless end devices (WED) need a peer point to establish a radio connection, which is a wireless access point (WAP). Plane separation is achieved by using different radio frequencies (channels, blue and orange dashed lines). Typically, a radio access point is connected to a wired network, which is the ethernet consist ring in this case. Thus, the WAP devices are connected to the CS devices, like normal end devices are. In this architecture, only regular devices are connected to CS and WAP devices. Also, time critical communication is not considered. WED and ED connected to the consist network can exchange data/information. Data exchange between planes is handled by CS devices.

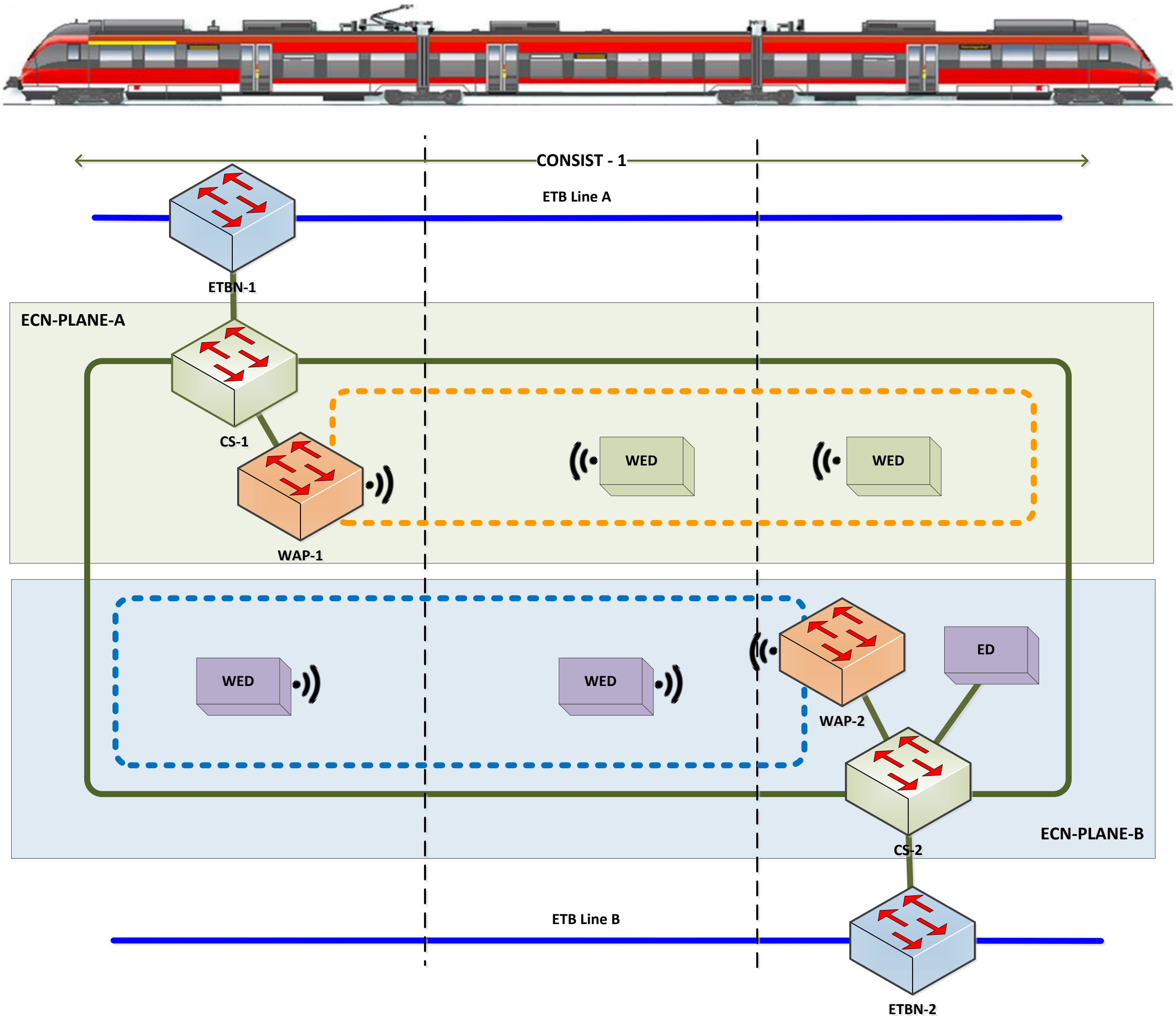


Figure 25: Overview wired ECN extended by WAP/WED (regular)

Wired ECN extended by WAP/WED (safe & TSN) – Variant B

The architecture depicted in Figure 26 is principally the same as shown Figure 25. In addition, this architecture includes safe end devices, wired (ED-S) and wireless (WED-S). According to the NG-TCN definition [07], the safe devices are connected to both planes in parallel. Assuming that, WAP devices as well as WED devices support TSN capabilities, then also WED devices operating time critical functions can be connected to the wireless network.

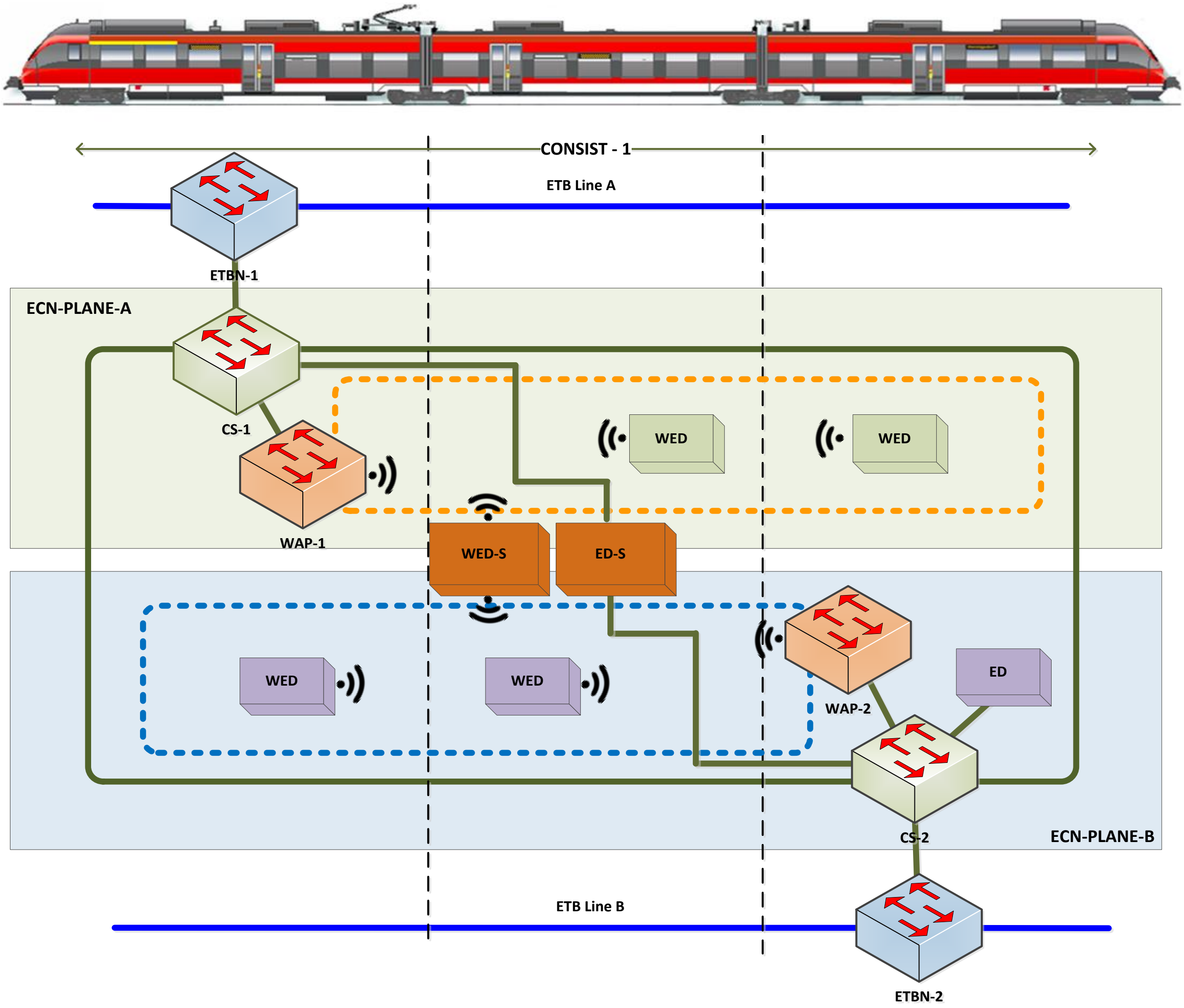


Figure 26: Overview wired ECN extended by WAP/WED (safe & TSN)

Wireless CN build up by WAP/WED (safe & TSN) – Variant C

Figure 27 depicts a fully wireless consist network. All end devices (WED) within the consist are using a radio link to connect to the WAP devices. Since no wired devices are foreseen, the CS devices are not present in the architecture anymore. The WAP devices are spanning a wireless consist network (MESH) offering the routing between the consist planes, the routing to and from the ETB lines and are managing the communication of the wireless end devices. Safe and TSN devices are still connected to both planes in parallel. Each WAP device is using two different radio links, one to establish a wireless consist network (WCN, red dashed line), like the ECN, and another radio link (blue and orange dashed lines) for the WED devices.

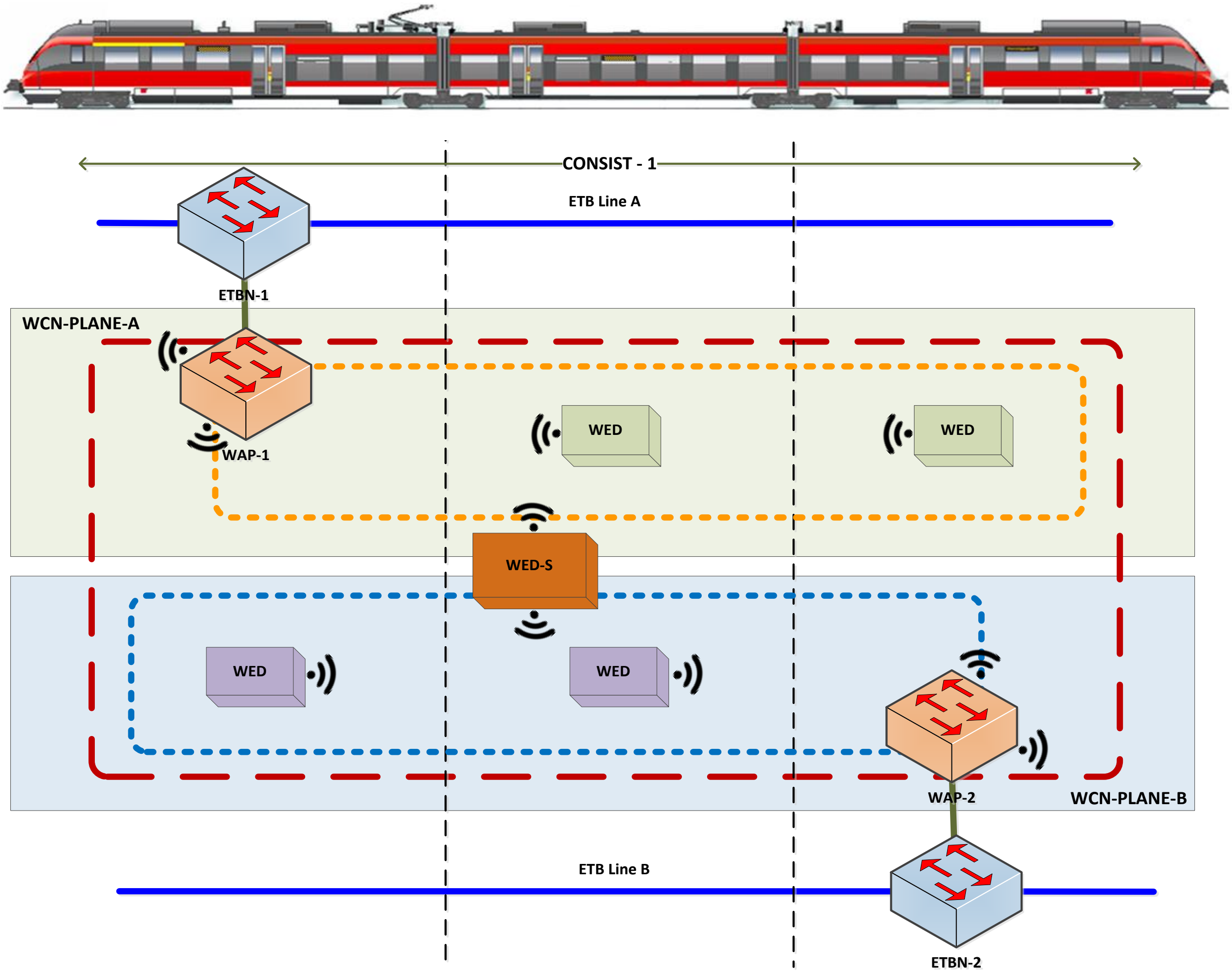


Figure 27: Overview wireless CN build up by WAP/WED (safe & TSN)

6.2.3 Constraints

Main goal in terms of communication is to achieve a secure and reliable network, enabling flawless data communication between communication peers. But, regarding radio-based communication there are some constraints present:

- radio coverage due to environmental aspects
- radio coverage due to technology selection
- available bandwidth due to technology selection

Coverage

In the architectures shown above, WAP device were put at the end cars only (Figure 25, Figure 26, and Figure 27). This assumes, that the WAP devices

- provide full radio coverage through the whole consist
- can handle the number of WED devices installed in the consist
- provide flawless operation and communication

This ideal conception is unlike to be realized. Appropriate countermeasures need to be considered. Since WED devices cannot be put on a concentrated place, the countermeasures are related to WAP devices.

In principle the coverage can be increased by

- increasing the number of WAP devices in the whole consist or
- placing antennas at appropriate positions in the consist.

Increasing the number of WAP devices has also advantages, like

- network availability (redundancy) or
- scalability of connected WED devices.

Bandwidth

The available bandwidth in a wireless network depends on technology and the number of end devices which share a radio link. Even though, radio links are separated into several communication channels, the data budget is limited and may be too low. Increasing the number of WAP devices

- will enable load balancing, by assigning WED devices to dedicated WAP devices only and
- will enhance data throughput between WED devices and towards the train backbone.

Choosing a wireless technology with a high bandwidth has the drawback of less radio coverage (lower radio range). This in turn can be compensated by increasing the number of WAP devices as well. However, more WAP devices will increase the global NG-TCN costs (higher maintenance costs because of higher probability of failures and higher acquisition cost)."

Figure 28 and Figure 29 depict further developed architectures (derived from variants B and C), where the constraints are considered. Compared to variant B, Figure 28 illustrates, that additional CS (CS-3..CS-6) and WAP (WAP-3..WAP-6) devices are added to the wired consist network structure. So, each car contains two CS and two WAP devices, one pair each on each plane.

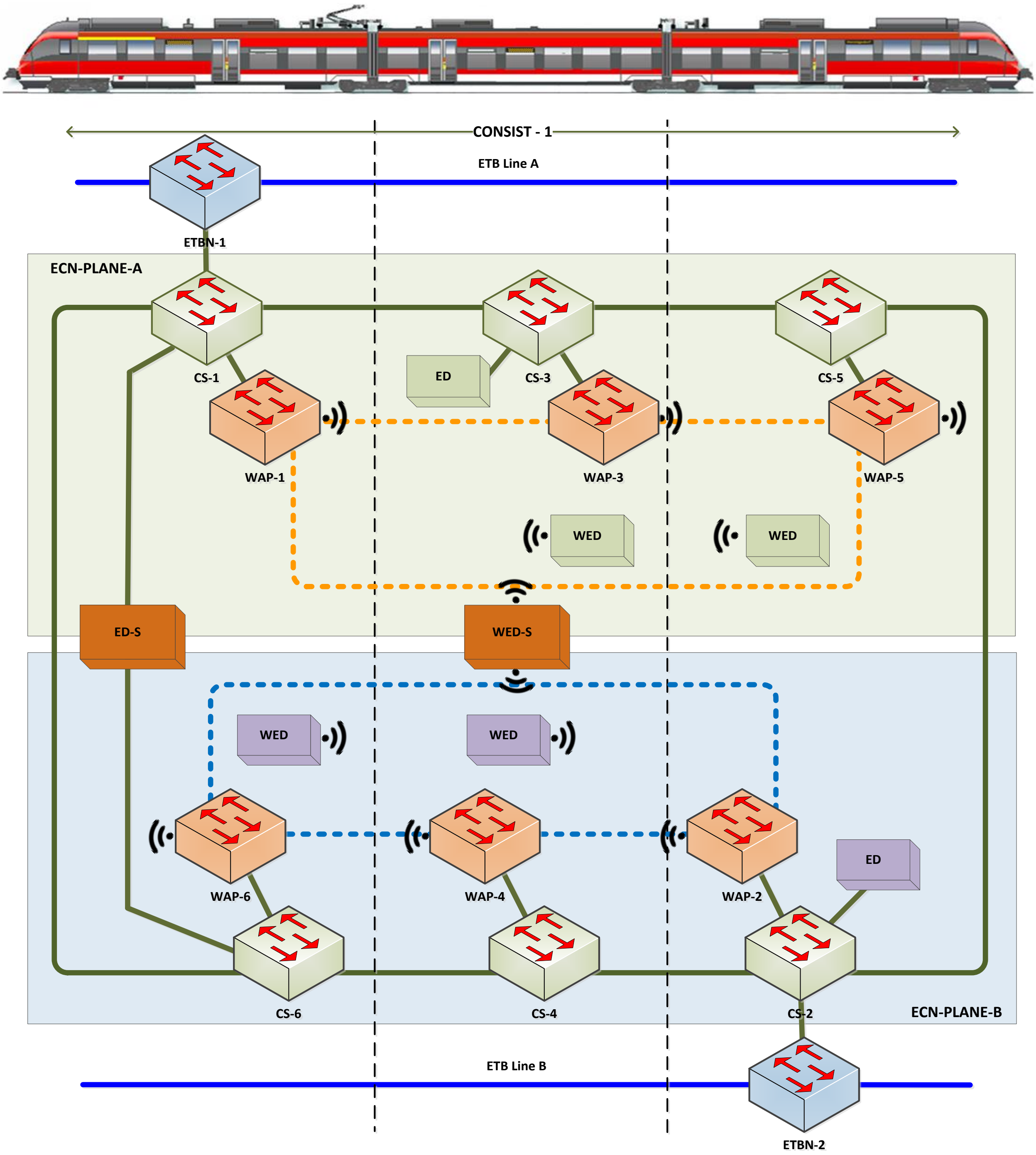


Figure 28: Overview wired ECN extended by WAP/WED (safe & TSN), multi WAP

Compared to variant C, Figure 29 shows, that additional WAP devices (WAP-3..WAP-6) are added to the wireless network (MESH structure) only. The additional WAP devices do not have connections to ETBN devices, following the NG-TCN concept [07].

The consist network is completely wireless. The WAP devices create a WLAN meshed network, based on the standard IEEE 802.11s, which is an amendment of IEEE 802.11 standard series. 802.11s supports a self-configuring multi-hop architecture to deliver broadcast/multicast and unicast messages efficiently (using appropriate routing protocols). This approach requires a high degree of technology (e.g. also the ability to support TSN), which in turn lead to high costs.

