NEW DEPENDABLE ROLLING STOCK FOR A MORE SUSTAINABLE, INTELLIGENT AND COMFORTABLE RAIL TRANSPORT IN EUROPE

D2.5 – Architecture for the Train and Consist Wireless Networks

Due date of deliverable: 30/04/2017
Actual submission date: 19/04/2017

Leader of this Deliverable: Michael Reismann (BT)
Reviewed: Y

Document status		
Revision	Date	Description
1	16/10/2015	First issue
2	09/03/2016	- Chapter 2.4: SIE proposal R2R-T2.5-I-SIE-015-01 included - Chapter 2.3.4, 2.3.9, 8: IKERLAN proposal R2R-T2.5-T-IK4-022-01 included - Chapter 2.3.6: CAF proposal R2R-T2.5-T-CAF-021-01 included - Chapter 2.3.1, 2.3.4.4: IKERLAN proposal R2R-T2.5-T-IK4-024-01 included
3	10/05/2016	- Chapter 2.3.2: BTD contribution included - Chapter 2.3.3: BTD proposal R2R-T2.5-T-BTD-029-01 included - Proposal of INTRODUCTION AND EXECUTIVE SUMMARY CHAPTERs - Headlines of subchapters 3, 4 and 5 (removed) updated/added - Appendix III - Requirement Traceability added - Chapter 2.1: ASB proposal R2R-T2.5-I-ASB-027-03 included - Chapter 1.1: BTD contribution included - Chapter 4: First draft architecture proposal included
4	08/06/2016	- Chapter 2.3.4, 8: IKERLAN proposal R2R-T2.5-T-IK4-042-01 included - Chapter 2.5: BTD contribution included - Chapter 3, 4 Structure updated
5	19/06/2016	Chapter 2.3.7, 2.3.8: SNCF contribution included
6	25/09/2016	- Chapter 2.5: added sub chapter 2.5.7 - Review Rework done in chapters: 2.5, - SNCF rework for chapter 2.3.7 and 2.3.8 included - Chapter 2: MEM proposal R2R-T2.5-T-MEM-055-01 included - Chapter 2.3.1, 2.3.4, 2.3.5: New content R2R-T2 5-D-BTD-003-05 included - Chapter 2.3.2 updated according review comments
7	19/10/2016	- Chapter 2.3.3 updated according review comments - Chapter 2.4 updated according review comments - Chapter 2.3.1, 2.3.4 and 2.3.5 updated according review comments and R2R-T2.5-T-IK4-066-01
8	07/11/2016	- minor corrections - removed Word comments of agreed review comments
9	01/12/2016	- added numbering to chapters of level 4 and 5 - Chapter 2.3.6 updated according to R2R-T2.5-T-CAF-021-03 - Chapter 3, 3.1, 3.2 added considering R2R-T2.5-T-BTD-076-02 - Chapter 4, 4.1, 4.6 - 4.8 added considering R2R-T2.5-T-UNC-069-02
10	09/12/2016	- added corrections according to R2R-T2.5-T-IK4-086-01 - changed format of figure reference - Chapter 2.1 replaced according R2R-T2.5-T-STD-050-01 - Appendix III, requirement IDs from R2R-T2.1-D-TRI-053-07 included - Chapter 2.4, Figure 39 updated
11	23/12/2016	- chapters added: 4.2, 4.3 - chapters updated: 4.7.1, 4.7.2, 4.7.3 - chapter 5 removed and replaced by chapter 4.6 - chapter 8 Appendix II – References updated - chapter 2.3.3 general statement included

		- chapter 7 Appendix I – Acronyms and Definitions updated
12	26/01/2017	- chapter 9, traceability table replaced by R2R-T2.5-I-CAF-087-01 - added chapter 3.1.5 - updated due to review report R2R-T2.5-R-BTD-094-02, sections 2.1 and 2.2 - chapter 3, 4 - R2R-T2.5-T-VOS-035-01 incorporated - chapter 9, , traceability table updated - chapter 3, 4 content enlarged and improved
13	07/02/2017	- chapter 4.4: IEEE 802.11ac added as considered standard - chapter 4.5 (FREQUENCY BAND, BANDWIDTH AND COVERAGE) added - chapter 4.8: title changed from “RECOMMENDATION FOR WIRELESS COMMUNICATION INSIDE CONSISTS AND VEHICLES” to “RECOMMENDATION FOR WIRELESS COMMUNICATION ARCHITECTURE INSIDE CONSISTS AND VEHICLES” - chapter 4.8.3 added (Combined approach for TCMS and OMTS), R2R-T2.5-T-ALS-093-01 partly incorporated - chapter 4.9.2: examples for devices in OMTS domain added - chapter 3.1.1 alternative discovery solutions added, R2R-T2.5-I-USB-072-01 incorporated
14	27/02/2017	- Chapter 3.1.1.1.2 and 3.1.1.2.2 added - OMTS replaced by OOS - Chapter 4 updated according to review comments in R2R-T2.5-R-BTD-102-04: * M12 defined as connector in chapter 5 * Footnote added related to 2012 edition of IEEE 802.11 * Clarification regarding jamming and OFDM added * Clarification regarding vehicle design and usage of mesh networks added * ETB/WLTB added in example chapter * Clarification regarding proposed wireless TCMS structure * Chapter with major properties of the different IEEE 802.11 standards added - Chapter 2.3.10 Availability (Redundancy) added, CAF input S.R2R-T2.5-I-CAF-001_03 incorporated - Chapter 6: CAF input from R2R-T2.5-I-CAF-107-02 incorporated - Chapter 3.1.1.3.6 Train Station cases created - Chapter 3.1.1.5 Conclusion updated - Chapter 2.1 updated according R2R-T2.5-T-STD-050-02. Update according to comments introduced in documents “R2R-T2.5-B-BTD-095-01 MoM_Review of R2R-T2.5-T-BTD-003-10” and “R2R-T2.5-B-BTD-103-01 Review of D2.5 R2R-T2.5-T-BTD-003-12”. These documents are the results of conversations between the partners of the tasks after the review of the Deliverable of the Task 2.5. - Chapter 3.7 WLTB Antennas updated according R2R-T2.5-T-STD-116-01
15	10/03/2017	- Reworked according review comments (report R2R-T2.5-R-BTD-122-03)
16	29/03/2017	- Update of Appendix III - Requirement Traceability, also added requirements 161 to 220, ref. R2R-T2.5-I-CAF-087-03

		- Chapter 3.1.7 Train Inauguration Inhibit created - Review comments according R2R-T2.5-R-BTD-122-04 solved
17	31/03/2017	Editorial modifications
18	19/04/2017	Final version after TMT approval

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	
CI	Classified, information as referred to in Commission Decision 2001/844/EC	

Start date of project: 01/05/2015 Duration: 30 months

REPORT CONTRIBUTORS

Name	Company	Details of Contribution
Pierre-Emmanuel Reb	ALSTORM	Chapter 4
Maria Rosaria Derosa	ANSALDO (ASB)	Chapter 2.1
Michael Reismann Armin Hagen Weiss Lars Högberg Uwe Fuhr Holger Koch	Bombardier Transportation (BT)	Chapter 1.1, 2.3.2, 2.3.3, 2.5, 2.3.10 Chapter 3, 3.1, 3.2, 4, 4.1, 4.6, 4.7, 4.8, 6 Appendix I, II
Eneko Echeverría Ioritz Irazustabarrena	CAF I+D (CAF)	Executive Summary & Introduction Chapter 2.3.6, 2.3.10, 6
Iñaki Val Aitor Arriola	IKERLAN (IK)	Chapter 2.3.1, 2.3.4, 2.3.4.4, 2.3.9
Juan Moreno	METRO DE MADRID (MEM)	Chapter 2.2
Francisco del Río	STADLER (STD)	Chapter 2.1, 3, 4
Hermann Jung	SIEMENS (SIE)	Chapter 2.4
Phillipe Laporte	Societe Nationale Des Chemins De Fer Francais (SNCF)	Chapter 2.3.7, 2.3.8
Dobromil Nenutil Martin Vítek	UNICONTROLS A.S (UNC)	Chapter 4, 6
Martin Mayr	University Salzburg (USBG)	Chapter 3.1.1.2

EXECUTIVE SUMMARY

The Roll2Rail project aims to develop key technologies and to remove already identified blocking points for radical innovation in the field of railway vehicles, as part of a longer term strategy to revolutionize the rolling stock for the future. The results will contribute to the increase of the operational reliability and to the reduction of the life cycle costs. This project started in May 2015 and it is supported by the Horizon 2020 program of the European Commission. Roll2Rail is one of the lighthouse projects of Shift2Rail and will contribute to Innovation Program 1. At the end of the project all the results will be further developed, leading to demonstration in real vehicles or relevant environments in Shift2Rail.

Going into detail, this Roll2Rail project covers different rolling stock topics such as Traction (WP1), TCMS (WP2), Car-Body-Shell (WP3), Running-Gear (WP4), Brakes (WP5), Vehicle Interiors (WP6) and transversal activities such as Noise (WP7) and Energy Management (WP8).

In that context, WP2 T2.5 work package's concrete goal is to make the definition of suitable architectures, redundancies, and interfaces of the new wireless networks for both the train-to-train and inter-consist communications and the selected applications. The proposed solutions shall fulfil the requirements and serve as inputs to the IEC TC9 WG43 in charge of the standardization of the train communication network (IEC 61375 standard).

In order to do a proper definition of suitable architecture, D2.1 – Specification of Wireless TCMS Requirements public document will be considered as main input, whereas T2.4 RAMS and Security analysis task will support the corresponding studies to guarantee that these new definitions satisfy required safety and security levels.

Nevertheless, as train to train communication (virtual coupling concept) is closely related to signalling norms (IP2 within Shift2Rail initiative), is out of the scope of current deliverable.

Anyway, as it has been done in D2.1, three function domains have been considered, which is synonym of having three networks: TCMS Network, OOS (Operator Oriented Services) Network and COS (Customer Oriented Networks). Therefore, these architectures definitions will need to handle these three different network types not only at vehicle level, but also at communications between consists or train level (train is considered as a composition of consists).

Finally, these architectures will be validated within T2.8 at laboratory level, but these results will remain confidential within the Roll2Rail project partners.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

The goal of this deliverable (D2.5 within WP2) is to define architectures for different function domains (networks) and different communication level using proposed technologies (D2.3 & D2.7) for satisfying defined requirements (D2.1 & D2.4 for Security). Moreover, T2.4 will support RAMS & Security analysis whereas T2.8 will be in charge of validating proposed architectures within this deliverable.
First of all, a summary of D2.1 document will be included, in order not having to check D2.1.
Secondly, a state of the art of general constraints for architecture definition has been included.
Thirdly, solutions for different function domains (TCMS, OOS and COS) at different communication level (inside vehicle, inside consist and consist to consist) has been defined.
Fourthly, a traceability matrix between D2.1 requirements and current deliverables chapters has been included.
Moreover, a conclusion chapter has been added to summarize achieved results.
Finally, it should be remarked that inputs are coming from the partners listed in the table of Recorded Contributors. The inputs are based on current knowledge of the partners and also on experience in various previous projects. More details on the contributions from each partner can be seen in the REPORT CONTRIBUTIONS chapter of current deliverable.

1.1 TRACEABILITY TO T2.1 REQUIREMENTS

In order to judge that all requirements given from T2.1 are considered in this architecture document, Table 17 lists all unique requirement IDs of [69] with a reference to the chapters in this document, which consider the requirements.

2 GENERAL CONSTRAINTS FOR ARCHITECTURE DEFINITION

2.1 END DEVICE CLASSIFICATION

End device classification is needed to build suitable and optimum architectures.
End device classification shall provide as input the minimum communication needs and constraints after review the synergies among the devices.
The network architecture shall provide effectively and efficiently the communication capabilities required by each End Device to operate properly.
The classification has been performed according to location (both logical, in *domain* and *services*, and physical, *main location*), related mechanical and electrical properties (*enclosure, mobility* and *power method*), *price*, communication parameters (*communication scope, data packet size, data rate, cycle time, jitter*) and ED units (*units per vehicle* and *units per consist*).
The detailed End Device Classification can be reviewed in R2R-T2.5-T-BTD-006-04 document [76]. Values included in that document are to be considered as reference estimation, so are only indicative or maximum values. The final quantity of devices and data parameters depends on the type of rolling stock equipped and final deployed solution.

A detailed description table of parameters follows.

Table 1: End Devices Classification Parameters

Classification Parameter	Description	Valid Values
FBS Reference	Designation of the End Device according to the nomenclature described in EN 15380-2	Valid acronym from EN 15380-2
Domain	Categorization of devices by their functional scope	[Comfort, Operational]
Service target	Network categorization according to the expected user of the devices and functions.	[TCMS, OOS, COS]
Main Location	General indication of the position in the train.	[inside car, roof, under frame, outside]
Enclosure	Detailed indication of the envelope location.	[passenger compartment, technical compartment, electrical compartment, cab, container, outside]
Mobility	Ability to shift or move freely and easily the device itself.	[fixed, moving, portable]
Power Method	Power supply solution.	[battery, DC]
Price	Estimation of the cost of one unit for that type of End Device.	[low (<200€), medium (<1000€), high (>1000€)]
Communication Scope	Expected area on the train where a data exchange is expected from/to the ED.	[vehicle, consist, train]
Data packet Size	Size of the data payload of the communication frame in bytes.	Integer Value
Data Rate	Quantity of data in bits generated per second for data exchange from the ED.	Integer Value

Classification Parameter	Description	Valid Values
Cycle Time	Time period for the repetition of process messages in seconds	Real Value
Latency	Time that elapses between the generation and reception of a data packet. Time measured in seconds.	Real Value
Jitter	Time deviation from the presumed reception time of a data packet. Time measured in seconds.	Real Value
Sources per Vehicle	Number of EDs of one type included in a Vehicle.	Integer Value
Sources per Consist	Number of EDs of one type included in a consist.	Integer Value

Definitions for mounting options of “Main Location” Classification Parameter:

Inside car: Identify the area where devices are mounted inside of the vehicle carbody
Roof: Identify the area where devices are mounted externally on the upper part of the train carbody
Under Frame: Identify the area where devices are mounted externally below the lower part of the train carbody
Outside Identify the area where devices are mounted externally on laterals or front and rear ends of the train carbody.

In case of devices that are not physically connected to the train itself, specific indication is include in the device list document. “Outside-Portable” value could be used in that case.

2.2 WIRELESS LINKS CLASSIFICATION

In order to get the communication requirements for the WTCN architecture the wireless devices need to be allocated to the domains (TCMS, OOS, COS) and the hierarchical network levels (inside consist or train backbone) according [76] and [69]. Table 2 lists the classification for the wireless devices.

Table 2: Link classification of devices according [76] and [69]

	Inside consist			Train backbone		
Wireless device	**TCMS**	**OOS**	**COS**	**TCMS**	**OOS**	**COS**
Smoke detection	x					
Fire detection	x					
HVAC	x					
Cab HVAC	x					
NAU (Network Audio Unit)	x					
Noise Sensor	x					
Inside display		x				
Side display		x				
Front display		x				
Info display		x				
Routemap		x				

	Inside consist			Train backbone		
Wireless device	**TCMS**	**OOS**	**COS**	**TCMS**	**OOS**	**COS**
Acoustic orientation beacon for visually impaired		x				
Hearing induction loop		x				
Personal seat infotainment display		x				
Conductor PDA		x			x	
Seat reservation controller		x			x	
Seat reservation display		x				
CCTV camera		x			x	
CCTV video recorder		x				
rear view camera		x			x	
pantograph camera		x			x	
Ticket vending machine		x				
Ticket validator / transit card validator		x				
PCS (Passenger Counting System)		x				
Seat occupation sensor		x				
Passenger counting door sensor		x				
DCU (Door Control Unit)	x					
LIM (Line Interference Monitor)	x			x		
Energy Measurement System	x			x		
AUX (Auxilaries)	x					
TCU (Traction Control Unit)				x		
Diesel engine control				x		
Gear Control	x					
BCU/WSP (Brake Control Unit/ Wheel Slide Protection)	x					
VCU (Vehicle Control Unit)	x			x		
RIO 48I/24O (Remote I/O)	x			x		
Conductor HMI	x			x		
Driver HMI	x			x		
CCTV HMI		x			x	
Loco driver's remote controller	x			x		
DAS (Driver Assistant System)		x			x	
PIS (Passenger Information System)		x			x	
Passenger information portal			x			x
PCU (Passenger Communication Unit)		x			x	
PA (Public Address)					x	
PAS (Passenger Alarm System) Part of PCU		x			x	
CFA (Call For Aid) Part of PCU		x			x	
JRU (Juridical Recorder Unit)	x					

	Inside consist			Train backbone		
Wireless device	**TCMS**	**OOS**	**COS**	**TCMS**	**OOS**	**COS**
Bogie Controller	x					
Headlight/tail lamp controller	x			x		
MCG (Mobile Communication Gateway)					x	
ATP (Automatic Train Protection)	x			x		
GPS receiver (integrated in the antenna)	x					
Multimedia content server			x			

2.3 ARCHITECTURE CONDITIONING PARAMETERS

2.3.1 Wireless link reliability and availability

One of the main concerns in wireless communications is multipath fading, which is the result of getting at the receiving end multiple copies of the transmitted signal with different amplitudes and phases. For instance, when a transmitter and a receiver are within line of sight, the strongest signal usually comes from the direct ray, while the reflected copies are normally weaker; however, in cases where the line of sight is obstructed, all the signals in reception are reflected copies of the transmitted signal, so their contributions become critical (see Figure 1). In fact, these contributions can be destructive and, as a consequence multipath fading may compromise the reliability of the communication system. In order to overcome these issues, diversity techniques arise as a suitable solution.

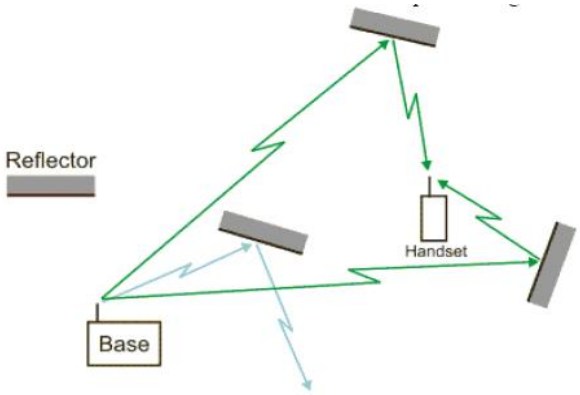


Figure 1: Simplified multipath propagation [60]

The main aim of diversity techniques is to guarantee that the information received has travelled through independent channels. A simple and clear example is the use of multiple antennas in the receiver. If the distance between the antennas is significant enough in terms of electrical length, the information received in each antenna is differently affected by multipath effects; thus, by selecting the antenna with higher received power, deep fading is avoided.
As diversity is based on statistically independent channels, its efficiency is dependable on the degree of correlation between the fading of the channels [61]:
There are several types of diversity techniques, such as spatial, temporal, frequency, angular and polarization diversity. All these techniques improve the performance against small-scale fading (multipath); in order to overcome large-scale fading, created by shadowing effects, a common technique is to use repeaters that forward an amplified version of the received signal, or Simulcast, where the different transmitters (in different locations) send the same signal simultaneously. On the other hand, the techniques described previously rely on modifications at physical level; other

techniques, such as Channel Coding and Interleaving, rely on changing the information sent. All the previous techniques are described below.

Spatial Diversity

This is the most used technique, and is based on deploying several antennas in reception in order to apply post-processing methods to the multiple copies of the transmitted signal. As already mentioned, a low correlation between the received signals is desirable; thus, it is important to determine the proper distance between the antenna elements [62], [63]. Different aspects have to be taken into account when defining this distance, such as the frequency of operation and the radiation distribution; hence, the separation between antennas will depend on the application. A general rule, applied in scenarios where the radiation is uniform, is to set the distance between antennas to $\lambda_0/4$ in order to avoid destructive multipath contributions [61].

Temporal Diversity

In time-varying channels, if the signals that travel through the wireless channel are received at different times they are supposed to be uncorrelated. In order to establish an adequate temporal distance, the Doppler frequency is taken into account. Therefore, the time spacing between signals must be at least $1/(2v_{max})$, where v_{max} is the maximum Doppler frequency [61].

Frequency Diversity

Frequency diversity consists of transmitting the same signal at different frequencies. As in the case of Time Diversity, the separation between the used frequencies must be large enough to guarantee uncorrelated channels; hence, the frequencies used for this purpose must be spaced more than the coherence bandwidth of the channel. In the case of jammer avoidance, the frequency separation will depend on the bandwidth of the jammer. The separation between both frequencies should be large enough to make it impossible for the jammer to interfere both of them.

Angular Diversity

Angular Diversity consists of using antennas with different radiation patterns; by doing so, multipath destructive contributions can be prevented as these patterns act as a spatial filter, attenuating the signals that arrive from certain angles.

Polarization Diversity

An additional way of taking advantage of different antenna configurations is to use Polarization Diversity. The propagation effects that take place in a wireless channel affect differently horizontally and vertically polarized signals; therefore, by using antennas with dual polarization in the receiver Polarization Diversity can be achieved.

Channel Coding

This technique is based on adding redundant data bits in the transmitted message. The transmitted redundant data is used by the receiver to detect or correct the errors introduced by the wireless channel (Forward Error Correction – FEC) without any feedback. Channel coding codes can be classified as:

1. Block codes
2. Convolutional codes
3. Trellis code modulation
4. Turbo codes
5. Low Density Parity Check (LDPC) codes

Interleaving

A communication link may suffer from burst errors due to wireless channel effects or even noise and interferences from other sources. It is possible to take advantage of the time diversity of the channel by coding the transmitted data interleaved along the time. This way, at the receiver, after

the data is again reordered, the errors become distributed along the message, so it is easier for channel coding techniques to recover the original message.
Figure 2 shows an example of antenna diversity. In this case the system allows the use of two antennas and the automated algorithm works as follows: on detection of a Synchronization Header (SHR) with a sufficient high signal level on one antenna, this antenna is locked for reception of Packet Header (PHR) and Physical Service Data Unit (PSDU). After the completed reception of a frame, this algorithm is carried out again to select the best antenna.

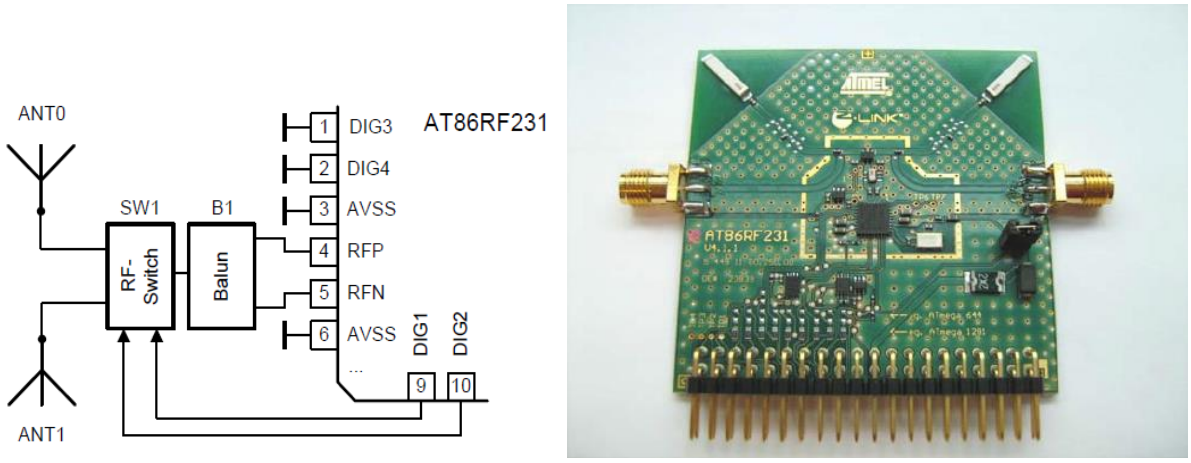
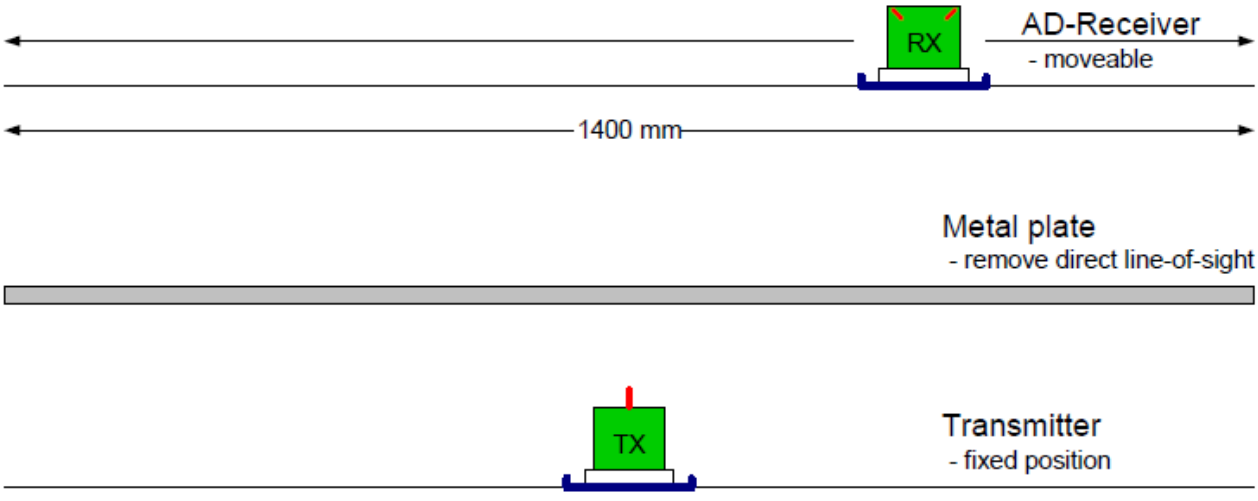


Figure 2: AT86RF231 Antenna Diversity Radio Extender Board [6].

Another example of antenna diversity is depicted in (see Figure 3), where measurements results of a 2.45 GHz multipath scenario are provided. Each curve represents the received signal power at each antenna: as can be observed, at certain points the received power between the two antennas varies more than 25 dB.



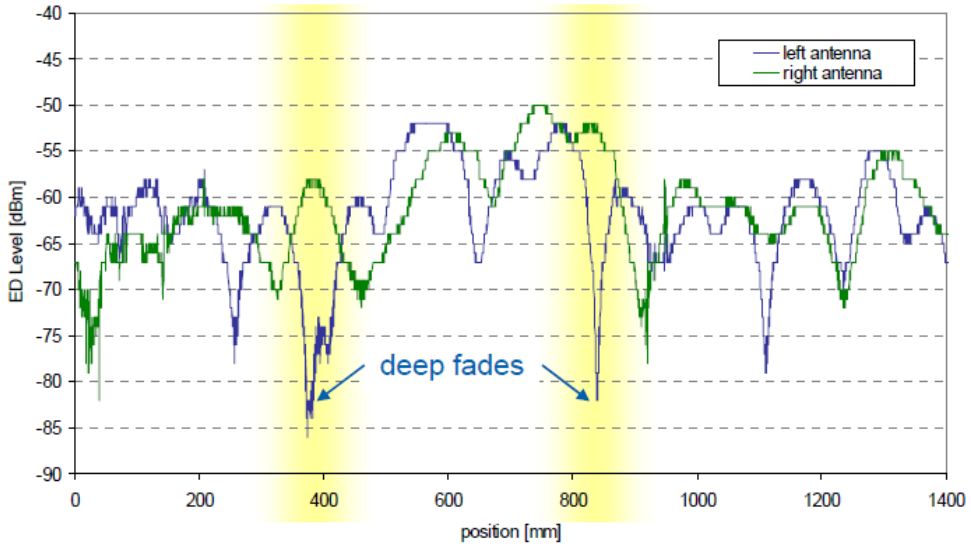


Figure 3: Antenna diversity: (a) Measurement setup, (b) measurement results [66].

In [66] frequency diversity is implemented. The authors choose frequencies of 900 MHz and 908 MHz, and the receiver is mounted on a moving platform. The measurement results for both frequencies are shown in Figure 4, where significant variations in the RSSI can be observed.

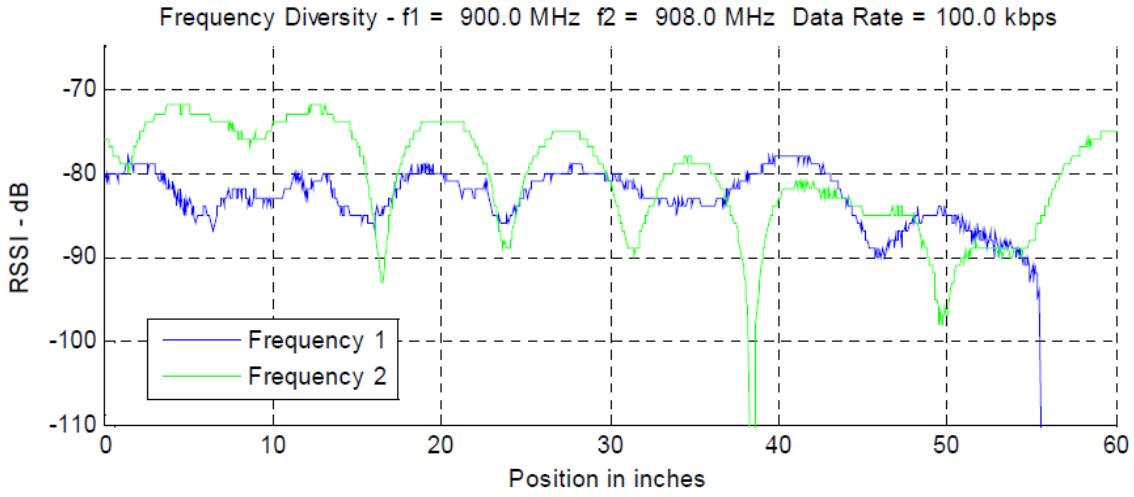


Figure 4: Frequency diversity results [66].

A particular case where diversity may suppose a great advantage is when a system is deployed in an area where there are potential interferers operating at the same frequency band. In this case, frequency diversity might be the difference between communication success and failure. For instance, Moxa's wireless access points [67] perform concurrent Dual-Radio Technology (see Figure 5), which basically consist of sending duplicate packets simultaneously at two frequency bands, thus achieving frequency diversity at the expense of using two independent RF modules. Ikerlan has also been working in developing a platform with frequency diversity by using Cognitive Radio (CR) and Software Defined Radio (SDR) techniques [68]. Cognitive Radio refers to RF systems which are aware of the characteristics of the environment they are operating on (e.g. by checking the availability of the RF spectrum using Dynamic Spectrum Access (DSA) algorithms), and change their operating parameters using Software Defined Radios, which are reconfigurable or reprogrammable radios that can support different functionalities at different times (e.g. changes in operating frequency, modulation, etc). In other words, thanks to the CR paradigm, the system

can take decisions according to the environment information, and reconfigure the parameters of a SDR. As a result of this awareness, and unlike Moxa's solution, frequency diversity can be performed just when it is required and with one RF module, using in this case a reconfigurable antennas to switch between 868 MHz and 2.4 GHz frequency bands. Active reconfigurable antennas fed by Bias-T devices are used in this platform; these antennas are controlled by MicroBlaze processors implemented in the transmitter and receiver Field Programmable Gate Array (FPGA) devices (see Figure 6). During the reconfiguration, the messages that the platform should transmit are discarded. However, these messages may be stored in a queue to transmit them when the reconfiguration is done. This platform transmits at 12.8 Mbps using a Quadrature Phase-Shift Keying (QPSK) modulation.