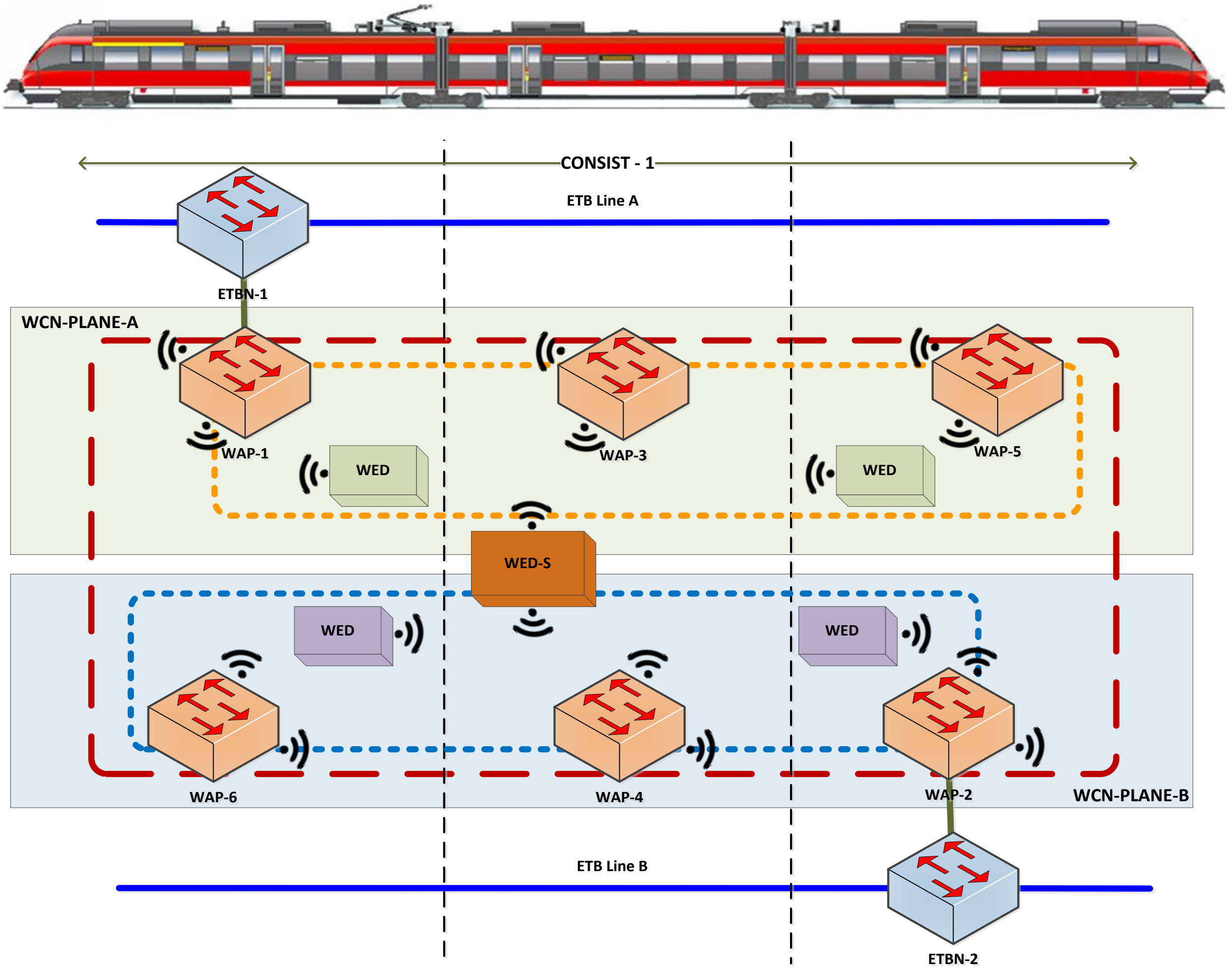


Figure 29: Overview wireless CN build up by WAP/WED (safe & TSN), multi WAP

A better radio coverage along the train could also be achieved by range extenders, so-called "repeaters". Their use is less expensive (less degree of technology), but also has disadvantages in terms of routing, bandwidth, transmission delay, interfering other radio channels, and security. Repeaters must always be compatible with the access point whose range they extend. Due to these drawbacks, the usage of repeaters is considered less beneficial for a wireless consist network.

6.2.4 Communication Layers

The communication layers define a framework which comprises all services which are related to the lower OSI communication layers (layers 1 until 4) and which are necessary to enable data communication between the radio devices connected to the IP-TCN. This in particular means:

Physical Layer:	Ethernet Links & Cables and Connectors Radio Links & Antennas
Data Link Layer:	MAC Switching Quality of Service (QoS) Traffic shaping / Traffic policing Virtual LANs (VLAN) Redundancy Wireless Access Point
Network Layer:	Addressing IP routing IP MC routing Redundancy (gateway redundancy)
Transport Layer:	UDP, TCP

More details about which layers are used on which interface are defined in chapter 6.3

6.2.5 RAMS Aspects

Reliability

A WAP device is treated as network device (ND). It is either connected to a CS or ETBN/WLTBN device. A WED device is treated as end device (ED) in the context of this specification and regarding RAMS aspects.

The reliability is in accordance with IEC 61375-3-4 2014 Annex A.4.

Availability

The availability of the wireless network components can be increased by redundancy. The redundancy is in accordance with IEC 61375-3-4 2014 subclause 4.5 Redundancy.

Maintainability

Fault detection

To support maintenance the WAP and WED devices provide status and counter information which allow pinpointing special network faults, be it either on the wired interface and/or on the radio interface.

Preventive maintenance

The WAP and WED devices contain no wearing off components requiring maintenance activities during their lifetime, like batteries or mechanical parts. However, it is possible to monitor parameters which may indicate a degradation of physical (electrical and mechanical) parameters which may lead to a failure over time.

Safety

There are no safety requirements defined for the WAP and WED devices, meaning that the wireless network, together with its defined services, can only be used for regular operation (black channel). However, by using SDTv2/SDTv4 as a safe end-to-end communication protocol, it is principally possible to exchange safety related data over the wireless network as well.

6.2.6 Quantities

The overall number of possible and addressable hosts in one consist subnet is defined as 16382 (according to IEC 61375-2-5). From network perspective WAP and associated WED are treated as ED (hosts). In addition, the number of WED is limited to the capabilities of the peer WAP. Table 30 presents an overview of the theoretical values (Number of maximum nodes).

6.2.7 Time Synchronisation

Time synchronisation is in accordance with IEC 61375-3-4 2014 subclause 4.10 End Device interface.

6.2.8 Security Aspects

The security of the wireless network can be improved by various measures. On the one hand, access to devices can be made more difficult by special structural features (the WAP and their cabling shall be in protected locked cabinets that cannot be accessed by not authorized person), insofar as they are static devices. On the other hand, wireless networks can be hidden from software point of view. Further measures like

- using encoded SSID name,
- enabling MAC Address filtering,
- knowing the devices which can connect,
- disabling remote WAP administration via wireless client,
- turning off WAP if not needed, and/or
- adding WIDS/WIPS to monitor the wireless system
- further improve network security.

6.2.9 TSN Aspects

Standardisation

According to the IEEE 802.1 Time-Sensitive Networking Task Group [19] two IEEE 802 standards are underway at present (802.1Qbz and 802.11ak). These standards make it legal to:

- integrate a bridge into a WAP (IEEE 802.11); and
- use a wireless station as a port on a bridge.

This in turn enables, using an IEEE 802.11 link interior to a network, instead of only at the edge. Upon completion these standards, the entirety of TSN is available for wireless links (IEEE 802.11).

Future Technology

According to [17] development and research activities are ongoing to overcome some of the limitations of current wireless technologies for the WLCN. In this sense, SHARP, WirelessHP and Wi-Fi 6 improve the performance of current Wi-Fi solutions, especially SHARP and WirelessHP in terms of deterministic medium access, and LTE Releases 15/16 (5G) improve the latency values of current LTE solutions.

SHARP is a Synchronous and Hybrid Architecture for Real-Time (RT) performance for scenarios where Ultra-Reliable and Low Latency Communications (URLLC) are demanded. SHARP provides Time Sensitive communications in both wired and wireless segments. The wired segment is a Time Sensitive Network (TSN) network which can provide RT over Ethernet, and the wireless segment is an extension of TSN which comprises a novel PHY layer and a Time Division Multiple Access (TDMA) Medium Access Control (MAC) layer.

Conclusion

In context of this specification, TSN cannot be used in wireless communication because the technology has still yet to be defined and developed.

6.2.10 MESH Aspects

A MESH network often is built up with mesh clients, mesh routers and gateways. While IEEE 802.11s is a wireless standard for mesh networking for IEEE 802.11 based devices, MESH in general is working with different wireless technologies including 802.11, 802.15, 802.16, cellular technologies and need not be restricted to any one technology or protocol.

Using the MESH technology in this project would support a completely wireless consist network. The CN will be built by radio links and routing protocols will make sure that data is optimally routed on the wireless links, see chapter 6.2.2 Variant C.

Apart from the fact that it would generally be possible to use MESH, there are aspects such as RAMS, TSN and security that indicate the opposite. There are also restrictions in the radio segment expected. In the already widely used radio spectrum (e.g. passenger Wi-Fi), a completely wireless CN would require additional bandwidth, which is at the expense of the bandwidth for other wireless end devices. Thus, the MESH technology is not part of this specification.

6.3 Interface specification for WLCN

6.3.1 General

According to the architecture presented in chapter section 6.2, a WAP is connected to either a CS or an ETBN (WLTBN analogously). In both cases, the WAP device is connected to an ED interface of the CS or ETBN. Figure 30 and Figure 31 show both possibilities.

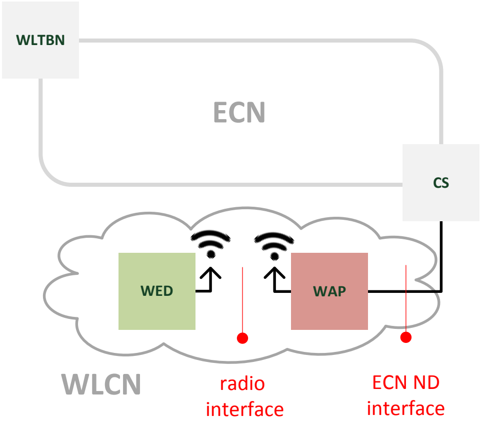


Figure 30: Wireless Access Interface via CS

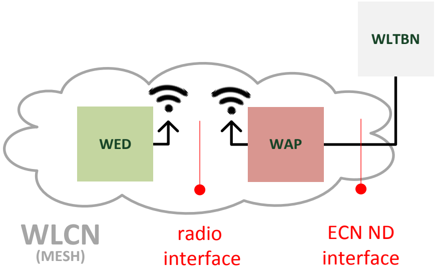


Figure 31: Wireless Access Interface via WLTBN

In the sense of IEC 61375-3-4 2014 a WAP device is a network device (ND). For the specification of the wired interface, IEC 61375-3-4 Subclause 4.9 is generally applicable. Since the WAP device is connected to an ED port to access the TCMS network, IEC 61375-3-4 Subclause 4.10 additionally applies to the definition of the wired interface.

The wireless interface is a new feature, which has not yet been defined in the IEC 61375 standard.

Basically, the radio interface of the WAP device is used to connect WED devices with the ECN (Figure 30) or WLCN (Figure 31). The ECN ND interface is the same for both networks (ECN and WLCN). In the case that WAP is connected to the CS, the CS establish a connection to the ECN which in turn offers also access to the TCMS network (train wide). In the other case the WAP device constitute a virtual WLCN (together with other WAP devices, using MESH technology) and is connected to the WLTBN for train wide communication.

6.3.2 ECN ND interface

The interface

- can have more than one physical Ethernet connection (e.g. if the device provides several separate radio interfaces (enabling separation of traffic to different LANs)
- main characteristics are listed in Table 31, with the restriction, that WAP devices are not supporting the TSN scheduled traffic.

Table 31: ECN ED interface characteristics

OSI Layer	Interface features
1	Two alternatives: • 8-wire CAT7 cable for 1000BASE-T Ethernet (IEEE802.3) or 100BASE-TX Ethernet • 4-wire CAT5e cable for 100BASE-TX Ethernet
2	Ethernet frame sending/receiving (IEEE 802.3 and IEEE 802.1), including VLAN tagging (IEEE 802.1Q)
3	IP incl. ICMP, IGMP
4	TCP/UDP
7	Exchange of ED/WED application data (conventional, based on TRDP or OPC-UA)

Physical Layer

In general, the physical layer is in accordance with the IEC 61375-3-4:2014 Subclause 4.9.4. To increase the bandwidth the standard allows using 1000BASE-T. However, the standard does not provide more precise information on protocols, cables, and connectors. The missing information is added in this document.

Protocols

10BASE-T and 100BASE-TX

The physical layer is in accordance with the IEC 61375-3-4:2014 Subclause 4.9.4.1.

1000BASE-T (GbE)

The physical layer is in accordance with IEEE802.3.

Cables

10BASE-T and 100BASE-TX

The physical layer is in accordance with the IEC 61375-3-4:2014 Subclause 4.9.4.2.

1000BASE-T (GbE)

Cables shall conform to ISO/IEC 11801 and IEC 61156-6. Class F (Category 7) with four twisted pairs shall be supported.

Cable gauge recommended for intra-car connection is 0,25 mm^2 (AWG24).

Connectors

10BASE-T and 100BASE-TX

The physical layer is in accordance with the IEC 61375-3-4:2014 Subclause 4.9.4.3.

1000BASE-T (GbE)

M12 X-coded connector (socket), defined in IEC 61076-2-109, should be supported on the ND side. In this case, M12 X-coded plug connector shall be used on the cable side.

Data Link Layer

The data link layer is in accordance with the IEC 61375-3-4:2014 Subclause 4.9.5.2, 4.10.3 respectively.

Network Layer

The network layer is in accordance with the IEC 61375-3-4:2014 Subclass 4.9.6, 4.10.4 respectively.

Transport Layer

The transport layer is in accordance with the IEC 61375-3-4:2014 Subclause 4.9.7, 4.10.5 respectively.

Application Layer

The application layer is in accordance with the IEC 61375-3-4:2014 Subclause 4.9.8, 4.10.6 respectively.

DHCP

DHCP Relay Agent Information Option, which is defined in IETF RFC 3046, may be supported by WAP. WAP may act as relay agent in order to assign specific IP addresses according to the information inserted by WAP.

6.3.3 Radio interface

This interface is the radio link between the devices WED and WAP. The interface can be based on different technologies depending on the intended function of the WED.

Based on the results in [17] and on the probable intended use (current and future), the following sections specify three technologies for use in the WLCN.

The main characteristics of this interface are listed in Table 32, with the restriction, that WAP and WED are not supporting the TSN scheduled traffic, at least time synchronization only.

Table 32: Radio interface characteristics

OSI Layer	Interface features
1 and 2	Radio link according to • IEEE 802.11 a/b/g/n/ac/ax (Wi-Fi, 2.4/5 GHz) • LTE (3GPP) • IEEE 802.15.4 (ZigBee)
2	Wireless security (IEEE 802.11i) Quality of Service (IEEE 802.11e, TS 23.401)
3	IP incl. ICMP, IGMP
4	TCP/UDP
7	Exchange of WED application data Note: from ECN perspective WAP is seen as an ED

From IEC 61375 perspective, a WLCN is a new feature, as it is radio technology. The following sub-chapter will specify the different layers. Whenever possible, reference is made to the IEC 61375 standard. Compared to the wired interface, most differences are in the physical and data link layers. The upper layers, network to application layer, are operating on same protocols. Deviations and additions are listed in the layer’s subchapters.

Physical Layer

Wireless physical link layers are not defined in IEC 61375-3-4 standard yet. The WAP can contain different physical radio interfaces. Depending on the used radio technology, the interface looks different.

IEEE 802.11 (Wi-Fi)

The Physical Layer of a WAP device shall conform to IEEE 802.11 a/b/g. Recommended is a conformance to IEEE 802.11 n/ac/ax which supports MIMO.

Transmission power

According to the distance between the communication partners, the transmission power may be adjusted, providing that the values requested to obey the local regulations are not exceeded.

For Wi-Fi an emission power of 100 mW is identified [17].

Frequency

In order to avoid interference between different wireless networks along a vehicle, the WLCN nodes provide several alternative radio frequencies. Table 33 lists channels and frequencies used by WLCN. In case that the frequencies are conflicting with the regulations of the radio administration authority, the operator applies for alternative frequencies compliant with such regulations.

Table 33: Frequencies used by Wi-Fi [21]

Protocol	Frequency [GHz]	Channel Width [MHz]	Modulation
IEEE 802.11ax	2.4 or 5	20, 40, 80, 160	MIMO-OFDM
IEEE 802.11ac wave2	5	20, 40, 80, 160	MIMO-OFDM
IEEE 802.11ac wave1	5	20, 40, 80	MIMO-OFDM
IEEE 802.11n	2.4 or 5	20, 40	MIMO-OFDM
IEEE 802.11g	2.4	20	OFDM
IEEE 802.11a	5	20	OFDM
IEEE 802.11b	2.4	20	DSSS
Legacy IEEE 802.11	2.4	20	DSSS, FHSS

Modulation

The modulation of the radio depends on the used protocol. Refer to Table 33 for the different Wi-Fi modulations.

Antenna

In order to guarantee the communication performances, the specifications of the antenna should support MIMO, 2,4 GHz band and 5 GHz band. The antenna shall be approved according to railway standards (EN 50155, EN 45545-2 and EN 50125-3) and IP 66/ IP 67.

The maximum allowed radiated power depends on the used frequency range and shall conform to local regulations.

These values of the overall radiation power shall not be exceeded by the gain of the antenna.

Antenna Cables

In order to guarantee the communication performances, the specifications of the antenna cables shall have an impedance of 50 Ohm and be usable for the Wi-Fi frequencies.

Connectors

Common connectors for antennas shall be used. This includes the following types:

- SMA, RP-SMA
- QMA
- N

- QN (QLF)

LTE (3GPP)

Transmission power

According to the distance between the communication partners, the transmission power may be adjusted, providing that the values requested to obey the local regulations are not exceeded.

For LTE an emission power of 1 W is identified (Table 4 of [18]).

Frequency

In order to avoid interference between different wireless networks along a vehicle, the WLCN nodes provide several alternative radio frequencies. Frequencies used by LTE are defined in [22] (not listed in this section due to the huge amount of frequencies). In case that the frequencies are conflicting with the regulations of the radio administration authority, the operator applies for alternative frequencies compliant with such regulations.

Modulation

The modulation is based on OFDM (with 64QAM) and SC-FDM. Access to the radio interface is provided in the downlink with OFDMA and in the uplink with SC-FDMA.

Antenna

In order to guarantee the communication performances, the specifications of the antenna should support MIMO for the used radio bands. The antenna shall be approved according to railway standards (EN 50155, EN 45545-2 and EN 50125-3) and IP 66/ IP 67.

The maximum allowed radiated power depends on the used frequency range and shall conform to local regulations.

These values of the overall radiation power shall not be exceeded by the gain of the antenna.

Antenna Cables

In order to guarantee the communication performances, the specifications of the antenna cables shall have an impedance of 50 Ohm and be usable for the LTE (3GPP) frequency bands.

Connectors

Common connectors for antennas shall be used. This includes the following types:

- SMA, RP-SMA
- QMA
- N
- QN (QLF)

IEEE 802.15.4 (ZigBee)

Transmission power

According to the distance between the communication partners, the transmission power may be adjusted, providing that the values requested to obey the local regulations are not exceeded.

For ZigBee an emission power of 10 mW is identified (IEEE 802.15.4).

Frequency

In order to avoid interference between different wireless networks along a vehicle, the WLCN nodes provide several alternative radio frequencies. Table 34 lists channels and frequencies used by IEEE 802.15.4. In case that the frequencies are conflicting with the regulations of the radio administration authority, the operator applies for alternative frequencies compliant with such regulations.

Table 34: Frequencies used by IEEE 802.15.4

Frequency [MHz]	Channel Width [MHz]	Modulation
868–868,6		BPSK
902–928	2	BPSK
2400–2483,5	2	QPSK

Modulation

The modulation of the radio depends on the used frequency. Refer to Table 34 for the different modulations.

Antenna

Since this technology mainly uses very small modules with integrated antennas, there are no special requirements for the external antenna. The modules shall be approved according to railway standards (EN 50155, EN 45545-2 and EN 50125-3) and IP 66/ IP 67.

The maximum allowed radiated power depends on the used frequency range and shall conform to local regulations.

These values of the overall radiation power shall not be exceeded by the gain of the antenna.

Antenna Cables

n.a.

Connectors

n.a.

Data Link Layer

Wireless data link layers are not defined in IEC 61375-3-4 standard yet.

IEEE 802.11

The IEEE 802.11 Data Link Layer is divided into two sublayers:

- The bottom portion of the Data Link Layer is the Media Access Control (MAC) sublayer, which is identical for all IEEE 802.11-based networks. The IEEE 802.11 standard defines operations at the MAC sublayer. The MAC sublayer acts as an interface between the lower layer PHY and the upper LLC sublayer.
- The upper portion is the IEEE 802.2 Logical Link Control (LLC) sublayer, which is identical for all 802-based networks.

MAC and LLC shall conform to IEEE 802.11 a/b/g/n.

MAC and LLC may be conforming to IEEE 802.11 n/ac/ax.

IEEE 802.1Q is currently not supported in IEEE 802.11 (VLAN tagging).

Traffic prioritisation (QoS) is defined in IEEE 802.11e and may be supported in aby the WAP device.

A WAP device according to IEEE 802.11 may support Wireless Consist Management (MESH), based on the standard IEEE 802.11s.

LTE (3GPP)

The LTE Data Link Layer is divided into three sublayers, providing mechanisms for reliability, security, and integrity:

- MAC protocol scheduling the medium access to the radio resources of LTE,
- RLC (Radio Link Control) protocol managing the segmentation or concatenation of data units, and
- PDCP (Packet Data Convergence Control) protocol performing ciphering tasks and optional IP header compression.

The MAC and RLC protocols conform to TS 25.322 (for 3GPP) and TS 36.322 (for LTE).

The PDCP protocol conform to TS 25.323 (for 3GPP) and TS 38.323 (for LTE).

QoS is defined in TS 23.401 and may be supported in the WAP device.

IEEE 802.15.4 (ZigBee)

Besides the physical layer IEEE 802.15.4 defines the MAC layer, enabling the transmission of MAC frames through the physical channel. LLC is not implemented.

MAC shall confirm to IEEE 802.15.4.

Note: Due to limitation in PHY (max. frame size up to 127 bytes), IEEE 802.15.4 does not use 802.1D or 802.1Q, i.e., it does not exchange standard Ethernet frames.

Network Layer

IEEE 802.11

Like all other IEEE 802 link layers, IEEE 802.11 can transport any network-layer protocol. Unlike Ethernet, IEEE 802.11 relies on IEEE 802.2 logical-link control (LLC) encapsulation to carry higher-level protocols (IPv4, ICMP, ARP). Thus, the network layer is in accordance with the IEC 61375-3-4:2014 Subclause 4.10.4.

LTE (3GPP)

There are three sublayers on the network layer:

- Non-Access Stratum (NAS), UE only,
- Radio Resource Control (RRC), and
- IP.

The NAS layer performs mobility with the core network using encrypted and integrity protected messages. On the RRC sublayer, all radio connections between the UE and the eNodeB are managed, including the configuration of all lower-level protocols down to the physical layer. Finally, the IP protocol handles transmissions to overlying transport protocols like TCP and UDP and, therefore, maintains connections to the IP network, e.g. WLCN, and thus, the network layer is in accordance with the IEC 61375-3-4:2014 Subclause 4.10.4.

RRC protocol conform to TS 25.331 (for 3GPP) and TS 36.331 (for LTE).

NAS protocol conform to TS 24.301 (for 3GPP).

IEEE 802.15.4 (ZigBee)

The MAC layer of IEEE 802.15.4 defines the upper layer of the technology. ZigBee is directly on top of the MAC layer.

The Network layer shall conform to ZigBee specification which is defined by the ZigBee Alliance.

IP connectivity shall be offered by ZigBee IP, which is an enhancement of ZigBee (using standard Internet protocols, such as 6LoWPAN, IPv6, PANA, RPL, TCP, TLS and UDP).

Transport Layer

IEEE 802.11

The transport layer is in accordance with the IEC 61375-3-4:2014 Subclause 4.10.5.

LTE (3GPP)

The transport layer is in accordance with the IEC 61375-3-4:2014 Subclause 4.10.5.

IEEE 802.15.4 (ZigBee)

The transport layer shall conform to ZigBee and ZigBee IP specifications which are defined by the ZigBee Alliance.

Application Layer

IEEE 802.11

The application layer is in accordance with the IEC 61375-3-4:2014 Subclause 4.10.6.

LTE (3GPP)

The application layer is in accordance with the IEC 61375-3-4:2014 Subclause 4.10.6.

IEEE 802.15.4 (ZigBee)

The application layer is in accordance with the IEC 61375-3-4:2014 Subclause 4.10.6.

6.3.4 List of Protocols

The following table (Table 35) lists all relevant protocols together with their relationship to the ISO OSI Layer they belong to, the affected network interface (IF) and their specification.

Table 35: List of used protocols

Protocol	OSI	IF: ECN ND	IF: Radio	Specification	Comment
100BASE-TX	1	X		IEEE 802.3	Fast Ethernet
1000BASE-T	1	X		IEEE 802.3	GbE
PoE	1	X		IEEE 802.3	Power over Ethernet (PD)
WLAN	1		X	IEEE 802.11	PHY level (FHSS, DSSS, OFDM, HR-DSSS, ERP)
LR-WPAN	1		X	IEEE 802.15.4	PHY level (DSSS)
EUTRAN	1		X	TS 36.201	PHY level (OFDM, OFDMA, SC-FDMA)
WLAN	2		X	IEEE 802.11	MAC (and LLC level)
LLC	2		X	IEEE 802.2	
WPA2	2		X	IEEE 802.11i	
MESH	2		X	IEEE 802.11s	Wireless Routing
RLC	2		X	TS 25.322, TS 36.322	
PDCP	2		X	TS 25.323, TS 38.323	
EAP	2	X		IEEE 802.1X	
EAPOL	2	X		IEEE 802.1X	EAP over LAN
LLDP	2	X		IEEE 802.1AB	
VLAN	2	X		IEEE 802.1Q	
QoS	2		X	IEEE 802.11e TS 23.401	“QoS” for WLAN “QoS” for LTE (3GPP)
AODV	3		X		Routing protocol; e.g. used by ZigBee
RRC	3		X	TS 25.331, TS 36.331	
NAS	3		X	TS 24.301	LTE UE only
ARP	3	X		RFC 826	

Protocol	OSI	IF: ECN ND	IF: Radio	Specification	Comment
ICMP	3	X		RFC 792	
IP	3	X		RFC 791	IP version 4
UDP	4	X		RFC 768	
TCP	4	X		RFC 793	
IGMP	4	X		RFC 2236, RFC 3376	Version 2 and 3
DHCP	7	X		RFC 2131	
DNS	7	X		RFC 1034, RFC 1035	
FTP	7	X		RFC 959	
NTP	7	X		RFC 1305	
SNMP	7	X		RFC 1901, RFC 1905, RFC 1906, RFC 1157	
SSH	7	X		RFC 4250	
syslog	7	X		RFC 5424	
TRDP	7	X		IEC 61375-2-3	IEC compliant IP-TCN

6.3.5 Monitoring

WAP and WED devices shall support status and monitor information for diagnostic purposes (like warnings, errors, network statistics, network security) and predictable maintenance work on the ECN ND interface (6.3.2). This information shall be provided in the format of:

- WAP: SNMP
- WED:
  - a) SNMP and/or
  - b) process or message data according to IEC 61375-2-3 Annex A

SNMP

The motoring information based on SNMP is in accordance with the IEC 61375-3-4:2014 Subclause 4.12.1.

IEEE 802.11

For IEEE 801.11 based devices the IEEE802dot11-MIB should be supported.

LTE (3GPP)

For LTE (3GPP) based devices SNMP according to TS 32.101 annex A [23] should be supported.

IEEE 802.15.4 (ZigBee)

n.a.

6.3.6 Configuration

To enable WAP and WED devices to communicate with each other via radio, their radio interface must be configured accordingly (e.g. operation mode, SSID, security credentials, known hosts, MAC-filtering, addressing mode). In general, a static configuration is recommended, which is set after each restart and can also be read from an external medium if required. In order to configure at least WAP devices remotely (globalized network management), the WAP device may offer a configuration download mechanism or may make use of the SNMP write functions. A device configuration via web interface shall be avoided.

6.3.7 Antenna

In order to provide a robust communication, appropriate antennas must be used at WAP and WED devices. The usage of antennas depends on spatial conditions, the distance to coverage, and number of WAP used per consist. To further improve the communication external antennas might be necessary instead of antennas in housing. It is very likely that WED devices can rather be equipped with a built-in antenna, whereas WAP devices certainly need to be equipped with external antennas to improve radio link quality. Furthermore, the quality of the radio signals can be improved by using technical features such as MIMO, spatial diversity or beamforming [18].

6.4 Design Constraints

During the specification of the WLCN it was noticed that there are differences compared to the conventional LAN technology. This section of the document highlights some differences.

6.4.1 Data Link Layer

VLAN

In both, the conventional TCN according to IEC 61375, and the NG-TCN developed in R2R and CTA, it is possible to virtually separate data traffic from related terminals on the physical lines of the network if the lines offer corresponding capacity margins. This could reduce the actual number of physical lines. TCN supports VLAN according to IEEE 802.1Q in the CS, WLTBN and end devices. Devices that are logically grouped by a virtual LAN use a unique VLAN ID (configuration element) on the Ethernet level.

IEEE 802.1Q is not supported in the area of wireless transmission technology (radio). However, data separation of related device groups can be achieved differently. In principle, devices that belong to an SSID (according to IEEE 802.11) form a common and separate communication group anyway. Data that is forwarded from this group by WAP to the LAN can be assigned a VLAN ID by configuring the WAP accordingly in order to identify the VLAN membership in the connected LAN (Figure 32 and Figure 33). Some WAP even offer a further grouping of the end devices by so-called virtual SSIDs (Figure 34). These in turn are converted to corresponding VLAN IDs in the LAN by configuration. In the case of wireless end devices, the VLAN ID configuration is not required at the expense of the radio module configuration.

This means that SSIDs or virtual SSIDs can be used to separate data from the different OOS and TCMS domains or to separate data within a domain and in relation to a specific control function.

In this context, aspects such as safety, security and reliability shall be considered and evaluated separately.

Figure 32 depicts the mapping of an SSID to a VLAN ID.

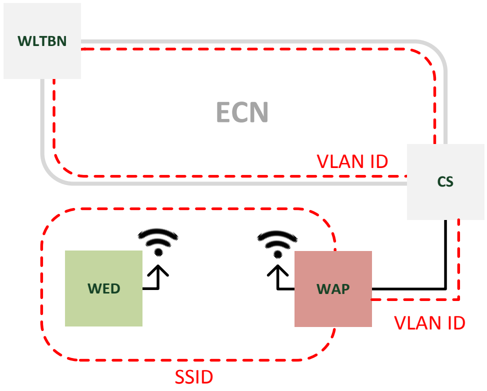


Figure 32: SSID to VLAN mapping

The WAP depicted in Figure 33 uses two radio interfaces, each connected to separate LAN interface. WED belonging to SSID A may communicate to ED which is part of VLAN 1. For WED belonging to SSID B a communication to ED in VLAN 2 is possible only.

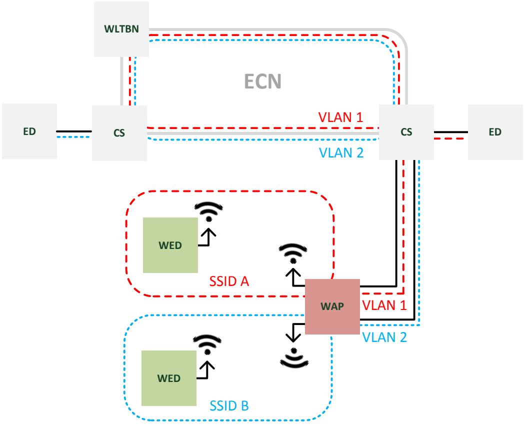


Figure 33: SSID to VLAN mapping, two radio and LAN interfaces

Figure 34 depicts in principle the same as Figure 33, however the WAP uses only one radio interface for providing virtual SSIDs. The virtual SSIDs can be mapped to different VLAN IDs on the wired interface.

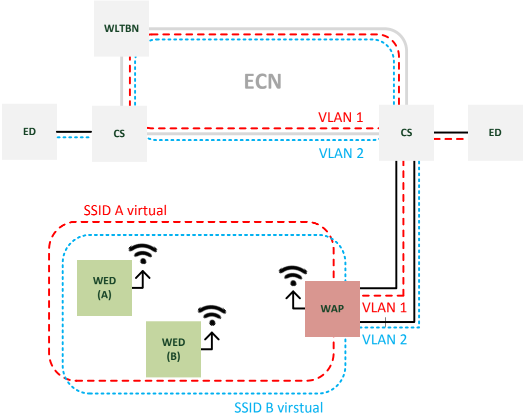


Figure 34: Virtual SSID to VLAN mapping

Data Separation

Assuming secure and reliable communication, the distribution of data from different domains (e.g. OOS and TCMS) within the same wireless network (shared WAP device) would be possible. If a logical separation of the data is still required (security), this could be realized with the help of different SSIDs or virtual SSIDs.

6.4.2 Transport Layer

Multicast

In an Ethernet network, multicast is a proper way to reduce the load on the network, when several stations receive the same data from a sender, e.g. multimedia data. Stations which want to receive data via multicast typically use IGMP to join a multicast group. The managed switches in between the sender and receivers will handle the multicast accordingly.

Since multicast wasn’t designed for Wi-Fi technology the handling of multicast differs and the handling leads to the effect, that multicast as well as broadcast data communication is slow compared to unicast. In the case of multicast/broadcast data will be sent at a kind of "lowest common denominator" transmission speed (the slowest station defines transmission speed) (see [24] and [25]). WAP vendors provide a “Multicast-to-Unicast Conversion” to improve the transmission speed. The WAP sends a unicast copy of the frame to each intended receiver, using IGMP snooping to determine peer receiver stations. Further benefit of this conversion is, that stations which aren’t the intended receivers don’t need to wake up to listen to the frame, reducing their power or battery consumption (if they support power save mode).

Load Balancing

Depending on the number of used WAP devices and associated WED devices the load by be spread to distribute the load evenly. The association is a configuration item and can be achieved by defining allowed WED devices per WAP device.

7. DETAILED SPECIFICATION OF THE MCG INTERFACE WITH THE ADAPTABLE COMMUNICATION SYSTEM

Figure 35 shows the interfaces of the Adaptable Communication System as it is described by X2Rail WP3. The MCG would act as an "App", see Figure 35. The proposed interface from X2Rail is SIP/IP based [26].

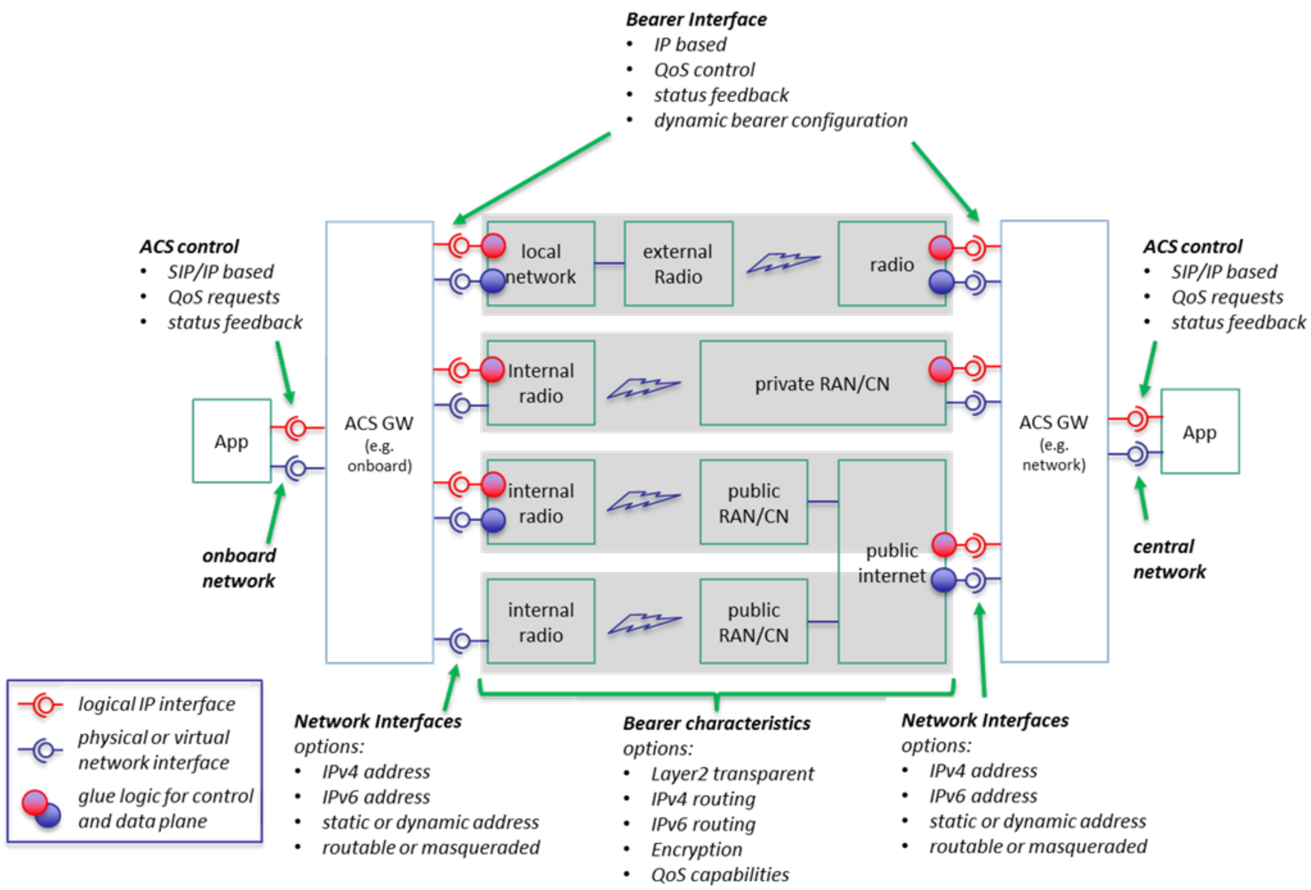


Figure 35: ACS interfaces with exemplary bearer configurations [26]

The ACS aims to provide an abstraction between the network connectivity on Layer 3 and multiple underlying radio technologies. The MCG can use the ACS where available and will directly use available radio systems otherwise. The MCG therefore can use the ACS as an underlying, managing service layer via a defined interface. This interface will be based on standard IT technologies and protocols. The technical details of this interface are currently under development. Standardization is in scope of ETSI TC RT and FRMCS project in close cooperation with X2Rail work packages.

The currently discussed solution by X2Rail is using the SIP protocol closely aligned to 3GPP MCX framework as a control protocol between the ACS and its clients (see Figure 35). The usage of this protocol is seen critical by CONNECTA -2 as it has some negative implications when used in a setup with firewalls. Therefore, CONNECTA-2 is proposing a more suitable and simple standard protocol for the information exchange between the ACS and its clients, e.g. http REST.

Since the standardization is driven by FRMCS, a detailed interface specification for the applications is not in scope of X2Rail WP3. The system specification from X2Rail WP3 [26] will define required content in a more generalized way and give some specifics as examples. These principles are then validated in the X2Rail demonstrators. The interface specification is thus done only on demonstrator level to achieve an integrated operation of the demonstrators.

For the integration of CONNECTA-2 and X2Rail demonstrators the following interface is planned:

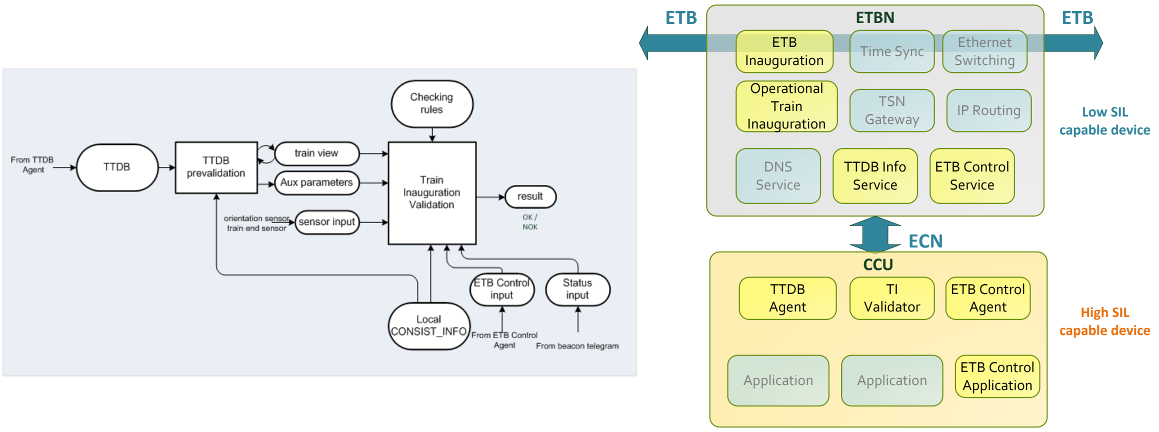
- Physical interface for MCG and GCG: Ethernet
- Logical interface: IPv4 with static addressing defined by ACS demonstrator (no DHCP/DNS). NATing is applied optionally in the train side ACS gateway to allow the usage of local addresses in the train networks
- Protocols:
    - control interface: an implementation of the application side SIP-client is provided by X2Rail, e.g. as a library. The library provides a simplified API to realize the main ACS functionalities and can be implemented as part of MCG and GCG. As a fallback in case of critical implementation problems, an external agent can statically register MCG and GCG and establish a connection via the ACS (procedure for non-ACS enabled devices)
    - data plane: the ACS supports unicast UDP, TCP and ICMP protocols. Different QoS profiles can be applied based on IP-addresses and protocol ports.

For demonstrator integration it is thus planned to shift the protocol interface from SIP protocol to the API provided by X2Rail. This API is not yet completely defined and will be aligned between X2Rail and the demonstrator owners of CONNECTA-2 WP2 and X2Rail WP3.

8. SPECIFICATION OF THE WIRELESS TRAIN INAUGURATION

8.1 General principles coming from NG-TCN

NG-TCN defined in CONNECTA D3.5 [06] maintains the splitting of the train inauguration in two phases by defining the train backbone topology discovery, called “ETB inauguration”, and defining the train composition discovery, called “operational train inauguration”. In order to provide the train composition information with a high safety integrity level (SIL4), the result of the train inauguration, namely the operational 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 TI Validator and the function split proposed for NG-TCN can be depicted in Figure 36.a) and Figure 36.b).



a)

b)

Figure 36: NG-TCN SIL4 Inauguration principles: a) TI Validator block diagram, b) Services involved in safe train inauguration

The Wireless Safe Train Inauguration over the WLTB should keep the same function split between ETBN and CCU, as well as the TI Validator in order to achieve train composition with high SIL. Moreover, although the train backbone topology discovery and the discovery of the train composition must be redesigned due to the wireless medium nature, the output of the Wireless Train Backbone (WLTBN) in the Wireless Safe Train Inauguration should be a TTDB with the same safety integrity level as the one achieved by ETBNs in wired medium.