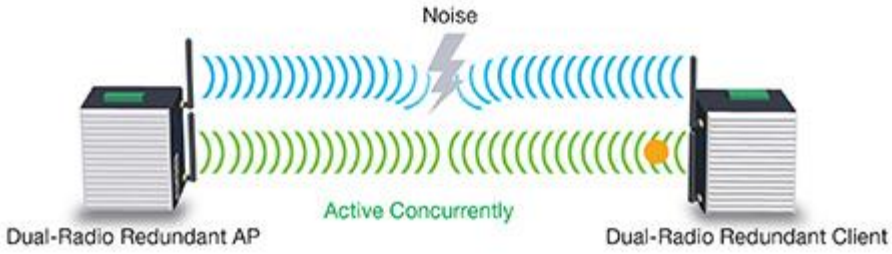


Figure 5: Concurrent Dual-Radio Technology [67]

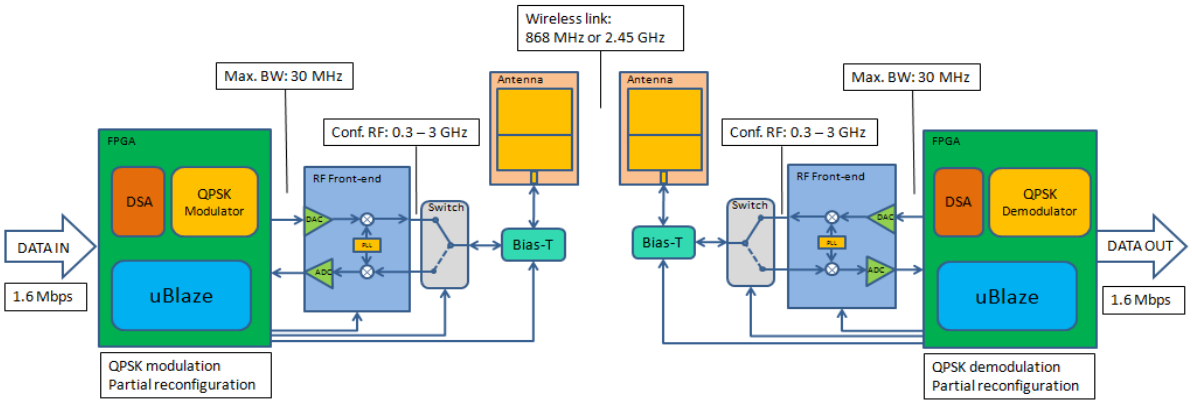


Figure 6: Ikerlan's Cognitive Radio (CR) platform [68].

All these diversity techniques are used nowadays in wireless communications, and therefore the applicability of any of them makes sense in railway applications.

2.3.2 Safety (SIL 2)

The main objective of the train communication system is to allow ED within a train to communicate with each other. The boundary between the train communication system and the ED is determined by the ED Interface (see Figure 7). This interface is defined for all OSI Layers, starting from physical characteristics (cable, connector type, electrical properties) to transport capabilities (lower level transport protocols) up to the application level (application profiles).

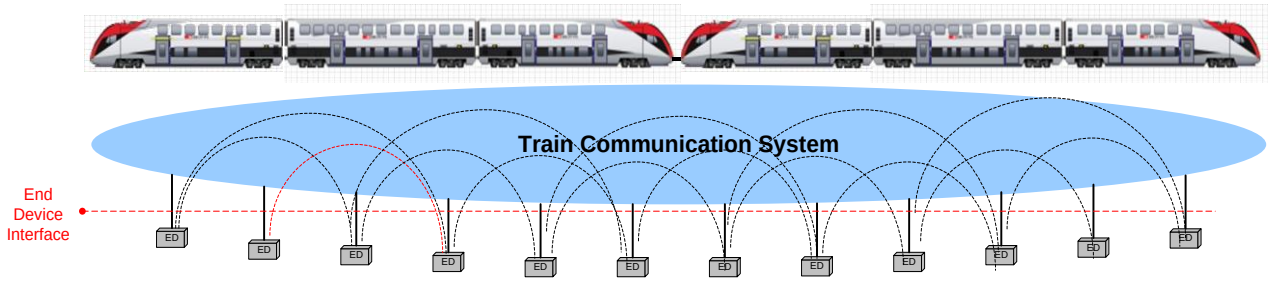


Figure 7: Train Communication System.

Beside the requirements for safe transmission systems of the EN 50159 standard, Safe Data Transmission has to be applied in case the data to be transferred from one end device to another end device is safety related.

2.3.2.1 Safe Data Transmission (SDT)

One possible solution for a safe data transmission is the Safe Data transmission concept according [77]. This Safe Data Transmission concept defines the architecture and the design of a safe data transmission protocol for the transmission of safety critical (= "vital") data between a safe data source (SDSRC) and one or many safe data sinks (SDSINK) through a heterogeneous communication network (Figure 8). The train communication network connecting SDSRC with SDSINK is treated as non-safe from a safety point of view.

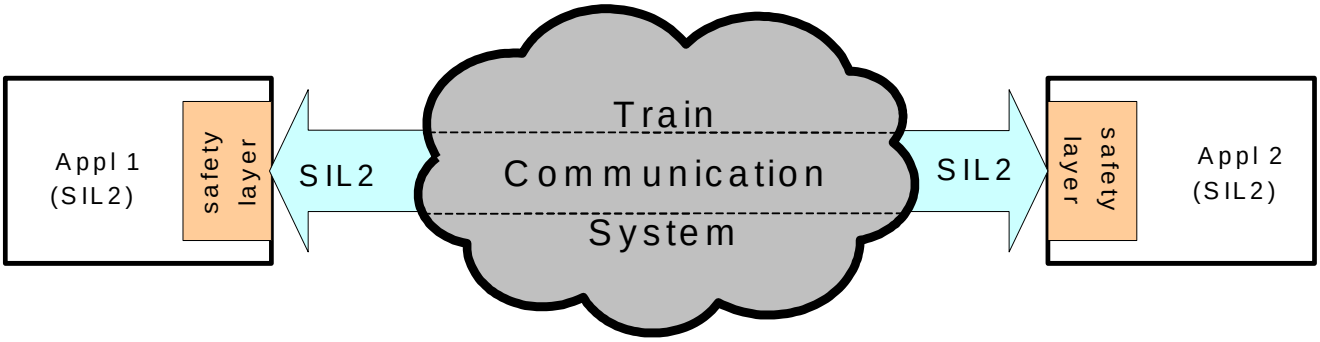


Figure 8: Simple SDT block diagram.

Vital process data shall be encapsulated in vital data packets (VDP) before transmission. A VDP according [77] consists of three parts (Figure 9):

Safety Identifier (SID, implicit field):	Unique identifier of the VDP. The SID is not transmitted, rather used as initial value for the safety code calculation.
VPD (Vital process data):	The safety critical application process data, refer [77]
VDP Trailer with check parameters:	These parameters are used by the SDSINK receiver to verify the correctness of a received VDP.

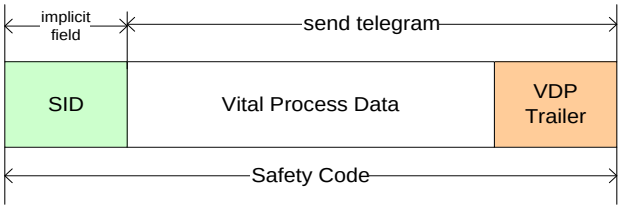


Figure 9: VDP structure (Example).

2.3.2.1.1 Safety Identifier

The Safety Identifier (SID) is a unique identification of the VDP within the train wide network, unique both in space (different SDSRC have different SID) and time (SID of SDSRC must change after train inaugurations changing the train topology).
This uniqueness must also be ensured when VDPs are only circulated in the local consist network (e.g. ECN), because it might happen that such a local VDP is transferred to a remote consist network by fault.
The SID is generated from a set of input parameters, which ensures the uniqueness of the SID, as depicted in Figure 10.

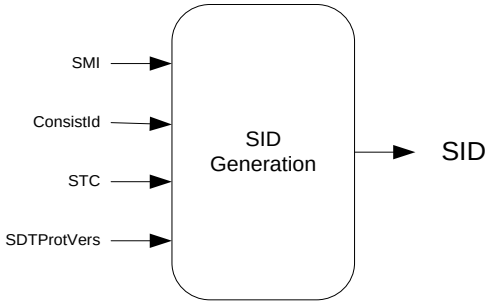


Figure 10: SID generation.

As the result of the SID generation needs to be a 32-bit unsigned integer value, a 32-bit CRC is generated over the data structure of the entries.

Table 3: SID generation input values

Entry	Description
SMI	Safety Message Identifier. Must be unique in the Consist.
SDTProtVers	Version of the SDTv2 Protocol
ConsistId	Unique Consist Identifier. Can for instance be the UIC identifier or a UUID
STC	Safe Topography Counter. The STC is a unique identification of the actual train composition as described in the following chapter Safe Train Inauguration.

2.3.2.2 Safe Train Inauguration

The train has a dynamic configuration, consists can be operational coupled or decoupled. The consist, which is a fixed assembly of vehicles, has a static configuration which doesn't change during operation.
The goal of the inauguration is to establish and to maintain the physical network, allowing communication between all end devices. The process of train inauguration aims to determine the sequence and orientation of connected consists and vehicles (= train topology) and also to provide application information about connected consists, vehicles and devices. The discovered train topology will be stored, together with the application related information, into a database which is accessible by all applications within the communication network.
The safe train inauguration basically consists of the following safety functions:

1. Safely determine the consist orientation data of the consists in the train
2. Safely determine the consist sequence data of the consists in the train
3. Safely determine the number of vehicles in the train
4. Safely determine change in train configuration (lengthening/shortening)
5. Safely determine safe application related information of each consist in the train

In order to determine the safety related data above, each consist detects the basic safety related data consist ID and coupler number from its neighbour consists.

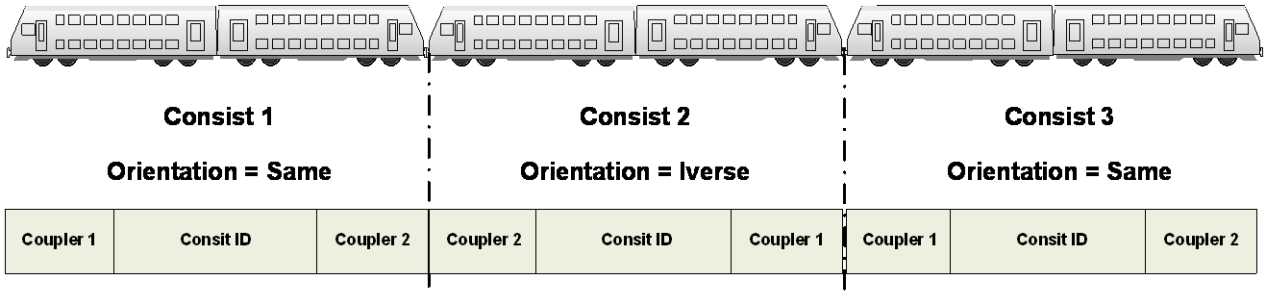


Figure 11: Safe train inauguration data.

All consists safely share its detected data with all consists in the train. Based on this information all consists in the train are able to safely calculate the train topology and generate the Safe Topography Counter by calculating a 32-bit CRC over the train topology data.
Each consist will come to the same STC result. In case a consist calculates a different STC by fault, all safe data sent by this consist is invalidated by Safe Data transmission on the receiving consists.

2.3.2.3 Fulfilment of the standard EN 50159

The standard EN 50159 [70] defines 3 categories of transmission systems which focussing in this case only on the TCMS operational domain (see chapter 2.4 for details): The main characteristics of the different transmission system categories are given in Table B.1 of [70], which is quoted here for convenience.

Table B.1 – 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 telecom 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.

2.3.2.3.1 Category 1 Transmission System

A category 1 transmission system consists of pieces which are under the control of the designer and are fixed during their lifetime. The criteria of a category 1 transmission system are defined as in Chapter 6.3 of [70].

For the special case of train inauguration, where several consist networks might be coupled over the train backbone, train wide communication is disrupted during the process of a train inauguration until the train inauguration is (successfully) finished. Thereafter, the train wide operational network is well determined with respect to its participants and will be again a closed system.

If a transmission system does not satisfy criteria A or B (PR1 or PR2) of 6.3.1, but fulfils criteria C (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 [70].

If a transmission system does not satisfy criteria C (PR3) of 6.3.1 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 [70].

2.3.2.3.2 Category 2 Transmission System

Category 2 transmission systems consists of systems, which are partly unknown or not fixed, however unauthorized access can be excluded. The train wide transmission system is considered to be a category 2 transmission system during the train inauguration process.

2.3.2.3.3 Category 3 Transmission System

Category 3 transmission systems consist of systems, which are not under the control of the designer, and where unauthorized access has to be considered.

2.3.2.3.4 Conclusion

In order to keep the effort economically justifiable for the safe or partly safe TCMS, it should be classified as a category 1 closed transmission system according [70]. However the question needs to be answered whether a TCMS network can still be seen as a closed system if it provides access points to the outer world. Several security mechanisms like firewalls and encrypting of safe date may be needed. It has to be analysed which threats exist and if countermeasures are available which are sufficient to not violate the closed system principle.

2.3.3 Security

The main target with security is to evaluate what risks the system is exposed to and to define appropriate countermeasures for unacceptable exposure. Several security risk models and approaches are defined in various standards, as an example refer to Figure 12.

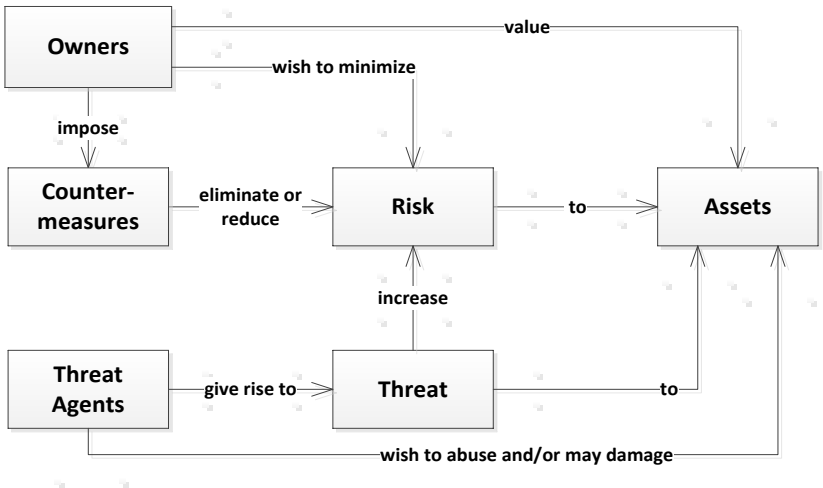


Figure 12: Security risk model defined in ISO/IEC 15408 and IEC 62443

The different security standards are analysed in R2R-T2.4-D-CAF-012 [57], section 4.1.1 and the security goals are defined in section 4.1.2. This should be seen as the initial approach used for R2R.
Note: Although a preliminary analysis has been written in R2R-T2.4-D-CAF-012 [57], non formal requirements for security are already collected and transferred to current deliverable. Therefore,

some preliminary assumptions and needs has been written in current deliverable in order to be able to close the deliverable on time. Anyway, once D2.4 is released, if any improvement of proposed architectures is needed, these improvements will appear in R2R-T2.4-D-CAF-012 [57].
Note: Cyber security will be analysed further and in a wider context within the Shift2Rail program TD2.11 with impact also on TD1.2, i.e. the main reference in terms of cyber security will finally be the deliverables out of Shift2Rail TD2.11.
The system architecture and networks are grouped into security zones with defined conduits connecting the different zones as described in section 2.4.
A separate threat and risk assessment, covering complete lifecycle of the system, is used to assign a security level for each security zone defining required countermeasures and their effectiveness. The IEC 62443 standard classifies security requirements into seven Foundational Requirements addressing all security aspects:

- Identification and authentication control. Define requirements for identification and authentication of all subjects before allowing them to access to the system.
- Use control. Define requirements for enforcing assigned privileges of an authenticated subject to perform the requested action on the system's objects (resources) and the monitoring of use of privileges.
- System integrity. Define requirements for ensuring integrity of the system to protect against unauthorized manipulation. The integrity protection is considered for both physical and logical assets.
- Data confidentiality. Define requirements for ensuring confidentiality of information in transit and on rest.
- Restricted data flow. Define requirements for segmentation of the system via definition zones and conduits to prevent the unnecessary data flows.
- Timely response to event. Define requirements for response to security violation.
- Resource availability. Define requirements for ensuring availability of the system resources against the degradation or DoS.

Note: The risk assessment needs to be supported by a continuous process to capture technology evolution that may give rise to new threats, which requires extended countermeasures by the system.
In addition, for all security zones, the system includes countermeasures/defences as defined EN50159 for a category 3 transmission system[1] and applying cryptographic techniques for encapsulating application and safety data inside additional security data layer.

2.3.4 Medium Access Control Protocol

Medium Access Control (MAC) protocols are responsible for controlling the medium access and deciding the underlying schedule for communication among the wireless devices. Taking into account the real-time requirements for TCMS communications, before starting the description of several MAC protocols for wireless communications, this section presents the new Time Sensitive Networking (TSN) standard for hard real-time communications. Notice that this standard only considers Ethernet communications, but it lays the foundation for the wireless medium. Therefore, it is more part of the state-of-the-art review than an architecture conditioning parameter.

2.3.4.1 Time Sensitive Networking (TSN)

The IEEE Time-Sensitive networking task group has defined a set of IEEE 802 Ethernet sub-standards called TSN (Time-Sensitive Networking). TSN as a whole is being developed to provide deterministic communication with real-time guarantees over Ethernet.
To make this possible, TSN uses queues based on priorities along with global time synchronization for a scheduled transmission of messages. Thus, all traffic classes may be transmitted over a standard Ethernet network without colliding among them. Several sub-standards are proposed by TSN and each of them specifies a different functionality. The main features proposed by TSN to extend the usefulness of standard Ethernet are going to be explained [71], [72].
Traffic scheduling is being standardized as IEEE 802.1Qbv. Existing priority mechanisms do not guarantee predictable time of delivery. In order to solve this, IEEE 802.1Qbv proposes to divide Ethernet traffic into different classes based on priorities. Switched networks will be responsible for scheduling this traffic in a deterministic manner through different queues. This concept is called as TAS (Time-Aware Shaper) in TSN. Each Ethernet frame will be assigned to a queue based on its priority. Queues have been previously defined within a schedule, and the transmission of packets will be sent during the scheduled time window. During these time windows, queues that are not transmitting will be blocked to ensure that non-scheduled traffic is not transmitted.
In order to block the queues, the concept of transmission gates is introduced. These gates are used to enable separate transmission queues and they can be open or closed. The state of the gates is defined within a schedule and the TAS opens and closes the transmission gate at specific times. At the time of choosing the next message to be transmitted, messages from those queues whose gates are open may be selected.
However, if minimal communication latency or an optimal bandwidth usage is required, the TAS concept is not enough; it is necessary to have pre-emption mechanisms.
In TSN, IEEE 802.1Qbu along with IEEE 802.3br are being standardized as pre-emption mechanism.
This mechanism is interesting when scheduled traffic is used because it can solve the following problem: if a non-time-critical frame is being transmitted just before the start of a scheduled time window, it can interfere with high-priority traffic. This pre-emption mechanism allows interrupting these frames to transmit the scheduled priority traffic. The interfering frame has to be fragmented and before the scheduled time window starts, a guard band is required. The length of this guard band needs to have the same size as the largest possible interfering fragment. After the transmission of the higher priority traffic, the transmission of the fragmented frame will be resumed. This mechanism implements a real-time control network in an application with scheduled transmissions.

Figure 13: Pre-emption mechanism proposed by IEEE 802.1Qbu [75]

On the other hand, to get bounded message latency in a deterministic communication, clock synchronization is needed. To achieve this in TSN, the 802.11ASrev sub-standard proposes new features to the existing IEEE 802.1AS standard used for Audio Video Bridging (AVB). 802.1AS standard, in turn, is an adaptation of the Precision Time Protocol (PTP) provided by IEEE 1588 standard.
To synchronize the clocks of the nodes in a network, synchronization mechanism uses a master-slave configuration. The master, called grandmaster, periodically sends timing information to the slaves and these synchronize their time base reference clock.

Moreover, 802.1ASrev introduces the ability to support multiple synchronization masters and the replication of them to support fault tolerance.
Although the definition of the standard IEEE 802.1Qci based on Per-Stream Filtering and Policing is in an initial state, it defines an important functionality particularly for critical control systems. These functions improve the robustness of the network detecting and attenuating interfering transmissions.
In order to filter streams, an input gate for each of them is proposed by 802.1Qci sub-standard. To make this possible, each gate has several functions such as a pass/no-pass function, an optional policing function and threshold counters.
To provide a robust and reliable communication, a redundancy management mechanism similar to PRP (Parallel Redundancy Protocol) and HSR (High-availability Seamless Redundancy) is defined in the IEEE 802.1CB sub-standard.
The goal of this mechanism is to send redundant copies of the messages in parallel over disjoint paths in the network providing redundancy. Normally, only critical traffic will be replicated because it is important that they always reach their destination. Moreover, even though the original message does not reach the receiver, the copy of the message will reach it. In the case that several identical messages reach the receptor, the duplicates will be discarded. Although the definition of the standard IEEE 802.1CB is in an initial state, the redundant mechanism defined probably will be based on sequence numbers.
Related to this, IEEE 802.1Qca will be responsible for defining how the path will be used by 802.1CB to send the redundant messages. Link speed, worst-case delay, and reliability will be considered among others to configure preferred routes for redundant paths.
Moreover, the sub-standard IEEE 802.Qcc defines an enhancement of the existing Stream Reservation Protocol (SRP) defined by IEEE 802.1Qat. For this purpose, a User Network Interface (UNI) is added for routing and reservation. Among the different mechanisms proposed deterministic stream reservation convergence, configurable stream reservation (SR) classes and streams and Support for Layer 3 streaming are found. This enhanced protocol achieves a reduction in the size and frequency of reservation messages.
In addition to these sub-standards, there are other sub-standards within TCN such as IEEE 802.1Qch, which is related to cyclic queuing and forwarding, and is still in a very early stage of development.

2.3.4.2 MAC protocols for wireless communications

MAC protocols for wireless communications can be mainly classified as: fixed assignment protocols, demand assignment protocols and random access protocols [1].
Fixed assignment protocols: wireless bandwidth resources are divided and assigned to nodes or links in a long term. Each node or link uses its own dedicated resource without the risk of collisions. Typical protocols include Frequency Division Multiple Access (FDMA), Code Division Multiple Access (CDMA), Space Division Multiple Access (SDMA), and Time Division Multiple Access (TDMA).

- FDMA: this technique divides the available frequency band into a number of subchannels; then, each of the resulting subchannels is assigned to a particular node which can transmit using exclusively its subchannel. Thus, FDMA requires frequency synchronization, relatively narrow-band filters and a receiver able to adjust its frequency to the channel used by the transmitter.
- CDMA: this method multiplies the narrow-band message signal by a very large bandwidth signal called the spreading signal. This spreading signal is a pseudo-noise code sequence that has a chip rate which is several orders of magnitudes bigger than the data rate of the message. Therefore, when using CDMA, the receiver must be aware of the codeword used by the transmitter.
- SDMA: this technique is based on controlling the radiated energy for each user. In order to cover different areas, spot beam antennas are used. These covered areas may be

served by the same frequency or different frequencies. This technique requires high implementation complexity for the antenna and signal processing knowledge.

- TDMA: similarly to FDMA technique, TDMA divides the available resources (in this case time) to distribute them among the nodes present in the network. Thus, a time slot is assigned to each node what allows the system to use the same frequency of operation.

Among these techniques, TDMA has been widely used in industrial Wireless Sensor Networks (WSN) as it is a simple technique that provides an orderly media access.

Demand assignment protocols: The resources are dynamically provided on demand to the nodes that require them. Thus, the assignment is limited to the duration required to communicate the data available at each moment. Once the communication is completed, the resources are released so that another node can take them. In order to achieve this functionality the transceiver must be switched on nearly all the time; and therefore, these protocols have high energy consumption.

Random access protocols: These are contention-based protocols intended for distributed control. They have a simple implementation with a full bandwidth available to any node but they do not ensure beforehand a successful transmission. There is no coordination between nodes to avoid collisions. Therefore, they are not suitable for time-critical applications that require deterministic guarantees. Nowadays, the most used random access protocols are based on CSMA. This mechanism is based on listening to the medium before transmitting, thereby determining whether the channel is free or not, and allowing transmission only in this case.

Latest research work on MAC protocols is mainly based on modifications or combinations of the protocols mentioned previously. The performance of a MAC protocol can be determined by different parameters such as throughput, delay and energy efficiency; thus, its design depends on which parameter is of more significance for a specific application. Therefore, as stated in [2], WSN MAC protocols can be divided in four categories: asynchronous, synchronous, frame-slotted, and multichannel. Asynchronous and synchronous ones are related to the mechanism of duty cycling in WSNs. In order to save energy, duty cycling is widely adopted in WSNs. In this technique, each node alternates between active and sleep states. Two nodes can communicate only when they are both active. In synchronous MAC protocols, neighbouring nodes are synchronized to wake up at the same time; therefore, the focus is on the delay reduction and throughput improvement. On the other hand, asynchronous MAC protocols focus on efficiently establishing communication between two nodes that have different active/sleep schedules. In order to achieve a high throughput, frame-slotted mechanisms allocate time slots in a way that two nodes within the two-hop communication neighbourhood are not assigned to the same slot, thus addressing collision and hidden terminal problem. However, a major concern is that the channel utilization is low when few nodes have data to send as time slots assigned to their neighbours are wasted. Regarding multichannel, it is employed to further improve network capacity. Distributed channel assignment and efficient cross-channel communication are two major challenging issues in multichannel MAC protocols.

2.3.4.2.1 Asynchronous MAC Protocols

The main characteristic of this kind of protocols is that each node chooses its active schedule in an autonomous manner. In the absence of synchronized schedules with other nodes, they achieve a lower duty cycle in comparison with synchronous MAC protocols, and with a lower throughput. In order to achieve this behaviour they use the following procedure: Nodes are in low-power sleep most of the time; hence, in order to indicate that there is an imminent packet transmission, the sender sends a preamble in advance. While the preamble is being transmitted, the other nodes see the channel as occupied. Some asynchronous MAC protocols are B-MAC [3], RC-MAC [4] or PW-MAC [5].

2.3.4.2.2 Synchronous MAC Protocols

It is possible to synchronized the active/sleep scheduler of the nodes to change their state at the same moment, at the expense of additional synchronization load.

In this kind of protocols, a node senses the channel to hear other node's schedulers. If it does not hear anything, it will act as a synchronizer. Therefore, it will define when it is going to change its

state to active and it will send its scheduler to the rest of the nodes in the network. All the nodes in the network will be synchronized to its scheduler.
Synchronous MAC protocols in literature are mainly focused on reducing delay and increasing throughput. Some techniques based on synchronous MAC protocols are S-MAC [6], DW-MAC [9], DMAC [10] and SCP-MAC [24].

2.3.4.2.3 Frame-Slotted MAC Protocols

This kind of protocols are based on the concept of slot used by Time Division Multiple Access (TDMA). TDMA provides high channel utilization when there is a lot of traffic to send. However, the nodes must be synchronized in order to avoid collisions between packets. Moreover, in TDMA based protocols usually, each node has an assigned slot whether or not it has data to transmit. This can lead to low channel utilization in cases where traffic is unpredictable. Next, some Frame-Slotted based techniques are reviewed.
In order to avoid wasted bandwidth issue when there is little traffic to send, Z-MAC [13] is proposed. This MAC combines CSMA and TDMA medium access mechanism to achieve better channel utilization. With Z-MAC a node with data to send can hijack an unused slot assigned to another node. Even though channel utilization is maximized, energy consumption is maximized too due to CSMA mechanism.
TRAMA [14] introduces another approach to increase channel utilization of TDMA. Instead of assigning all slots of the frame to the nodes of the network, nodes that have data to send will request these slots. Moreover, TRAMA provides a priority-ordered slot assignation. However, this can lead to high energy consumption and delay maximization.
With the aim to maximize the throughput at the sink node, TreeMAC [15] is proposed. This proposal introduces an extra dimension to the TDMA in order to avoid interferences. To make this possible frame and slot assignment are defined to eliminate horizontal and vertical two-hop interferences respectively. This implementation has into consideration that the nodes in the same level use different frames, so the collision is avoided.
In many applications, a node can receive data from multiple nodes and each time this happens it should change its state to active state when it is going to receive a packet and to sleep state when reception is successful. Instead of this operation, there are in literature many implementations such as Crankshaft [16] and PMAC [17] in which time slots are assigned to receivers rather than to transmitters, so receivers know when they need to change their state to active to listen to the packet. The main advantage of this kind of protocols is that only the target nodes have to wake up. However, this mechanism does not guarantee collision avoidance, as a transmitter does not know if another node is transmitting at the same time.

2.3.4.2.4 Multichannel MAC Protocols

Given that radio bandwidth in WSNs is limited, parallel data transmission has recently attracted attention as many WSN platforms have emerged with multichannel support. In multichannel MAC protocol there are two main issues to solve: Distributed channel assignment and efficient cross-channel communication.
One of the MACs that supports multichannel is called MMSN [18]. This MAC implements an algorithm in which all nodes of the network know what channel is used by their neighbours. To make this possible, each node has to choose a channel that is not selected by any of their neighbours. This condition is taken into account for all nodes within two-hop distance. Moreover, toggle snooping and toggle transmission mechanism are introduced to allow communication through different channel chosen by two nodes. This has to lead to high energy consumption.
On the other hand, in [19] a MAC is proposed with the aim to minimize inter-channel communication. For this reason, they consider putting together those nodes that use the same channel to communicate as they claim that communication in the same channel incurs less

overhead. To achieve this, each node in the network sends regularly how many times it has acquired the channel with success and how many times it has failed. Depending on the probability to succeed, a node will change the channel or not. Other examples of protocols based on Metric Optimization are TMCP [20] and GBCA [21], which aim at minimizing the total interference in a network.

In MC-LMAC [22] a hybrid TDMA and FDMA MAC protocol is proposed. As in the MAC proposed in [18], each node has to choose a channel that is not selected by any of their neighbours, although in this case a slot/channel pair is chosen, instead of simply choosing a channel. Moreover, in MC-LMAC it is possible that a node selects to use the same slot as its neighbour, but both must have different channels. As it happens with traditional TDMA, the channel utilization is low when there are few nodes with data to transmit.

As in the previous implementation, time slots can be assigned to receivers rather than transmitters. In multichannel MAC protocols, Y-MAC [23] is one of the proposals in literature that is based on this technique. As MC-LMAC, Y-MAC is an hybrid TDMA and FDMA MAC protocol. Y-MAC superframe is based on a broadcast phase and unicast phase. In the previous one, the nodes that have broadcast packets have to contend for sending them. Regarding the unicast period, each node has an assigned slot. These slots are exclusives within two-hop distance but, as shown in Figure 14, nodes are allowed to change to the next channel in the coming slot when successful packets are received in their own slot. MuChMAC [24] is another proposal in literature where time slots are assigned to receivers and, as Y-MAC, it is hybrid too. The main difference between them is that in MuChMAC, each node chooses the receiving channel for each slot following a pseudo-random hopping sequence.