For the safe TTDB calculation by the WLTBN, the proposal made by Roll2Rail for the wireless train inauguration may be valid, although the achievable safety integrity level should be analysed in detail. In the following lines a new Topology Discovery procedure adapted to direct Consist-to-Consist (C2C) communications and the train composition discovery are explained.

8.2 Train Topology Discovery

The Train Topology Discovery is linked to the radio technology to be used for the WLTB. The radio system shall be able to create wireless communication network between the consists of the train unit without any railway-specific function. Due to the wireless domain peculiarities there are a couple of functions that are foreseen:

- WLTBN shall have a mechanism to discover adjacent WLTBNs, i.e. WLTBN form adjacent consist in DIR 1 and DIR2.
- Only WLTBN of the coupling group shall be able to communicate with each other, excluding messages coming from other sources (other consists from other train units).
- WLTBN participating in the WLTB should be able to create a local forwarding table for the WLTBN which is not achievable with a single hop (for the multihop topology option). The following protocols are under consideration: AODV (RFC 3561) [12], OLSRv2 (RFC 7181) [13] and B.A.T.M.A.N. advanced [14].

These functions and the protocols to achieve them will be explained in detail within the WLTB specification.

8.3 Train Composition Discovery

8.3.1 General

Once all WLTBN are logically within the same network (independently if it's over direct link or through intermediates WLTBN), different consists shall be able to identify the ID and the direction of the adjacent consists. In order to do so, RFID transponders installed in the frontend and backend of the consist should transmit the adjacent consists the following information:

- the consist identifier (consist id) of the local consist
- the direction information (end in direction 1 or end in direction 2) of the local consist
- the identifier of the WLTB and WLTBN
    - WLTB ID (this ID must be unique)
    - WLTBN ID (these IDs must be unique), the adapted ETBN MAC address will be taken.

With this information each WLTBN should be able to create its own “partial view” of the topology. Using a similar message structure as the one described in the IEC 61375-2-5 for the TTDP Topology frame (see Annex A), each WLTBN can share its partial view and from this information each consist can create its own Train Network Directory (TNDir) as illustrates Figure 37. Since the RFID transceiver may retrieve multiple WLTBN IDs (in case WLTBN redundancy), the WLTB identifier is used to send in each WLTB the corresponding WLTBN ID.

.

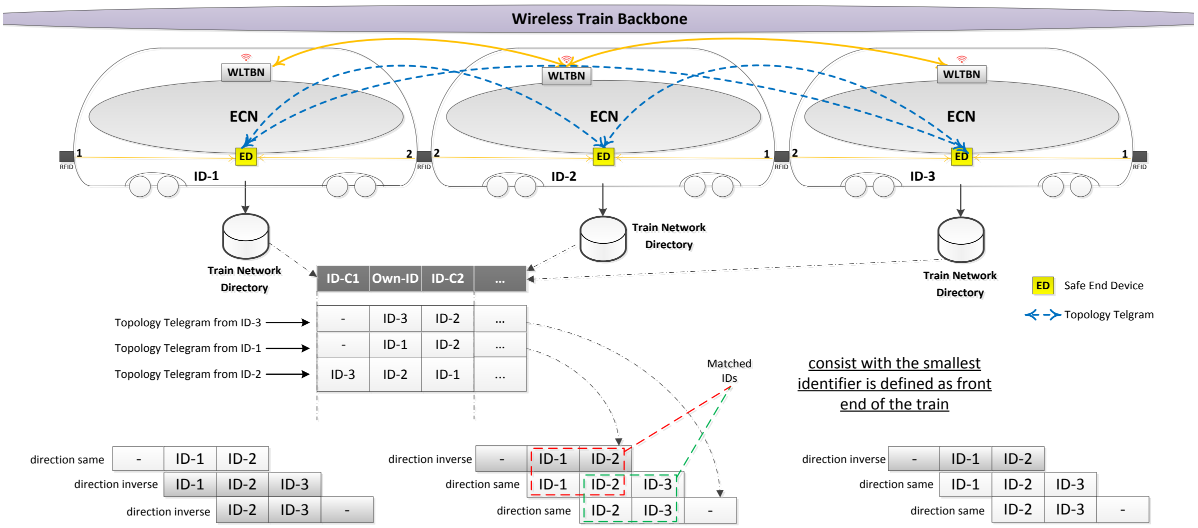

Wireless Train Backbone
WLTBN
WLTBN
WLTBN
ECN
ECN
ECN
ED
ED
ED
1
2
2
1
2
1
RFID
RFID
RFID
RFID
ID-1
ID-2
ID-3
Train Network Directory
Train Network Directory
Train Network Directory
ID-C1 Own-ID ID-C2 ...
Topology Telegram from ID-3 → - ID-3 ID-2 ...
Topology Telegram from ID-1 → - ID-1 ID-2 ...
Topology Telegram from ID-2 → ID-3 ID-2 ID-1 ...
ED Safe End Device
Topology Telgram
Matched IDs
consist with the smallest identifier is defined as front end of the train
direction same - ID-1 ID-2
direction inverse ID-1 ID-2 ID-3
direction inverse ID-2 ID-3 -
direction inverse - ID-1 ID-2
direction same ID-1 ID-2 ID-3
direction same ID-2 ID-3 -
direction inverse - ID-1 ID-2
direction same ID-1 ID-2 ID-3
direction same ID-2 ID-3 -

Figure 37: Safe Train Inauguration Procedure

In case a L2 forwarding protocol like B.A.T.M.A.N. advanced [14] is used, the TTDP topology frame structure could be used with minimum changes.

The information needed for the TTDB calculation with SIL2 must be transmitted using the frame structure defined in Annex A, which contains information obtained from RFID transponders. The safety analysis to be made within this task will have to evaluate whether the data integrity protection is enough or additional safety measures have to be adopted. Depending on the result, the data integrity may be provided by a CRC based on SC-32 within the TOPO FRAME structure defined in Annex A.

The Train Composition Discovery phase runs in the AETBN and independently of the Train Topology Discovery one. This means that the AETBN starts sending TTDP TOPOLOGY frames as soon as it turns on, although until the routing/forwarding table is calculated by Wireless Devices within the Train Topology Discovery phase, the messages sent to unreachable nodes will be discarded.

In order to reduce the wiring in the consist, RFID transponders may be connected to the WLTBN through the ECN. However, this will imply to ensure safety integrity. A safety analysis should evaluate whether this safe data transmission shall be covered by SDTv4 (setting the SafeTopoCount to 0) or a CRC based on SC-32 would be sufficient.

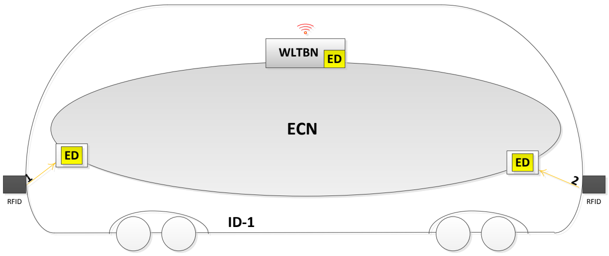


Figure 38: RFID transceivers connected though the ECN

8.3.2 Train Composition Discovery with redundant WLTBNs

In the previous lines the Train Composition Discovery protocol over the WLTB has been described. However, this protocol does only cover the case when each consist only has a single WLTBN. However, due to WLTB availability reasons it may be necessary to install multiple WLTBNs in each consist. The main reasons for that are to overcome availability problems in case of WLTBN failure and to overcome wireless channel unavailability. Therefore, multiple WLTBNs working on different frequencies may be needed. This approach, comparing to the wired ETB does not create a single train-level network but two, each of them working on different frequencies. That is to say, a WLTBN of the WLTB-1 will not be able to communicate to a WLTBN from the WLTB-2 since both work in different frequencies in order to provide the desired channel diversity.

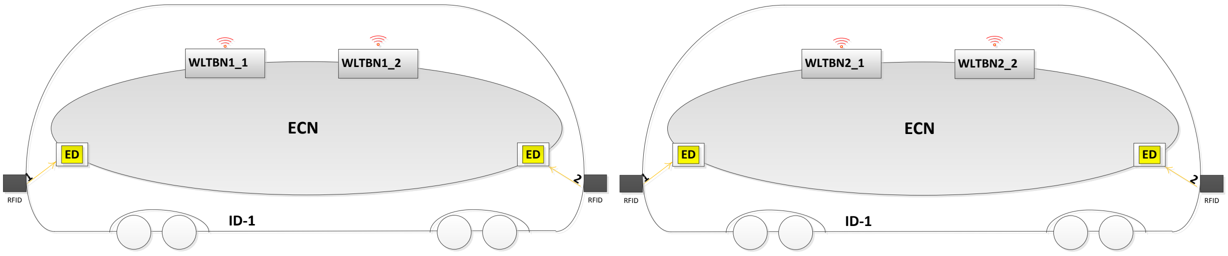


Figure 39: Architecture with redundant WLTBNs

Within this redundant architecture the wireless inauguration could be made in two ways: 1) using the WLTBN redundancy for the Train Composition Discovery, i.e. the result will be a single SIL2 TTDB; or 2) performing independent Train Composition Discovery besides a CSTINFO exchange in each WLTB, i.e. the result will be two SIL2 TTDB.

A) Single Train Composition Discovery with multiple WLTBN

This approach uses both WLTB (WLTB-1 and WLTB-2) to create a single TTDB. In order to do so, the RFID transceivers in each consist send the data retrieved from the adjacent consists to a common multicast address to which both WLTBN in the consist are listening (represented in blue in Figure 40).

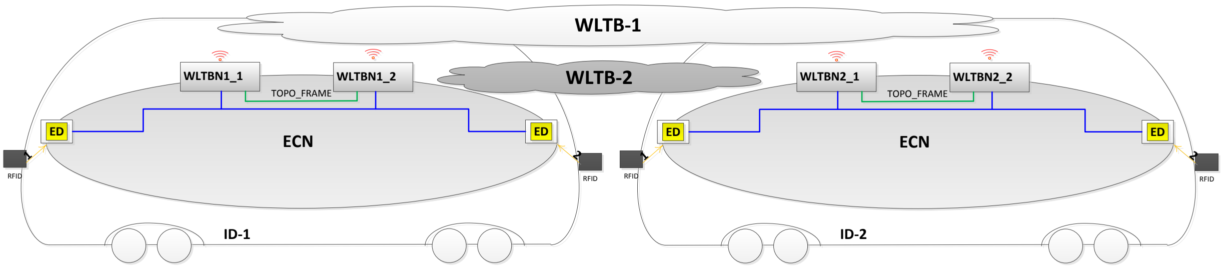


Figure 40: Wireless common inauguration with redundant WLTBNs

With this information each WLTBN in the consist will perform the Train Composition Discovery described in section 8.3.1 and the CSTINFO exchange from IEC 61375-2-3. However, as the goal is to get a common TTDB, both WLTBNs in the consist must communicate in order to exchange their results and one of them will act as “Master”, responsible to provide information to the CCU, and the other as “Slave”[13]. To communicate the TTDB between both WLTBNs the TTDB manager interface defined in the IEC 61375-2-3 [10] over a dedicated VLAN (represented in green in Figure 40) will be used. For this TTDB data sharing, the “Slave” WLTBN will act as ED ECSC and the “Master” WLTBN as ECSP. The “Master” WLTBN will compare the retrieved information with its own TNDir and CSTINFO. This way, if one WLTBN in the train composition fails the information corresponding to that consist can be obtained from the other WLTB. In case the TNDir or CSTINFO from the slave WLTBN is contradictory[14] with the master’s one, then the inauguration will fail. After this TTDB calculation, in case it is successful the TTDB is sent back to the slave WLTBN, otherwise the inauguration failure is communicated to the slave WLTBN. Figure 41 summarizes in a sequence diagram the data exchange for this approach.

[13] The Master and Slave role can be handled with VRRPv3 as proposed in NG-TCN for ETBN redundancy.

[14] Note that contradictory information here does not mean absence of information but different received information from neighbor WLTBN such as different CstOrientation for the same consist.

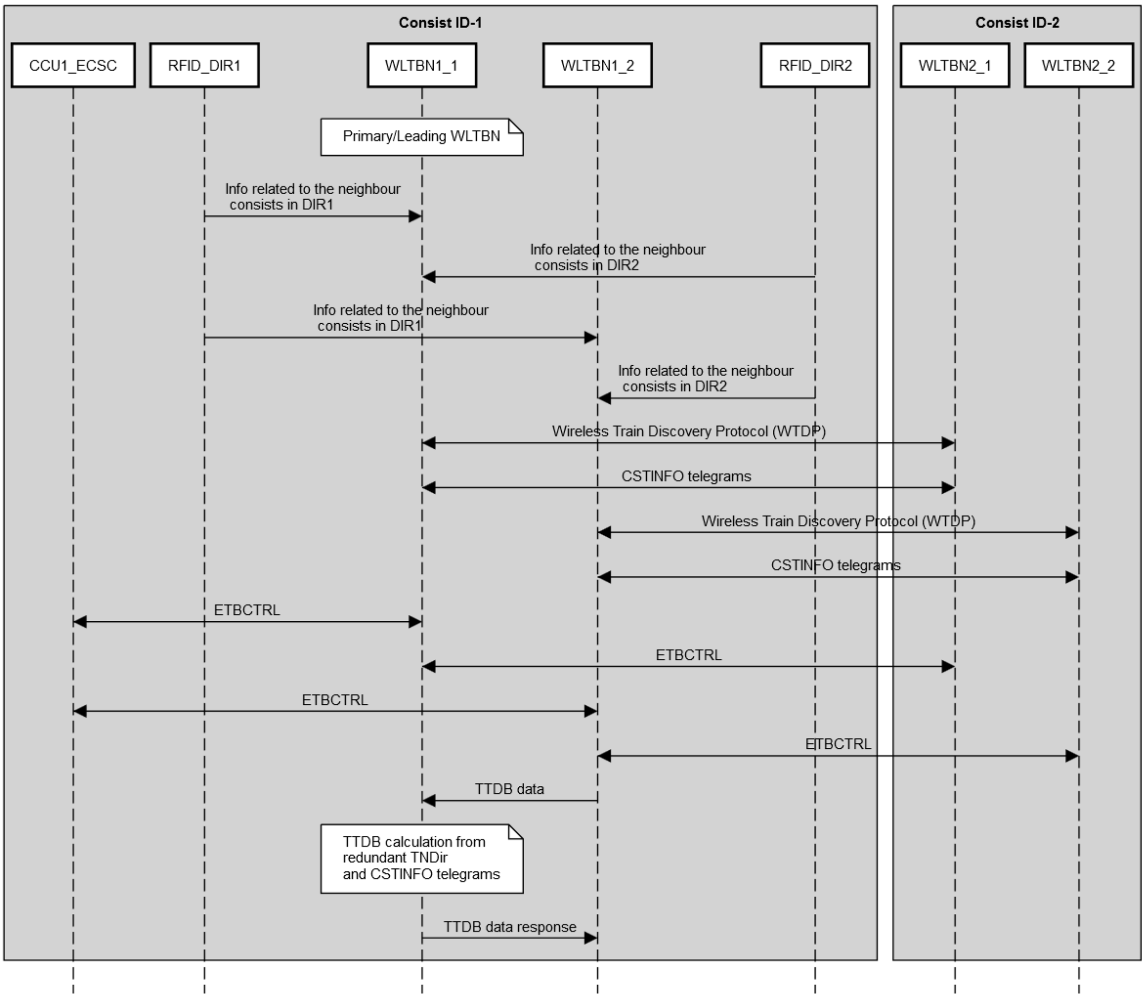

Consist ID-1
Consist ID-2
CCU1_ECSC
RFID_DIR1
WLTBN1_1
WLTBN1_2
RFID_DIR2
WLTBN2_1
WLTBN2_2
Primary/Leading WLTBN
Info related to the neighbour consists in DIR1
Info related to the neighbour consists in DIR2
Info related to the neighbour consists in DIR1
Info related to the neighbour consists in DIR2
Wireless Train Discovery Protocol (WTDP)
CSTINFO telegrams
Wireless Train Discovery Protocol (WTDP)
CSTINFO telegrams
ETBCTRL
ETBCTRL
ETBCTRL
ETBCTRL
TTDB data
TTDB calculation from redundant TNDir and CSTINFO telegrams
TTDB data response

Figure 41: Wireless Inauguration Sequence Diagram

In summary, the folowing roles for involved equipment are distinguised:

- For the connection between master WLTBN and CCU:
  - Master WLTBN -> performs as ECSP
  - CCU -> Performs as ECSC
- For the connection between WLTBNs
  - Master WLTBN
    - Performs as ED in TTDB manager interface to retrieve the TTDB from the slave WLTBN.
    - Performs as ECSP in TTDB manager interface to send the TTDB data response after calculating the TTDB with the information coming from both WLTBNs.
  - Slave WLTBN

- Performs as ECSP in TTDB manager interface to send the TTDB to the master WLTBN.
- Performs as ED in TTDB manager interface to retrieve the TTDB data response after calculating the TTDB with the information coming from both WLTBNs.

Note that in current inauguration process explained in IEC 61375-2-3 and IEC 61375-2-5, as well as in the Safe Inauguration proposed in CTA:D3.5 [06] for the NG-TCN, the CSTINFO is transmitted only by one ETBN. This is not the case for the Wireless Inauguration.

Once a SIL2 TTDB has been obtained by the process explained above the TI Validation in this case may be carried out using the methods explained in sections 8.4.1 and 8.4.2.

Example of TNDir calculation

In this example there are three consists coupled and carrying out the inauguration (see Figure 42). The WLTB-2 in partially unavailable, meainnig that its RDs are working but its AETBN is not available.

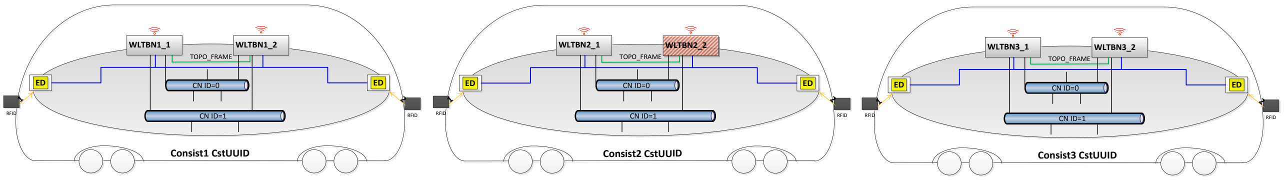


Figure 42: Example inauguration topology

This situation produces two different TNDir tables in the WLTB-1, Table 36, and in the WLTB-2, Table 37. While Table 36 has all the needed data to create the TNDir, the Table 37 was created without the TOPOLOGY frames coming from the WLTBN2_2.

Table 36: TNDir obtained from WLTB-1

	uint8[16]	uint32							
	CstUUID	b31..b30	CN Id	b23..b22	Subnet Id	b15..b14	ETBN Id	b7..b2	CstOrientation
0	Consist1 CstUUID	0	1	0	1	0	1	0	'01'B
1	Consist1 CstUUID	0	2	0	2	0	1	0	'01'B
2	Consist2 CstUUID	0	1	0	3	0	2	0	'10'B
3	Consist2 CstUUID	0	2	0	4	0	2	0	'10'B
4	Consist3 CstUUID	0	1	0	5	0	3	0	'01'B
5	Consist3 CstUUID	0	2	0	6	0	3	0	'01'B

It is worth noting that in Table 37 the CstUUID and CstOrientation corresponding to Consist2 have been included although no direct information has been received from Consist2. This information comes from the TOPO frames received from Consist1 and Consist2, which include the information obtained from their respective RFID transceivers (i.e. Consist2 CstUUID, DIR, WLTB ID and WLTBN ID).

Table 37: TNDir obtained from WLTB-2

	uint8[16]	uint32							
	CstUUID	b31..b30	CN Id	b23..b22	Subnet Id	b15..b14	ETBN Id	b7..b2	CstOrientation
0	Consist1 CstUUID	0	1	0	1	0	1	0	'01'B
1	Consist1 CstUUID	0	2	0	2	0	1	0	'01'B
2	Consist2 CstUUID	0		0		0	2*	0	'10'B*
3	Consist2 CstUUID	0		0		0	2*	0	'10'B*
4	Consist3 CstUUID	0	1	0	5	0	3	0	'01'B
5	Consist3 CstUUID	0	2	0	6	0	3	0	'01'B
(*) Information obtained from the RFID transceivers and transmitted by the adjacent neighbour consists.									

Since Table 36 and Table 37 have no contradictory topology data then the complete TNDir is taken, that is the Table 36. This TNDir is sent by the WLTBNs of the WLTB-1 to the WLTBNs of WLTB-2 in order to keep TNDir coherence between both redundant WLTBNs.

B) Redundant Train Composition Discovery

This approach will carry out the procedure exmplained in section 8.3.1, having as outcome two SIL2 TTDB, each of them corresponding to one of the two redundant WLTB (WLTB-1 and WLTB-2). The comparison between them by the TI Validator is explained in section 8.4.3.

8.4 TI VALIDATION

As previously mentioned, the TI Validator makes use of independent input information for the highly safety critical parameters ‘consist orientation’ and ‘train end’. For the wired safe train inauguration a proposal for a validation based on special beacon frames that can distinguish the orientation of the consist was specified. However, due to the multipath effect produced in wireless environments it is not possible to use this proposal. For the Wireless Safe Train Inauguration the following alternatives are proposed:

8.4.1 Train lines

This alternative is based on using train lines to verify the train-end and the orientation as it has been made traditionally. As it is depicted in Figure 43 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.

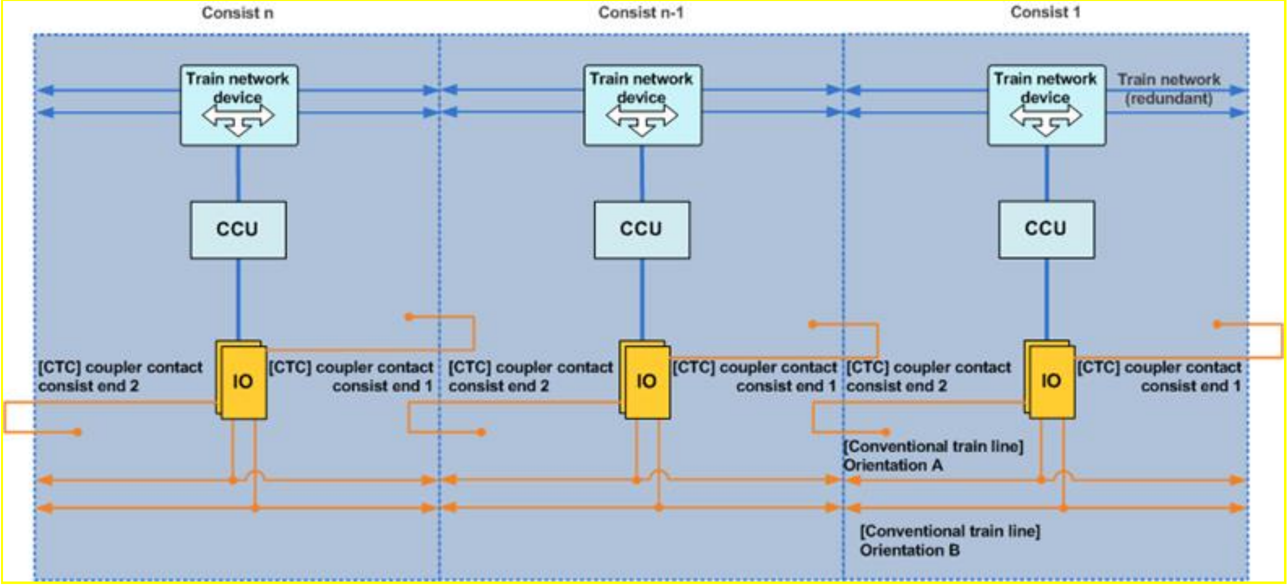

Consist n
Consist n-1
Consist 1
Train network device
Train network device
Train network device
Train network (redundant)
CCU
CCU
CCU
[CTC] coupler contact consist end 2
IO
[CTC] coupler contact consist end 1
[CTC] coupler contact consist end 2
IO
[CTC] coupler contact consist end 1
[CTC] coupler contact consist end 2
IO
[CTC] coupler contact consist end 1
[Conventional train line] Orientation A
[Conventional train line] Orientation B

Figure 43: Independent check with train lines (traditional way, source [06])

8.4.2 Additional SIL2 RFID transceivers

This alternative is based on using SIL2 RFID transceivers as independent sensor for TI validation. In order to ensure diversity with respect the RFID transponders used in Train Composition Discovery, these devices will be provided by different manufacturer. These transponders, located also in the frontend and backend of the consist, could be either connected to the CCU or communicate with the CCU ensuring data integrity (i.e. using SDTv4 or a CRC based on SC-32).

8.4.3 Comparison with another WLTB plane inauguration in parallel

This alternative is based on carrying out the wireless inauguration in parallel when two independent WLTBN are available, each one working in a different frequency. Figure 44 illustrates the redundant Train Composition Discovery and TTDB calculation explained in section 8.3 in each WLTBN of the consist, each one connected to one ECN plane. WLTBN-1 and WLTBN-2 will independently inaugurate and yield independent results. Since both inaugurations will produce a SIL2 TTDB, the comparison of both TTDB by the TI Validator could produce a SIL4 Train Inauguration. With this approach, each set of WLTBN and RFID transponder pair would provide enough diversity with respect to the other set used by:

- Removing common communication failures in the wireless link, i.e. using frequency diversity.
  Removing common RFID reading failures, i.e. using different manufacturers.

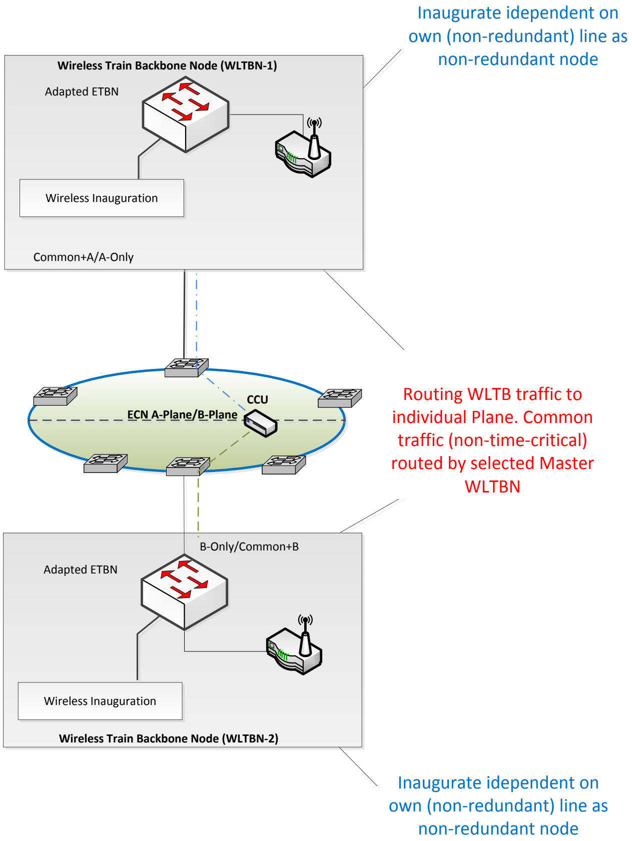

Inaugurate idependent on own (non-redundant) line as non-redundant node
Wireless Train Backbone Node (WLTBN-1)
Adapted ETBN
Wireless Inauguration
Common+A/A-Only
CCU
ECN A-Plane/B-Plane
Routing WLTB traffic to individual Plane. Common traffic (non-time-critical) routed by selected Master WLTBN
B-Only/Common+B
Adapted ETBN
Wireless Inauguration
Wireless Train Backbone Node (WLTBN-2)
Inaugurate idependent on own (non-redundant) line as non-redundant node

Figure 44: Wireless parallel inauguration

The procedure explained above allows obtaining high SIL inauguration using a parallel inauguration principle. However, the main handicap of this approach is the lack of availability during the inauguration process comparing to other alternatives. More details about this comparison are provided in section 8.5.

8.5 AVAILABILITY VS. SAFETY

The inauguration approach presented in section 8.3.2.A) together with a TI Validation explained in section 8.4.2 may provide up to SIL4 inauguration. Figure 45 depicts the complete architecture. Note that the RFID transceivers used for TI Validation communicate to the CCU and not to the WLTBNs of the consist (i.e. the RFID connected by blue logical link are used for TTDB calculation whereas the ones connected by red logical link are used for TI validation. For this communication a different multicast address is used.

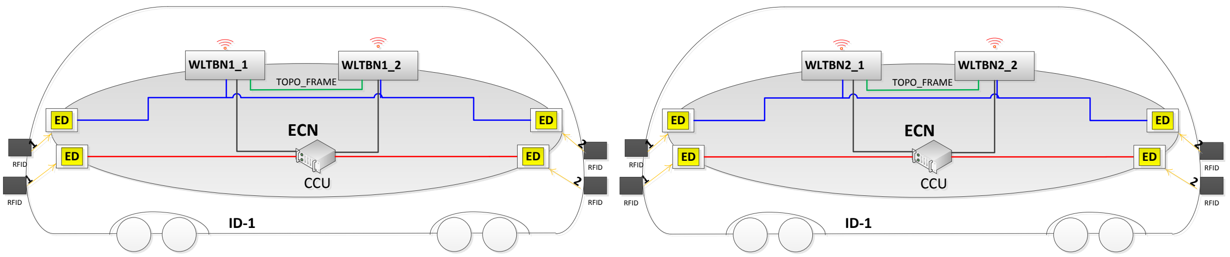


Figure 45: Wireless common inauguration with redundant WLTBNs

In the Table 38 the possible failures will be described in order to analyse their impact in the inauguration:

Table 38: Simplified failure analysis for common inauguration with redundant WLTBNs

ID	Failure	Effect	Possible mitigation
1	One WLTBN of another consist is unavailable	The TTDB is created combining information from both WLTBN, i.e. Train Network Directory (see IEC 61375-2-5 [11] section 8.8.5) and CSTINFO (see IEC 61375-2-5 [11] Annex E).	Not needed.
2	One WLTBN of own consist is unavailable	The TTDB is created by both WLTBN.	Not needed.
3	Two WLTBN of one consist are unavailable	Inauguration fails.	None
4	One RFID transceiver is unavailable	Inauguration fails.	Duplicated RFID transceivers in each consist edge for Train Composition Discovery.
5	Two RFID transceivers placed in different couplers of the same	Inauguration fails.	Duplicated RFID transceivers in each

	consist are unavailable		consist edge for Train Composition Discovery.
6	Two RFID transceivers placed in the same coupler of the same consist are unavailable	Inauguration fails.	None

The parallel inauguration described in section 8.3.2.B) may provide up to SIL4 inauguration, however it is highly weak against availability failures. In the Table 39 the possible failures will be described in order to analyse their impact in the inauguration:

Table 39: Simplified failure analysis for parallel inauguration

ID	Failure	Effect	Possible mitigation
1	One WLTBN of one consist is unavailable	TTDB from both planes are not the same. The inauguration fails.	None
2	One WLTBN of own consist is unavailable	Inauguration fails.	None
3	Two WLTBN of one consist are unavailable	Inauguration fails.	None
4	One RFID transceiver is unavailable	Inauguration fails.	Duplicate RFID transceivers in each plane.
5	Two RFID transceivers placed in different couplers of the same consist are unavailable	Inauguration fails.	Duplicate RFID transceivers in each plane.
6	Two RFID transceivers placed in the same coupler of the same consist are unavailable	Inauguration fails.	None

As it is shown in Table 38 and Table 39a compromise between safety and availability in the inauguration will be needed, since achieving a SIL4[15] Train Inauguration with high availability without increasing the costs due to the duplication of every single element looks very difficult. However, from the comparison between both proposals, the common inauguration with redundant

[15] It is not the goal of this deliverable to provide a complete safety analysis of the proposed wireless inauguration. This analysis will be provided in the future within the Shit2Rail framework.

WLTBNs presented in section 8.3.2.A) together with a TI Validation explained in section 8.4.2 looks the most promising alternative.

8.6 Functional distribution of the WLTBN

The WLTBN is functionally divided in two main components that may be integrated in the same device or in different devices depending on the implementation of the WLTBN. These two components are: The adapted ETBN which carries out the railway-specific functions carried out traditionally by the ETBN according to IEC 61375 [11]; and the Radio device which covers the functions needed for the establishment of the wireless train backbone network and the interconnection of the involved WLTBN within the same Train Unit. Figure 46 depicts the function distribution in two different devices, concentrating the topology calculation functions in the adapted ETBN which is expected to be low SIL capable device as it is in wired NG-TCN.

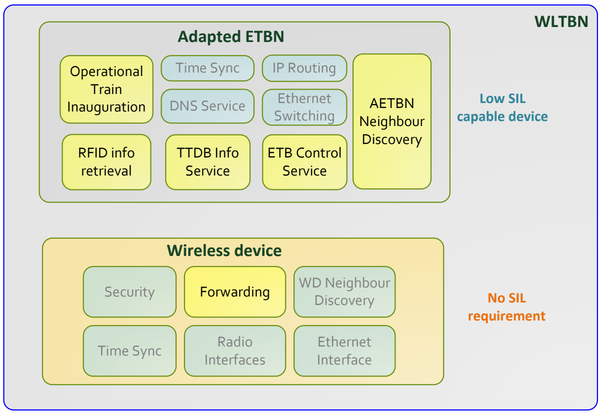


Figure 46: Example of WLTBN divided in two devices

Comparing to the ETBN description for the NG-TCN, the following functions introduced for the WLTBN worth to be defined.

8.6.1 RFID info retrieval function

The acquisition of the needed data, listed in section 8.3 may be done connecting directly the RFID transceivers to the AETBN or using the Consist Network. It is not under the scope of this document to specify the Consist Network to be used; however this data shall be sent from the RFID transceiver to the AETBN safely. Therefore, this information shall be protected by SDTv4.

8.6.2 Forwarding function

As explained in 5.3.2 the forwarding protocol to be used in the demonstrator for TCMS domain, in which inauguration will happen, will be B.A.T.M.A.N.

8.6.3 Neighbour Discovery Function

The neighbour discovery function is needed at two levels. On the one hand, the Radio Devices (RD) of the WLTBN shall be aware of the neighbours participating in the WLTB. Moreover, it shall have an updated forwarding table which allows reaching WLTBN out of the radio range using multihop forwarding. On the other hand, the AETBN shall be aware of the aliveness of other AETBNs of the WLTB in order to verify that the topology has not changed and wireless links are correct.

It is clear that the first neighbour discovery shall be performed by the RD as it is part of their forwarding protocol. However, for the second one, three different approaches may be taken.

Variant A

The first approach is to take the neighbouring table generated by the RD and share it cyclically with the AETBN. The main advantage of this approach is the reutilization of the RD messages to generate the forwarding/routing tables; therefore no additional messages would be introduced in the channel. The main drawback though is the need of a dedicated protocol to share this information or a specific TLV to be transferred between the RD and the AETBN using LLDP.

Variant B

This approach performs this AETBN neighbour discovery and aliveness awareness procedure implicitly within the Wireless Train Discovery Protocol explained in section 8.3 and the TOPO_FRAME structure specified in Annex A. This approach implies the reduction of the cycle time for this periodic frame exchange. In order to determine the new cycle time of this periodic frame exchange the following considerations have been evaluated.

The IEC 61375-2-5 identifies a link recovery time of 200 ms. In the WLTB context this means that there has to be a mechanism able to trigger a VRRP mastership change in case any WLTBN of the WLTB is not responding. Considering the VRRP mastership change need about 30 ms, then the detection mechanism would need a maximum timeout of 170 ms. If the TTDP TOPOLOGY approach is used, then the timing would be equivalent to 4 times the TOPO_FRAME's cycle time. From two previous conditions, we get that the TOPO_FRAME cycle time should be 43.75 ms ≈ 40 ms.

Although this cycle time reduction seems a big channel overhead and an overload for AETBNs, it has to be considered that the removal of HELLO messages is reducing about 4 messages per 100 ms. Moreover, since in topology steady state, i.e. when the topology CRC does not change, the TTDP TOPOLOGY handling (IEC 61375-2-5 section 8.9.2) does not compute the whole content of the frame, the computing time increase should not be unaffordable by AETBNs.

Variant C

This variant is based on the TTDP HELLO timing specified in the IEC 61375-2-5. The reference periods are:

- SlowPeriod 100 ms
- SlowTimeout 1,3 × SlowPeriod = 130 ms
- FastPeriod 15 ms
- FastTimeout 3 × FastPeriod = 45 ms

Detection time = SlowTimeout + FastTimeout = 175 ms

While the reuse of Wireless Train Discovery Protocol explained in section 8.3 is desirable for normal mode, i.e. with slow period and timeout, its use in fast mode may end in ETBN overload since the processing of TOPO_FRAME structures requires higher capacity. Therefore, for fast mode a *ping* to 239.192.0.129 address is proposed. This *ping*, i.e. *ICMP echo request* and *ICMP echo reply*, is send only when the slow timeout expired for one of the AETBN neighbour list. Note that, as this neighbour aliveness function is used to handover quickly from active WLTBN to passive WLTBN in case any other WLTBN of the same WLTB is unavailable, therefore it is used after train logical topology is build. This message follows a request/response scheme, that is, the request is sent to all WLTBN using an IP multicast transmission so that all AETBN participating in the WLTB will answer.

Figure 47 depicts how the heartbeat messages are used within the fast mode when the TOPO_FRAME is not received before the normal mode timeout expires. It is worth noting that Wireless Train Discovery, i.e. the exchange of TOPO_FRAMES, and Neighbour Discovery are different functions working in parallel in the AETBN. This means that Wireless Train Discovery is only responsible to track TOPO_FRAME timeouts and trigger the fast mode if necessary. In case of link failure, a VRRP master change will be trigger so that the WLTB data exchange is sent through the redundant WLTBN.

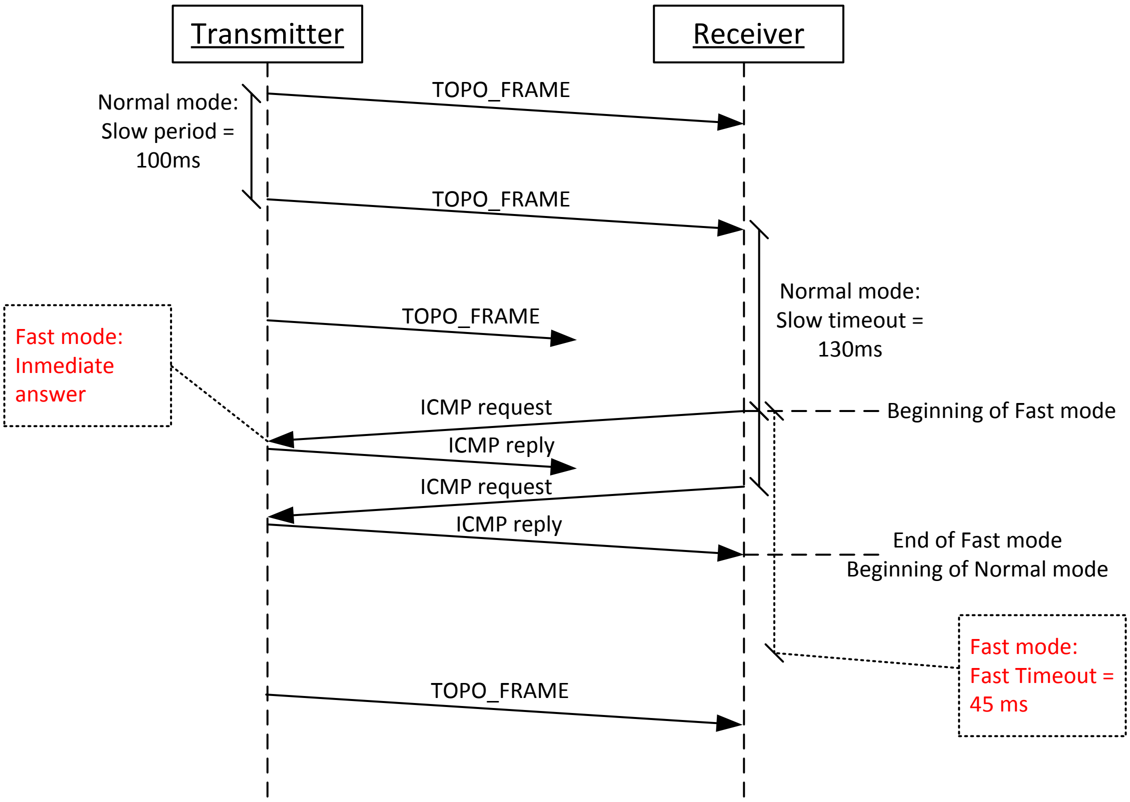


Figure 47: Neighbour Discovery normal mode and HEARBEAT recovery

From previous options, the **Variant B** is selected because it provides higher RD independence and does not require further specific implementation.

9. ADAPTATION OF SDTV4 FOR WIRELESS NETWORKS

This chapter describes the adaptation[16] of SDTv4 to use in wireless transmission systems as specified in [06] and for which the safety analysis was provided in [05] for wired networks. It will be investigated if further measures are required to adapt SDTv4 for wireless technologies. The basis of the investigation are the safety protocols already approved for wireless data transmission in safety critical systems which are mainly used in industrial environments and which also follows the “black channel” approach according to IEC 61508 as well as the assumptions under which the safety analysis was made in [05].