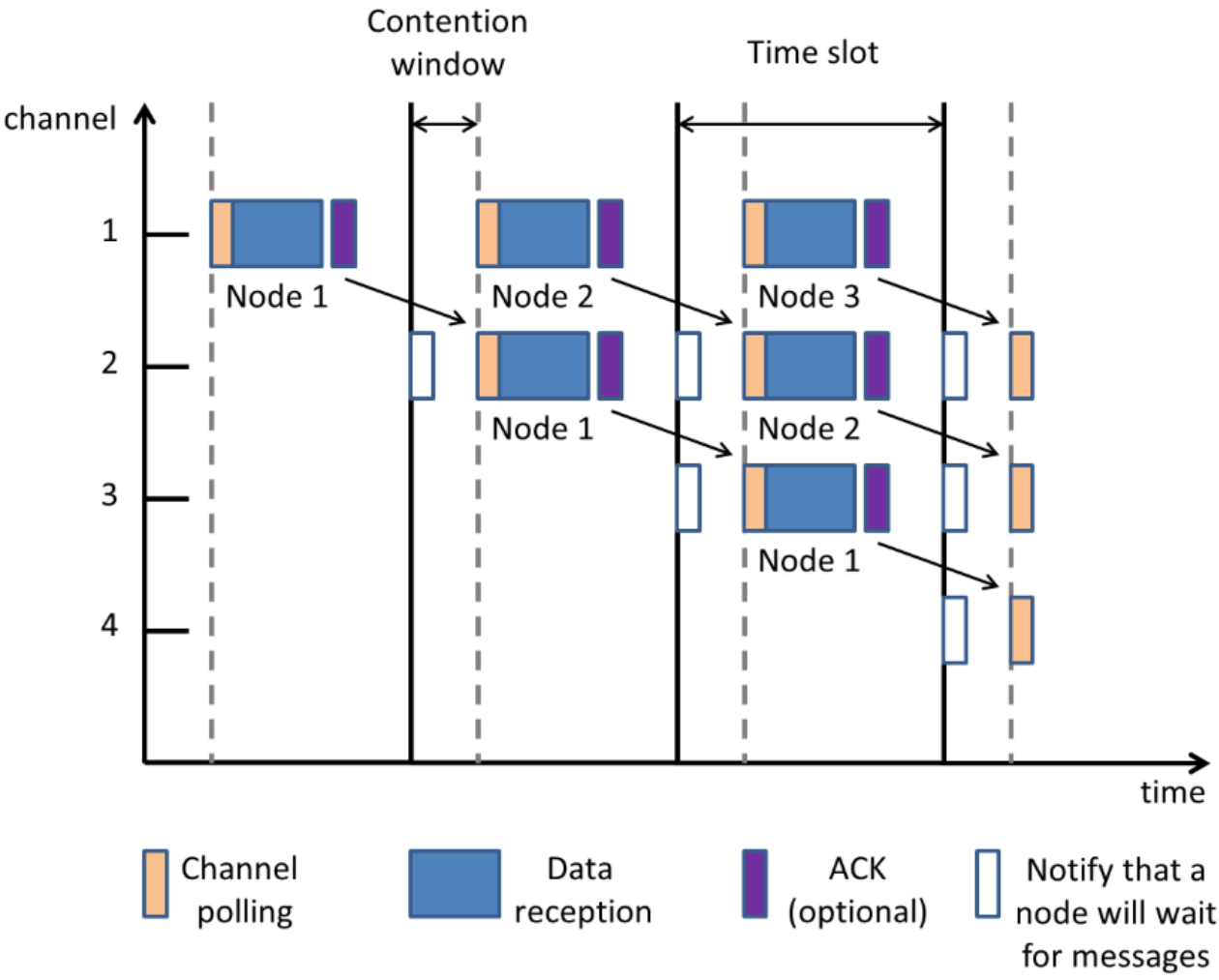


Figure 14: Channel hopping mechanism in Y-MAC [2]

So far the basic MACs have been reviewed, as well as some techniques that introduce different variations into the basic MACs in order to provide different solutions but with no specific purpose. Usually, WSN applications regarding industrial automation take into consideration a deterministic and reliable communication when designing MAC protocols. Moreover, these applications normally have real-time requirements. In [25] an extensive review is carried out of different MAC protocols for mission-critical applications in WSN. The authors conclude that most MACs analyzed are not capable of accomplishing the requirement related to reliable transmission for these applications as they are mainly focused on minimizing energy consumption.
In order to complete the survey on MAC protocols, in the following lines some protocols specially designed for real-time systems are summarized [27].
RRMAC [26] proposes a tree topology MAC based on TDMA medium access mechanism. This implementation ensures that the sink node will receive the data from the source nodes in a single superframe. Moreover, for making possible a synchronized network, beacons are used. As soon as a node receives a beacon frame, it will adjust its clock and will execute the scheduled based period in which each node will transmit in its own slot. RRMAC also considers non-real-time traffic, so it offers a contention period.
Dual-mode real-time MAC [28] protocol includes two modes: unprotected and protected mode. The first one is represented in Figure 15 (a). This mode takes into account two parameters: Maxrange which indicates the maximum communication range of the node, and backoffunprotected. This mode is used to send emergency packets at high speed, so if an emergency packet is sent by a node, the other nodes in the network will listen to nodes backoffunprotected. It is possible to choose a node like a relay so if the backoffunprotected expires and no emergency message has been received, this node will retransmit the packet. Therefore when this method is used there might be collisions between different nodes. This issue is addressed by the protected mode shown in Figure 15 (b). This mode uses signalling packets to achieve high reliability. Using these packets, source nodes can reserve all the nodes on the way to the sink node, and these reserve nodes will not transmit new packets, avoiding collision between nodes.

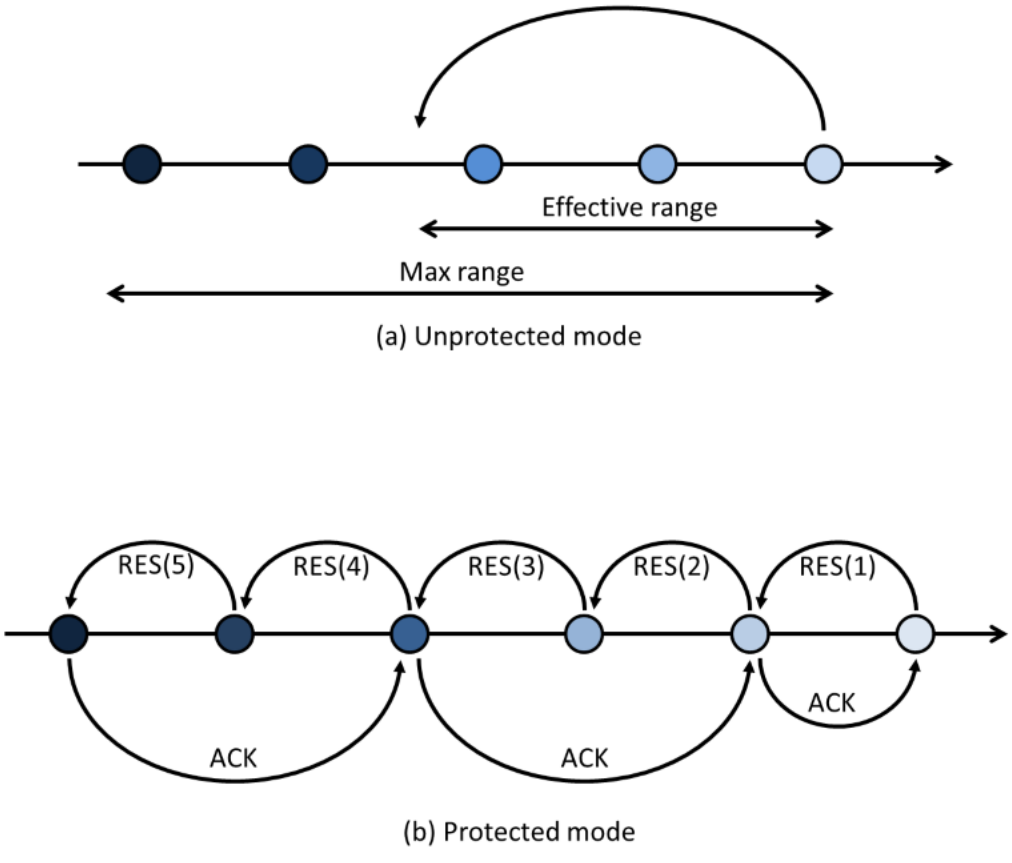


Figure 15: Algorithm of dual-mode real-time MAC protocol [27]

TOMAC protocol [29] is implemented for one-hop mesh topologies. The aim of this protocol is to ensure that the messages are delivered in an orderly way. To accomplish this, messages are ordered by priorities and those with the highest priority will be sent before. An unsuccessful transmission leads to an increase of packet priority.
The goal of SUPORTS [30] is to increase the probability that the packets arrive within its deadline, taking into account the delay of each them. For that, SUPORTS proposed a least-laxity based scheduler which will be responsible for ordering the packets delivery.
Virtual TDMA for Sensors (VTS) [31] provides a TDMA access scheme. The superframe of this scheme will have the same number of slots as nodes are in the network. VTS is based on S-MAC but, unlike this, in VTS a control packet called CTL is used as SYNC packet. The virtual superframe is formed once each node in the network has sent its first CTL. Then the node that has the slot will perform the CCA and it will send CTL packets to the entire network. VTS proposal uses CSMA/CA to exchange data between nodes.
Another proposal is presented in [32]. The algorithm proposed, called Channel Reuse-based Smallest Latest-start-time First (CR-SLF), uses the spatial channel reuse to schedule packets. The goal of this protocol is to have parallel transmissions without interfering with them. To achieve this, the algorithm is divided into 3 phases: first, the highest priority packet is going to be chosen by the scheduler. Second, the packet is allocated in one of the parallel transmissions. Finally, the time when the message is completely received by the next hop node is updated, and a new packet for the next hop is inserted in the transmission group.
Energy Based Real-Time MAC Protocol: Low-Power Real-Time (LPRT) [33] is presented as a hybrid TDMA-CSMA/CA MAC protocol that follows a star structure. A slotted superframe is proposed by LPRT. The superframe includes a contention period and a contention-free period (CFP). The base station will start the transmission at the beginning of the superframe sending beacon frames and these will determine the transmissions during the CFP.

2.3.4.3 Scheduling

Wireless Sensor Networks used in industrial processes require highly reliable and timely data delivery. To fulfil such demanding requirements, specialized MAC protocols are employed. Scheduled based protocols such as TDMA, have better performance compared to contention-based protocols especially when there are heavy traffic conditions. Therefore, if a reliable and deterministic communication is required TDMA based protocol are suitable [36]. Yet, in TDMA-based protocols it is very important to have a schedule that provides time for transmissions and retransmissions of the packets.
When there is a fixed amount of nodes in the network and the environment does not change, it is appropriate to use a static scheduling. Thus, a valid schedule can be achieved in an offline way without having to change it at runtime. However, getting a valid schedule is a tricky question. It has to be also raised that, even in relatively static environments, conditions change and schedules do not remain valid forever; hence, a schedule management framework may be required. The authors in [37] proposed not only to collect data at deployment time but to augment it during network operation, and periodically this data set may be used to determine a new schedule.
In the following lines it is summarized how schedules may generally be constructed for industrial process monitoring and control applications.
To explain the approach we take as an example the topology shown in Figure 16a. In order to ensure a deterministic communication, a TDMA based scheduler is assumed. In each slot a packet and ACK are transmitted to a one-hop distance node. The proposed scheduler is shown in Figure 16b. In the first slot, node A transmits its own data to node B. In the second slots, node B transmit to node D the A node's data. In the third slot, node B transmits its own data to node D and finally in the slot four, the node C transmits its own data to node D.
In case of needing to retransmit a packet, it is possible to modify this scheduler. The new approach is shown Figure 16c. It can be seen that the scheduler is the same, with the difference that after the data transmission slot there is a slot (marked with an R) for retransmissions.

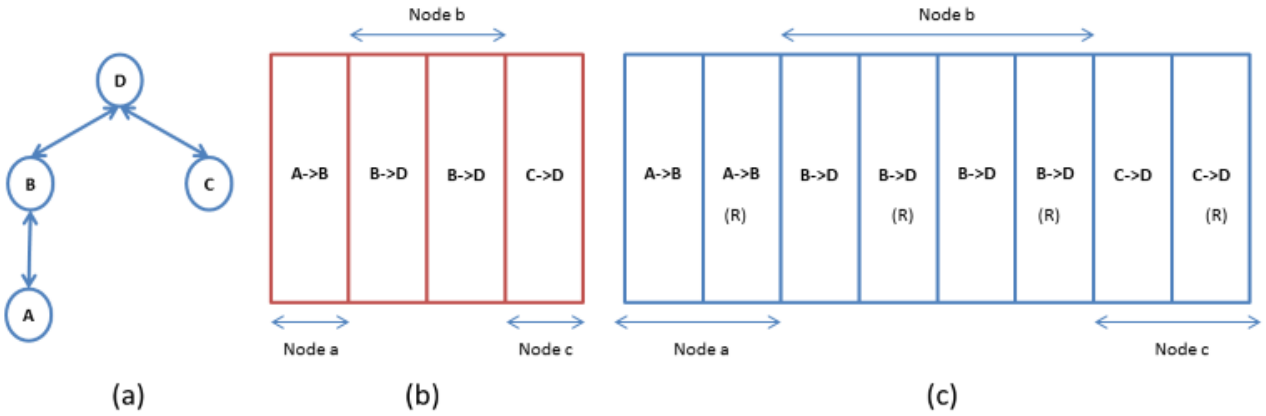


Figure 16: Simple topology and possible schedules for error free and lossy channels [37]

There are other techniques to provide reliability to the schedules. Common methods are Expected Transmission Count (ETX) or Packet Reception Rate (PRR) [37].
The epoch length can be reduced if not all nodes are within communication range of each other. In this case spatial re-use of TDMA slots is possible and the epoch length can be reduced.
Generally, in industrial applications, the nodes are not grouped within one network but there are a large number of small networks, whose sink nodes are connected via a wired backbone infrastructure [37]. Within each wireless network, nodes are generally in interfering range of each other and spatial re-use is generally not possible. However, it is important to reduce the interference range of a network in order to allow the operation of other nearby networks.

2.3.4.3.1 Schedule Algorithms:

As stated in [36] schedule algorithms may have different objectives, design constraints and assumptions. Regarding the objectives, four are identified as the most studied ones in literature: minimizing schedule length, minimizing latency, minimizing energy consumption and maximizing fairness.
In mission critical application, common in industrial environments, it is very important to reduce the latency of the transmissions. Although minimizing the schedule length may as well minimize the latency under certain conditions, most algorithms do not consider the average latency experienced by individual packets at each hop [36]. Additionally, the chosen network topology has a very important role in terms of reducing the delay of the transmissions, but also the opposite can occur. For example, a line topology may have a high reliability but high latency because of the larger number of hops between source nodes and sink.
In literature, several algorithms focused on minimizing latency can be found. For instance, the aim of the proposal in [38] is to minimize the transmitted latency. In this implementation a node that act as a relay is needed. So, data is transmitted to them and then it is transmitted through them towards the sink node. The scheduler is constructed according to the distance in a number of hops. The scheduler is defined in order to fulfil with the minimum worst case latency.
Another algorithm which aims to minimize latency is proposed in [39]. The authors consider receiver-based scheduling that meets the requirements of the ZigBee standard. In this standard, nodes change their state to active for receiving data from their children and change their state to active again to transmit those packets. As in the previous proposal, a minimum latency scheduler is defined previously. Then, an algorithm goes into action to provide better schedule.

2.3.4.3.2 Schedule-Based MAC Protocols:

Schedule-based protocols, normally based on TDMA medium access mechanism, are able to guarantee a determined end to end delay [42]. There are many proposals that accomplish this characteristic.

One of these proposals that guarantees end-to-end delay is RT-Link [43]. Based on TDMA scheduling, it considers two types of slots in its active state. On one hand, there are Scheduled Slots (SS) that are assigned to the nodes. On the other hand, there are Contention Slots (CS), which use a random slotted Aloha algorithm to decide which node have to transmit. This proposal is suitable to perform mission critical applications. Nevertheless, it needs a special hardware to obtain time synchronization, so this limits its usability.
On the other hand due to the difficulty to construct a schedule without a network planning beforehand PEDAMACS [44] is proposed. This MAC is based on TDMA too. First of all, the sink node needs to discover the network topology that has a tree structure. To accomplish that, a signal-to-interference-plus-noise (SIRN) is used by the nodes. Then, the sink node will define and send to all the nodes in the network the slot schedule taking into account the information collected. The scheduler algorithm considers that the packets generated before the scheduling frame are going to be delivered to the sink node by the end of the scheduling phase.
Recently other MAC protocols are presented [45] that use multiple channel concept. In these cases, nodes need to synchronize in time as well as in the frequency domain. For instance, HyMAC [45] is a hybrid TDMA/FDMA protocol that contains scheduled and contention slots. The sink node defines a minimum delay schedule taking into account the topology of the network. To do this, the sink will assign time slots and frequency channels for each node in the network. The throughput with this hybrid MAC is increased with respect to TDMA-only based schedulers.
In literature it is also possible to find protocols focused not only on reducing delays but on increasing reliability as well. For instance, Multi-Path and Multi-SPEED Routing (MMSPEED) protocol [46] provides traffic differentiation and guarantees delay and reliability in the communications. To service differentiation, an important issue in mission critical application with mixed periodic and non-periodic traffic, a routing protocol is introduced in the network layer. On the other hand, in order to get a reliable communication, probabilistic multipath forwarding perspective is adopted by MMSPEED. As in other MACs, protocols defined previously, nodes that act as relays are used to accomplish that.
GinMAC protocol can deliver data in a timely and reliable manner [35]. It is a TDMA based protocol, which follows a tree topology and uses a low duty cycle to save energy when nodes have nothing to transmit. The dimensioning of the TDMA frame is performed in a static manner being dependent on the number of nodes in the network. Therefore, if the network changes, the frame should be designed again. Moreover, this frame is composed of 3 types of slots: Basic (each node will have an assigned slot and will use it to transmit information to the root node or vice versa, ensuring that this will be transmitted in the period of a frame. The frame has upstream and downstream slots), additional (used to increase robustness, they will be used if the transmission in basic slots fails) and unused (used to improve the working cycle). It should be mentioned that the slots (including additional) are exclusive, and they cannot be used by other nodes in the network. An example of a possible GinMAC topology can be seen in Figure 17.a, in Figure 17.b the corresponding scheduled frame is shown.

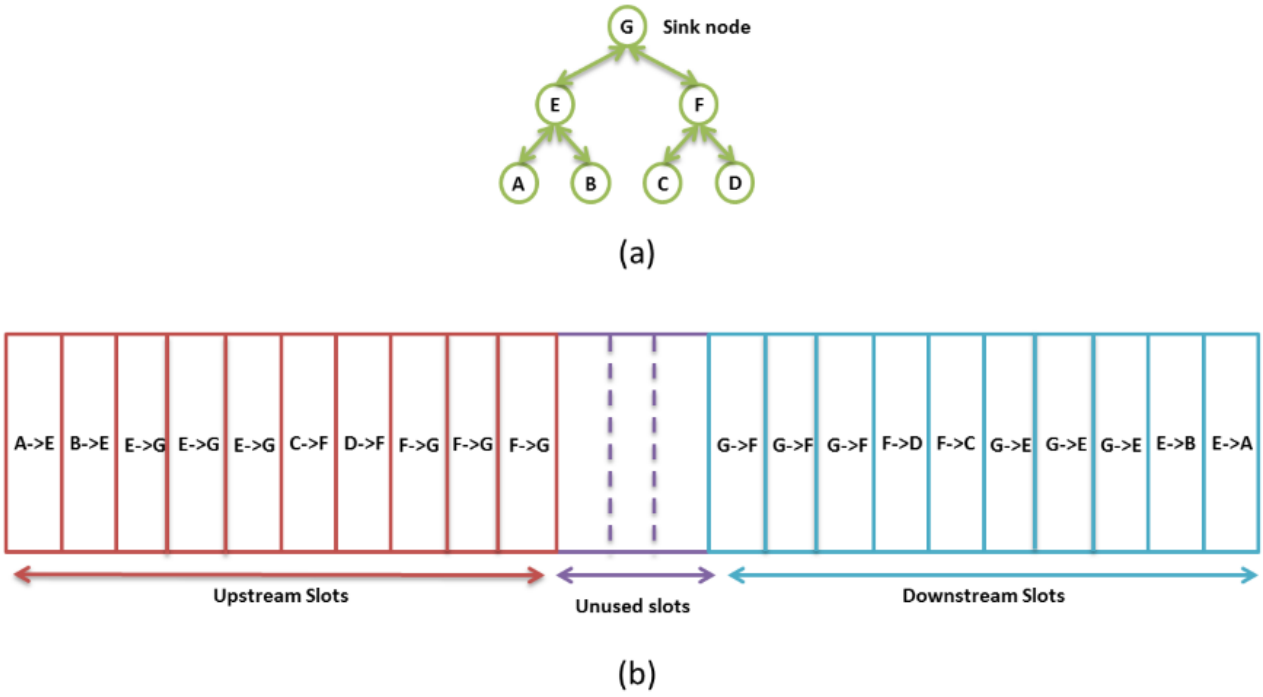


Figure 17: GinMAC protocol [35]

WirelessHART [47] is the first open wireless standard and a wireless mesh network technology for process automation applications. This standard uses the physical layer of the IEEE 802.15.4 standard but implements its own data link layer, whose MAC is based on a schedule solution. The media access mechanisms used by WirelessHART are TDMA, FDMA and CSMA. It provides end-to-end reliability of almost 100% through the use of multiple features such as the frequency hopping or searching for alternative paths in case of channel degradation. However, WirelessHART does not deal with packet loss and this can create delay and determinism issues.

2.3.4.4 Summary

Real-time traffic is demanded by TCMS, and as it has been stated before, scheduled-based protocols such as TDMA are the best option to ensure the requirements of this traffic. Also, a multichannel transmission can be used jointly in order to increase the throughput of the system. However, to ensure a reliable and deterministic communication, the TDMA MAC demands a scheduler that provides time for transmissions and retransmissions of the data. The choice of the specific type of scheduler is independent from the selected MAC layer, although all schedulers will require operation over a TDMA MAC layer. In this section, several TDMA and multichannel MAC layers as well as scheduler algorithms to be used in railway applications have been detailed.

2.3.5 Interference

The wireless MACs described in 2.3.4 must cope with interference in order to allow a reliable communication, as even though interferences operate at the physical layer the MAC layer gets also affected. For example, interferences occupy the wireless channel and therefore block the channel access mechanisms, and they also increase the packet error rate and as a consequence the number of retries. This means that MAC layers that implement temporal or frequency diversity (e.g. Frequency Hopping techniques) will be more robust against interferences. Below, interference sources in wireless communications are explained and related to railway applications. Then, the traditional interference sources found in wireless communication and some techniques to reduce them are presented.

Interferences in wireless communications can be divided into two categories: man-made interferences, and those caused by natural phenomena. They are described below.

2.3.5.1 Natural Interference

Natural events, such as snow storms, electrical storms, rain particles or solar radiation, cause natural interference. This interference is known as static or atmospheric noise. This kind of interference is not normally taken into account because it does not cause many problems with modern digital data equipment.

2.3.5.2 Man-made Interference

2.3.5.2.1 Co-channel Interference:

This type of interference takes places when the signal causing the interference has the same frequency as the desired signal.

2.3.5.2.2 Adjacent Channel Interference:

Adjacent channel interference is caused by undesired signals that are close to the channel of the desired signal. Two types of adjacent channel interferences can be distinguished: *in-band interferences*, which refer to those interferences which occur inside the bandwidth of the desired signal, and *out-of-band interferences*, which occur outside the bandwidth of the desired signal. The rejection to the adjacent channel interference is related to the selectivity of the RF receiver; this parameter is related to the selectivity of the RF and Intermediate Frequency (IF) filters.

2.3.5.2.3 Spurious Interferences:

Spurious interferences refer to signals at frequencies other than the nominal frequency of the receiver, at which the RF receiver is also able to generate a valid output. For instance, in superheterodyne receivers the main spurious interference is the *Image Frequency*. The Image Frequency is a frequency separated a distance equal to IF from the local oscillator of the receiver, and in the opposite direction of the RF frequency (i.e. at a distance 2*IF from the RF frequency) (see Figure 18).

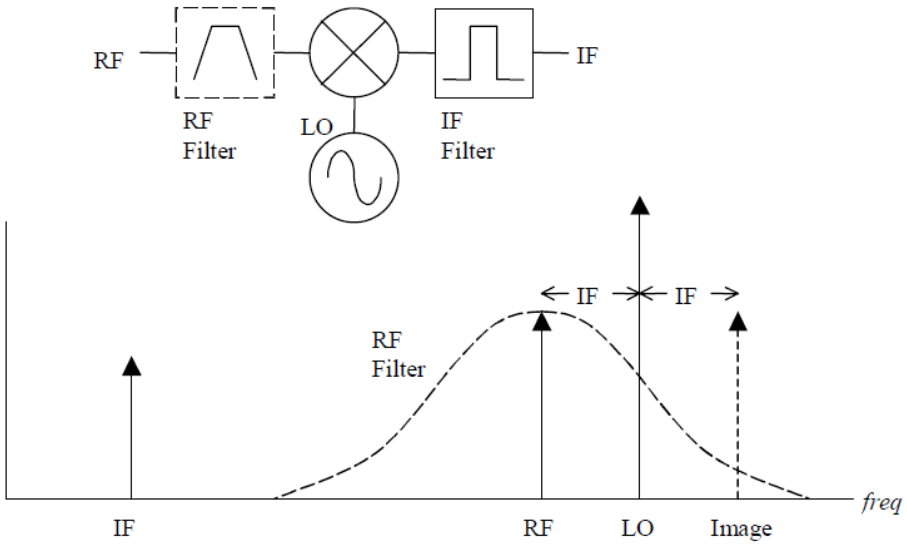


Figure 18: Intermediate Frequency conversion [59].

The Image Frequency is a strong interferer and therefore needs to be filtered before the mixer or in the mixer itself. In order to allow a proper filtering of the Image Frequency, it is desirable to choose

a high value for the IF frequency; this results in a larger separation between the Image Frequency and the RF frequency, what eases the filtering at the RF stage.
In railway environments, interference is normally caused by unintentional EMI sources, that is, equipment that have no radiation functionality and their interference corresponds to spurious emissions. Furthermore, radio systems used in railway such as ERTMS, CBTC, TETRA, etc. may also be an interference source. More information about interference sources in railway environments is provided in [58].

2.3.5.3 Techniques to reduce interference

There are several techniques to reduce interferences in wireless communication systems. They can be divided into direct and indirect methods [58]. In the following lines, some techniques regarding both methods are explained.

2.3.5.3.1 Direct Methods for Interference

Direct methods aim to mitigate interferences by adding specific functionalities (including hardware or software resources) into the system. It should be raised that direct methods work towards interference reduction rather than prevention.

Frequency Hopping

Frequency Hopping (FH) allows the system to perform a periodic change of the transmission frequency. This frequency variation takes places into a limited bandwidth and follows a pseudorandom pattern known to both transmitter and receiver. This interference mitigation technique is based on the principle that a narrowband interference is unlikely to cause interferences issues at a certain frequency and at the next frequency of the hop pattern. Then, by using this method, the spectrum of the transmitted signal is spread, which results in an improvement of the system's robustness against narrowband interferences.

Direct Sequence Spread Spectrum

By using Direct Sequence Spread Spectrum (DSSS) technique, the signal spectrum is spread prior to signal transmission (see Figure 19). This is accomplished by multiplying the data signal by a pseudo random spreading code. Both transmitter and receiver know the spreading code, and thus signal can be recovered in reception. As it was mentioned in the case of Frequency Hopping, by spreading the signal the robustness against narrowband interferences can be greatly improved.

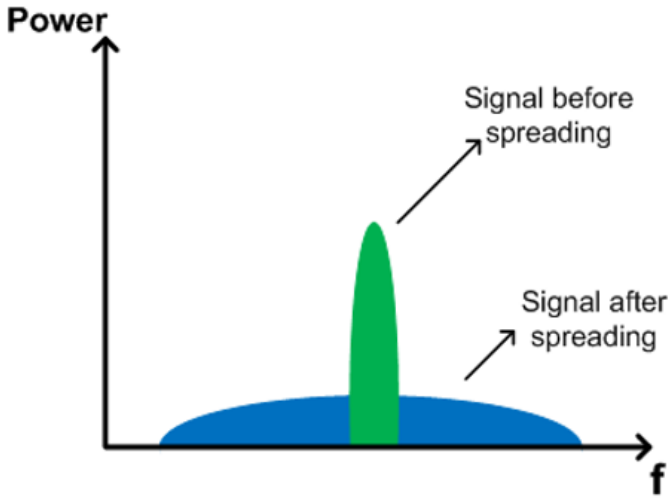


Figure 19: DSSS signal before and after spreading

2.3.5.3.2 Indirect Methods for Interference Reduction

Unlike direct techniques, the main purpose of indirect methods is to prevent the presence of interferences in the receiver by properly designing the architecture of the system.

Steered Beam Radiation Pattern

As mentioned in chapter 2.3.1, by using a proper antenna radiation pattern, multipath components can be effectively attenuated. The same applies to others sources of interferences. For instance, in cellular systems, interferences between adjacent cells, caused by users and base stations, can be significantly mitigated if the beams of antennas are steered towards the objective user/base station rather than using antennas with omnidirectional pattern. For illustrative purposes, a sketch comparing omnidirectional and beam-steered antennas in a cellular cell is shown in Figure 20.

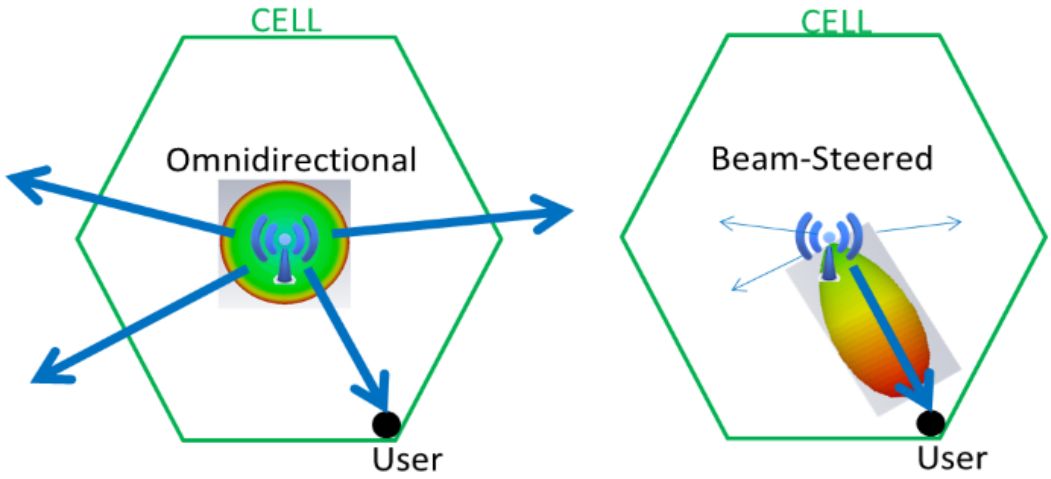


Figure 20: Omnidirectional vs beam-steered radiation pattern

Fractional Loading Factor

In cellular systems, the total amount of co-channel interference at a base station is directly related to the number of cells that are using the same channel as the cell of interest. At this point, the loading factor concept is introduced as the probability that a certain channel is in use within a cell. Essentially, the fractional loading factor technique consists in reducing the loading factor by restraining the number of channels that can be used simultaneously within a cell at the expense of decreasing the maximum cell's capacity.

Diversity

As it has been already mentioned, by using diversity techniques the system's performance can be greatly improved. Regarding interference mitigation, it has been shown that spatial filtering is possible, for example by using radiation pattern diversity. A more detailed explanation regarding diversity techniques can be found in section 2.3.1.