9.1 Introduction of wireless safety in industrial automation systems

Wireless solutions are increasingly being used in industrial automation systems, because of their flexibility and reliability. Statistically 70 % of machine down time is caused by cable breakage or contact problems. This fact also gives rise to the use of mobile devices. Furthermore, wireless networks enable applications that are simply not possible with a cable connecting moving parts of a system. Machine and systems manufacturers expect more than simply high levels of reliability and data security from the wireless solution they use – they also wish to see that their requirements with regard to functional safety are being met. Wireless systems are required to satisfy these complex demands, irrespective of whether they have been developed specifically for industrial applications or are based on standard technologies such as Wi-Fi IEEE 802.11 or Bluetooth.

When connecting components of a safety related system – like PLCs or sensors and actuators – however, manufacturers are facing serious issues. Wi-Fi according to standard IEEE 802.11 is widely regarded unsuitable as communication channel for real-time and safety applications. Non-determinism and interference liability lead to packet loss or exceeded and variable latency times due to retransmissions. Nevertheless, wireless technologies are spreading also to safety-related applications. Wireless communication is realized by sending messages bit by bit from transmitter to receiver (serial mode communication). This resembles quite much the method used in field buses. There are already several field buses, which are validated to be used in safety related applications. Many similar risks are relevant also in wireless communication systems, but wireless systems introduce also some new risks and the probability of failures is often higher than in wired systems. When all the risks or threats are considered, safety requirements determined, adequate measures are applied to minimize risks and the system is validated, wireless communication can be relevant possibility in safety-related machinery applications.

In industrial applications, for safety related systems, it is important and necessity to achieve safe communication. The standard industrial network technologies such as Profibus, Profinet, Interbus, Can-Open and Ethernet does not provide safe communication. To achieve safety or safe communication for safety related systems, these technologies have been developed or modified as PROFIsafe (PROFIBUS safety or PROFINETsafety), Interbus-Safety, CANopen-Safety and Safe

[16] adaptation means: What must be modified/changed/adjusted in terms of protocol, environment or infrastructure for SDTv4 to be used in a wireless environment?

Ethernet. These safety protocols provide higher reliability, higher SIL levels (up to SIL-3 (Safety Integrity Level 3) for industrial safety related systems.

At present, the demand or the interest is largely growing not only to use the safe communication but also to use safe wireless communication. Of course, the above mentioned safe wired industrial network technologies cannot be completely replaced with safe wireless communication. However, to have the advantages of wireless communication such as network architecture flexibility, mobility, economic advantages and depending on the application requirements, the need for the use of safe wireless communication in industrial applications especially for safety related systems is largely growing.

9.2 Wireless Safety Generic Communication Issues with Measures

Achieving safe wireless communication up to SIL4 using SDTv4 at best with few modifications and few adjustments, or avoiding additional measures is the major goal of this chapter. This is achieved by assuring that the information transmitted is received by the receiver without any transmission error and erasure (loss) of the information. As there is no such system with zero risk, wireless communication cannot have zero transmission errors and erasure of information; this is due to noise, interference, and fading effects.

For wireless communication, transmission error and erasure of the information that occur cannot be avoided, but they can be overcome by reducing or by detecting them. For this to achieve, safety methods as discussed in the International Standard IEC 62280 have to be implemented according to [30]. IEC 62280 is the standard document of “Railway applications – Communication, signaling and processing systems – Safety related communication in transmission systems” and especially Annex A and parts which are mapped from the earlier version of IEC 62280-2 within table E.1 of the document specifies safety related communication in “**open transmission systems**” i.e. for safe wireless communication.

To explain the differences between open and closed transmission systems and for a better understanding of the results of the safety analysis, which will be explained again below, the categorization according to chapter 6.2 and 6.3 of IEC62280 [30] is presented again:

9.2.1 General aspects of classification[17]

There are many factors which can influence the threats to a safety related communication system.

For example it is possible that transmission services can be obtained by the signalling system user from private or public telecommunications service providers. Under such service provision contracts, the responsibility of the service provider for guaranteeing performance of the transmission system can be limited.

Therefore the significance of threats (and hence the requirements for defences) depend on the extent of control exercised by the user over the transmission system, including the following issues:

[17] Source: chapter 6.2 of IEC 62280: 2014 [30]

- the technical properties of the system, including guarantees of reliability or availability of the system, the extent of storage of data inherent in the system (which could affect delay or re-sequencing of messages);
- the consistency of the performance of the system over its life (e.g. as changes to the system, and changes to the user base are made), and traffic loading effects of other users;
- access to the system, depending on whether the network is private or public, the degree of access control exerted by the operator over other users, the opportunity for misuse of the system by other users, and the access available to maintainers to reconfigure the system, or gain access to the transmission medium itself.

Following these issues three categories of transmission systems can be defined.

9.2.2 Criteria for the classification of transmission systems[18]

Criteria for Category 1 transmission systems

A transmission system can be considered to be of Category 1 if the following preconditions are fulfilled.

Pr1 The number of pieces of connectable equipment – either safety related or not – to the transmission system is known and fixed. As the safety related communication depends on this parameter, the maximum number of participants allowed to communicate together shall be put into the safety requirement specification as a precondition. The configuration of the system shall be defined/embedded in the safety case. Any subsequent change to that configuration shall be preceded by a review of their effects on the safety case.

Pr2 The characteristics of the transmission system (e.g. transmission media, environment under worst case conditions, etc.) are known and fixed. They shall be maintained during the life cycle of the system. If major parameters which were used in the safety case are to be changed, all safety related aspects shall be reviewed.

Pr3 The risk of unauthorized access to the transmission system shall be negligible. If a transmission system satisfies all the above preconditions, it may be considered as Category 1 and a closed system and, if so, it shall comply with a generally reduced set of processes and requirements given in Clause 7 of [30].

Criteria for Category 2 transmission systems

If a transmission system does not satisfy the preconditions 1 or 2 (Pr1 or Pr2), but fulfils precondition 3 (Pr3) it shall be considered as Category 2 and an open system, and shall be assessed with a more comprehensive set of processes and requirements given in Clause 7 of [30].

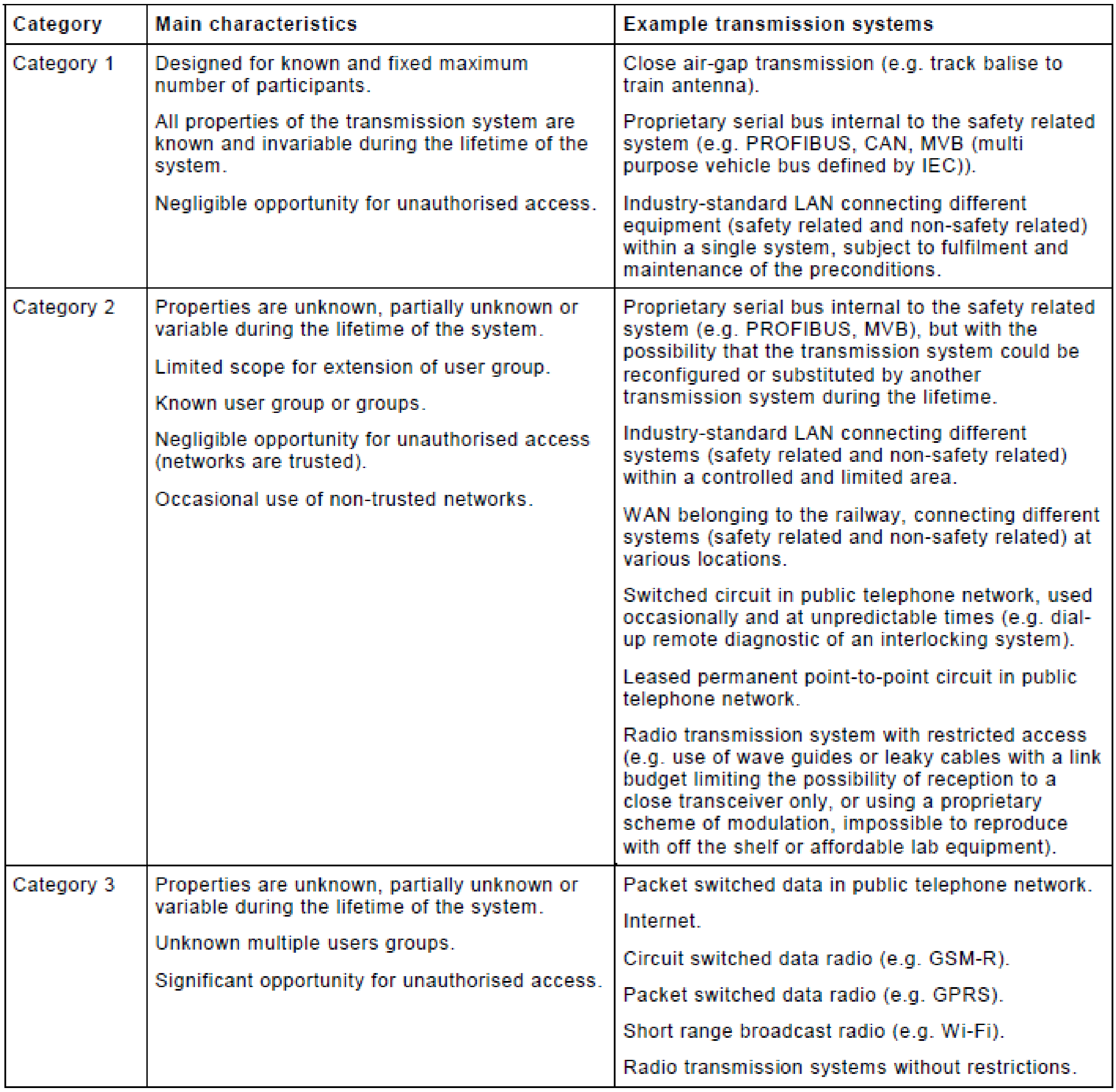
Criteria for Category 3 transmission systems

If a transmission system does not satisfy the precondition 3 (Pr3) then it shall be considered as Category 3 and an open system, and shall be assessed with the full set of processes and requirements given in Clause 7 of [30].

[18] Source: chapter 6.3 of IEC 62280: 2014 [30]

Table 40 (Source: B.1 of [30]) shows the main characteristics of the 3 different categorized transmission systems and shows different examples to illustrate them:

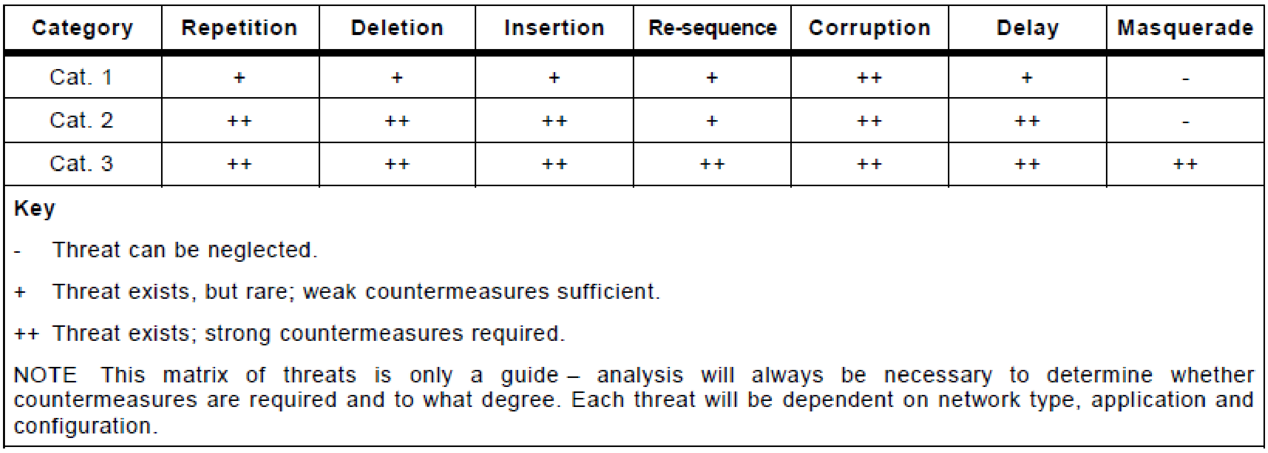
Table 40: Categories of transmission systems



Category	Main characteristics	Example transmission systems
Category 1	Designed for known and fixed maximum number of participants. All properties of the transmission system are known and invariable during the lifetime of the system. Negligible opportunity for unauthorised access.	Close air-gap transmission (e.g. track balise to train antenna). Proprietary serial bus internal to the safety related system (e.g. PROFIBUS, CAN, MVB (multi purpose vehicle bus defined by IEC)). Industry-standard LAN connecting different equipment (safety related and non-safety related) within a single system, subject to fulfilment and maintenance of the preconditions.
Category 2	Properties are unknown, partially unknown or variable during the lifetime of the system. Limited scope for extension of user group. Known user group or groups. Negligible opportunity for unauthorised access (networks are trusted). Occasional use of non-trusted networks.	Proprietary serial bus internal to the safety related system (e.g. PROFIBUS, MVB), but with the possibility that the transmission system could be reconfigured or substituted by another transmission system during the lifetime. Industry-standard LAN connecting different systems (safety related and non-safety related) within a controlled and limited area. WAN belonging to the railway, connecting different systems (safety related and non-safety related) at various locations. Switched circuit in public telephone network, used occasionally and at unpredictable times (e.g. dial-up remote diagnostic of an interlocking system). Leased permanent point-to-point circuit in public telephone network. Radio transmission system with restricted access (e.g. use of wave guides or leaky cables with a link budget limiting the possibility of reception to a close transceiver only, or using a proprietary scheme of modulation, impossible to reproduce with off the shelf or affordable lab equipment).
Category 3	Properties are unknown, partially unknown or variable during the lifetime of the system. Unknown multiple users groups. Significant opportunity for unauthorised access.	Packet switched data in public telephone network. Internet. Circuit switched data radio (e.g. GSM-R). Packet switched data radio (e.g. GPRS). Short range broadcast radio (e.g. Wi-Fi). Radio transmission systems without restrictions.

The relationship of the transmission system category to the countermeasures to be taken is shown in Table 41 (Source: B.2 of [30]). It can be seen, that the higher the category, the higher the requirement for the error detection measures to be taken.

Table 41: Threat/category relationship



Category	Repetition	Deletion	Insertion	Re-sequence	Corruption	Delay	Masquerade
Cat. 1	+	+	+	+	++	+	-
Cat. 2	++	++	++	+	++	++	-
Cat. 3	++	++	++	++	++	++	++

Key

- Threat can be neglected.

+ Threat exists, but rare; weak countermeasures sufficient.

++ Threat exists; strong countermeasures required.

NOTE This matrix of threats is only a guide – analysis will always be necessary to determine whether countermeasures are required and to what degree. Each threat will be dependent on network type, application and configuration.

The analysis of the SDTv4 as done in chapter 4.3 of **¡Error! No se encuentra el origen de la referencia.** has had the main task to prove the SIL4 ability of the safe data transmission channel taking into account the requirements defined in chapter 3.4.1 of **¡Error! No se encuentra el origen de la referencia.**. The methodology for the safety analysis done in chapter 4.3 of **¡Error! No se encuentra el origen de la referencia.** was described in chapter 4.1.2 of **¡Error! No se encuentra el origen de la referencia.**. Different types of architectures and topologies where the safety layer is part of a safety function were introduced in **¡Error! No se encuentra el origen de la referencia.** especially the contribution to chapter 3.5.3 (SIL4 Safe Data Transmission protocol) of the **¡Error! No se encuentra el origen de la referencia.**.

This analysis of SDTv4 in **¡Error! No se encuentra el origen de la referencia.** focused on a single transmission channel regarding the requirement ID_60012 of **¡Error! No se encuentra el origen de la referencia.**.

ID_60012	**ED-S shall use at least a single-channel communication system. Redundancy may be used optionally for increased availability**

The analysis of the safety layer as done in chapter 4.3 of ¡Error! No se encuentra el origen de la referencia. **has been carried out under the following additional assumptions:**

1. A “black channel” approach was exclusively taken into account.
2. The “failsafe”-principle was applied. => A failsafe state has to be defined on the receiver side.
3. The SIL4 capability of the safety layer was proven generically.*[19]

[19] The use of the defined error detection mechanisms described in D3.5 [06] must be sufficient for the manufacturers to reach the required SIL (here up to SIL4) for the transmission channel without a re-assessment of the error detection mechanism itself by the notified bodies.

4. The safety case of the ED-S itself was out of scope of [05].
5. The transmission system was regarded as category 1 transmission system as defined in chapter 6.3.13 of IEC 62280:2014 [30] and as an A0 communication system concerning Annex C of IEC 62280:2014*[20]
6. Although this was out of the scope of the task 3.3 of CTA1, wireless transmission of safety related data up to SIL4 through the safety layer shall also be possible as part of the black channel. The analysis of the safety code has been done considering a “wired channel” (“closed system”), hence for wireless systems, considered “open systems”, the necessary additional security mechanisms should be added. Furthermore, if wireless transmission channels are used, availability restrictions should be taken into account as well.

Important for the adaption and the use of SDTv4 in wireless networks in this context is the last mentioned bullet point (no. 6) which results together with the requirements for open transmissions systems coming from Table 41 in essentially 2 additional requirements:

1. **Implementation of security measures to support safety over a wireless transmission channel**
2. **Availability and determinism of a wireless transmission channel**

9.3 Security issues to support safety over a wireless transmission channel

Cryptographic techniques are primarily used in security critical applications. However, there may also be useful applications of cryptographic techniques in safety critical systems. For wireless systems it is obvious to investigate cryptographic techniques for transmission of signals between ED-S.

The basic idea of cryptography is to provide algorithms that make it impossible to read a message for anyone but the sender and the intended receiver. Most cryptographic systems apply a key as part of the process, where the key is input to the encryption and decryption algorithm.

As mentioned at the beginning of the chapter, the idea is to use the security measures of the already for wireless applications approved safety protocols from the fieldbus level for SDTv4 as

[20] The transmission system has been classified as category 1 (closed system) due to the fact, that wireless transmission of safety related data is limited to the use within the TCMS domain. For the virtual separation of the TCMS and the OOS domain, also special security measures have to be taken into account independent from the use of the safety layer. This analysis is done within this project in chapter 5 and Annex B.

well. One of these safety protocols approved for wireless applications is PROFIsafe. The additional security measures refer to IEEE 802.11 [31] and IEEE 802.15.1 [33] taken from chapter 9.8 of IEC 61784-3-3 [34] and adapted to SDTv4.

Security measures

Before any deployment of a safety application with SDTv4 and wireless components an assessment for dangerous threats such as eavesdropping or data manipulation shall be executed as pointed out in [35].

In case of no threat, no security measures are necessary.