Dynamic Methods

Another group of methods, more sophisticated than the others are the Dynamic Methods, like Coordinated Multipoint in LTE (CoMP), where two or more base stations coordinate their transmissions to avoid interfering each other. There are many CoMP methods and some of them can also be static (S-ICIC) or dynamic (D-ICIC). For train communication systems this kind of technique is suitable for both inter-consist (i.e. consist-to-consist) and intra consist communications; in the first case each consist could have one base station (e.g. LTE), while in the

second case the base stations (or WiFi access points) could be located inside each vehicle of the consist.
From all these techniques to reduce interference, any of them can be applied in the context of a wireless train communication system. More specifically, inter-consist links are a suitable point-to-point scenario for directional antennas which reduce the impact of interferences with spatial filtering. In inter-consist scenarios most interferences will come from outdoor communication systems (e.g. LTE, TV, FM, etc), while in the intra consist scenario interferences will come from communication systems from the passengers (i.e. smartphones: WiFi, LTE,..). In both scenarios, the use of dedicated frequency bands for train communications will reduce the impact of interferences. However, this does not guarantee protection against malicious interferers; for this case, the use of narrow-beam directional antennas and frequency diversity with large separation between frequency bands are more effective options.

2.3.6 Quality of Service Parameters

In network architectures Quality of Service is defined commonly as the ability to provide mechanisms for carrying out each service with success in a common network medium.
In the definition of the architecture of the Wireless TCMS network, an overall performance should be required, or in other words, there should be some mechanisms to assure that each service or application has the required resources.
The definition of QoS was appearing in the computer network architecture while the required performance was increasing, in terms of acceptable time delay. This is faced mainly when the transferred data is related to voice or image, and a delay on the reception could lead to an invalid service of the network.
There is an effort of different standardization groups to define the QoS. The ITU-T (ITU Telecommunication Standardization Sector) defined in 1994 firstly and in the next years some recommendations to provide consistency of related standards. The IETF (Internet Engineering Task Force) also provided some Request for Comments (RFC) related to QoS with the aim of requesting discussion and suggestions for improvements.
In the train environment, the different provided services demand a QoS control to guarantee that each one is carried out correctly. For example, a highly demanding service like video streaming for CCTV should not interrupt a service related with safety functions if the same medium is shared for both services. Also real-time systems are used on-board, so these devices will be constantly sending or receiving data which sometimes exceeds their throughput rate.

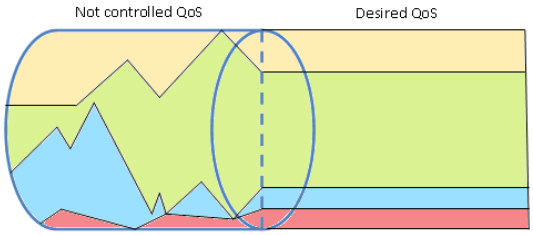


Figure 21: Difference between not controlled QoS network and controlled one

In the Figure 21, the difference between a controlled network and not controlled one is shown. The communication services that share a unique network are represented in different colours. On the one hand, the uncontrolled traffic demand could lead to a service interruption in the worst case, but in most cases provides not prioritized data rate for each function or service. Furthermore, safety functions could not be carried out without a QoS control, because there is no guarantee that a service interruption is not going to occur.
With a good QoS implementation, in the same medium, a broader data rate could be provided for video streaming for CCTV and smaller one for other less demanding services. This is the unique way to share a wireless network medium with the guarantee that all the services will be provided without an interruption due to an overflow in data rate demand.

2.3.6.1 Network performance parameters related to QoS

2.3.6.1.1 Data Rate

The data rate is the capacity of a network to transmit an amount of data in a certain portion of time. This capacity is expressed in multiples of bits per second.
Regarding the QoS, this capacity could be reduced drastically if all data streams access the network with the same priority. This is commonly referred as a low throughput. For this reason, a data rate management could be used to allocate a portion of it for each service or user of the network.
The data rate allocation could be defined statically, if the data rate for each stream could be predefined, or could be defined dynamically.

2.3.6.1.2 Latency (End to End Delay)

Latency is the term to refer the delay time for a packet when trying to reach the destination. The latency has three main different sources:

- Medium propagation time: This is the minimum latency needed for an electromagnetic signal to reach the destination.
- Intermediate node delay: A certain packet could reach the destination through an intermediate node, which routes the data and increases the overall latency.
- Queuing delay: Normally, the packets to be sent arrive faster than the transmitter capacity, so a queue should manage this situation. As the queue is growing, the latency increases, so it works like a buffer. If the maximum size of the buffer is reached, new packets will be dropped.

In the different Wireless TCMS applications, low latency requirements could be requested due to a real time communications in the train environment.

2.3.6.1.3 Jitter (Packet Delay Variation)

The Packet Delay Variation (PDV) is the deviation in the delay time for a certain data packet. This is also known as Jitter, and to measure it the lost packets are not taken into account.
The variations of the packet transfer delay or latency are typically produced by the buffering, because sometimes the queue is longer than usual.
The Jitter or PDV is not very problematic for TCP communications, because although some packets could reach the destination in different order, the receiver could rebuild the data. However, for audio or video streaming applications could be a problem, because a high delay variation could lead to a perceptible delays in the receiver and should require the implementation of larger buffers in the receiver part.

2.3.6.1.4 Error Rate

Error rate is the relation between the number of lost packets and the ones that have been sent. When a packet is lost, this should be retransmitted again to the receiver, and so introduces also a delay.
There are different error sources to consider lost packets:

- Data integrity errors detected by the receiver. This could be for example checksum error detection caused by interference, fading etc.
- Full queue error. This occurs when a buffer is full and no more data could be sent.

2.3.6.2 Mechanisms to achieve QoS

Once the network performance factors are known, some QoS mechanisms are going to be presented in this chapter. Is it important to keep in mind the OSI network model to understand where are applied the mechanisms or methods.

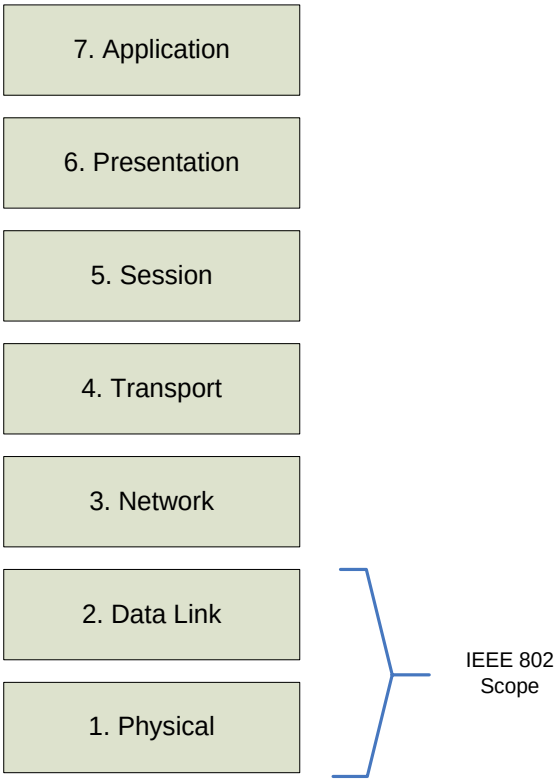


Figure 22: OSI network model

In this chapter the mechanisms are going to be divided in two groups, the mechanisms that can be applied in Data Link and Physical layers and the ones that are applied in Network and upper layers.
The main difference between the scope of Data Link layer and below and the Network layer and above is that a suitable technology selection could add a QoS support in the lower layers and so there wouldn't be necessary to apply so much effort in the upper layers. For example, the different standard extensions defined in 802.xx allow network traffic management to guarantee a QoS on this level.
On the other hand, a QoS implementation in upper layers will work with different technologies, and so, becomes in more generic solution regardless of the used transmission medium.
Anyway, some mechanisms could be applied in different layers and others are not related directly to an OSI Model layer.
The Figure 23 shows graphically a general approach to commonly used mechanisms to achieve QoS. Applications data packets are firstly identified by the classification mechanism and it assigns a specific priority or class. Depending on the class or priority of the data packet it will be added to a specific queue. Finally, the data packet scheduler transmits the data with a certain criteria depending on its type.

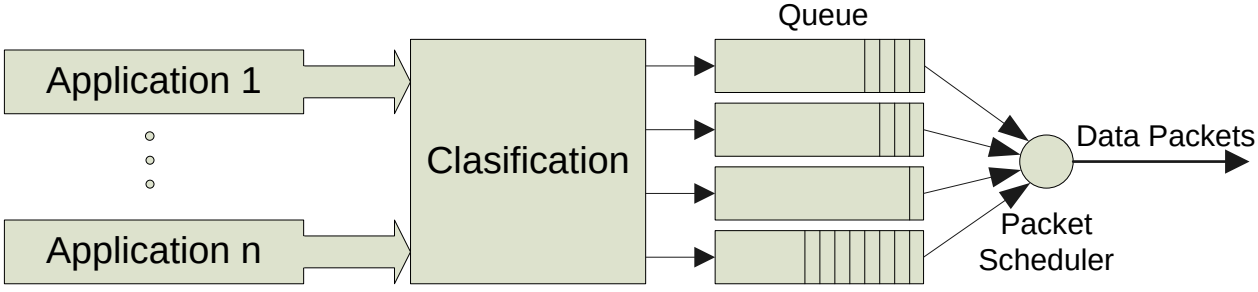


Figure 23: Data packet general classification design

2.3.6.2.1 Data Link Layer

For example, there are standards that implements QoS methods at Data Link layer, like 802.16 (WiMAX) or 802.11e (correction of WLAN). These standards implement some improvements at MAC level (OSI Layer 2) that allow a QoS. If the used technology or transmission medium takes into account the QoS, these methods won't be necessary and only the higher level ones (if needed) could be used.

Channel Access Method:

In a wireless network medium, a common communication channel is shared between multiple users or applications. If more than one application tries to send data through the channel, collisions could happen. Consequently, the wireless network needs a channel access method to avoid collisions and guarantee that all the data packets are sent.
There are multiple types of channel access methods that avoid the collisions in a certain channel, and they are based on multiplexing scheme:

- Frequency Division Multiple Access (FDMA): It uses different frequency bands for each data stream. Used 1G or 4G (OFDMA) for example.
- Time Division Multiple Access (TDMA): It uses differenced time slots for each transmitter. Is used for example in 2G.
- Code Division Multiple Access (CDMA)/Spread Spectrum Multiple Access (SSMA): It employs a spread-spectrum technology and special coding scheme to enable a number of transmitters to send data through the same channel. It is used in 3G for example.
- Space Division Multiple Access (SDMA): It uses directional antennas to send data to different physical areas.

Packet Scheduling:

This method selects a packet to send from the packets waiting in the queue. It decides which packet from which queue are scheduled for transmission in a certain period of time (see Figure 23).

- **FIFO (First Input First Output):** This data packet scheduling technique is the simplest one. The data is introduced from the top of the queue and released from the bottom (see Figure 24.

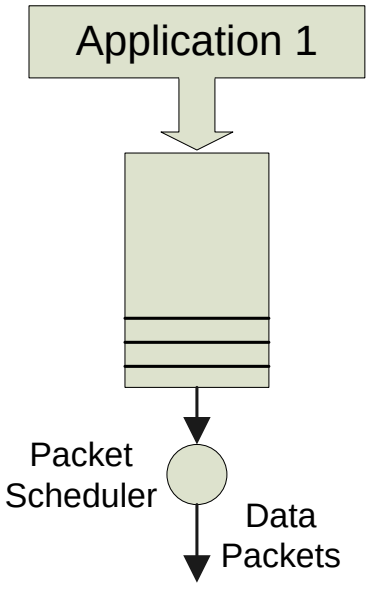


Figure 24: FIFO packet scheduling method

The FIFO queuing method provides what is known as best effort service. This means that all the services or applications will have the same priority and latency, and so if a certain service requests higher data rate, the others will suffer a data rate decrease and latency increase.

- **Priority Queuing:** The priority queuing scheme uses multiple queues and there is a priority assignment for each one (see Figure 25).

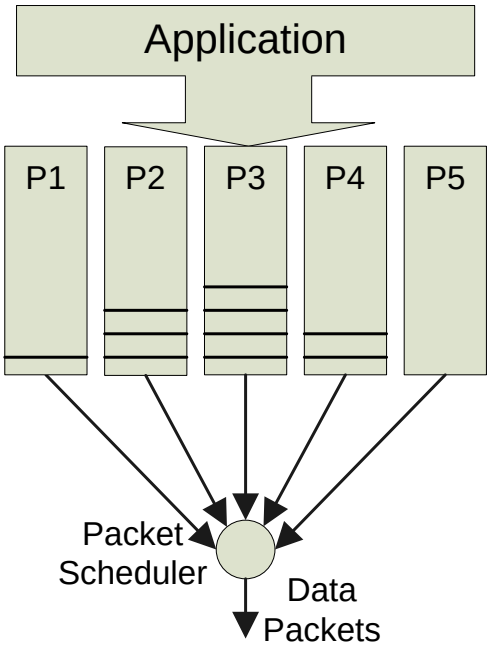


Figure 25: Priority queuing scheduling method

In this case the services or applications fill the queues depending on the priority. The higher priority queue (P1 in Figure 25) packets are transmitted first, and then, the lower priority ones (P2, P3 and so on). The lowest priority queue packets will be transmitted only when the rest of queues is already empty. Each queue also could be identified with a “class” instead of a priority. This concept is more general, and also is used in priority queuing. A class could be related to a priority and/or data source identifier.
This method enables a higher data rate and lower latencies for high priority queues and lower data rate and higher latencies for the lower priority ones.

Traffic Policing

Traffic policing is referred to monitoring connection traffic and comparing the activity levels against pre-defined thresholds (policies). Traffic policing typically results in packet loss on the receiving side as messages gets dropped when the sender exceeds policy limits. When the exceeded data is buffered instead of dropped and sent when possible, traffic shaping is used.
The Traffic Policing mechanism is typically implemented with the token bucket algorithm (see Figure 26).

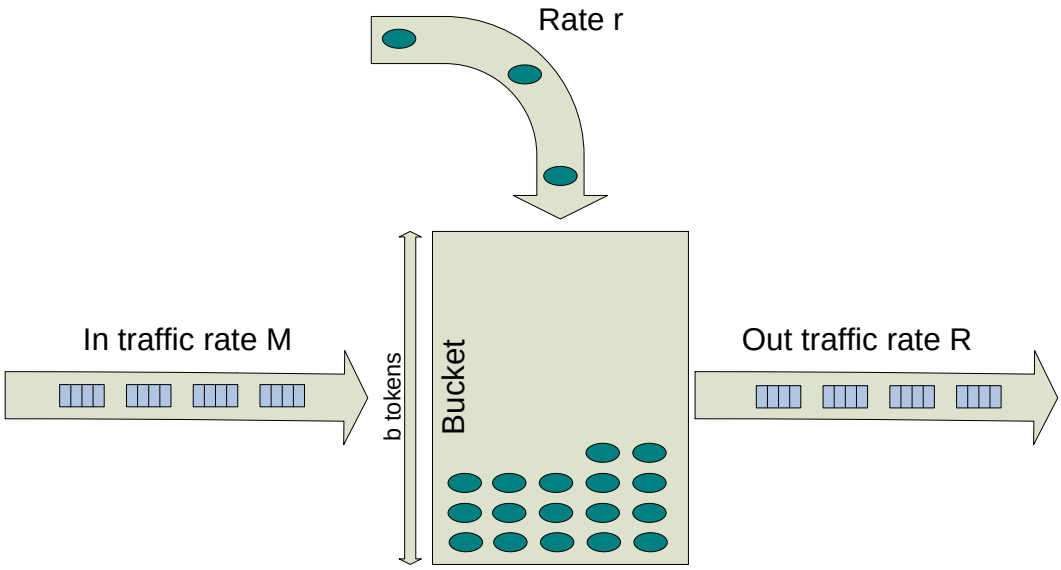


Figure 26: Token bucket algorithm

In this algorithm, an analogy of a token bucket is used. This bucket has a size of b bytes and is filled with tokens at rate *r*. When a new packet arrives, it retrieves a token from the bucket (if not empty) and the packet is sent to the outgoing traffic stream. If there are enough tokens the outgoing rate (*R*) will be the same as the incoming rate (*M*). If the incoming traffic rate is greater than *r,* the outgoing traffic rate will be the same (*M*), but the bucket will start to decrease its token level. Once the bucket is empty the output rate will be limited to *r*.

2.3.6.2.2 Network Layer

Classification

At Network layer and above, there are multiple data packet classification methods. In this chapter a method per each layer will be presented.

- **Network layer classification**
  In the third layer of OSI Model, the header could be used to classify the data packets. The IPv4 and IPv6 standards define a priority field that could specify a datagram's precedence and request a route for low-delay and high-throughput.
  In the case of IPv4, this field is composed by 6 bits for DSCP (Differentiated Services Code Point), where up to 64 classifications could be done.
  In IPv6, a Traffic Class field is defined and it is 8 bit wide. This enables a wider classification possibility than the previous version of the internet protocol.
- **Transport layer classification**
  For transport layer, a classification based on the 5 tuples (source address, destination address, source port, destination port, and the transport protocol) can be implemented. It provides the maximum granularity due to the number of fields to identify the packet. If the data packets pass through a firewall that uses Network Address Translation, the original IP address will be hidden, and so, the packet identification will differ from the expected one.
- **Application or user classification**
  In this case, the field user/application identification (ID) could be used. This identifier could be pre-assigned, or could be dynamically set when a central node allows joining a new session to a user. All the packets from this user will have this unique identifier.

Admission Control

If different users or services are joining the same network dynamically, an admission control mechanism can be implemented. When a new session is going to be accommodated the QoS parameters should not be affected, if there is not enough resources available, the admission control mechanism will reject the new session until the parameters guarantee that the required QoS could be guaranteed.
The admission control mechanism could be implemented in different locations. If Wireless Train Backbone architecture is used with Wireless Train Backbone Nodes for each consist network, this mechanism should be implemented in each train backbone node (WLTBN) as shown in Figure 27.

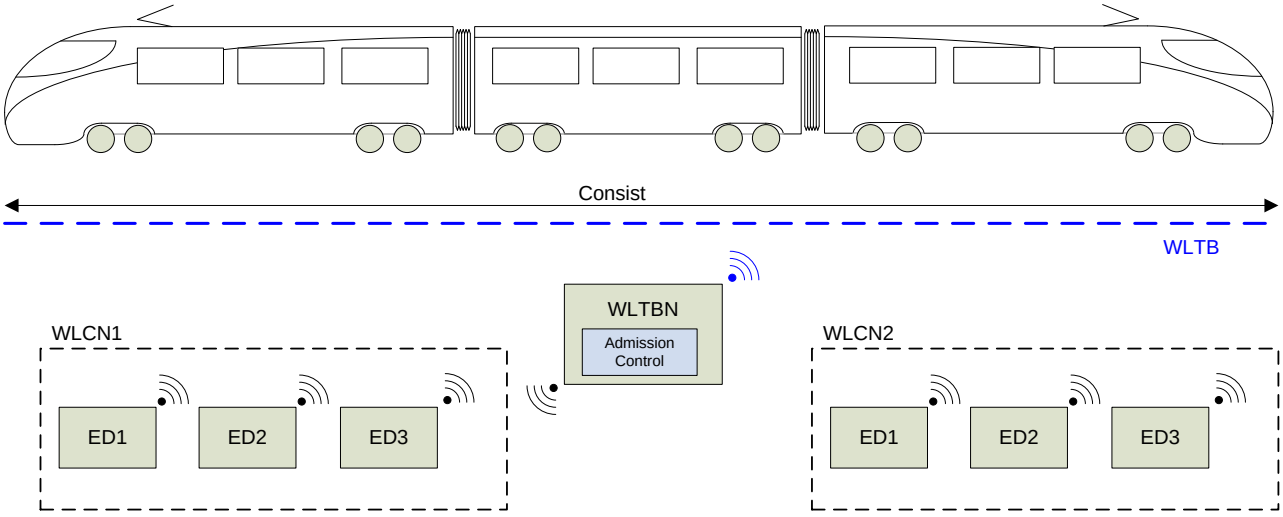


Figure 27: Wireless train network architecture devices

Over-provisioning

In the train environment sometimes the traffic load could be estimated in advance. This means that the traffic needed per service or application is well defined and is quantifiable.
In this kind of environment, a method of QoS is to over-provision the network so that capacity is based on peak traffic estimates.
One problem in that solution is that the cost of the infrastructure will be higher due to a higher data rate needed, but the implementation of QoS mechanisms could be expensive also. In general if not high data rate is needed, this could be a better solution than adding QoS mechanisms in other levels.

Multipath Routing

In the Transport Layer (OSI Model 4th layer) there is an option of use Multipath TCP (MPTCP). This is an effort towards enabling the simultaneous use of several IP-addresses/interfaces by a modification of TCP that presents a regular TCP interface to applications, while in fact spreading data across several sub-flows. Benefits of this include better resource utilization, better throughput and smoother reaction on failures. This protocol was implemented firstly in the Linux Kernel in 2013, but some additional implementations have been added for FreeBSP or Android for example.

2.3.6.2.3 Resource Reservation

The mechanisms presented provides QoS at a device level. In a Wireless TCMS network the coordination between the devices is vital to achieve a complete QoS. The resource reservation mechanisms allow the network to share the information about the needed traffic by an application along the devices in the end-to-end path through the network. So, if every device can reserve the necessary data rate, the application can begin transmitting.
Resource Reservation Protocol (RSVP) is a well-known resource reservation signalling mechanism. RSVP operates on top of IP, in the transport layer, so it is compatible with the current TCP/IP based mechanisms (i.e., IPv4, IP routing protocol, and IP multicast mechanism) and can run across multiple networks. RSVP's main functionality is to exchange QoS requirement information among the source host, the destination host, and intermediate devices. Using this information, each network device will reserve the proper resources and configure its traffic handling mechanisms in order to provide the required QoS service. Once the reservation process is complete, the sender host is allowed to transmit data with an agreed traffic profile. If a device or network element on the communication path does not have enough resources to accommodate the traffic, the network element will notify the application that the network cannot support this QoS requirement.

2.3.6.3 Architectural Basic Concepts Related to QoS

Perhaps this chapter should not be included 2.3.6 (Quality of Service Parameters) as indicated in the aim of the document but it could be helpful for chapter 2.4 (Basic architecture concepts)

2.3.6.3.1 Types of Architectures

Depending of the network types we are referring to, different architectures for QoS could be presented. First centralized networks will be taken into account, and then the ad hoc or decentralized network will be considered for an architecture presentation.

2.3.6.3.2 Infrastructure Network

In centralized networks, there is a central node which implements the admission control of the network. In Figure 28 two types of devices are shown, one is the Central Node, and the other one is the End Host. The central node regulates the communications, and so all the data from a source is received first by the central node and then sent to the destination. Due to this architecture, the admission control of the network is implemented there (centralized), but the traffic handling and packet scheduling is included in all the devices. In blue the resource reservation flow is shown, which is shared by all the devices.

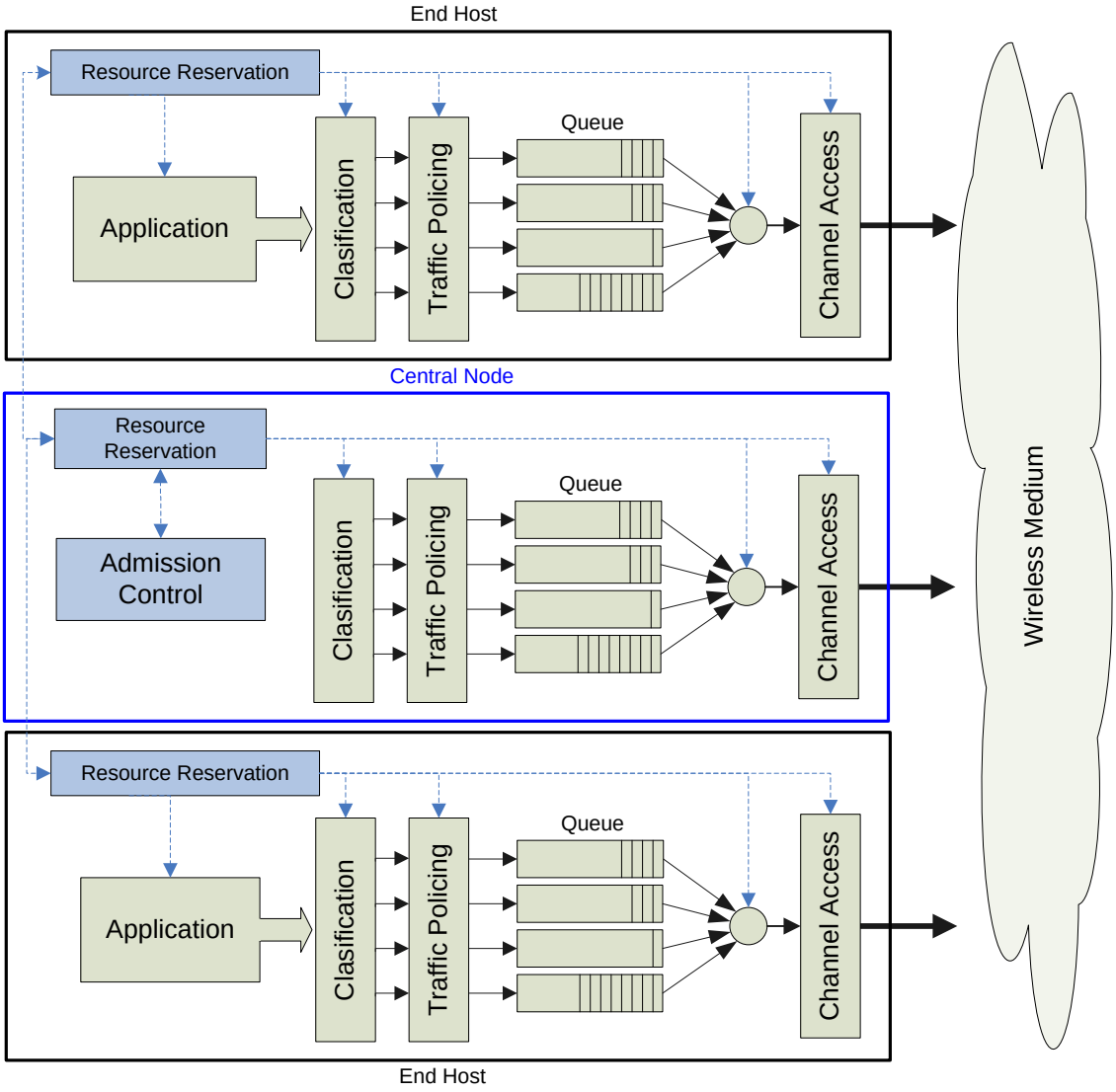


Figure 28: QoS Architecture of an Infrastructure Wireless Network

2.3.6.3.3 Ad hoc Network

In an ad hoc network all the devices participate in routing by forwarding data for others, so the mechanisms of classification, traffic policing or packet scheduling resides in all of them. Anyway, one of the network hosts should be selected to have the role of admission controller (see Figure 29). A network with an admission controller typically is called “multi hop ad hoc network”.

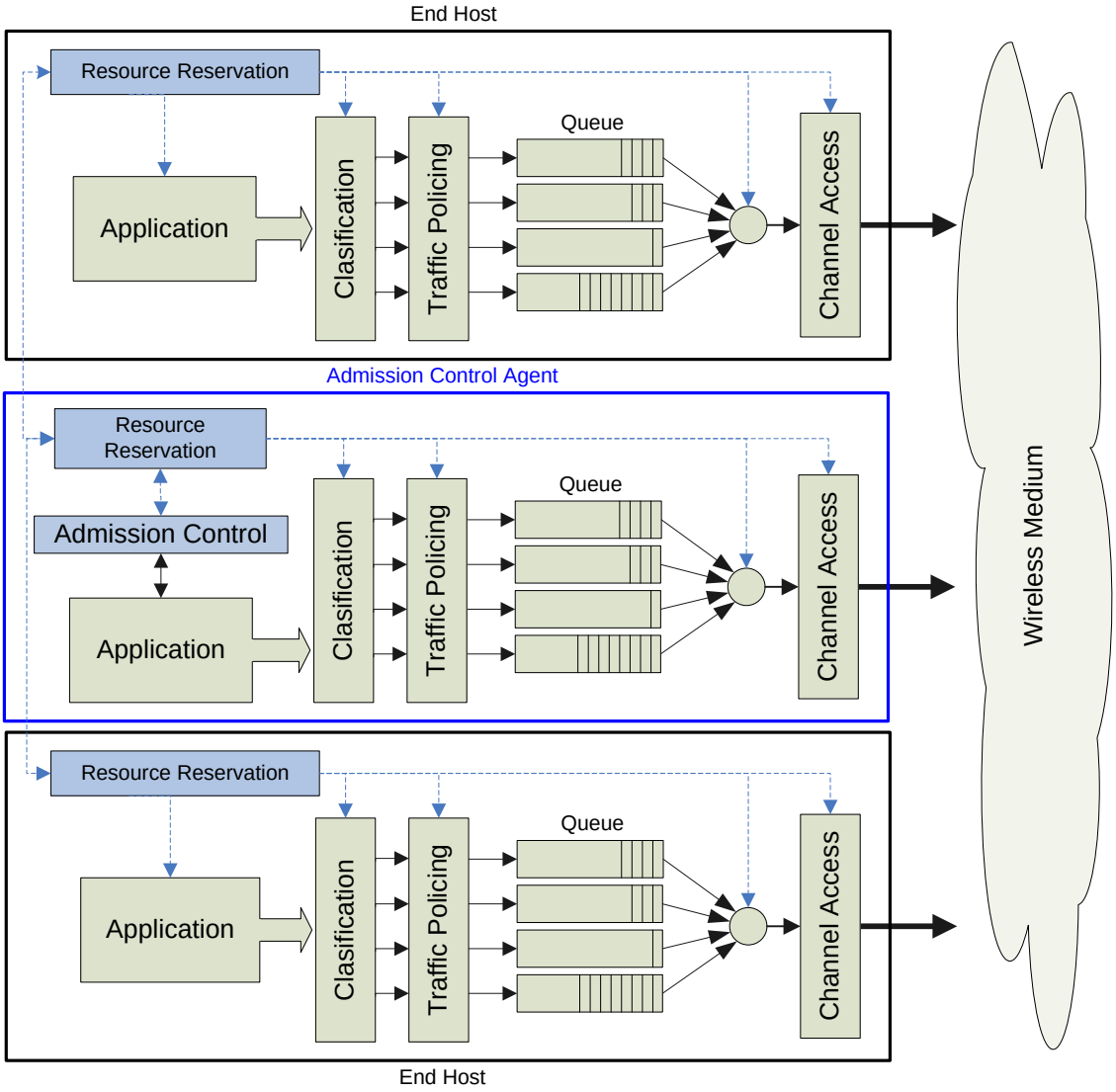


Figure 29: QoS Architecture of an Ad hoc Wireless Network

2.3.6.4 QOS RELATED TO TECHNOLOGY SELECTION

Depending on the technology selection for each function domain different QoS capabilities are provided by the standards.
Two technologies are selected to focus on the analysis of the QoS support, WiFi and LTE. Other technologies are discarded due to the low probability of selecting them for the wireless TCMS network (backbone or consist communications).
In principle, 802.11 was not oriented to the QoS, but as it will be mentioned, an amendment was introduced to support QoS communication. On the other hand, LTE took into account the QoS from its beginning, and so, it is better oriented to QoS.

2.3.6.4.1 QOS vs. WI-FI (802.11e)

In general, standard 802.11 does not have a QoS support. But in 2005 a new approved amendment was introduced, the 802.11e. It is focused in delay-sensitive applications, such as Voice over Wireless LAN and streaming multimedia
802.11e is a proposed enhancement to the 802.11a and 802.11b wireless LAN (WLAN) specifications. It offers quality of service (QoS) features, including the prioritization of data, voice, and video transmissions. The 802.11a, 802.11b, and 802.11e standards are elements of the 802.11 family of specifications for wireless local area networks (wireless LANs or WLANs).
802.11e enhances the 802.11 Media Access Control layer (MAC layer) with a coordinated time division multiple access (TDMA) construct, and adds error-correcting mechanisms for delay-sensitive applications such as voice and video.
There are two methods to address the QoS in the MAC level, the Enhanced Distribution Channel Access (EDCA) and the HCF (Hybrid Coordinated Function) Controlled Channel Access (HCCA).

EDCA

On the one hand, the improvement on the MAC protocol is achieved with the Enhanced Distribution Channel Access (EDCA). It defines eight priority levels, enabled by four transmit queues. This method is explained in the chapter 2.3.6.2.1.
Each queue provides frames to an independent channel access function, each of which implements the EDCA contention algorithm. When frames are available in multiple transmit queues, contention for the medium occurs both internally and externally, based on the same coordination function, so that the internal scheduling resembles the external scheduling.

HCCA

The HCCA, uses a Hybrid Coordinator (HC), who controls the access to the medium. The HC has privileged access to the medium because it can initiate a transmission after waiting a shorter time than the shortest backoff delay of any station using EDCA. Under control of the HC, a nearly continuous sequence of frame exchanges can be maintained, with short, fixed delays between frames. The inter-frame delay does not increase with increasing traffic, unlike the contention window used in EDCA access.
Every station sends a Reservation Request frame to request medium from the HC, then it gives access to the medium to send packets during a time defined by the HC.
There is no possibility of collisions, except from stations on the same frequency that are not under control of the HC. HCCA supports parameterized QoS, where specific QoS flows from applications can have individually tailored QoS parameters, and tighter control of latency and scheduling.

2.3.6.4.2 QOS vs. LTE

The LTE introduces a relatively simple QoS concept consisting of different traffic classes and some QoS attributes to define traffic characteristics of the traffic classes.
Providing end-to-end QoS requires mechanisms in both the control plane and the user plane (see Figure 30). Control plane mechanisms are needed to allow the users and the network to negotiate and agree on the required QoS specifications, identify which users and applications are entitled to what type of QoS, and let the network appropriately allocate resources to each service. User plane mechanisms are required to enforce the agreed-on QoS requirements by controlling the amount of network resources that each application/user can consume.

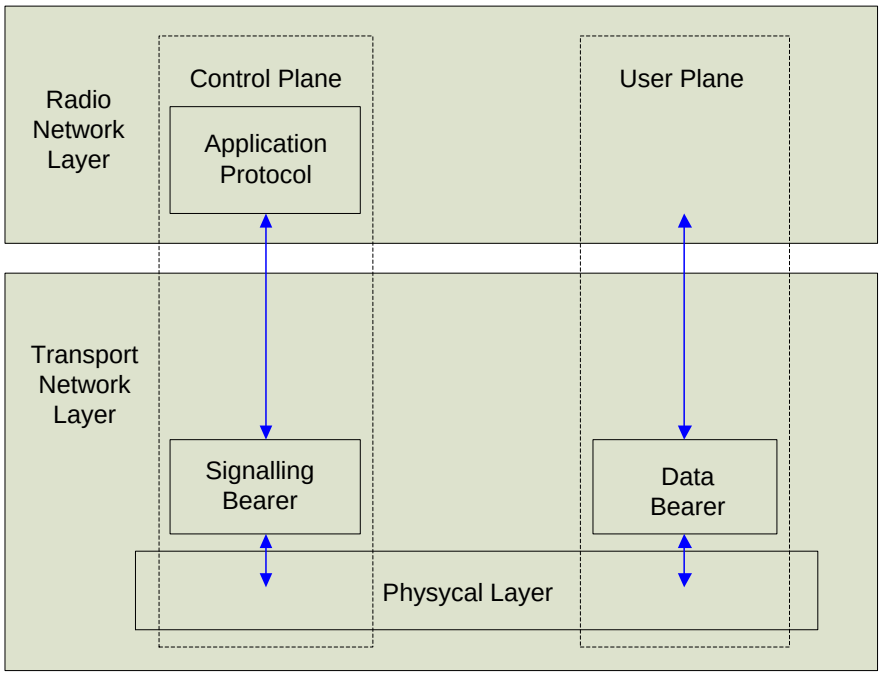


Figure 30: LTE protocol architecture

QoS Class Identifier (QCI)

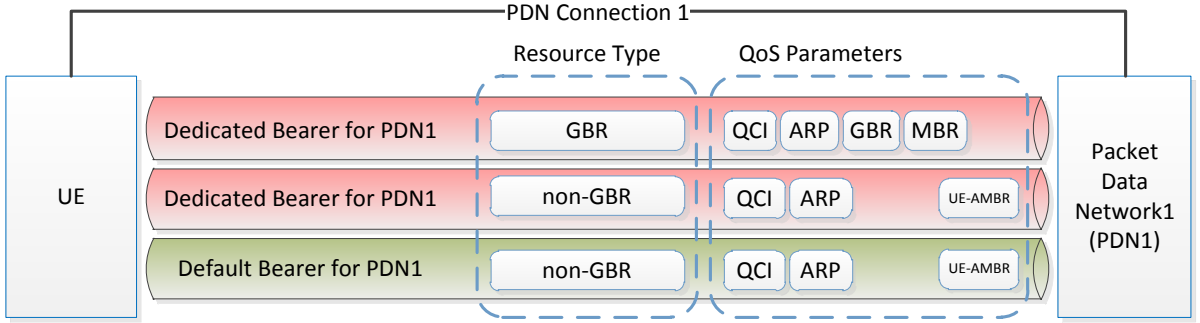
QCI is an identifier defining the quality of packet communication provided by LTE. It is associated to different parameters like:

- Guaranteed Bit Rate (GBR)
- Non-Guaranteed Bit Rate (non-GBR)
- Priority Handling
- Packet Delay Budget
- Packet Error Loss rate

In general, there are 9 different levels of QCI (1-9), but 4 additional levels where added for Mission Critical Communications (65, 66, 69 and 70).

Default and Dedicated Bearers

There are different types of bearers, and each one has associated its own properties. Bearer in a fixed broadband LTE network is similar to a virtual traffic management concept.



ARP: Allocation and Retention Priority

QCI: QoS Class Identifier

UE-AMBR: User Equipment - Aggregated maximum Bit Rate

Figure 31: Bearers used for QoS in LTE

One is the dedicated bearer and the other one is the default bearer. The dedicated bearer is always established when there is a need to provide QoS to specific service (like VoIP). Dedicated bearer can be subdivided into Non-GBR and GBR types.
GBR provides guaranteed bit rate and is associated with parameters like GBR and MBR

- GBR: The minimum guaranteed bit rate per EPS bearer. Specified independently for uplink and downlink.
- MBR: The maximum guaranteed bit rate per EPS bearer. Specified independently for uplink and downlink.

On the other hand, Non-GBR bearer does not provide guaranteed bit rate and has parameter like A- AMBR and UE- AMBR

- A-AMBR: APN Aggregate maximum bit rate is the maximum allowed total non-GBR throughput to specific APN. It is specified interdependently for uplink and downlink.
- UE -AMBR: UE Aggregate maximum bit rate is the maximum allowed total non-GBR throughput among all APN to a specific UE.

Like shown in Figure 31, default bearer can only be non-GBR type.

2.3.7 Power consumption of wireless devices

The power consumption of the wireless devices shall be consistent with the typical global requirements of passengers' safety. An example is given by the requirement of the TSI LOC&PAS (Technical Specification for Interoperability) clause 4.2.10.4.1, Emergency lighting: " for units of maximum design speed higher than or equal to 250 km/h, during a minimum operating time of three hours after the main energy supply has failed, [...] for units of maximum design speed lower than 250 km/h, during a minimum operating time of 90 minutes after the main energy supply has failed."
Note: "TSI LOC&PAS" stands for "COMMISSION REGULATION (EU) No 1302/2014 of 18 November 2014 concerning a technical specification for interoperability relating to the 'rolling stock — locomotives and passenger rolling stock' subsystem of the rail system in the European Union"
Depending on the architecture of the wireless links, a strategy may be adopted to lower the global consumption of the wireless devices in order to fulfil this requirement.
The devices shall fulfil the requirements of the EN 50155 especially relatively to their alimentation and consumption, and to the temperature range defined in Class Tx of its Table 1.

2.3.8 Size and location of wireless devices

The wireless devices maximum size and weight must be compliant with the usual maximum definitions of electronic devices:

- Maximum dimensions (h x l x p): 6U (3U recommended) x 482,6 mm (19 in.) x 220 mm. NB: 1U = 44,45 mm.
- Maximum weight: 15 kg.

The mounting of the devices shall fulfil the EN 50155, especially for fixing performances (EN 50155, 9.2.2), that may impact on maintenance employees or passengers' safety in case of train collision.
The preferred location for the devices shall be closed compartment inaccessible for unauthorised personal, in order to prevent any interference by passengers (e.g. protection against unwanted access to the system, and protection against electric hazard).
The location of wireless devices shall guarantee maintenance employees and passengers against any electrical shock or hazard while operating. In particular, the device shall be properly earthed. The reference for device earthing and protection against electrical hazards is the EN 50153.
The location and the fixing of the wireless device shall insure its resistance to rolling stock shock and vibration environment, as defined in EN 61373.

2.3.9 Regulations (exposition to radiation)

Exposition to electromagnetic radiation can be quantified as Specific Absorption Rate *(SAR)* and field exposure levels. SAR, expressed in watts per kilogram of tissue, quantifies the rate of energy absorption in the human body [49]; it takes into account only the absorption of the RF signal, and therefore does not consider non-thermal effects [50]. On the other hand, exposure levels refer to electric field, magnetic field, or power carried by a plane wave, measured in the absence of the person.
A reference document for exposition limits in Europe is the Council Recommendation of 12 July 1999 on the limitation of exposure of the general public to electromagnetic fields (0Hz to 300 GHz) - (1999/519/EC) [51]. This Recommendation is based on the guidelines of the International Commission for Non-Ionizing Radiation Protection (ICNIRP), and provides a EU framework for national policies and measures and for EU legislation and standards on EMF exposure.

2.3.9.1 Specific Absorption Rate (SAR):

The properties of the human body are mainly electrical, as the body is composed of water, electrolytes, and complex molecules with large net dipole moments. Therefore, its content of magnetic materials is not relevant. This means that human body will absorb energy from the electric field, and this is why only the electric field inside the body is considered to evaluate the exposure in the near field of RF sources.
By definition, the power absorbed per unit volume is obtained multiplying the current density ($\vec{J}$) by the conjugate of the electric field in the tissue ($\vec{E}^*$) [52]:

$$P_v = \frac{1}{2}\vec{J} \cdot \vec{E}^* \quad (W/m^3) \tag{4.13}$$

Using the effective conductivity of the tissue (σ):

$$P_v = \frac{1}{2}\sigma\left|\vec{E}\right|^2 \quad (W/m^3) \tag{4.14}$$

Therefore, the power absorbed per unit mass (i.e. SAR) is obtained from the previous expression introducing the density of the tissue (ρ, in kg/m3):

$$P_g = \mathrm{SAR} = \frac{\sigma}{2\rho}\left|\vec{E}\right|^2 \quad (W/kg) \tag{4.15}$$

Regarding SAR limits, there is no global regulation. For example, European SAR limits are based on [53] and establish a maximum SAR of 2W/Kg averaged on a 10-g volume, while USA limits are based on [54] and establish a maximum SAR of 1.6W/Kg averaged on a 1-g volume. Some worldwide SAR regulations are summarized in Table 4.

Table 4: SAR limits [49]

	Australia	Europe	USA	Japan	Taiwan	China
Measurement method	ASA ARPANSA	(ICNIRP) EN50360	ANSI C95.1b:2004	TTC/MPTC ARIB		
Whole body	0.08 W/kg	0.08 W/kg	0.08 W/kg	0.04 W/kg	0.08 W/kg	
Spatial peak	2 W/kg	2.0 W/kg	1.6 W/kg	2 W/kg	1.6 W/kg	1 W/kg
Averaged over	10 g cube	10 g cube	1 g cube	10 g cube	1 g cube	10 g
Averaged for	6 min	6 min	30 min	6 min	30 min	

SAR can be measured directly using body phantoms (either solid or liquid), or it can be obtained through electromagnetic simulation. In order to homogenize SAR measurements, a standard phantom head with homogeneous tissue properties called Specific Anthropomorphic Mannequin (SAM) has been defined, along with standard calibration and measurement protocols [55]. The two main methods for SAR evaluation are the E-field method [65] and the thermographic method [56]. Regarding simulations, available EM simulation packages provide SAR values, although measurements are still necessary for certification. A simulation standard for SAR certification is currently under development.

2.3.9.2 Exposure levels

In Table 5 exposure limits for electric field, magnetic flux density and power density are summarized for the frequency range of 2 GHz – 300 GHz.

Table 5: Electric and magnetic field exposure limits in the frequency range of 2 – 300 GHz [64]

Frequency range	E-field strength [V/m] (RMS)	H-field strength [A/m] (RMS)	B-field (μT)	Equivalent plane wave power density (W/m^2)
2 ≤ f ≤ 300 GHz	61	0.16	0.20	10

2.3.10 Availability (Redundancy)

The train communication system is essential for the train operation. Especially the train backbone communication needs to be highly reliable, because it is needed for the execution of train wide functions, which in case of a failure leads to a non-operational train. The demand of consist network reliability may depend on the vehicle class e.g. leading vehicle, traction vehicle or coach. In case a consist fails, e.g. consist is unpowered, it could be tolerable if it is a coach which may be not important for keep the train operable. In this case it has to be ensured that the failed consist does not interrupt the train backbone communication to the other consists.
Independent from the communication technology end devices connected to the consist network need to communicate via the consist network, the train backbone node, and the train backbone to other end devices in other consist (see Figure 32).

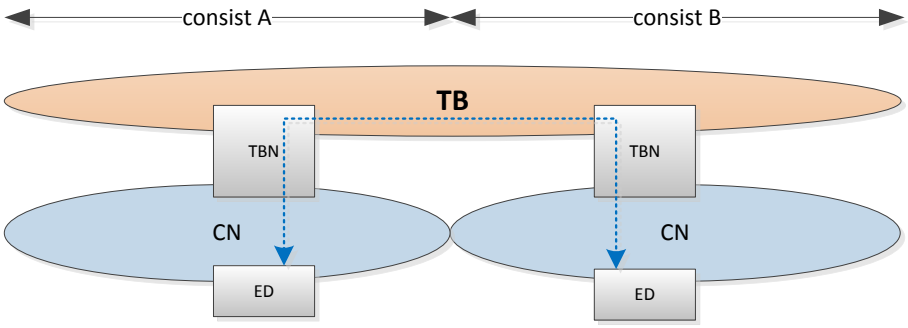


Figure 32: End device to end device communication via train backbone

Availability is usually calculated using commonly known formulas for mean time between failures (MTBF) and mean time to repair (MTTR).
MTBF is predicted time between failures of a system during operation; MTBF can be calculated as the arithmetic average time between failures of a system. The MTBF considers failures which place the system out of service and assumes that the failed system is immediately repaired.

Actions like scheduled maintenance are not considered within the definition of failure. Equipment vendors provide MTBF values for equipment and hardware modules.
MTTR is the time taken to repair a failed system. Systems may recover from failures automatically or by manual repair. With dynamic recovery (e.g. with dynamic routing around link or node failures), MTTR depends on the time needed for detection and for the actual recovery or traffic via the new path.
As mentioned in the deliverable of D2.4 [83], availability (A) is calculated from the MTBF and MTTR in following manner:

$$A = \frac{\mathrm{MTBF}}{\mathrm{MTBF} + \mathrm{MTTR}}$$

A typical way to improve the availability is to use redundancy of the network nodes, this leads to a better failure rate (MTBF) and so to a better value of A.
The further description is focused on the train communication infrastructure and does not consider the availability of the end devices. Since LTE for the train backbone and WLAN for the consist network has been identified as suitable technologies, the reliability of LTE train backbone node and WLAN routers will be analysed in more details.
To ensure continuous, reliable and efficient operation of the communication system, the wireless TCMS could set strict requirements regarding the availability of the communication system. These requirements are not necessarily supported by regular commercial mobile networks (see [83] for details).

2.3.10.1 Availability of Wireless Train Backbone Communication

Network resilience should be based on high-availability and redundancy solutions on multiple layers. Most resilience features needed in the train communication network are commonly available from LTE manufacturers. However, commercial LTE networks may not implement resilience fully to fulfil all Wireless TCMS requirements. Most network elements have high-availability designs, for example, to recover from hardware failures. Pooling of elements and load balancing between core elements improves system reliability and guarantees network service availability, even if a single node fails.
Centralized functions like management systems and core network elements (EPC, see chapter 3 Figure 47) are usually located in at least two separated places (e.g. consists). Connectivity between sites and network elements supports resilience against link and node failures.
In the backbone two main different types of LTE elements must be distinguished: UE and eNodeB

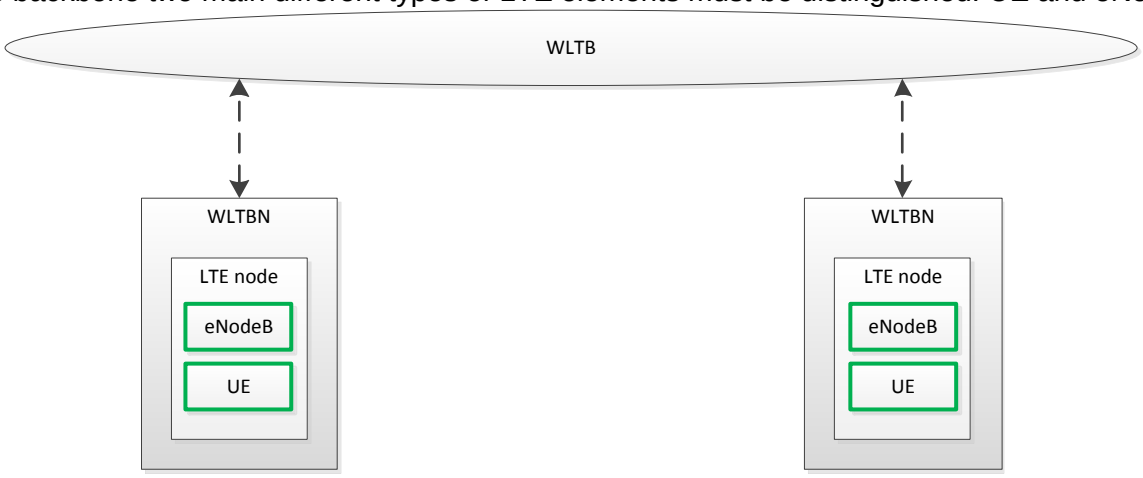


Figure 33: Backbone architecture network elements (WLTBN)

The WLTBN connects the backbone network with the consist one, and lets the different EDs to exchange the information between them, even if they are located in different consists.
These network elements are composed by different devices. On the one hand the eNodeB is the element which gives connection to the different UEs and enables the inauguration process of the

different consists in a train. In this case, it shall comprise also the EPC (Evolved Packet Core) of the LTE network.
The UE is the element that contains the information obtained from the EDs regarding the neighbour consist identifiers (using an RFID interface).
In principle, one eNodeB is sufficient to achieve the overall backbone communication, taken the advantage of the coverage range (more than 2 kilometres), and the connection capability to all the UEs present in this area. But for inauguration purposes, every consist needs to have one WLTBN, and therefore, one eNodeB on it.
Also, one UE per consist could give the possibility to inaugurate the train (and to enable the backbone communication), as mentioned before, sending the neighbour consist identifiers to the eNodeB.

2.3.10.1.1 Redundant Train Backbone Nodes

To analyse the need of redundancy, it is important to have (as it is mentioned in chapter 2.3.10) the MTBF values for each equipment used as a network nodes in the backbone. This could determine which kind of redundancy is necessary in each case.
As a first proposal, two kinds of redundancies are proposed, one for UE and the other one for eNodeB.

2.3.10.1.1.1 Redundant UE

On the Figure 34, two UEs are used to obtain the information from the backbone. This gives an improved availability giving an UE fault tolerant architecture.
The information from the ED with the neighbour consist identifier is received by two different UE. Only one could be active and the other one can start communicating if a UE fault is detected.

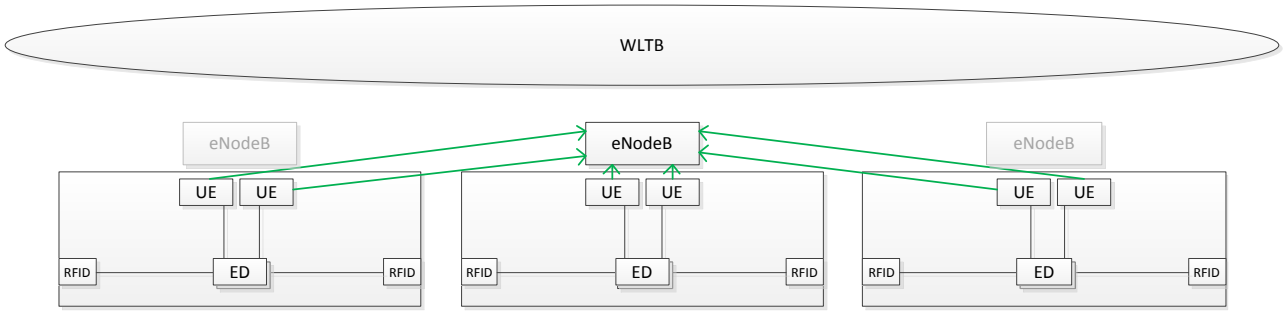


Figure 34: Redundant UE

2.3.10.1.1.2 Redundant eNodeB

On the other hand, an additional eNodeB could be provided per consist. It gives an availability improvement if an eNodeB is not available.

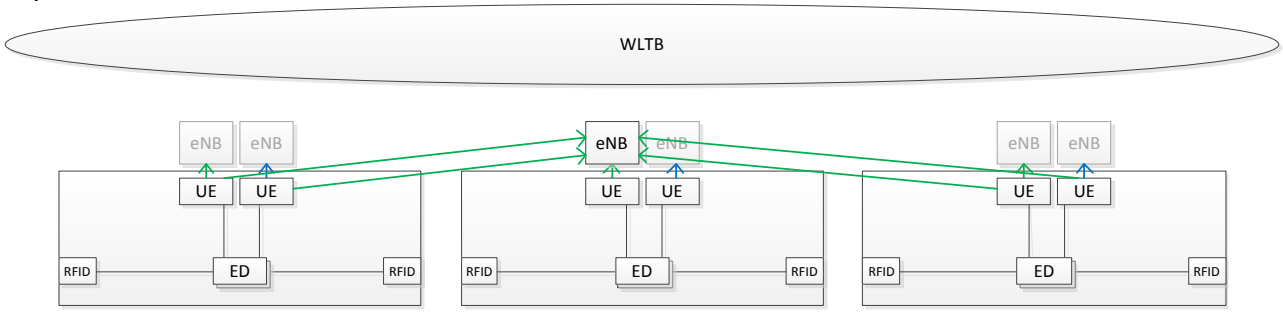


Figure 35: Redundant eNodeB

2.3.10.2 Availability of Wireless Consist Network Communication

The WLCN infrastructure consists of several devices as shown in Figure 36: routers, gateways which in this case are the UE of the WLTBN, wireless access points (AP), and relay stations (RS). As already stated above the further availability description is focussed on the wireless communication infrastructure and does not consider the wireless end devices. Each highly reliable end device needs to have two independent wireless access adapters or a second complete end device for redundancy implemented in the consist.

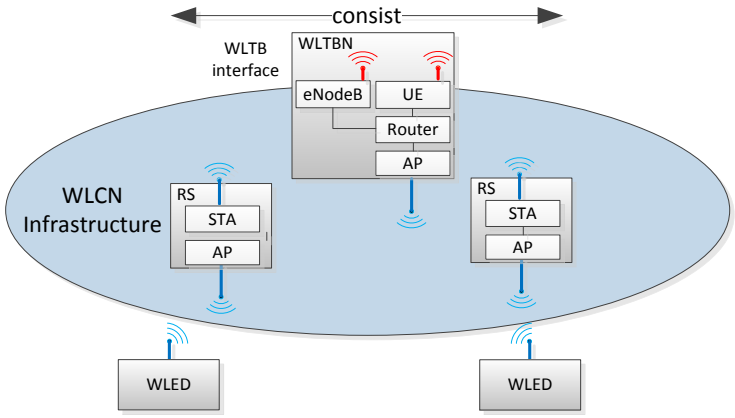


Figure 36: Communication infrastructure of the WLCN

Compared to wired communication channels the wireless communication channels have a higher error frame rate. But considering retransmission of the MAC the error frame rate of wired and wireless communication are comparable (see for [87] and [88] details). As a consequence the availability of the WLCN infrastructure depends mainly on the devices of wireless infrastructure.

2.3.10.2.1 Redundant aspects of the WLCN

In order to improve the availability redundant devices for the wireless communication infrastructure can be applied. This can be archived by using redundant wireless routers and access point but as well by choosing locations for the access points which enables end devices to connect to a second redundant access point in case one access point fails. In Figure 37 the WLED is able to communicate via RS1 or RS2 to other WLEDs in the WLCN.

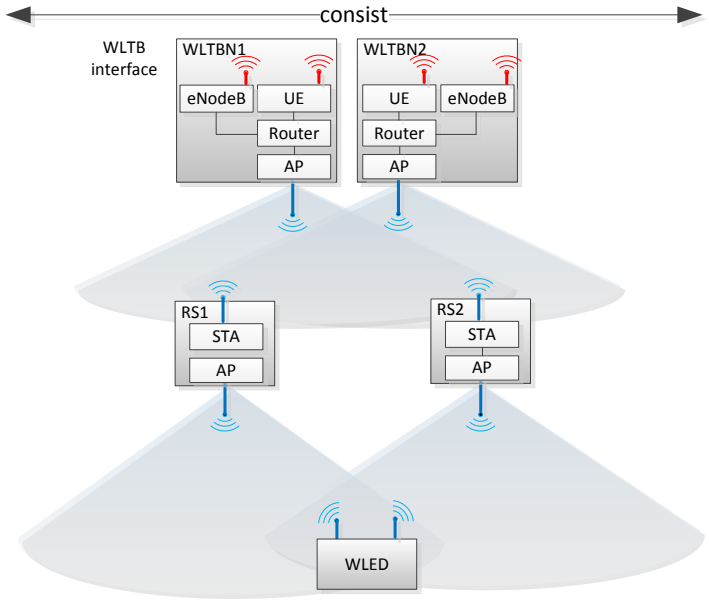


Figure 37: Example of a redundant communication WLCN infrastructure

2.4 BASIC ARCHITECTURE CONCEPTS

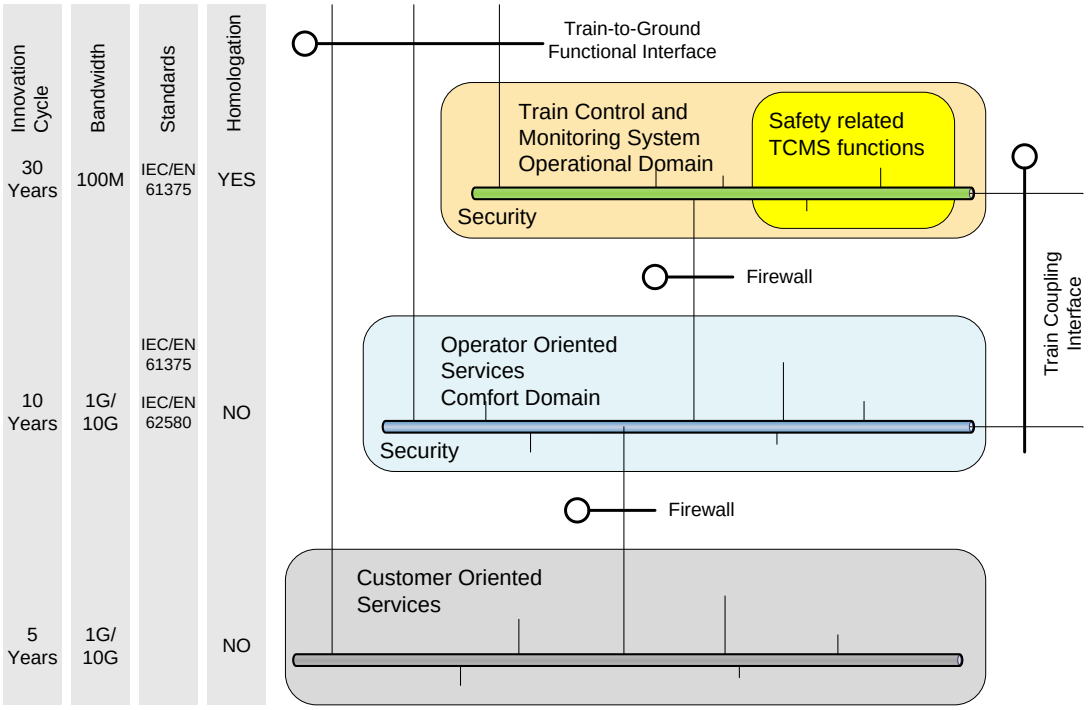


Figure 38: 2.4 Basic Architecture Concepts (interface view)

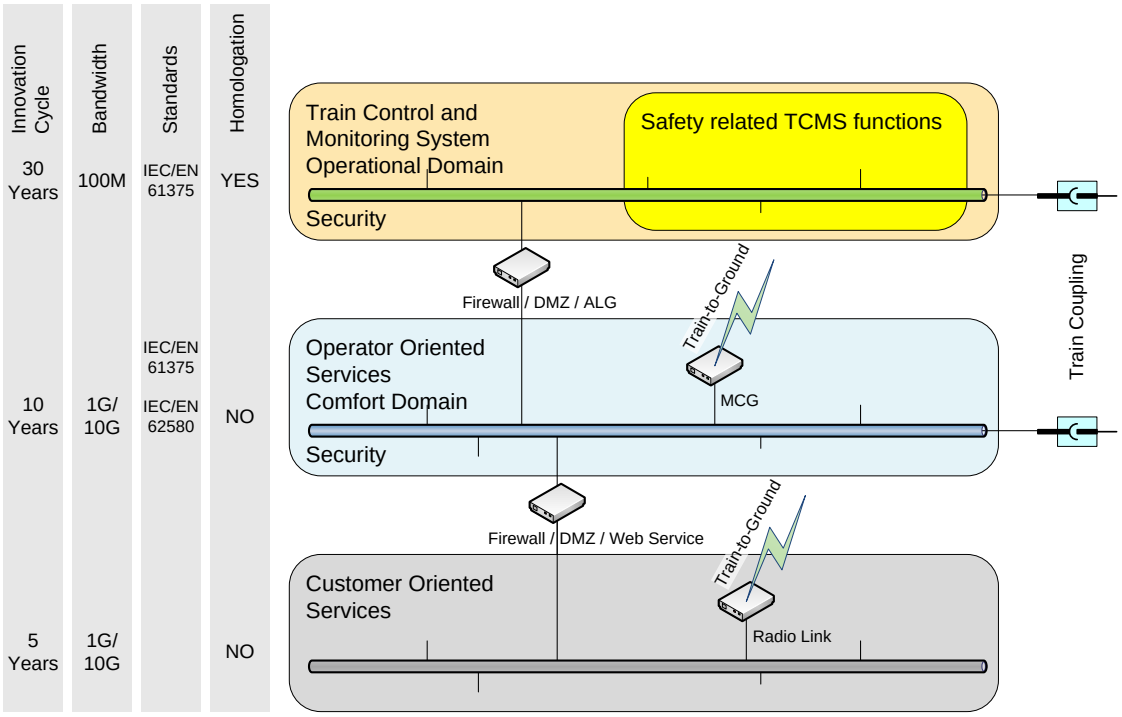


Figure 39: 2.4 Basic Architecture Concepts (deployment example)

The general network architecture shall follow the separation in different functional domains (see WP2.1) and use independent networks (at least logical, when no independent physical networks are implemented) for different domains

- TCMS network
  - ♦ All functions and devices that requests a homologation shall be located in the TCMS network
  - ♦ All safety related functions are located in the TCMS network
  - ♦ TCMS network shall be insensitive to changes in other networks
- OOS Network
  - ♦ Adding new devices to this network, e.g. to provide a new function, shall be possible without influencing the TCMS network.
  - ♦ There will be some innovation of functions and devices in this network during the lifespan of the train
- Customer Network
  - ♦ There shall be a separated network for customer oriented services, too
  - ♦ There will be a lot of innovation of functions and devices in this network during the lifespan of the train
  - ♦ Customer devices, e.g. mobile phones or tablets, will be able to connect to this network
- Communication between TCMS network and OOS network is controlled by a firewall and/or an application level gateway (ALG).
- Communication between OOS network and customer network is controlled by a firewall. Some web services located in OOS network are reachable from customer network. A complete isolation of OOS and customer network is not possible if information, e.g. a live stream of a front facing camera generated in OOS, shall be available in customer network.
- There is no direct connection between the customer network and the TCMS network. All the data from TCMS network to customer network shall go through ALGs and firewall between TMCS and OOS networks and ALG/firewall between OOS and customer

network. Only one-directional data flow (TCMS -> OOS -> cust.) shall be possible for the data originating in the TCMS network.