There are two possible threats identified so far:

- Wilful changes of parameters of ED-S and safety programs
- Attacks on the cyclic communication, for example simulation of the safety communication

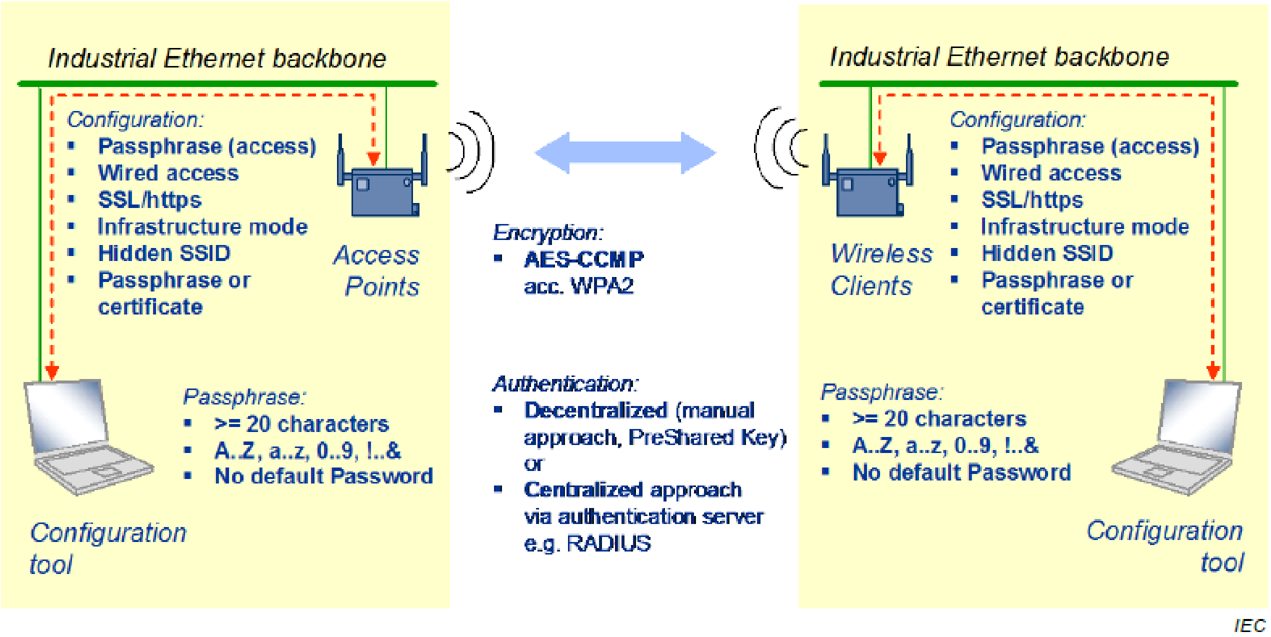
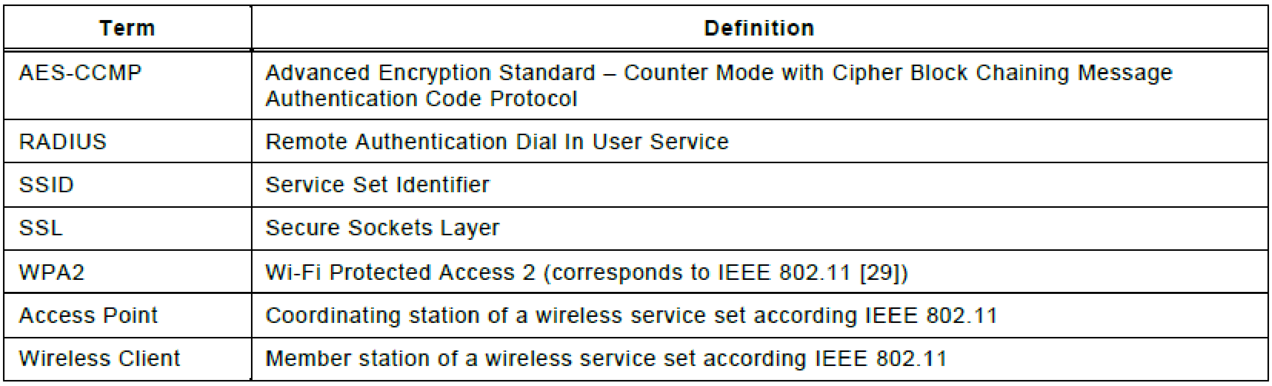


Figure 48: Security for WLAN networks (Source: Figure 85 of [34])

The terms used in Figure 48 are specified in Table 42.

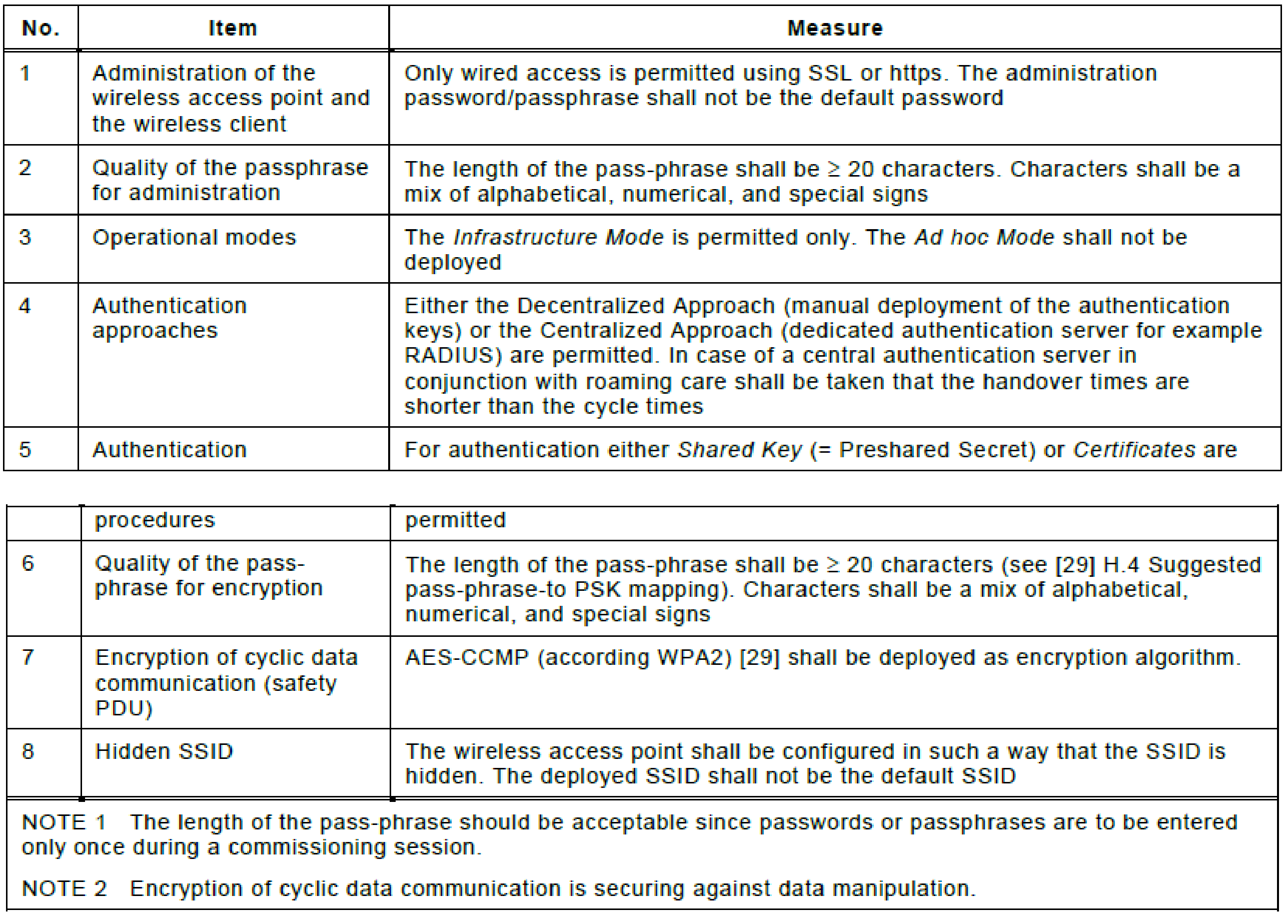
Table 42: Definition of terms in Figure 48 (Source: Table 31 of [33])



Term	Definition
AES-CCMP	Advanced Encryption Standard – Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
RADIUS	Remote Authentication Dial In User Service
SSID	Service Set Identifier
SSL	Secure Sockets Layer
WPA2	Wi-Fi Protected Access 2 (corresponds to IEEE 802.11 [29])
Access Point	Coordinating station of a wireless service set according IEEE 802.11
Wireless Client	Member station of a wireless service set according IEEE 802.11

In order to secure the wireless network against these cases the measures in Table 43 shall be considered according to IEEE 802.11 for industrial WLAN as pointed out in IEC 61784-2 for class A devices.

Table 43: Security measures for WLAN (Source: Table 32 of [33])



No.	Item	Measure
1	Administration of the wireless access point and the wireless client	Only wired access is permitted using SSL or https. The administration password/passphrase shall not be the default password
2	Quality of the passphrase for administration	The length of the pass-phrase shall be ≥ 20 characters. Characters shall be a mix of alphabetical, numerical, and special signs
3	Operational modes	The *Infrastructure Mode* is permitted only. The *Ad hoc Mode* shall not be deployed
4	Authentication approaches	Either the Decentralized Approach (manual deployment of the authentication keys) or the Centralized Approach (dedicated authentication server for example RADIUS) are permitted. In case of a central authentication server in conjunction with roaming care shall be taken that the handover times are shorter than the cycle times
5	Authentication procedures	For authentication either *Shared Key* (= Preshared Secret) or *Certificates* are permitted
6	Quality of the pass-phrase for encryption	The length of the pass-phrase shall be ≥ 20 characters (see [29] H.4 Suggested pass-phrase-to PSK mapping). Characters shall be a mix of alphabetical, numerical, and special signs
7	Encryption of cyclic data communication (safety PDU)	AES-CCMP (according WPA2) [29] shall be deployed as encryption algorithm.
8	Hidden SSID	The wireless access point shall be configured in such a way that the SSID is hidden. The deployed SSID shall not be the default SSID
NOTE 1 The length of the pass-phrase should be acceptable since passwords or passphrases are to be entered only once during a commissioning session. NOTE 2 Encryption of cyclic data communication is securing against data manipulation.		

In order to secure the wireless network the measures in Table 45 shall be considered according IEEE 802.15.1 [33] for Bluetooth as pointed out in IEC 61784-2 for class A devices.

Figure 49 is providing an overview on the security measures.

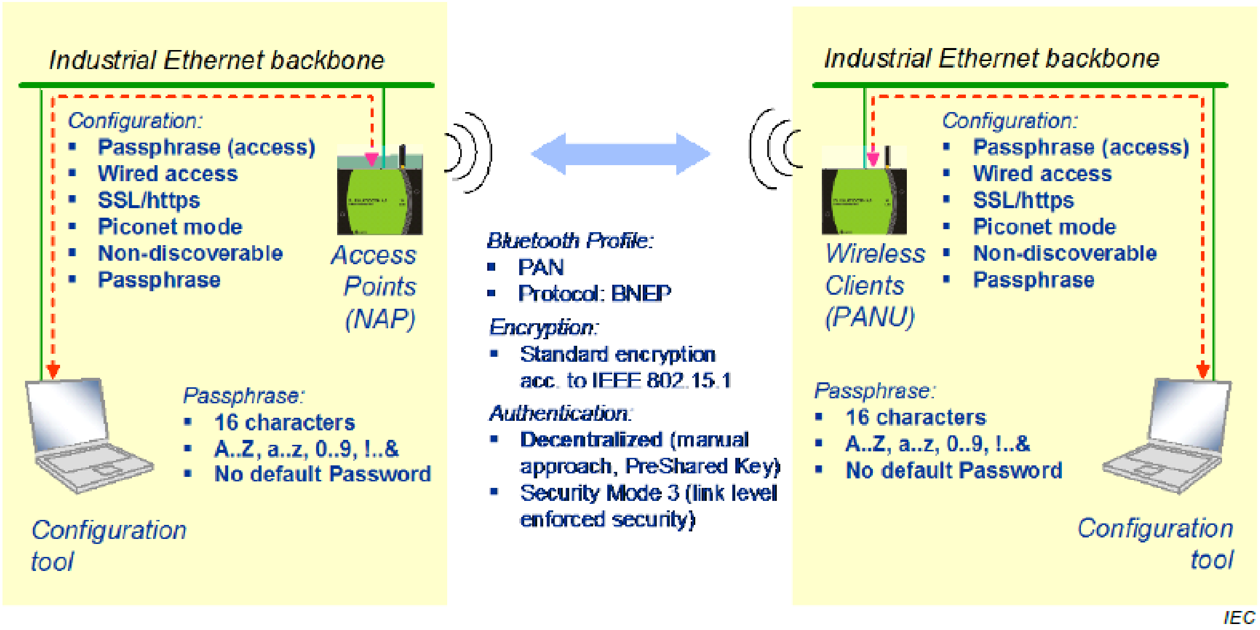


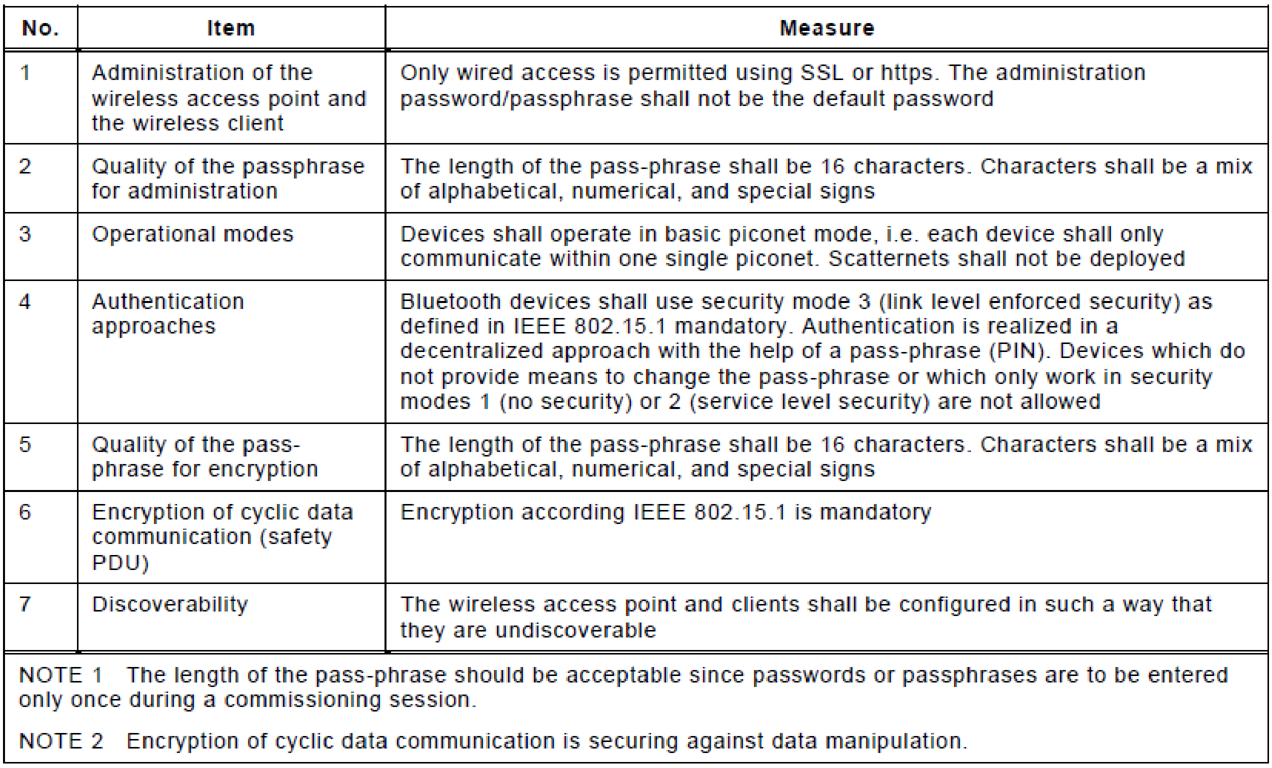
Figure 49: Security for Bluetooth networks (Source: Figure 86 of [34])

The terms used in Figure 49 are specified in Table 44.

Table 44: Definition of terms in Figure 49 (Source: Table 33 of [33])

Term	Definition
SSL	Secure Sockets Layer
PAN	Personal Area Network
BNEP	Bluetooth Network Encapsulation Protocol
NAP	Network Access Point
PANU	Personal Area Network User
Access Point	Coordinating station (master) of a wireless piconet according IEEE 802.15.1 [30]
Wireless Client	Member station (slave) of a wireless piconet according IEEE 802.15.1

Table 45: Security measures for Bluetooth (IEEE802.15.1) (Source: Table 34 of [33])



No.	Item	Measure
1	Administration of the wireless access point and the wireless client	Only wired access is permitted using SSL or https. The administration password/passphrase shall not be the default password
2	Quality of the passphrase for administration	The length of the pass-phrase shall be 16 characters. Characters shall be a mix of alphabetical, numerical, and special signs
3	Operational modes	Devices shall operate in basic piconet mode, i.e. each device shall only communicate within one single piconet. Scatternets shall not be deployed
4	Authentication approaches	Bluetooth devices shall use security mode 3 (link level enforced security) as defined in IEEE 802.15.1 mandatory. Authentication is realized in a decentralized approach with the help of a pass-phrase (PIN). Devices which do not provide means to change the pass-phrase or which only work in security modes 1 (no security) or 2 (service level security) are not allowed
5	Quality of the pass-phrase for encryption	The length of the pass-phrase shall be 16 characters. Characters shall be a mix of alphabetical, numerical, and special signs
6	Encryption of cyclic data communication (safety PDU)	Encryption according IEEE 802.15.1 is mandatory
7	Discoverability	The wireless access point and clients shall be configured in such a way that they are undiscoverable

NOTE 1 The length of the pass-phrase should be acceptable since passwords or passphrases are to be entered only once during a commissioning session.

NOTE 2 Encryption of cyclic data communication is securing against data manipulation.

The measures listed in Table 43 and Table 45 to be taken against the listed threats are similar for Wi-Fi and Bluetooth. Since LTE is also considered as a wireless technology for WLTB and WLCN, the configuration of the endpoints and access points should be done in a similar way, depending on how the wireless access points can generally be configured there.

Operating modes and the dynamic behaviour of the WLTB:

The operational modes (3) of Table 43 and Table 45 recommend the “infrastructure mode” for WLAN and the “basic piconet mode” for Bluetooth. This recommendation does not present a problem in fixed configured networks in which the sender/receiver address relationship of ED-S is well defined.

Due to the dynamic behaviour of the WLTB (WLTB propose a mesh network scheme and not infrastructure based one) it should be evaluated if the use of **peer authentication methods** are sufficient enough from the security point of view and as a further precondition, both the wireless access point and the wireless clients must support these methods.

9.4 Availability and Determinism of a Wireless Transmission Channel

One of the major challenges with wireless transmission is a sufficient availability. The user shall establish appropriate measures to ensure sufficient availability wherever roaming overtimes or communication blackouts due to reflection or interferences, or other causes for nuisance trips are possible. Nuisance trips may lead to switching off or removal of safety equipment (foreseeable misuse).

State of the art:

Industry:

Different working groups and alliances for example Avnu Alliance, 5GACIA and 3GPP are working on the topic wireless Time-sensitive Networking (TSN). Wired TSN for industrial use is undergoing acceptance and deployment.

The Avnu Alliance (see [36]) for example, is a community creating an interoperable ecosystem of **low-latency, time-synchronized, highly reliable networked devices using open standards**.

To achieve all these general requirements (low-latency, time-synchronized, highly reliable network) a roadmap is defined in [36]. The roadmap for integrating wireless TSN into industrial TSN systems takes a conservative, phased approach allowing confidence **in reliability of wireless TSN to be gradually increased.**

The term “wireless” in the Avnu approach (document [36]) is used in the broadest possible sense and includes free-space optical, Li-Fi, Bluetooth, IEEE 802.11g/n etc., small (nano, pico) cells: 3G, 4G, LTE, and includes anything else that involves information transfer using the electromagnetic spectrum, including various forms of visible and invisible light, i.e. free-space optical, while [37] is introducing TSN on 5G.

Automotive:

Concerning quantitative values of reliability and latency in 5G networks the [37] describes that from 3GPP Release 16, 5G will support vehicle-to-vehicle (V2V) communication for connected cars by means of the 5GNR sidelink. The sidelink was designed for the specific needs of V2V communication with the aim of enabling various levels of automated driving but still has similarities with communications with AGVs. The goal of 3GPP standardization efforts for the 5GNR sidelink is a reliability of **99.999% with a maximum latency of 3ms**. Communication via the 5GNR sidelink is more predictable as most of the devices within any communication group are static and in close proximity. The suitability of D2D (Device to Device) for industrial communication **depends on further research and standardization work** (3GPP Rel 17/18) aimed at achieving the **required degree of reliability**.

10. CONCLUSIONS

The main goal of CONNECTA-2 task T1.1 was to provide an evolved Wireless Train Control and Monitoring (WTCMS) architecture able to overcome the drawback detected in Roll2Rail and CONNECTA-1 projects. From the outputs of these two projects, the Wireless Train Backbone (WLTB) and Wireless Consist Network (WLCN) have been redesigned, adapting them to the state-of-the-art wireless technologies and also making them compatible to their evolution.

CONNECTA-2 highlighted the difficulty to cover all train-level traffic with a single LTE-based network, as well as the complexity and high cost of equipping one EnodeB and one UE in each consist. Following the current trends in other transportation industries, such as automotive industry, a new WLTB architecture based on LTE-V2V and IEEE 802.11s communications have been specified. The use of these two different radio technologies for TCMS and OMTS domains has found as the optimal solution to allocate the data traffic with such different requirements. The selection of the radio technologies have been made in close collaboration with Safe4RAIL-2 project. Moreover, apart from the most suitable radio technology from the current state-of-the-art, upcoming technologies, such as 5G, have been studied. 5G has been identified as a technology to be studied for WLTB and WLCN in detail once it is ready in the market due to its NR-V2X, high data-rate and URLL features. While 5G is not fully available in the market, this deliverable describes the current technologies to be implemented in CONNECTA-2 urban and regional demonstrators in order to functionally validate the proposed architectures, although it is expected that the performance will be much lower than the one to be provide by 5G or Wi-Fi 6.

Additionally to the WLTB and WLCN specification, this task has started the alignment with IP2 X2Rail project in order to work on a common interface which allows the integration of TCMS MCG and the ACS been specified by X2Rail. The main goal of this ongoing work is the minimization of telecommunication equipment in the train, integrating the communications needed by different on-board systems in a single communication device.

Finally, the good harmony and cooperative atmosphere existing between CONNECTA-2 and Safe4RAIL-2 projects must be highlighted, which has made it possible to address open technical discussions. Based on this cooperation, Safe4RAIL -2 will continue in the next months with useful investigations for WTCMS, such as the investigation on TSN features for WTCMS in order to provide similar level of time determinism that the wired NG-TCN. In future project, it is expected that the complete safety analysis for Wireless TCMS, including the wireless inauguration will be made.