- Coupling between consists is done logically separately for each network to keep distinct networks.
- Train to ground communication is done using the train to ground functional interface. An example of a possible deployment is the location of a MCG in OOS.

2.5 INTERFACES

2.5.1 General

Beginning with a look back to a reduced standard wired architecture this chapter summarizes potential interfaces on a wireless architecture in regard to a train network and also a mixture of wired and wireless train networks.

2.5.2 Wired TCN (state of the art)

To achieve interoperability basically three network interfaces are of interest, which are depicted in Figure 40 showing the IEC 61375 compliant TCN standard architecture:

- ETB link
- ECR trunk link
- ED link

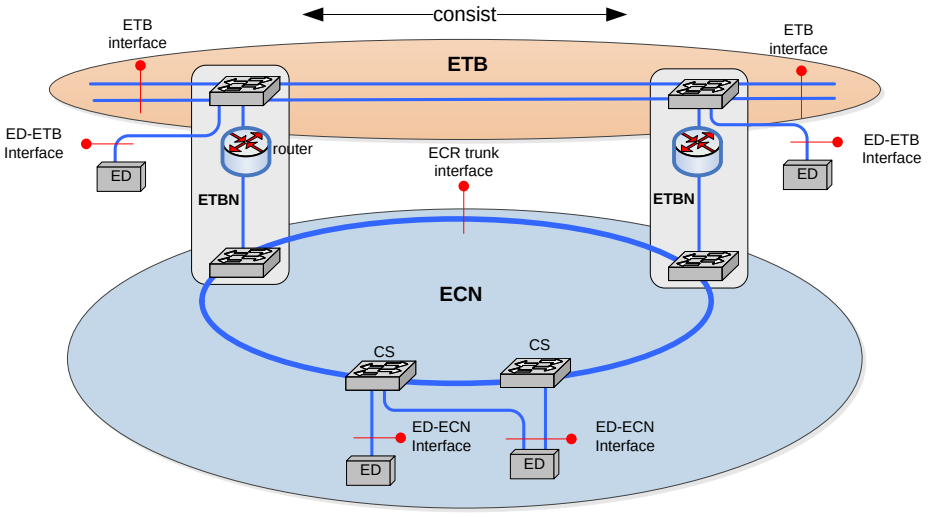


Figure 40: Physical protocol interfaces in standard IP-TCN architecture

It should be noted that Figure 40 shows redundancy information for ETB and ECN. In the later viewing of the wireless system the aspects of redundancy are not considered. This will be done in the chapters of the architectural definitions.

2.5.2.1 ETB interface

The interface on the ETB link is mainly used for the exchange of train wide application data. It is also used by the ETBN to perform the train inauguration. This interface is specified in IEC61375-2-5 (lower communication layers) and IEC61375-2-3 (upper communication layers). Functions on application layer will be specified in IEC61375-2-4 (currently under construction).

2.5.2.2 ECR trunk interface

The interface on ECR trunk link is mainly used for the exchange of train wide and consist internal application data. Train wide data are directed to/from the local ETBN which routes the data to the ETB, see IEC61375-3-4 for details. The interface is also used for ring management (redundancy).

2.5.2.3 ED-ETB interface

This interface is used by ED directly connected to the ETB for data exchange among themselves.

2.5.2.4 ED-ECN interface

This interface on ED link connects ED to ECN via managed switches. Over this interfaces all the services offered by IP-TCN towards EDs are supported. The conditions, which an ED has to fulfil to be connectable to IP-TCN, are defined within IEC61375-3-4.

2.5.3 Wireless TCN

Compared to the wired TCN standard architecture, a wireless based architecture should achieve the same interoperability between network components, based on definitions in IEC61375 and shall achieve at least the same performances, while guarantying the compatibility with actual wired TCN solutions.
On wired based networks TCN is divided into separate functional areas (ETB and ECN). The separation is achieved by the cabling. The areas are connected by using special hardware (train- and ring-switches). End devices are connected to the switches. The interfaces are well defined, ref. 2.5.2, and enable data communication on the train network. Figure 41 depicts a simplified overview of wireless elements and the functional network areas (WLTB and WLCN).

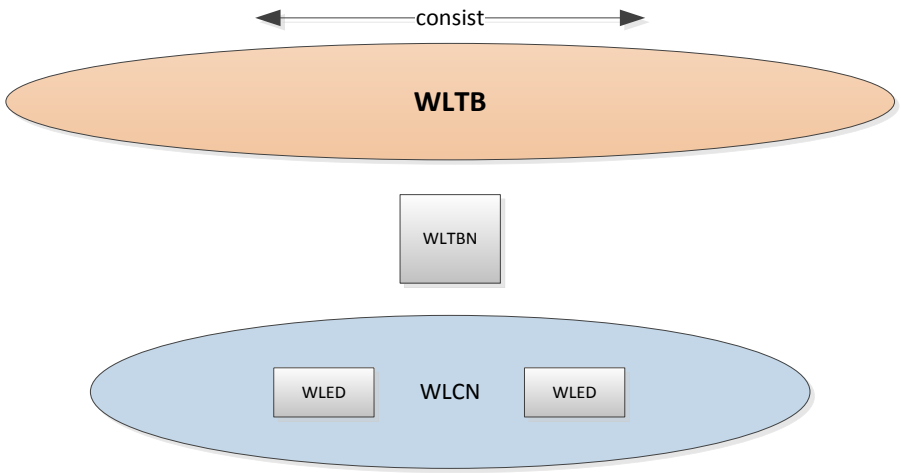


Figure 41: Overview of WTCN architecture

- WLTB: WireLess Train Backbone represents the network area where WLTBNs communicate, train wide communication
- WLTBN: WireLess Train Backbone Node is a wireless device enabling communicating between WLTB and WLCN
- WLCN: WireLess Consist Network represents a group of end devices belonging to local consist network; local consist communication or train wide data routed by the WLTBN
- WLED: WireLess End Device; using communication infrastructure

Compared to wired architecture, the number of main links reduces to two, optionally to three:

- WLTB link
- WLED link
- WLC trunk link (optionally)

The main links are described with the help of an abstract representation in Figure 42.

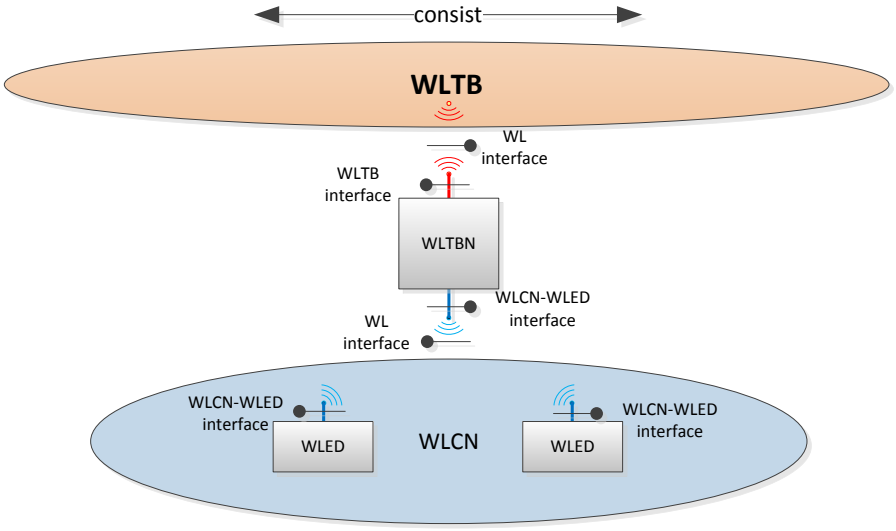


Figure 42: Physical protocol interfaces in wireless architecture

2.5.3.1 WLTB Interface

The interface on WLTB link is mainly used for the exchange of train wide application data. It is also used by the WLTBN to perform the train inauguration. This interface will be specified in a new part of IEC61375 (IEC61375-2-x), defining the lower communication layers for wireless communication (as a result of the R2R project) The upper communication layers of this interface is defined in IEC61375-2-3. Functions on application layer will be specified in IEC61375-2-4 (currently under construction).

2.5.3.2 WLCN-WLED Interface

The interface on WLED link connects WLED to WLCN via managed wireless access points (WLTBN). Over this interfaces all the services offered by TCN towards WLEDs are supported.
The conditions, which a WLED has to fulfil to be connectable to WLCN are at the moment not defined in IEC61375. IEC61375 will need new standard part or parts, defining conditions for wireless based communication network similar to IEC61375-2-5 and IEC61375-3-4.
This interface is also used for the exchange of train wide and consist internal application data. Train wide data are directed to/from the WLTBN which routes the data to the WLTB.

2.5.3.3 WL interface

The interface is present on WLTB and WLED links. It is used to exchange IP data between the network components (access points and clients). Depending on the kind of technique used (WLAN or LTE), this interface is specified within IEEE 802.11 (WLAN) or IEEE 802.16 (LTE) in principal.

2.5.3.4 WLCN trunk interface (optionally)

Depending on technology chosen and the physical configuration of the consist, a "wireless consist trunk" similar to ECR trunk link (ref. 2.5.2) may be considered. In this case the WLCN will be composed by several “access points” constituting the wireless consist trunk link, which is in turn connecting to the WLTBN. The interface is present between WLTBN and wireless consist trunk. The "access points" on wireless consist trunk will provide WLCN-WLED interface for connecting the end devices.

2.5.4 Combination of wireless and wired TCN

2.5.4.1 Coupling consists of different technology

To achieve interoperability between wired and wireless TCN architectures basically one main network interface is of interest. Figure 43 depicts a link on the train backbone.
To enable data communication between wired consist A and wireless consist B, either consist A or B must have a network component which is able to access the physical link of the peer consist. Due to backward or forward compatibility the connecting network component needs to be placed in the appropriate consist. Figure 43 depicts an abstract overview of a physical connection based on ETB.

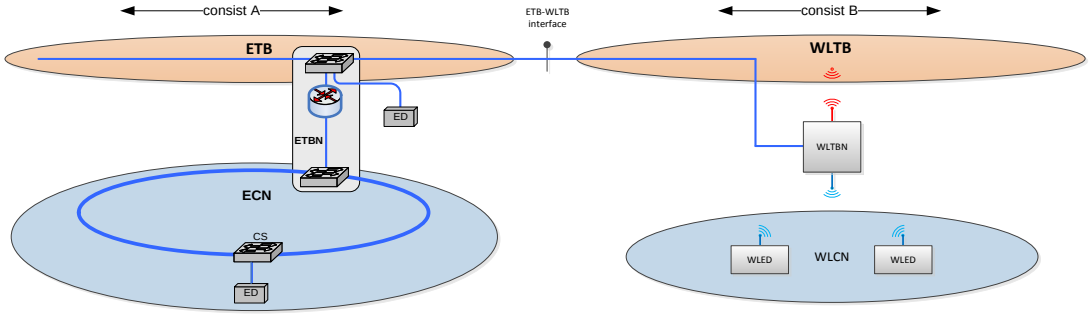


Figure 43: Physical protocol interfaces between wired and wireless architecture

2.5.4.2 ETB-WLTB Interface

The interface in the ETB-WLTB link is mainly used for the exchange of train wide application data. It is also used by the ETB nodes to perform the train inauguration. From TCN point of view this interface is specified in IEC61375-2-5 (lower communication layers), IEC61375-2-3 (upper communication layers) and IEC61375-2-4 (application layer).
Apart from its wireless interface a WLTBN needs an additional physical interface to access the ETB link. The WLTBN also needs a kind of converter (ALG) to handle data transmission between wired and wireless networks (gateway function).
Besides the physical interface mentioned above also some logical interfaces are of interest, when consist of different communication technique are combined, see Figure 44.

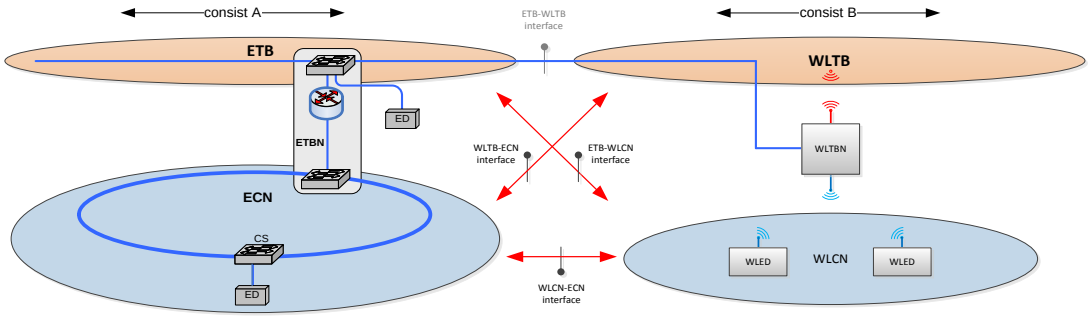


Figure 44: Logical protocol interfaces between wired and wireless architecture

2.5.4.3 ETB-WLCN Interface

The interface in the ETB-WLCN link is mainly used for the exchange of train wide and consist internal application data. Train wide data are directed to/from the ETBN (train switch) in consist A which routes the data to the WLCN in consist B. From TCN point of view this interface is specified in IEC61375-3-4.

2.5.4.4 WLTB-ECN Interface

The interface in the WLTB-ECN link is mainly used for the exchange of train wide and consist internal application data. Train wide data are directed to/from the WLTBN in consist B which routes the data to the ECN in consist A. From TCN point of view this interface is specified in IEC61375-3-4.

2.5.4.5 WLCN-ECN Interface

The interface in the WLCN-ECN link is mainly used for the exchange of consist internal application data. WLCN and ECN shall form one IP network . Consist internal application data are directed to/from local WLCN to remote ECN and vice versa via the train backbones ETB and WLTB. From TCN point of view this interface is specified in IEC61375-3-4.

2.5.5 Protocols

In order to achieve interoperability between the different network components TCN uses a lot of communication protocols which all need to be well specified. Most of the supported protocols are standard Ethernet or IP based protocols, but there are also some protocols which have been specially developed for TCN (e.g. TRDP).
The following table (Table 6) lists all relevant protocols together with their relationship to the ISO OSI Layer they belong to, the affected network interface and their specification.

Table 6: List of used protocols

Protocol	OSI	Interface			Specification	Comment
		ED	CN	TB		
100FDX	1	x	x	x	IEEE 802.3	
GbE	1	x	x		IEEE 802.3	
WLAN	1 & 2	x	x		IEEE 802.11	
LTE	1 & 2			x	IEEE 802.16	
VLAN	2	x	x	x	IEEE 802.1Q	
Link Aggregation	2			x	IEEE 802.1AX	
LLDP	2	x		x	IEEE 802.1AB	

Protocol	OSI	Interface			Specification	Comment
		ED	CN	TB		
IP	3	x	x	x	RFC 791	
IPSec	3	x	x	x	RFC 4301	
ARP	3	x	x	x	RFC 826	
TTDP	3			x	IEC61375-2-5	IEC61375 compliant IP-TCN, Inauguration, Train Topology
UDP	4	x	x	x	RFC 768	
TCP	4	x	x	x	RFC 793	
ICMP	4	x	x	x	RFC 792	
IGMP	4	x			RFC 3376	
VRRP	4		x		RFC 5798	
DHCP	7	x	x		RFC 2131	
SNMP	7	x	x	x	RFC 1901, RFC 1905, RFC 1906	
DNS	7	x	x		RFC 1034, RFC1035	
TRDP	7	x	x	x	IEC61375-2-3	IEC61375compliant IP-TCN
FTP	7	x	x	x	RFC 959	
NTP	7	x	x		RFC 958	
SSH	7	x	x	x	RFC 4250	

2.5.6 Inter domain interfaces

According to Figure 39 networks are clustered into functional domains:

- TCMS operational domain → TCMS network
- Operator oriented domain (OOD) → OOS network
- Customer oriented domain (COD) → Customer network

Data communication between the domain networks are usually required. However, this applies only to specific data. Other data in turn may not leave a local domain network. Firewalls or specific ALGs are appropriate network components to achieve a controlled data flow between the domain networks.

2.5.7 Other physical interfaces

Besides the above mentioned TCN related interfaces wireless devices, the access points or end devices, need to be

- powered,
- configured,
- and maintained.

2.5.7.1 Power

Wireless devices need to be connected to appropriate power supply, eventually redundant power supply to increase availability. Power supply system shall provide mechanisms supporting controlled shutdown of devices to reduce loss of data (e.g. enabling devices to store runtime

information on some kind of physical memory before the power is finally switched off). See 2.3.7 for more details about the requirements for the power supply.

2.5.7.2 Configuration

Wireless devices need to be configured to achieve proper operation. The devices need an interface to access configuration information, which might be provided by a connected configuration plug (e.g. an USB or another type of storage hardware). The configuration interface shall be protected against any malicious access.

2.5.7.3 Maintenance

Wireless devices shall support an interface to access the device for maintenance or diagnostic reasons (e.g. serial port to connect a service PC or development environment). The maintenance interface shall be easily accessible by the maintenance teams. This interface shall be protected against any malicious access.
The maintenance interface must give access to all the proper variables needed to carry out tests on the train in case of system failure repair (e.g. port management, redundancy configuration settings, etc.).
It must be possible to give access to maintenance or diagnostic information of all the wireless devices on a centralized interface by sending the devices maintenance information on the train networks.

2.5.8 Functional Layer

From functional point of view a wireless TCN shall provide the same function as a wired one. The functions are mainly:

- inaugurate train network
- determine train topology and configuration
- provide orientation information for coupled elements
- manage leading vehicle information
- distribute train topology and configuration
- confirm train configuration
- manage train network operation
- manage train network access
- transmit data

2.5.9 Other constrains

On wired system some technical topics where covered by hardware either by wire or by specific network components (e.g. switch). This has to be considered when designing a wireless architecture.

2.5.9.1 Grouping of devices

Grouping of devices in wired system is used to assign network components to logical areas or functional domains like TCMS operational or on-board multimedia and telematic subsystem/services domains. This enables separation of data communication in the communication network. When defining the wireless architecture and the wireless interfaces, it must be considered that grouping is possible. Grouping also depends on the technique used (WLAN or LTE).

2.5.9.2 Redundancy

In order to achieve redundancy in the wired systems network lines are doubled and network components (switches) are connected in a ring structure. Appropriate IP protocols are used to

handle the redundancy. Depending on the used technique (WLAN or LTE) redundancy can be achieved by redundant hardware (access point / base stations) or by hardware related capabilities of the wireless equipment (e.g. wireless radio range).

2.5.9.3 Other wired communication media

On wired systems also other wired techniques might be used, like:

- WTB interface between WTB and WLTB
- MVB interface between MVB and WLCN
- CAN interface between CAN-based network and wireless system

For the time being it is unclear if the wireless architecture has to consider interfaces toward these media. Apart from this situation, it is in principal possible to integrate devices which are offering an interface to WTB, MVB or CAN via appropriate gateways, either realized in hard- or software or both.

2.5.9.4 Inauguration

In order to calculate the train topology for train wide communication on wireless TCN, couplers are extended with RFID technology. Wireless TCN need to have a proper interface to the RFID information.

2.5.9.5 IT Security

IT Security constraints shall be addressed when designing a wireless TCN, especially those concerning the interfaces. These constraints depend on the technique used (WLAN or LTE) and are the object of Roll2Rail WP2 Task T2.4.

3 WIRELESS ARCHITECTURE FOR CONSIST TO CONSIST COMMUNICATIONS

As already mentioned in chapter 2.3.2, the main purpose of the train communication system is to allow end devices (ED) within a train to communicate with each other. According to [79] two hierarchical network levels are defined for the general train network architecture (Figure 45).

1. Train backbone level
2. Consist network level

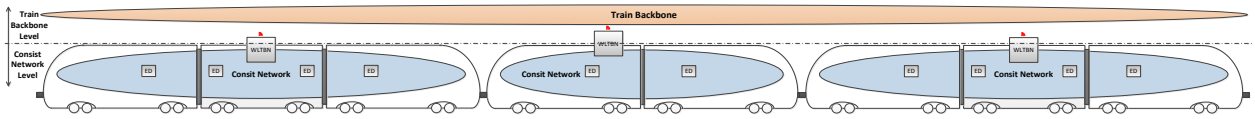


Figure 45: General train network architecture

A wireless train backbone node (WLTBN) in each consist interconnects the consist network level with the train backbone level. The communication between the consist networks is only possible via the train backbone and WLTBN. Therefore, a WLED shall not be able to connect to any AP in other consists directly (see Figure 46).

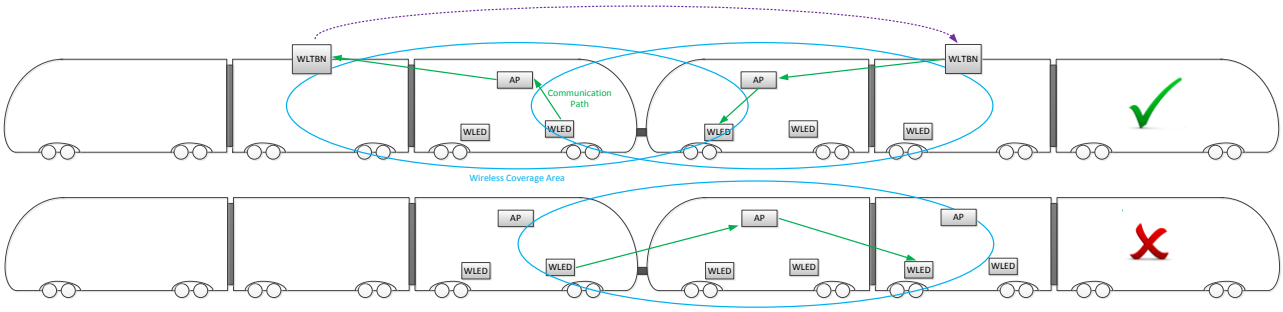


Figure 46: Consist to consist communication principle

EDs in the same consist can communicate without using the train backbone or the WLTBN.
The train backbone is used for the consist to consist communication. LTE has been selected as suitable technology for the train backbone (see also [80]). The LTE technology supports transmission distances up to 20 Km depending on the category of LTE equipment and a data transfer rate up to 100 Mbit/s. These values fit to the requirements listed in [69]. The LTE technology has been designed for mobile use cases and not to be used for rail communication networks. Figure 47 describes a transformation from original use case to the railway use case.

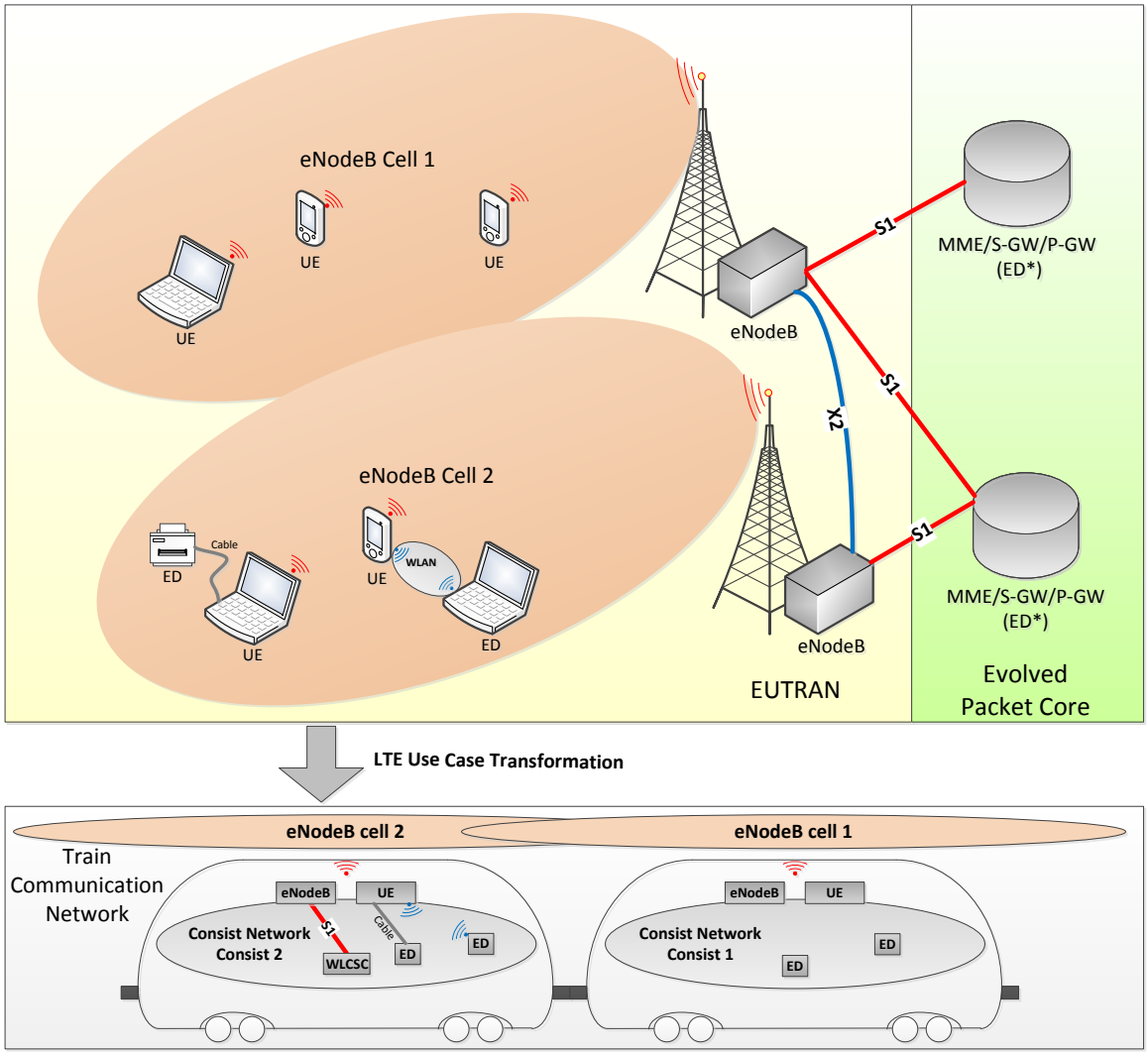


Figure 47: LTE Use Case Transformation

One difference is that in a classic LTE communication system the position of the User Equipment is moving and equipment like eNodeB and Evolved packet Core are fixed. In the LTE train communication system the complete system is moving but all equipment is relatively fixed from communication distance point of view. Necessary tasks of the Mobility Management Entity (MME), Serving Gateway (S-GW), and Packet Data Network Gateway (P-GW) which are part of the Evolved Packet Core (EPC) will be executed on one or several special end devices (WLCSC). The tasks executed on the WLCSC will be described in further chapters of this document.
As described in chapter 2.4 the general network architecture shall follow the separation in the following different functional domains:

- Train Control and Monitor System (TCMS) network
- Operator Oriented Services (OOS) network
- Customer Oriented Services (COS) network

Figure 48 describes the principles of a train backbone architecture of a consist. The functional domains are separated but connected via gateways (GW) exchanging data in an absolutely controlled way. The gateways may contain firewalls and other mechanisms controlling the internal access in the consist from one domain to another (see chapter 4 for details). The separation on train backbone level is done by using 2 train backbones. First one for the communication within the TCMS domain, which can be also safety related, the second one for the regular train backbone communication of the other domains. Communication of passengers between consists is not foreseen via WLTB. This communication is handled via train to ground communication (via MCG, see also chapter 4.8).

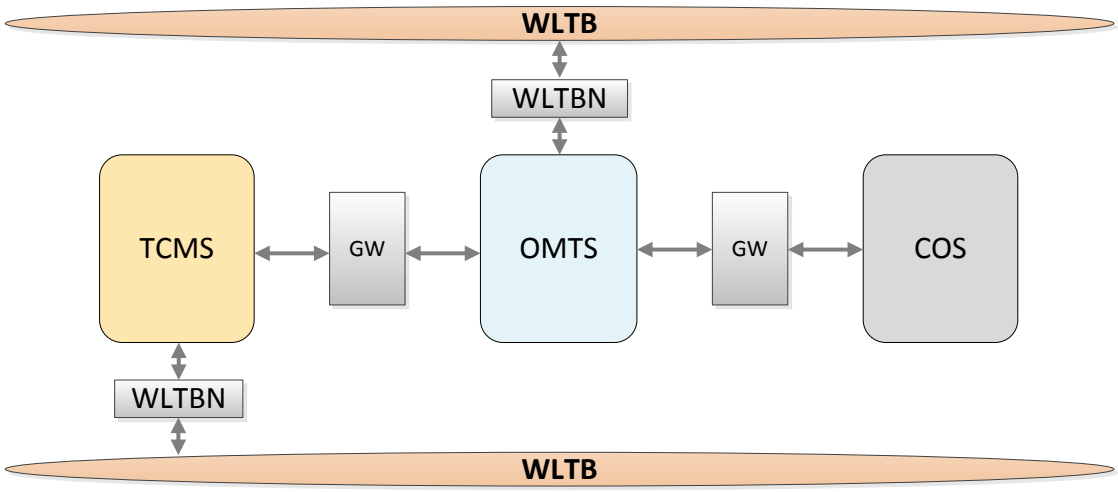


Figure 48: Train backbone architecture of a consist

The following subchapters describe the train backbone architecture and consist to consist communication. Chapter 4 describes the architecture of the consist network and the communication inside the consist.

3.1.1 Train Discovery

To achieve data communication on the train backbone level, first of all the communication partners need to be discovered. Since the train/train set composition can vary (e.g. coupling of consist or a failing consist within the train), the chosen mechanism should be able to cope with varying scenarios.
According to [80] LTE technology equipment is used on backbone level. Due to this some preconditions exist:

- a User Equipment (UE, representing a LTE client) can only be connected to one backbone node (eNodeB, representing a LTE access point for UEs) at same time
- multiple UEs can be connected to one eNodeB
- each consist contains at least one UE and one eNodeB (vehicles not operating alone e. g. coaches may not need eNodeB)

In order to support train discovery the consist couplers at each end of the consist need to be equipped with a RFID transponder and a RFID reader. The RFID transponder provides the following data to the coupled consist:

- the consist identifier (consist id) of the local consist
- the direction information (front end – 1 or back end – 2) of the local consist
- the number of vehicles in the local consist
- the identifier of the own eNodeB
- the identifier of the own UE (SIM card id)

Other preconditions:

- in the case of having redundant UE's, both use the same SIM card id but only one could be active at the same time
- each consist provides additional coupler criteria (physical contact with the signal coupled/not coupled) to detect lengthening/shortening safely
- the UE of a consist makes use of the data provided by the RFID, e.g. uses the consist identifier to establish a connection with a peer UE by adding the UE to the eNodeB 's whitelist
- a safe end device (WCSC) is used
    - to get RFID data from the couplers and
    - to provide this data to the LTE equipment (UE and eNodeB)
- LTE sending power needs to be adapted to maximum train length (LTE range is 0 -20km)
- LTE devices (eNodeB and UE) as well as the couplers need to have a control/management interfaces which are accessible by the controlling end device (ED), see section 3.1.5 for further details.
- Distribution and handling of the inauguration result is done according to [77] (ECSP-ECSC interface)

Due to technical constraints of the LTE, four concept ideas for the train discovery are described in the following chapters 3.1.1.1 to 3.1.1.4. There may exist others which are not evaluated here. Chapter 3.1.1.5 compares the pros and cons of these concept variants and recommends the best fitting one.

3.1.1.1 Variant A

The following Figure 49 depicts a rough overview of the setup for train discovery within a single consist. The yellow arrows show which elements will exchange data for the train discovery.

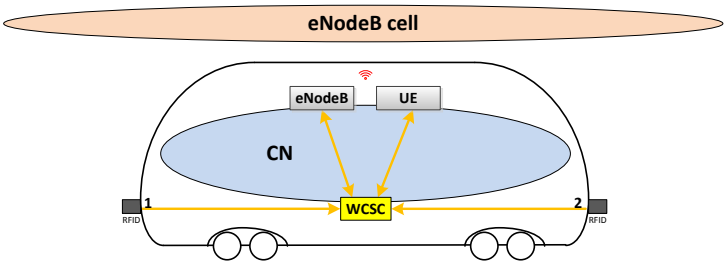


Figure 49: Abstract view of a consist for network discovery

At the beginning of the discovery the WCSC will read RFID data from both ends (couplers) and propagate the data to the local UE and eNodeB using given interfaces (of UE and eNodeB). These devices will use the data to setup connections to other peers in the train. The UE will use the data to connect to the peer eNodeB. The eNodeB will use the data to grant access for the peer UE. The eNodeB uses a kind of access list which only contains IDs of UEs which are allowed to connect (white list approach; at initial start this list is empty).
To allow both, a fast train backbone discovery and a latency optimised train-wide communication the inauguration of the WLTB is split in three steps

- The discovery starting at both ends[2]
- The selection of the Master eNodeB
- Distribution and handling of the inauguration result according to [77] (ECSP-ECSC interface)

The following chapters will explain further details.

3.1.1.1.1 Establish train wide LTE network

Figure 50 depicts a train composed of three consists.

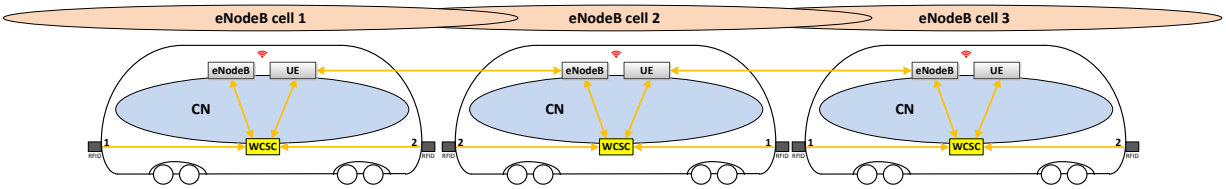


Figure 50: Abstract view of three consists for network discovery

Discovery sequence:

1. The WCSC reads consist IDs of coupled consist(s) from RFID in the couplers 1 and 2.
2. The WCSC inserts the found consist IDs in its local eNodeB database (white list) and hands over these consist IDs to its local UE.
3. The discovery starts from both ends of the two end consists, by connecting the UEs to the eNodeBs with the consist ID found at the connected end / not yet treated end.
4. Safe exchange of own and all available coupled consist information:
    a. the identifier (consist ID),
    b. the direction information, and
    c. the number of vehicles.

[2] Detection of end nodes is handled by the controlling end device (WCSC); it knows which couplers are coupled.

5. The WCSC removes the new connected consist ID from the own white list of the own eNodeB.
6. Repeating of steps 3 to 5 for all further consists until all consists of the train are discovered.

Timings:

- Duration to connect one or more UE to an eNodeB is < 500ms (time for successful connection to be measured). 500ms can be reached in case of timeouts/refuse of connection

3.1.1.1.2 White list discovery

After the LTE network has been established, the controlling end device of each consist will

- send local consist information (consist ID, coupler 1 and 2 data) to a peer consist and
- receive consist information from a peer consist.

If the controlling end device (WCSC) is not an “end node”, then it adds its local consist information to the received information and sends it to the next consist. According to 3.1.1.1.3 one consist in the “middle” gets the information from two ends, containing all information of all consists from both ends. The controlling end device (of the middle consist) computes a table, representing all consist information. Based on this table the end device defines a white list and decides which consist shall run the master eNodeB. The list and master definition is distributed to all consists. All consists adapt to this definitions and acknowledge the information.

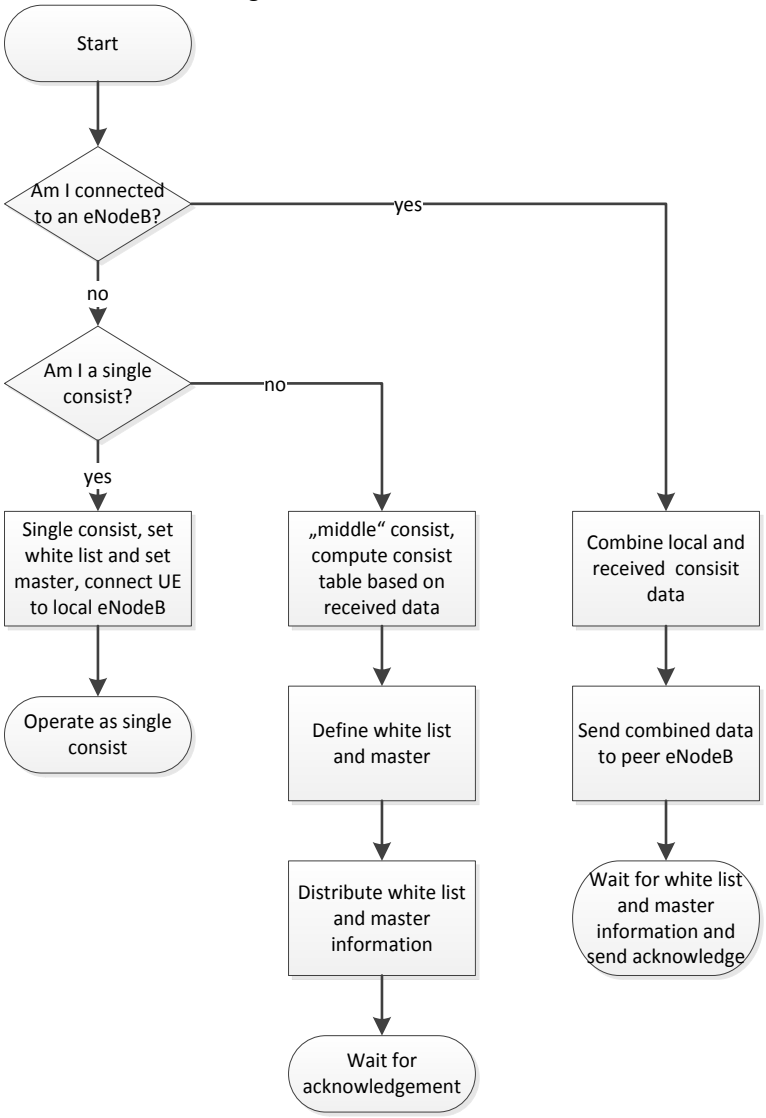


Figure 51: White list discovery algorism (Variant A)

3.1.1.1.3 Selection of the master eNodeB

After a successful discovery a latency optimized communication shall be set up. This means, only one eNodeB, the so called master eNodeB, of the train shall be active, see Figure 52. All other UEs shall connect to the master eNodeB. The master eNodeB selection will be processed by the controlling end device (WCSC).

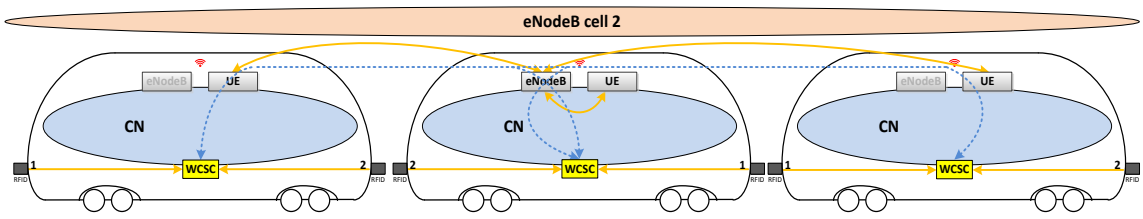


Figure 52: Abstract view of three consists with master eNodeB

After established connections the UEs are working as gateways between LTE train backbone and Consist Network (CN). Communication between WCSCs is now possible (blue dashed lines). Inauguration as well as train topology definition can be handled next, see 3.1.2.

WLTB front end selection:

1. Compare the IDs of the two end consists and define the consist with the lower ID as the front end of the train. The WLTB front end selection will be processed by the controlling end device (WCSC).

Master eNodeB selection sequence:

1. Select an eNodeB in the middle[3] of the train as master and establish communication between all UEs via one eNodeB as precondition for a train-wide communication.
2. Set up all eNodeB white lists, adding all consist IDs of the train.
3. Set all eNodeBs (except master) to standby.
4. Connect all UEs to the master eNodeB (typical time to be measured, worst case 500ms in case of timeouts/refused connections)
5. If the master eNodeB is not available select as new master eNodeB the eNodeB of the consist which is the next towards the back end of the train (seen from the previous selected master eNodeB). Repeat 3 and 4.

3.1.1.1.4 Powerless consist handling

The train backbone discovery needs to handle the use case that a UE can't establish a connection towards a coupled consist known by the RFID information data.

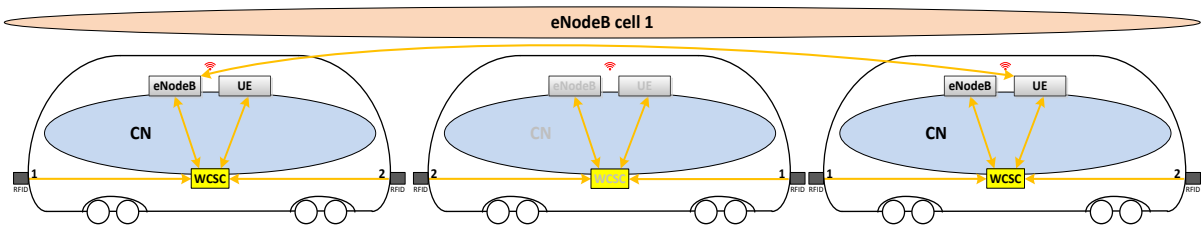


Figure 53: Abstract view of three consists with one failing eNodeB

[3] At a train with an even number of consists the master eNodeB will be the eNodeB of the consist closed to the middle and nearest to the defined front end of the train.

Discovery sequence:

1. UE tries to connect to its neighbour eNodeB, but fails.
2. After a timeout of e.g. 5s[4] the UE tries to connect to another potential eNodeB.
3. At the same time, an eNodeB of a consist which has not been contacted within 2.5s[4] by its neighbour's UE adds the IDs of all UEs that try to connect in its white list.
4. In the case of successful connections, the consists exchange the own coupled consist information (at least ID). If both consists are detecting the same ID as neighbour (same powerless consist), the identifier of the connected UE can be kept in the white list of the eNodeB data base. Otherwise the UE will be disconnected and the related identifier will be removed from the white list of the eNodeB DB.
5. A new master will be defined as described in 3.1.1.1.3

3.1.1.1.5 Lengthening/Shortening detection

The discovery mechanism shall be able to detect a change in the train backbone composition, means adding or removing one or more consists. An additional coupler criteria shall be used to check the integrity of the train. This coupler criteria is continuously checked in each consist. In the case of a change of the coupler criteria a shortening (change from coupled to uncoupled) or lengthening (change from uncoupled to coupled) happened. After a composition change the discovery principles mentioned above and a new safe train inauguration have to be applied to setup the new train composition. Because the train length is safety related a lengthening or shortening have to be applied safely.

3.1.1.2 Variant B

In order to support train discovery the consist couplers at each end of the consist need to be equipped with a RFID transponder and a RFID reader. The RFID transponder provides the following data to the coupled consist:

- the consist identifier (consist id) of the local consist
- the direction information (front end – 1 or back end – 2) of the local consist
- the number of vehicles in the local consist
- the identifier of the own eNodeB
- the identifier of the UE (SIM card id)

Other preconditions:

- each consist is equipped with one eNodeB and two UEs.
- each consist provides additional coupler criteria (coupled/not coupled) to detect lengthening/shortening safely
- the UEs of a consist make use of the data provided by the RFID, e.g. uses the consist identifier to establish a connection with a peer eNodeB
  - RFID chip 1 additionally holds the identifier of UE1 (SIM card id)
  - RFID chip 2 additionally holds the identifier of UE2 (SIM card id)
- a safe end device (WCSC) is used
  - to get RFID data from the couplers and
  - to provide this data to the LTE equipment (UE and eNodeB)
- LTE communication range needs to be adapted to maximum train length (LTE range is 600m - 20km)
- LTE devices (eNodeB and UE) as well as the couplers need to have a control/management interfaces which are accessible by the controlling end device (WCSC), see section 3.1.5 for further details.

[4] Provided by Thales, to be measured, lower value appreciated.

The following Figure 54 depicts a rough overview of the setup for train discovery within a single consist. The yellow arrows show which elements will exchange data for the train discovery.

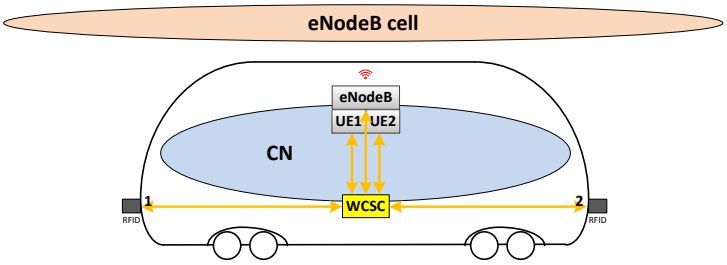


Figure 54: Abstract view of a consist for network discovery

At the beginning of the discovery the WCSC will read RFID data from both ends (couplers) and propagate the data to the local UEs and eNodeB using given interfaces. These devices will use the data to setup connections to other peers in the train. The UEs will use the data to connect to the peer eNodeB. The eNodeB will use the data to grant access for the peer UE. The eNodeB uses a kind of access list which only contains IDs of UEs which are allowed to connect (white list approach).
To allow both, a fast train backbone discovery and a latency optimised train-wide communication the inauguration of the WLTB is split in three steps

- The discovery starting at each node
- The selection of the Master eNodeB
- Distribution of the inauguration result according to [77]

The following chapters will explain further details.

3.1.1.2.1 Establish train wide LTE network

Figure 55 depicts a train composed of three consists.

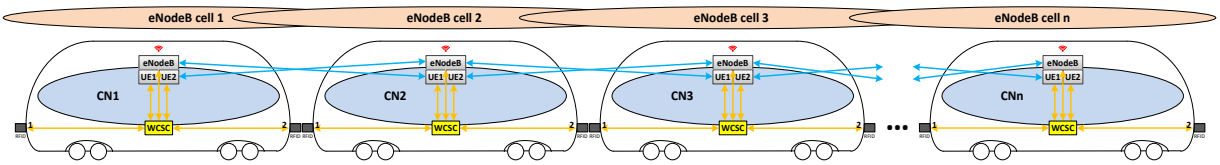


Figure 55: Abstract view of "n" consist for network discovery

Discovery sequence:

1. The WCSC reads consist IDs of coupled consist(s) from RFID in the couplers 1 and 2.
2. The WCSC inserts the found consist IDs in its local eNodeB database (white list) and hands over these consist IDs to its local UEs.
3. The discovery starts in each consists in parallel, by connecting the UEs to the preferred peer eNodeBs. UE1 connects to the eNodeB to the end1 and UE2 connects to eNodeB to the end2.
4. Safe exchange of own and all available coupled consist information:
    a. the identifier (consist ID),
    b. the direction information, and
    c. the number of vehicles.

Timings:

- Duration to connect one or more UE to an eNodeB is < 500ms (time for successful connection to be measured). 500ms can be reached in case of timeouts/refuse of connection

3.1.1.2.2 White list discovery

After the LTE network has been established, the controlling end device of each consist will

- send local consist information (consist ID, coupler 1 and 2 data) to peer consists and
- receive consist information from peer consists.

The controlling end device (WCSC) adds its local consist information to the received information and sends it to the next consist. Information received on direction 1 (means that coupler 1 is coupled) shall be forwarded in the opposite direction 2 and vice versa. Thus each consist gets the consist information from all other consists involved. The controlling end device (of the leading consist) computes a table, representing all consist information. Based on this table the controlling end device defines a white list and decides which consist shall run the master eNodeB. The list and master definition is distributed to all consists. All consists adapt to this definitions and acknowledge the information.

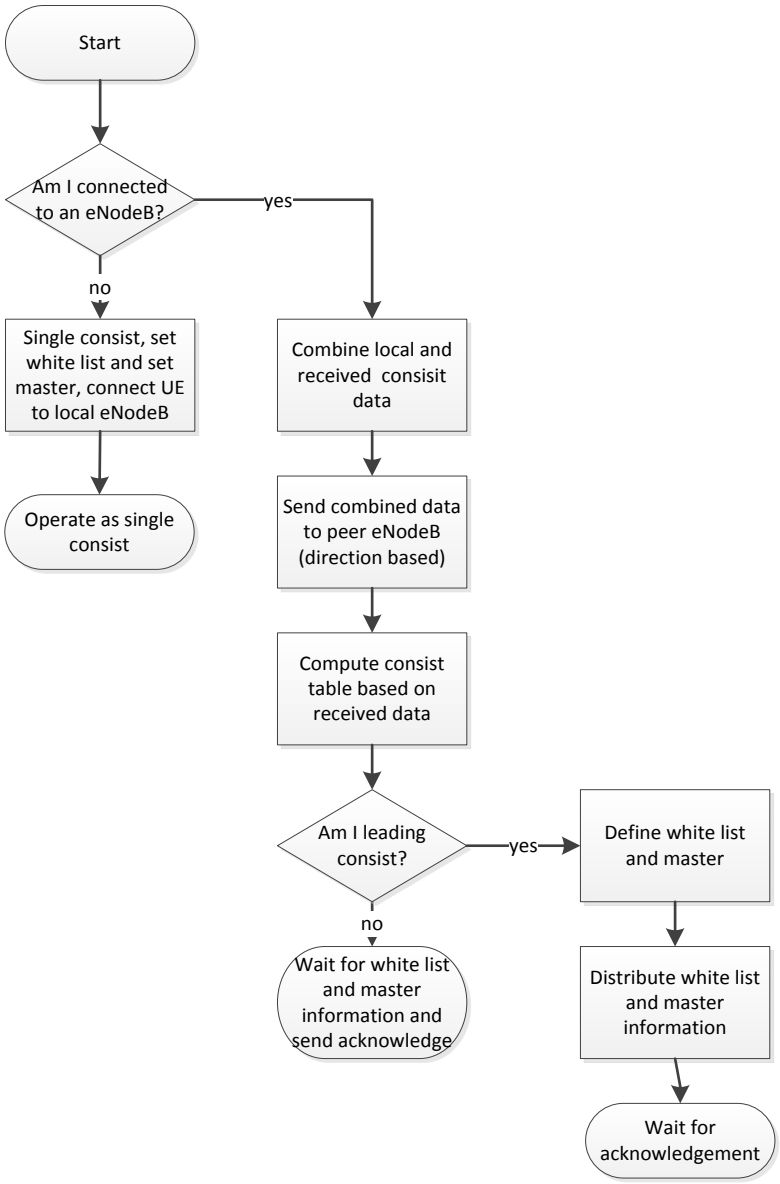


Figure 56: White list discovery algorism (Variant B)

3.1.1.2.3 Selection of the master eNodeB

After a successful discovery a latency optimized communication shall be set up. This means, only one eNodeB, the so called master eNodeB, of the train shall be active, see Figure 52. All UE1s shall connect to the master eNodeB. All UE2s shall connect to the standby eNodeB.

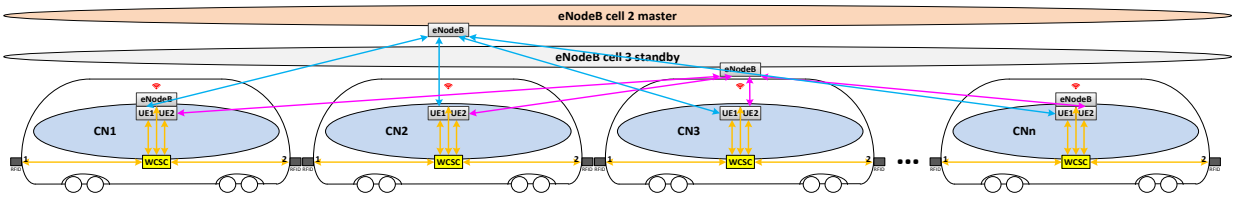


Figure 57: Abstract view of "n" consist with master eNodeB

After established connections the UE1s are working as gateways between LTE train backbone and Consist Network (CN). Communication between WCSCs is now possible. Inauguration as well as train topology definition can be handled next, see 3.1.2.

WLTB front end selection:

1. Compare the IDs of the two end consists and define the consist with the lower ID as the front end of the train.

Master eNodeB selection sequence:

1. Select an eNodeB in the middle[5] of the train as master.
2. Select a standby eNodeB near to the master eNodeB.
3. Set up all eNodeB white lists, adding all consist IDs of the train.
4. Connect all UE1s to the master eNodeB (typical time to be measured, worst case 500ms in case of timeouts/refused connections)
5. Connect all UE2s to the standby eNodeB (typical time to be measured, worst case 500ms in case of timeouts/refused connections)

3.1.1.2.4 Powerless consist handling

The train backbone discovery needs to handle the use case that UEs can't establish connections towards coupled consists known by their RFID information data.

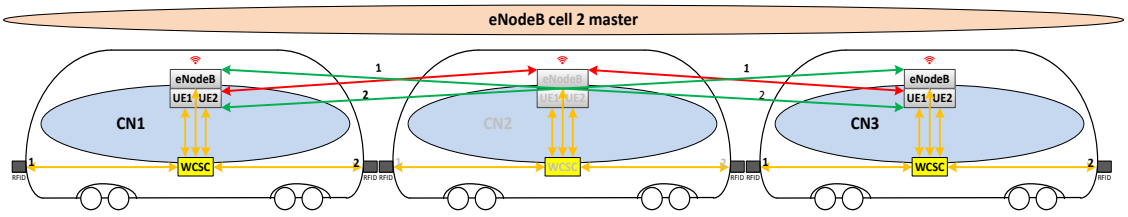


Figure 58: Abstract view of three consists with one failing eNodeB

Discovery sequence:

1. The UEs of consist CN1 and CN3 try to connect [1, red arrows] to the eNodeB from consist CN2 first

[5] At a train with an even number of consists the master eNodeB will be the eNodeB of the consist nearest to the defined front end of the train.

2. The UEs can't connect (detected by timeout) and the eNodeB whitelist is updated with all UE ids previously trying to connect
3. The UEs try to connect again and can now connect [2, green arrows] to the next consists eNodeB
4. A script/external protocol is triggered, ensuring the now connected UE is from the consist seeing consist CN2 as its neighbour
5. All other UE connections are cancelled and the whitelist is updated
6. A new master will be defined as described in 3.1.1.1.3

3.1.1.2.5 Lengthening/Shortening detection

The discovery mechanism shall be able to detect a change in the train backbone composition, means adding or removing one or more consists. An additional coupler criteria shall be used to check the integrity of the train. This coupler criteria is continuously checked in each consist. In the case of a change of the coupler criteria a shortening (change from coupled to uncoupled) or lengthening (change from uncoupled to coupled) happened. After a composition change the discovery principles mentioned above have to be applied to setup the new train composition.

3.1.1.3 Variant C

In this variant each consist of the train contains one UE and one eNodeB, same as for variant A (see Figure 49).

3.1.1.3.1 Establish train wide LTE network

After the train is powered, there is one dedicated consist at one end of the train e.g. leading consist which is switching active its UE end eNodeB. All other consist in the train activate the UE only (see Figure 59). The white list at the active eNodeB is empty. No UE can connect to the active eNodeB.

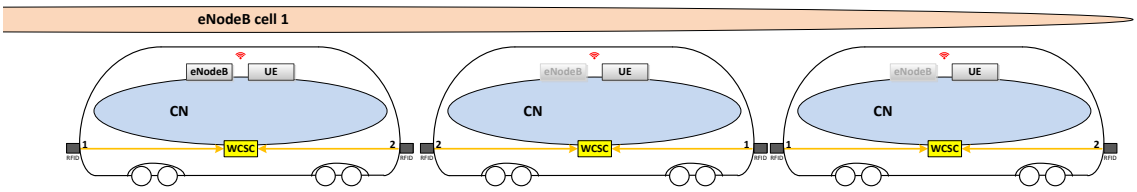


Figure 59: Abstract view of three consists for network discovery

Discovery Sequence:

1. In a first step the WCSC of the active eNodeB enables the active eNodeB to accept all UE to connect.

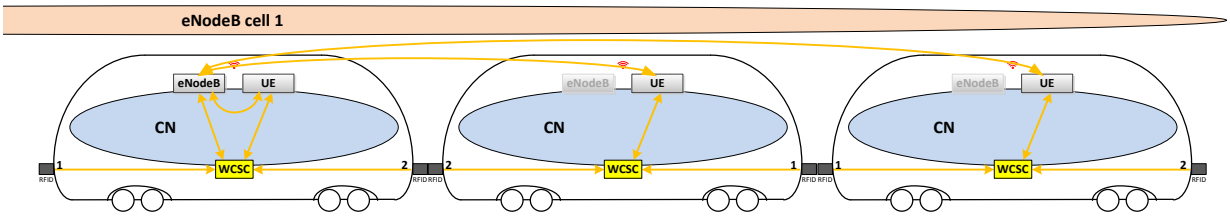


Figure 60: Abstract view of three consists with master eNodeB add train end

2. As soon as an UE is connected to the active eNodeB, the WCSC of the active eNodeB requests the coupler data from the WCSC of the consist the UE belongs to.
3. With the coupler data of all consists the WCSC of the active eNodeB discovers the white list containing all UEs in the train (see chapter 3.1.1.3.2 for details).

4. After discovering the white list the WCSC of the active eNodeB set the white list of the active eNodeB according the detected UEs belonging to the train. Only UE registered as valid consists in the train can from now on connect the active eNodeB.
5. In order to improve the radio conditions for the train backbone communication the WCSC of the active eNodeB (master eNodeB) can move the master eNodeB function to another consist in the train (see chapter 3.1.1.3.2 for details)

3.1.1.3.2 White list discovery

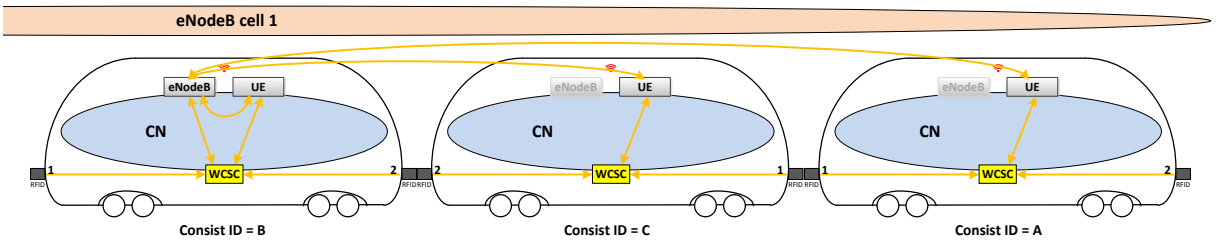


Figure 61: Train example for white list discovery

Table 7: Example of Contact List (Entry Nr. 3 Is not part of the train)

Entry Nr.	Consist ID	Coupler 1	Coupler 2	UE ID
1	C	A	B	xx
2	A	C	-	yy
3	D	G	H	ww
4	B	-	C	zz

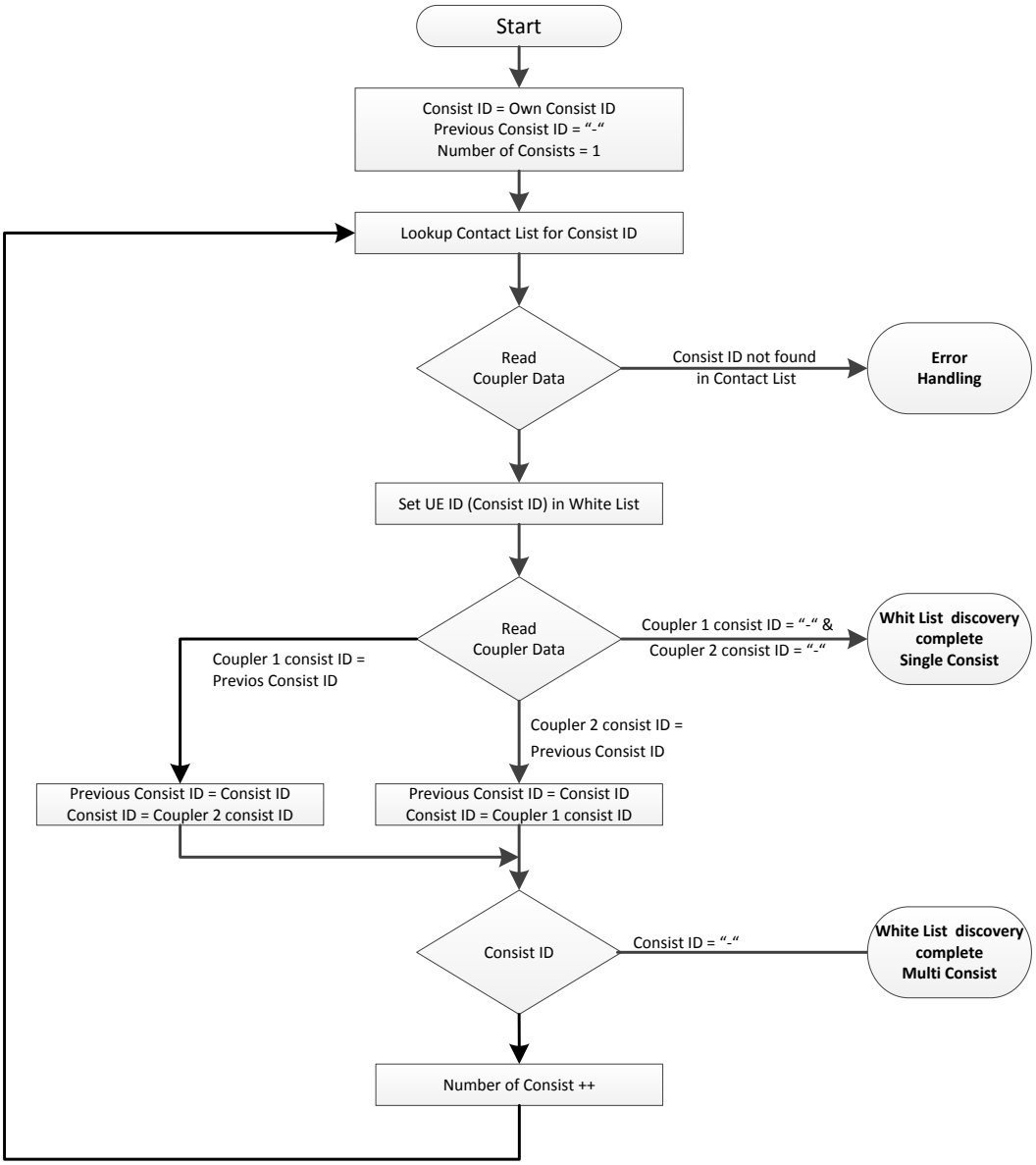


Figure 62: White list discovery algorism (Variant C)

3.1.1.3.3 Selection of the master eNodeB

From radio condition point of view it is not optimal to have the master eNodeB at one end of the train. Therefore it makes sense to transfer the master eNodeB to the middle of the train because this position provides the shortest distance to all UEs in the train. As result of the white list discovery the number of consists in the train is known as well. With this the WCSC of the eNodeB at the end of the train is able to address the approximately middle consist and transfer its white list to the WCSC of middle consist. A handshake mechanism between both WCSCs ensure that the WCSC at the new master eNodeB position has received the white list. After the white list has been successfully transferred, the WCSC at the new master eNodeB position enables its eNodeB and

set the received white list. The WCSC of the master eNodeB at the end position disables its eNodeB (see also Figure 63).