A Annex – Wireless Train Discovery Protocol with SC-32 CRC

```
TTDP-PROTO-ID::= ARRAY [4] OF CHARACTER8 {87, 84, 68, 80}
       -- Definition of Wireless Train Discovery Protocol identification string =
       "WTDP" -- in ASCII

ETBN-INAUG-STATE::= ENUM8 {              -- Definitions for the ETBN state machine
       Init (0)
       NotInaugurated (1),
       Inaugurated (2),
       ReadyForInaug (3)
       -- Other values shall never be used
}
ETBN-ROLE::= ENUM8 {                     -- Definition for ETBN node roles
       EtbnRoleUndefined (0),
       EtbnRoleMaster (1),
       EtbnRoleBackup (2),
       EtbnRoleNotRedundant (3)
       -- Other values shall never be used
}
DIR-LINK-INFO::= RECORD {                -- RFID transceiver information in a given
                                         -- direction
       rfidLineAstatus ANTIVALENT2,      -- Line A status
       rfidLineBstatus ANTIVALENT2,      -- Line B status (in case of redundancy)
       rfidAdistIdent LINE-IDENT,        -- RFID distant Id. from Line A
       rfidBdistIdent LINE-IDENT         -- RFID line distant Id. from Line B (in case
                                         -- of redundancy)
}
ETB-TLV::= RECORD {                      -- Definition of TTDP topology ETB specific TLV
       etbTlvHeader TLV-HEADER {         -- ETB TLV header values
              tlvType (1),
              tlvLength (0..511)
       },
       tlvCS UNSIGNED16,                 -- TLV checksum
       protoID TTDP-PROTO-ID,            -- WTDP protocol Id. string
       protoVersion UNSIGNED32 ('01000000'H), -- protocol version of the
                                         -- ETB Inauguration Protocol (1.0.0.0)
       lifeSign UNSIGNED32,              -- Sequence number of packet
                                         -- always incremented and overflow

       etbnInaugState ETBN-INAUG-STATE, -- Status of the ETBN state machine
       etbnNodeRole ETBN-ROLE,           -- Current role of the ETBN
       reserved1 UNSIGNED6 (0),          -- padding bits for 8-bit alignment

       etbnInhibition ANTIVALENT2,       -- Informs about an inhibition request
                                         -- from this node. Local information from ETBN
                                         -- see HELLO frame note 6 for field coding
       reserved2 UNSIGNED6 (0),          -- padding bits for 8-bit alignment
       remoteInhibition ANTIVALENT2,     -- see 15 for role explanation
                                         -- and HELLO frame note 6 for field coding
       connTableCrc32 UNSIGNED32,        -- CRC32 of the internal Connectivity Table

       etbnDir1LinkInfo DIR-LINK-INFO,   -- Orientation information in direction 1
       etbnDir2LinkInfo DIR-LINK-INFO,   -- Orientation information in direction 2

       dir1MacAddr MAC-ADDR,             -- MAC address of the neighbour node
                                         -- in direction 1
       ownMacAddr MAC-ADDR,              -- own MAC address
       dir2MacAddr MAC-ADDR,             -- MAC address of the neighbour node
                                         -- in direction 2
       Dir1CstUuid ARRAY [16] OF UNSIGNED8,    -- Consist Universal Unique ID
       OwnCstUuid ARRAY [16] OF UNSIGNED8,     -- Consist Universal Unique ID
       Dir2CstUuid ARRAY [16] OF UNSIGNED8,    -- Consist Universal Unique ID

       owRadioId MAC-ADDR,              -- own radio device MAC address

       nDir1Etbn UNSIGNED8 (0..62),     -- Number of ETBN detected at the dir1 side
                                        -- of the ETBN
       nDir2Etbn UNSIGNED8 (0..62),     -- Number of ETBN detected at the dir2 side
                                        -- of the ETBN
       nCstUuid UNSIGNED8 (0..62),      -- Number of CstUuid detected

       reserved3 UNSIGNED16 (0),        -- padding bytes for 32-bit alignment
       dir1EtbnVector ARRAY [nDir1Etbn] OF MAC-ADDR,
                                        -- Unordered ETBN list detected at the dir1
                                        -- side, each neighbour ETBN is described by --
                                        -- its MAC address
       dir2EtbnVector ARRAY ALIGN 32 [nDir2Etbn] OF MAC-ADDR
                                        -- Unordered ETBN list detected at the dir2
                                        -- side, each neighbour ETBN is described by --
                                        -- its MAC address

}

ETBN-CN-CNX::= BITSET32 {  -- Definition for CN connections bitmask
                           -- for each bit, FALSE (0) means “not connected”, TRUE (1) -
                           ---- means “connected”
       cn01 (0),           -- Consist network #1
       cn02 (1),           -- Consist network #2
       -- ... to be filled with all intermediate values
       cn31 (30),          -- Consist network #31
       cn32 (31)           -- Consist network #32
}

CN-TYPE::= ENUM8 {
       cn-MVB (1),
       cn-NotUsed (2),
       cn-CAN (3),
       cn-Ethernet (4)
       -- Other values shall never be used
}

CN-TLV::= RECORD { -- Definition of WTDP topology CN specific TLV
       cnTlvHeader TLV-HEADER {                -- CN TLV header values
              tlvType (2),
              tlvLength (0..511)
       },
       tlvCS UNSIGNED16,                       -- TLV checksum
       etbTopoCnt UNSIGNED32,                  -- CRC32 of the internal
                                               -- "Train Network Directory"
       ownEtbnNb UNSIGNED8 (1..32),            -- Static relative position of the ETBN
                                               -- in the Consist
       lengthen ANTIVALENT2,                   -- lengthening state
       shorten ANTIVALENT2,                    -- shortening state
       reserved1 UNSIGNED4 (0),                -- 4-bit padding for 8-bit alignment
       nEtbnCst UNSIGNED8 (0..32),             -- Number of ETBN in the Consist
       nCnCst UNSIGNED8 (0..32),               -- Number of CN in the Consist
       cnToEtbnList ARRAY [nEtbnCst] OF ETBN-CN-CNX,
                                               -- List of CNs attached to ETBNs
       cnTypes ARRAY ALIGN 32 [nCnCst] OF CN-TYPE
                                               -- Types of Consist networks
}
```

```
WTDP-TOPOLOGY-TLV::= RECORD {                   -- WTDP TOPOLOGY specific TLV
        etbTlv ETB-TLV,                         -- ETB topology specific TLV
                                                -- (TTDP mandatory)
                                                -- Used to build "Connectivity Table"
                                                -- (Physical Topology)
        cnTlv CN-TLV,                           -- Consist Networks specific TLV (TTDP
                                                -- mandatory)
                                                -- Used to build "Train Network
                                                -- Directory"
                                                -- (Logical Topology)
        otherTlvs SEQUENCE OF GEN-TLV,          -- optional list of TLVs
        eolTlv EOL-TLV,                         -- End Of TLV list (mandatory)
        crc UNSIGNED32                          -- SC-32 computed over record
                                                -- (seed value: 'FFFFFFFF'H)
}

WTDP-TOPOLOGY-FRAME::= RECORD { -- TTDP TOPOLOGY frame definition
        destAddr MAC-ADDR ('0180C2000010'H),    -- Destination MAC multicast address
(see
                                                -- IEEE 802.1D)
        srcAddr MAC-ADDR,                       -- Source MAC address (ETBN sender's)
        vlanHdr TTDP-VLAN-HDR,                  -- TTDP VLAN header
        etherType UNSIGNED16 ('894C'H),         -- EtherType id. for IEC TTDP topology
                                                -- protocol
        reserved1 UNSIGNED16 (0),               -- padding bytes for 32-bit alignment
        etbTlv ETB-TLV,                         -- ETB topology specific TLV (TTDP
                                                -- mandatory)
                                                -- Used to build "Connectivity Table"
                                                -- (Physical Topology)
        cnTlv CN-TLV,                           -- Consist Networks specific TLV (TTDP
                                                -- mandatory)
                                                -- Used to build "Train Network
                                        Directory"
                                                -- (Logical Topology)
        etherCrc UNSIGNED32                     -- Ethernet frame CRC (see IEEE 802.3)
}
```

B Annex – Security measures for the Wireless Train Backbone and Wireless Consist Network

B.1 Overview

In this Annex, the security measures for the wireless train backbone and wireless consist network are described. The security measures must be distinguished into those that deal with the development of the core technology, and those which deal with the actual projects, in which the WLTBN and WLCN are deployed. Hence, in section B.2 the security measures for the development are discussed and section B.3 the security measures for projects.

In CONNECTA phase 1 a Product and Solution Security (PSS) process was developed to handle cybersecurity in trains [28]. As point out there, this process must be conducted when an actual project containing a train with the WLTBN and WLCN is done. The cybersecurity measures which need to be taken then depends on the context and must be derived from a Threat and Risk Analysis (TRA). Since it will take 8-10 years until the WLTBN and WLCN will make their way into the real deployments, which is a long time in term of cybersecurity and it can be expected; that the context will drastically change from today, the value of conducting a TRA today is limited. However, in the remainder of this Annex some generic remarks on such a TRA are made and some measures are derived. The TRA consists of the steps shown in Figure 50.

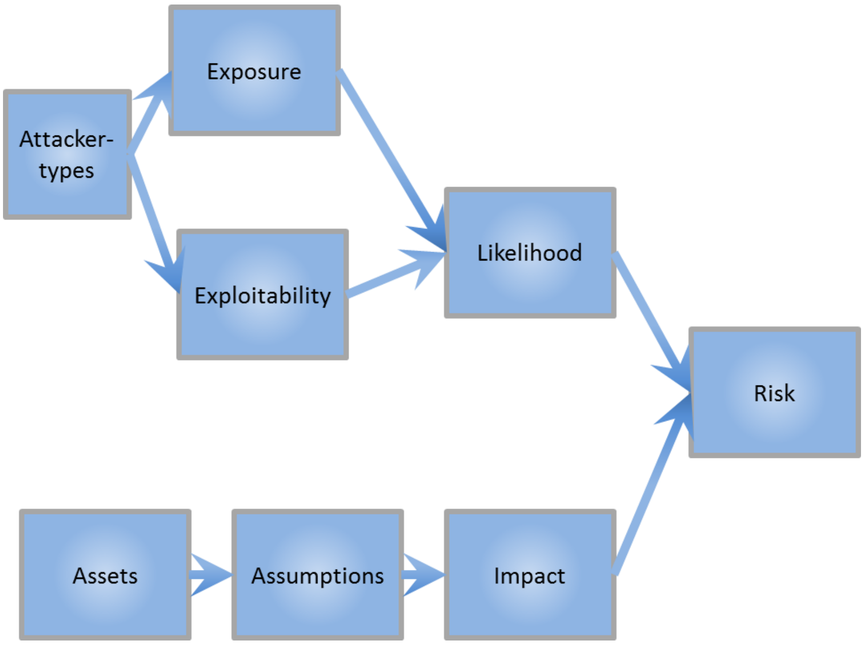


Figure 50: Steps of the TRA

B.2.1 Attacker types

It has to be defined which attackers are considered. Possible attackers or threat actors are:

- Unskilled Hacker / Script Kiddy
- Skilled Hacker
- Security Researcher
- Penetration Tester
- Malicious User
- Malicious Privileged User / Staff
- Negligent User
- “Negligent Privileged User / Staff (e.g. administrators, service engineers)”

Currently, in the context of cybersecurity for rail vehicles, the main attackers considered are script kiddies, skilled hackers and security researchers. Malicious users, i.e. staff, are usually left out, as the entire rail system is built around the assumption that staff have the option to manipulate the system if it is necessary for operation, e.g., to deactivate the brakes if the train is towed. Attackers such as organized crime or nation states are not considered, as it cannot be the responsibility of a train manufacturer to defend against them, but rather here a national defence strategy, which gives requirements to train manufacturers is needed.

B.2.2 Likelihood

In order to evaluate threats one has to assess, how easy it is for an attacker to access its target (exposure) and how easy it is to exploit a vulnerability (exploitability).

B.2.3 Assets

An important aspect of a TRA is the system overview, in which the considered assets and their interfaces are listed. In this case, the system overview can be taken from chapters 2 and 6 of this document.

B.2.4 Assumptions

Assumptions on the operation of the system needs to be made. In this case, a normal railway operation is assumed. In contrast to systems from other sectors, in a rail vehicle the attacker has easy access to the control system, as he can disguise as a passenger. While with a wired train control system this can be mitigated by locking up the cables and components, for WLTBN and WLCN it must be assumed that the attacker has access to the air interface.

B.2.5 Impact

In an impact matrix each threat is assigned a rating. The impacts are sorted by confidentiality, integrity and availability. The highest rating is for an attack on the integrity causing safety impact, i.e., an attack which causes safety-relevant functions to fail. For railway operators also availability is an important topic, as unavailable trains lead to compensation costs and negative press coverage. Compared to those to the ratings with regard to confidentiality are relatively low.

B.2.6 Risk

The risk is evaluated by defining threats and analysing the likelihood and the impact.

B.3 CYBERSECURITY MEASURES

B.3.1 Overview

Since the impact cannot be changed for threats with a severe impact the likelihood must be reduced. With regard to exposure, in a wireless system the exposure is generally high. An attacker with a device using the wireless protocol like Wi-Fi or LTE can stage an attack. This is in contrast to wired systems, where if the cables and devices are locked up, a physical barrier has to be overcome in order to attack.

Hence, the exploitability must be reduced. This can be done by implementing a set of requirements such as those of IEC 62443-3-3 [29]. They are sorted in seven foundational requirements which are discussed in the following. However, it must be noted, that this based on a guess how the cybersecurity context in 8-10 year will be and a through TRA which may yield higher or lower requirements must be done then.

B.3.2 FR 1 – Identification and authentication control

In wired systems, the authentication can be done with physical access control by locking up the components and cables and only giving authorized personnel access. Hence, in wireless systems it is essential to employ appropriate identification and authentication methods. For this a certificate infrastructure will be required.

B.3.3 FR 2 – Use control

The same rationale as for FR 1 applies and a certificate infrastructure can be configured for use control as well.

B.3.4 FR 3 – System integrity

In the context of rail vehicles threats on system integrity are the most critical, because by maliciously manipulating the software of the control system, safety-relevant impacts can be caused. Defence in depth is required, so in addition to the authentication and use control further measures are needed. State-of-the art encryption is required. While in today’s trains with closed systems malware protection is usually not required, this is expected to change for WLTBN and WLCN.

B.3.5 FR 4 – Data confidentiality

While data theft in the context of train control systems can lead to the loss of intellectual property, it is usually not considered as a severe impact today. In WLTBN and WLCN it must be considered, that unless state of the art encryption is used, the threshold for such attacks is very low.

B.3.6 FR 5 – Restricted data flow

For this FR there is no difference between the wired and wireless setting, so the same requirements as for wired systems apply.

B.3.7 FR 6 – Timely response to events

Since the wireless setting makes attacks more attractive, it must be assumed that despite all the measures taken, some attacks will be successful. For this, as a further line of defence, a state-or-the-art intrusion detection must be employed, to detect attacks.

B.3.8 FR 7 – Resource availability

Wireless systems attract Denial-of-service (DoS) attacks, e.g., by jamming the wireless channel. This is one of the hardest threats to defend against. State-of-the-art resource management and DoS protection mechanisms are required.

B.4 CONCLUSION

Cybersecurity in the WLTBN and WLCN yields certain challenges, which are distinct from wired systems. However, since the cybersecurity landscape is very dynamic and it is impossible to guess the context and technology level in 8-10 years, no specific requirements can be derived. Hence, a TRA needs to be done when actual projects deploying WLTBN and WLCN are developed. In this Annex it was derived, what the focus must be and what probable resulting requirements are needed when deploying WLTBN and WLCN.

REFERENCES

[01] CONNECTA D1.2 - TCMS Use Case, http://projects.shift2rail.org/download.aspx?id=b9f9d9bc-a865-419c-b829-188bd3153ec9.

[02] CONNECTA D1.3 Function based architecture

[03] CONNECTA D1.2 Use Cases final EXCEL sheet

[04] CONNECTA Use Cases v807_2018-11-26

[05] CONNECTA D3.3 – Report on RAMS and Security Analysis

[06] CONNECTA D3.5 – Drive-by-Data Architecture Specification

[07] CTA-T3.1-D-ANS-023-08 Drive-by-Data Network Requirements

[08] CTA-T1.5-T-SNF-026-06 D1.5 High Level Requirements List

[09] R2R-T2.5-D-BTD-003-18 D2.5 Architecture for the Train and Consist Wireless Networks

[10] IEC 61375-2-3 – Communication Profile

[11] IEC 61375-2-5 – Ethernet Train Backbone

[12] Ad hoc On-Demand Distance Vector (AODV) Routing: https://tools.ietf.org/html/rfc3561

[13] The Optimized Link State Routing Protocol Version 2: https://tools.ietf.org/html/rfc7181

[14] B.A.T.M.A.N.: https://www.open-mesh.org/projects/open-mesh/wiki

[15] UIC 556: Information Transmission in the train (train bus), 2009.

[16] CONNECTA D2.4 Report of C2C Wireless Communication Tests

[17] Safe4RAIL-2-D2.6 State Of Art WLCN - PU - M08

[18] Roll2Rail, D2.2 - Characterisation of the Railway Environment for Radio Transmission. 2016

[19] Current state of IEEE 802.1 Time-Sensitive Networking Task Group., Norman Finn. 2014

[20] Safe4RAIL-2-D2.1 – Requirements of LTE Equipment and ETBNs for wireless TCMS

[21] INTEL. IEEE 802.11 Wi-Fi protocol summary. Available from: https://www.intel.com/content/www/us/en/support/articles/000005725/network-and-i-o/wireless-networking.html#legacy

[22] 3GPP TS 36.101: "Technical Specification Group Radio Access Network", V16.2.0 (2019-06)

[23] 3GPP TS 32.101: "Telecommunication management; Principles and high level requirements"

[24] How to get the most from 802.11 multicasting, http://www.wireless-nets.com/resources/tutorials/802.11_multicasting.html

[25] Multicast over Wireless, https://wirelesslywired.com/2019/05/02/multicast-over-wireless/

[26] X2Rail-1 Deliverable D3.3: Specification of the Communication System and Guideline for Choice of Technology, version 1.1 29.01.2019

[27] Masahiro NOGAMI, Nobuhiko NAKAMURA, Kouji SAITO, *Contactless electrical coupler providing large capacity transmission by visible light communication technology*, WCRR2019, Tokyo, 2019.

[28] CONNECTA D4.4 – Cybersecurity for the Functional Distribution Framework; CTA-T4.4-T-SIE-151-03

[29] IEC 62443-3-3 Industrial communication networks – Network and system security – Part 3-3: System security requirements and security

[30] IEC 62280:2014 Railway applications – Communication, signalling and processing systems – Part 1: Safety-related communication in closed transmission systems

[31] IEEE 802.11-2012, IEEE Standard for Information technology – Telecommunications
and information exchange between system – Local and metropolitan area networks –
Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and
[32] Physical Layer (PHY) specifications

[33] IEEE 802.15.1-2005: IEEE Standard for Information technology – Telecommunications and information exchange between systems-Local and metropolitan area networks – Specific requirements

[34] IEC 61784-3-3: Ed3 2016-07 Industrial communication networks – Profiles – Part 3-3: Functional safety fieldbuses – Additional specifications for CPF 3

[35] PROFINET Guideline: PROFINET Security, V2.0, November 2013. Order-No. 7.002

[36] Avnu Alliance® White Paper Industrial Wireless Time-Sensitive Networking: RFC on the Path Forward: Version 1.0.3 – Friday, January 5, 2018, Authors: Stephen F Bush (GE Global Research) Chair: IEEE P1913 - Software-Defined Quantum Communication Chair: 1906.1-2015 - IEEE Recommended Practice for Nanoscale and Molecular Communication Framework Guillaume Mantelet (GE Transportation) Contributors: Brant Thomsen (Harman International) Ethan Grossman (Dolby Laboratories)

[37] Integration of Industrial Ethernet Networks with 5G Networks: November 2019 “5G Alliance for Connected Industries and Automation” Published by: ZVEI – German Electrical and Electronic Manufacturers’ Association 5G Alliance for Connected Industries and Automation (5G-ACIA), a Working Party of ZVEI Lyoner Strasse 9 60528 Frankfurt am Main, Germany

[38] IEC 61375-2-6: Electronic railway equipment – Train communication network – Part 2-6: On-board to ground communication

[39] Ó. Seijo, Z. Fernández, I. Val and J. A. López-Fernández, "SHARP: A novel hybrid architecture for industrial wireless sensor and actuator networks," 2018 14th IEEE International Workshop on Factory Communication Systems (WFCS), Imperia, 2018, pp. 1-10. doi: 10.1109/WFCS.2018.8402358