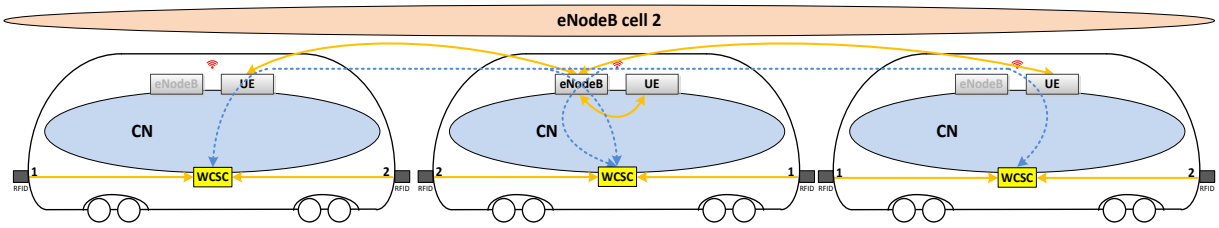


Figure 63: Abstract view of three consists with master eNodeB add train middle

3.1.1.3.4 Powerless consist handling

In case a consist is powerless its UE will not connect to the active eNodeB at the end of the train and therefore the white list discovery cannot be completed successfully (see also Figure 62). In this case an error handling is necessary.
It can be automatically handled if only one consist is powerless because the coupler data of both neighbour consists are indicating the same missing consist.
In the case that more consists are missing a manual handling (train correction) needs to be applied.

3.1.1.3.5 Lengthening/Shortening detection

Lengthening and shortening of the train is handled in same way as for Variant A chapter 3.1.1.3.5.

3.1.1.3.6 Train Station cases

This variant is special because in a station the discovery phase of one train can have an impact on the discovery phase of another train, when both trains execute their train discovery at the same time. In the Variant C the UE is for a short time able to connect to another train. This is very unlikely because the discovery phase is very short (approximately 1 second). Figure 64 to Figure 68 describing different train discovery aspects to be considered.
Figure 64 shows the situation each UE connects to the correct eNodeB of the train.

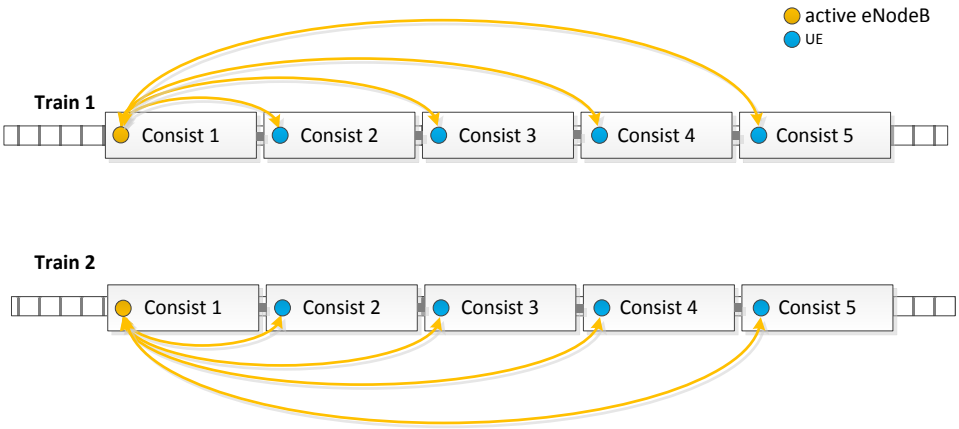


Figure 64: Train discovery result example 1

Figure 65 describes the case when a UE of train 1 connects to the eNodeB of train 2. This case will be resolved because it looks for the train as a powerless consist (see also chapter 3.1.1.3.4). Also train will ignore the UE of train 1 and disconnect the UE of train 1 when its train discovery phase has been finished

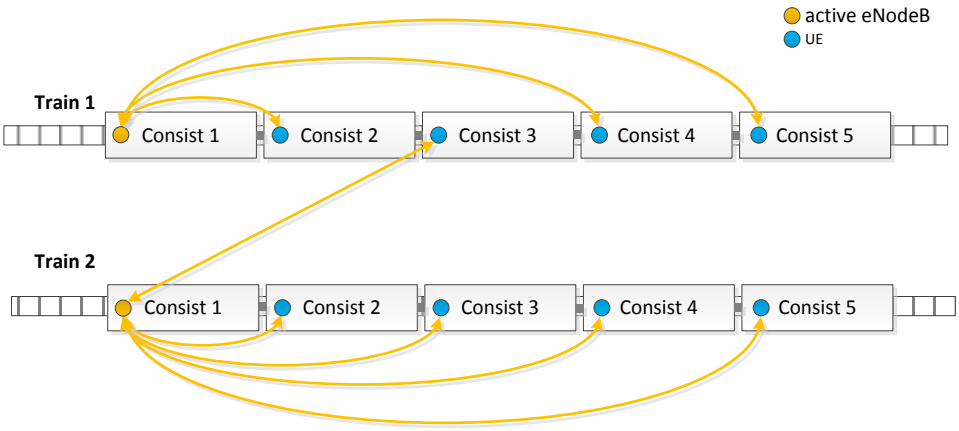


Figure 65: Train discovery result example 2

Figure 66 describes the case when 2 UE of train 1 connects to the eNodeB of train 2. Also this case will be resolved because it looks for the train as 2 non-successive powerless consist (see also chapter 3.1.1.3.4). Also train 2 will ignore the UEs of train 1 and disconnect the UE of train 1 when its train discovery phase has been finished.

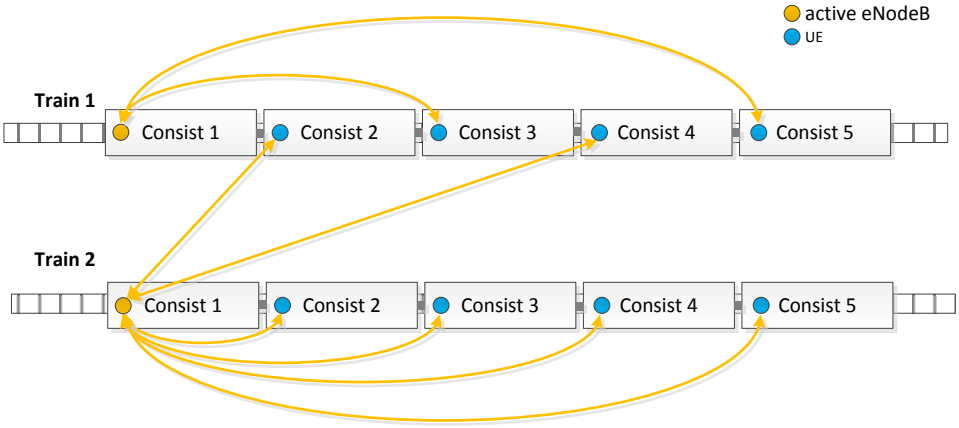


Figure 66: Train discovery result example 3

Figure 67 describes the case when 1 UE of train 1 connects to the eNodeB of train 2 and 1 UE of train 2 connects to the eNodeB of train 1. This case will be resolved as well because it looks for train 1 and train 2 as powerless consist (see also chapter 3.1.1.3.4). Train 1 will ignore the UE of train 2 and train will ignore the UE from train 1. Both foreign UEs will be disconnect when train 1 and train 2 discovery phase has been finished.

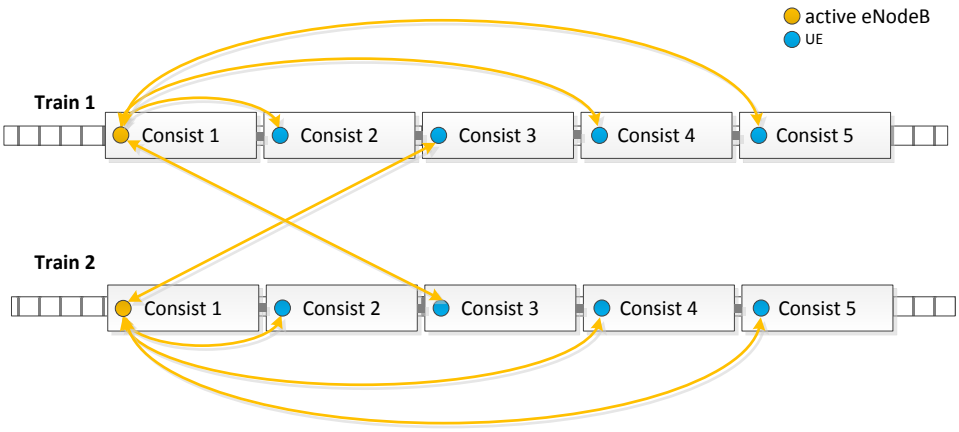


Figure 67: Train discovery result example 4

Figure 68 describes the case when 2 consecutive UEs of train 1 connects to the eNodeB of train 2 and 2 consecutive UEs of train 2 connects to the eNodeB of train 1. This case can result in a deadlock because both trains are not able to disconnect the foreign UEs. This situation can be resolved by disable the eNodeB for randomly short time (e.g. 1 sec +/- 200 ms). After enable again the discovery phase will be executed again. The case that the same deadlock as before appears again is close to impossible.

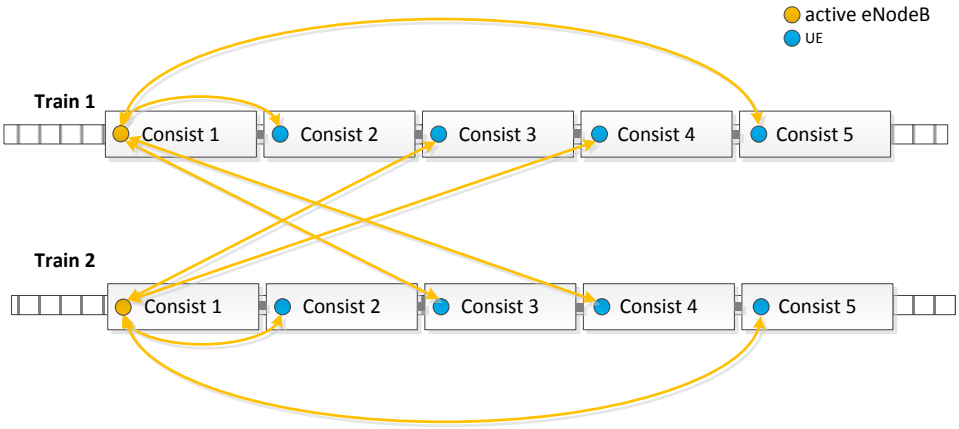


Figure 68: Train discovery result example 5

3.1.1.4 Variant D

This variant looks similar to Variant C (see chapter 3.1.1.3) with the difference that the active eNodeB at the end of the train connects step by step with al consist in the train.

3.1.1.4.1 Establish train wide LTE network

After the train is powered, there is one dedicated consist at one end of the train e.g. leading consist which is switching active its UE end eNodeB. All other consist in the train activate the UE only (see Figure 59). The white list at the active eNodeB is empty. No UE can connect to the active eNodeB.

Discovery Sequence:

1. In a first step the WCSC of the active eNodeB enables the active eNodeB by writing the white list to only accept the own and the next neighbour consist UE to connect.

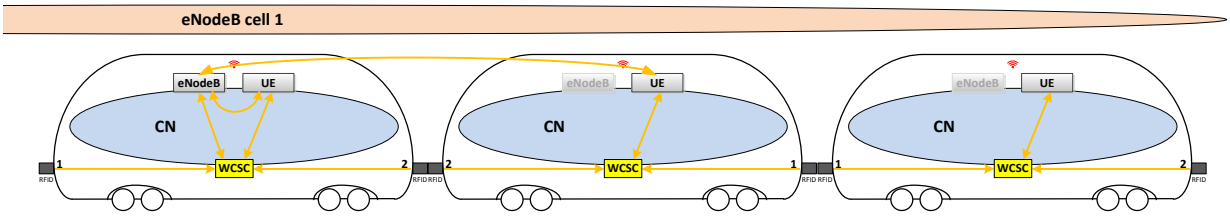


Figure 69: Abstract view of three consists with master eNodeB add train end initial step

2. As soon as the next neighbour UE is connected to the active eNodeB, the WCSC of the active eNodeB requests the coupler data from the WCSC of the next neighbour and includes the received UE ID into the white list of the active eNodeB.
3. Step 2 is repeated until the received coupler data indicates that there is no next consist coupled and the second end of the train has been reached. With this step the discovery is completed.

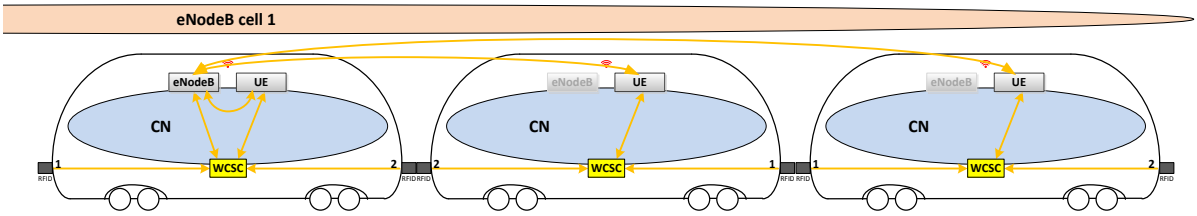


Figure 70: Abstract view of three consists with master eNodeB add train end, discovery completed

3.1.1.4.2 Selection of the master eNodeB

The selection of the master eNodeB is same than for the Variant C chapter 3.1.1.3.3.

3.1.1.4.3 Powerless consist handling

In the case one or more consists are missing a manual handling (train correction) needs to be applied.

3.1.1.4.4 Lengthening/Shortening detection

Lengthening and shortening of the train is handled in same way as for Variant A chapter 3.1.1.3.5.

3.1.1.5 Conclusion

The table below gives an overview about the pros and cons of each train discovery variant:

Table 8: Train Discovery Conclusion Matrix

Variant	Complexity of Discovery Algorism	Achievable Discovery Time	Complexity on resolving Powerless Consist	HW Effort	Max number of active eNodeB [2)]
A	high	long, will not meet requirement SRWTCMS_051	high	middle	500

Variant	Complexity of Discovery Algorism	Achievable Discovery Time	Complexity on resolving Powerless Consist	HW Effort	Max number of active eNodeB [2)]
B	high	long, will not meet requirement SRWTCMS_051	high	high	500
C	low	short, will meet requirement SRWTCMS_051 [3)]	low	low [1)] / middle	50
D	low	middle, hard to meet requirement SRWTCMS_051	high	low [1)] / middle	50

[1)] For the case that e.g. coach needs to have an eNodeB.
[2)] Assumption: Max number of active eNodeB = 50 trains according requirement SRWTCMS_149 * each train contains 10 consists. In variant C UEs of other trains can interact with eNodeBs of a train (see chapter 3.1.1.3.6).
[3)] Risk that in worst case the inauguration time requirement (SRWTCMS_051) will be not met.
Looking at the table above the discovery variant C provides the most advantages even there is very small probability that the inauguration time requirement (SRWTCMS_051) is exceeded in worst case.

3.1.2 Safe Train Inauguration (Distribution of Train Inauguration Results)

After the train discover phase has been completed, the train inauguration procedure starts in order to enable each ED in the train retrieving the train configuration (result of train inauguration).
This is necessary because the white list of the eNodeB contains an unsorted list of the consist IDs only (see also chapter 3.1.1). Among other parameters like vehicle properties, the train configuration contains the safety related order and orientation of each vehicle. The WLTB inauguration is working similar to the procedure for ETB (see IEC 61375-2-5 [78], TTDP message description).
A dedicated device in each consist sends a topology telegram about its neighbour discovery to all other dedicated devices in the other consists of the train multicast via the WLTB. In principle, this dedicated device can be any safe device in a consist. Because the train inauguration is safety related it makes sense to use a simple safe computer than a complex and expensive safe WLTBN for this purpose.

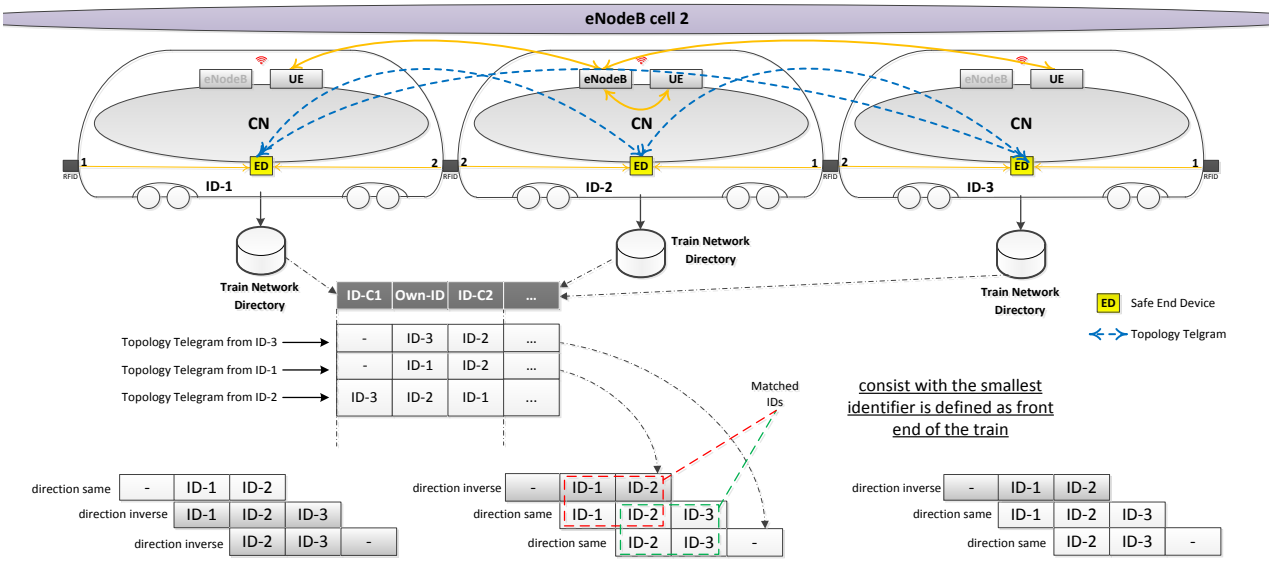


Figure 71: Safe Train Inauguration Procedure

With the topology telegram of all other consists the dedicated device of each consist is able to calculate an ordered and oriented list of all vehicles in the train and stores it in the train network directory. The dedicated device in each consists has to sort the train network directory in a way that it contains the order and orientation of each consist and vehicle (see also Figure 71 for details). The train inauguration procedure follows the following rules:

- The consist at the end of the train which has the smallest consist identifier is defined as the front end of the train.
- The front end consist of the train has the consist number 1
- Subsequent consists in the train with the reference direction 2 are numbered in ascending order staring with 2 and ending with consist number of the bottom consist.
- The train reference direction always point in the direction of the consist at the front of the train (see Figure 72).

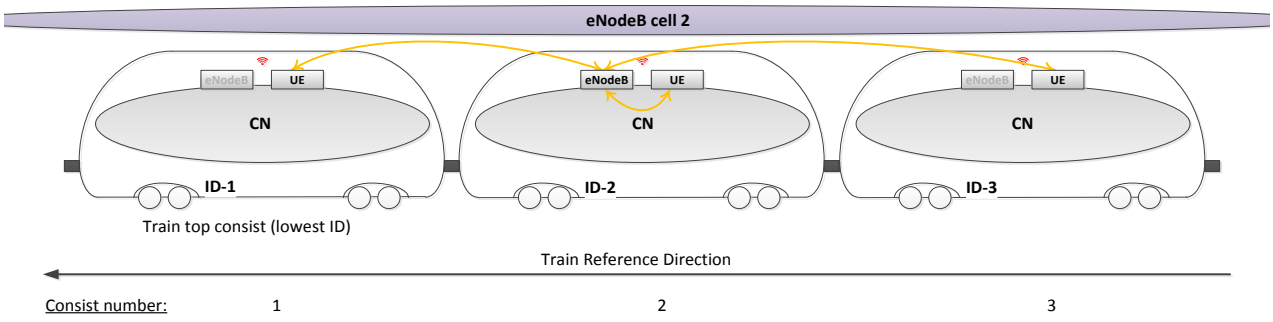


Figure 72: Train top consist reference

3.1.3 Regular Communication between End Devices in different Consists

According to [69] for the train-wide communication between TCMS End Devices the following main data classes have to be considered:

- Process Data including Supervision Data (according to [77], Annex A), latency <= 3..5 * cycle time
- Message Data (according to [77], Annex A), latency <= 250 ms
- Best Effort Data (IP), latency <= 250 ms

If at application level URI-addressing and address translation is used, it shall be used like defined in [77]. IP-addressing shall be done according to [78].
Specific attention shall be paid to WLTBN Dynamic IP Routing Management (according to [78]). While unicast routing tables of the WLTBNs are updated using the Train Topology Discovery Protocol results, multicast routing tables of the WLTBNs need to be updated after each new inauguration or when a new multicast group shall be used (see [78]).

3.1.4 Safe Communication between End Devices in different Consists

For the train-wide safe communication between TCMS End Devices the following main data classes have to be considered:

- Process Data (according to [77], Annex A)
- Message Data (according to [77], Annex A)

For the safe communication (up to SIL2) for both data classes [77], Annex B shall be applied. It defines the Safe Data Transmission Protocol SDTv2 as a mean to create a safe communication path between a safety related data source and one or multiple data sinks. Figure 73 shows the logical communication layers adding the SDTv2 protocol.

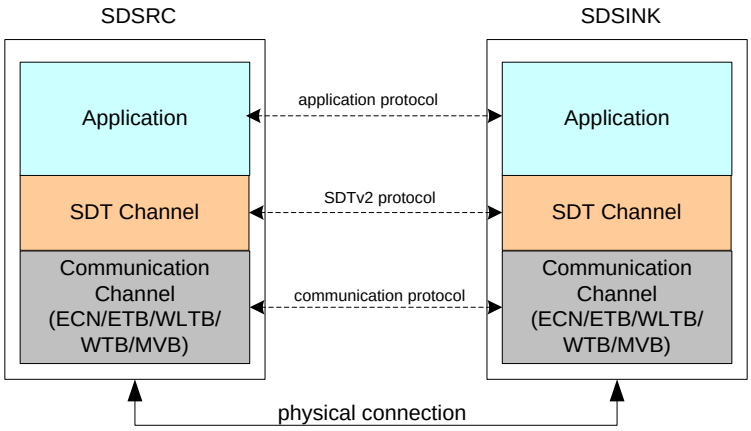


Figure 73: Logical Communication Layers

3.1.5 Interfaces and Services for Train Discovery

In order to control the train discovery a TCMS end device (WCSC) is used. This end device is connected with the LTE equipment and with the couplers on both ends, as depicted in Figure 49. A protocol (see 3.1.6) is using services provided by the LTE equipment and couplers to handle the train discovery. The following chapters are listing services considered to be used for these purposes.

3.1.5.1 Coupler services for WCSC

Message/Process data interface to exchange data with RFID units (coupler 1, coupler 2).
Services:

- **Configuration:**
  - get RFID information
- **Status:**
  - get coupling state (isCoupled)
  - get coupling information (peer RFID information)

3.1.5.2 LTE eNodeB services for WCSC

Message/Process data interface to exchange data with LTE eNodeB unit.
Services:

- **Configuration:**
  - get white list[6] entry/entries
  - set white list (add or remove entry/entries to/from the list)
  - set master/backup mode?
- **Status:**
  - get number of connected UEs
  - get new connection trigger
  - get connection lost trigger
  - get details of connected UE
    - RFID
    - Consist ID
  - get connection details (e.g. link quality, transmission rate, link error)
- **Control:**
  - activate/deactivate eNodeB
  - allow/deny connections
- **Communication:**
  - Data exchange with connected UEs
  - Routing between connected UEs

3.1.5.3 LTE UE services for WCSC

Message/Process data interface to exchange data with LTE UE unit.
Services:

- **Configuration:**
  - get identification information
  - set identification information
    - RFID
    - Consist ID
- **Status:**
  - get connection state information
  - get connected trigger
  - get connection lost trigger
  - get details of connected peer eNodeB
    - eNodeB ID?
  - get connection details (e.g. link quality, transmission rate, link error)
- **Control:**
  - connect UE to remote eNodeB
  - connect UE to local eNodeB
  - disconnect UE from an eNodeB
- **Communication:**
  - Data exchange between UEs
  - Routing between connected EDs

3.1.6 Train Discovery Protocol

As already written in 3.1.1, 3.1.1.1.1, and 3.1.1.1.3 the LTE based network components need to be connected in a proper way, constituting a communication network that enables the train

[6] The white list contains a list of UEs which shall be able to get access to the eNodeB, establishing a data connection.

inauguration according to [78]. At the moment LTE network technology does not offer an appropriate mechanism to achieve train discovery and setting up a wireless train backbone for communication. An additional application, running on a TCMS end device (or at the UE device), has to support the train discovery by controlling the LTE equipment by using offered services (see 3.1.5) and a control protocol (e.g. named “Train Discovery Protocol”). Such a protocol does not exist yet and needs to be defined and implemented.

3.1.7 Train Inauguration Inhibit

A train inauguration happens normally always if there is a change in the WLTB topology (e.g. caused by a train lengthening or train shortening). However, there might be operational conditions, e.g. during a train coupling, where train inaugurations are not allowed. For this purpose the WCSC provides a function which enables the vehicle application to suppress (inhibit) a train inauguration. In case the application inhibits the train inauguration the current train inauguration results are frozen and no safe train inauguration according chapter 3.1.2 is executed. During train inauguration is inhibited the train discovery is still working but unchanged safe train inauguration results are reported to the application even the train discovery detects coupled or decoupled consists. In case the WCSC detects coupling or decoupling of consist during train inauguration is inhibit the WCSC additionally reports this to the application.

3.2 Operator Oriented Services

3.2.1 Communication Functions

The OOS (Operator Oriented Services) architecture for consist to consist communication has to support the following functions:

- Regular Communication between End Devices in different Consists

3.2.1.1 Regular Communication between End Devices in different Consists

According to [69] for the train-wide communication between TCMS End Devices the following main data classes have to be considered:

- Best Effort Data (IP)
- Streaming Data (RTP), latency <= 100ms for audio, <= 500 ms for video

If at application level URI-addressing and address translation is used, it shall be used like defined [77]. IP-addressing shall be done according to [78].
Specific attention shall be paid to WLTBN Dynamic IP Routing Management (according to [78]). While unicast routing tables of the WLTBNs are updated using the Train Topology Discovery Protocol results, multicast routing tables of the WLTBNs (containing at least 10 static IPV4 multicast routes) need to be updated after each new inauguration or when a new multicast group shall be used (see [78])

3.3 Customer Oriented Services

3.3.1 Communication Functions

Communication functions for COS (Customer Oriented Services) in regard to consist to consist communication are not defined because COS data is not supposed to be handled on train backbone level at all.

3.4 REDUNDANCY

3.4.1 Train Backbone Redundancy

As described in Figure 48 the architecture contains two train backbones at least. One for the TCMS domain and one for the OOS and COS domain. For train operation it is absolutely necessary that TCMS can communication over train backbone. For train operation it is acceptable that OOS train backbone communication is not available. In case the TCMS is disturbed (e g. by a jammer), the LTE backbone used by OOS (and if not disturbed) can be switched off for OOS. The now released frequencies are taken over by TCMS.

3.4.2 Train Backbone Device Redundancy

To increase the availability of the WLTB in a consist, at least the controlling end device (WCSC) as well as the UE of a consist need to be redundant, see Figure 74. Both UEs of a consist shall have the same ID. Only one UE shall be active.
Due to the fact that, except in case of LTE train backbone discovery, there is only one eNodeB per train active, redundant eNodeBs are not necessary.

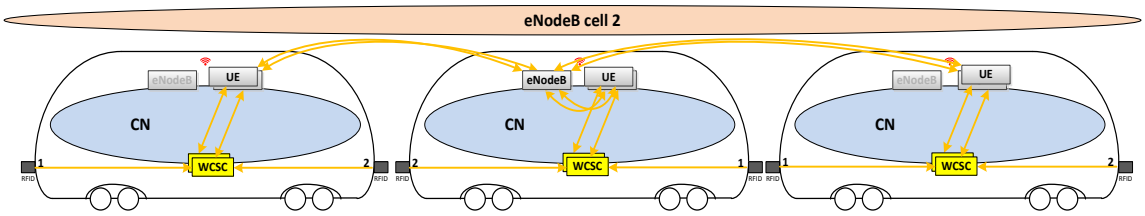


Figure 74: Abstract view of three consists with redundancy

Depending on availability requirements for a consist it is also possible to implement redundant WLTBNs (eNodeB and UE) and antennas (see Figure 75 and Figure 76).

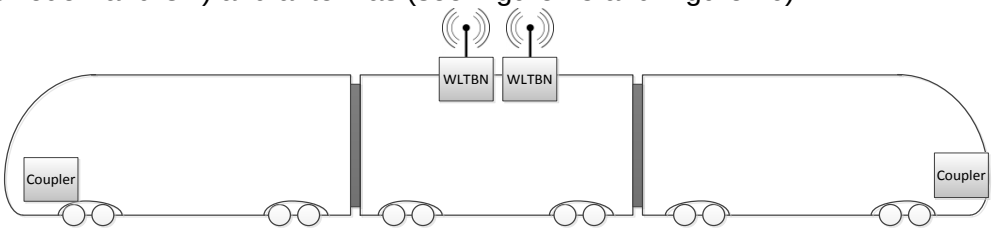


Figure 75: Redundant WLTBN with omnidirectional antennas

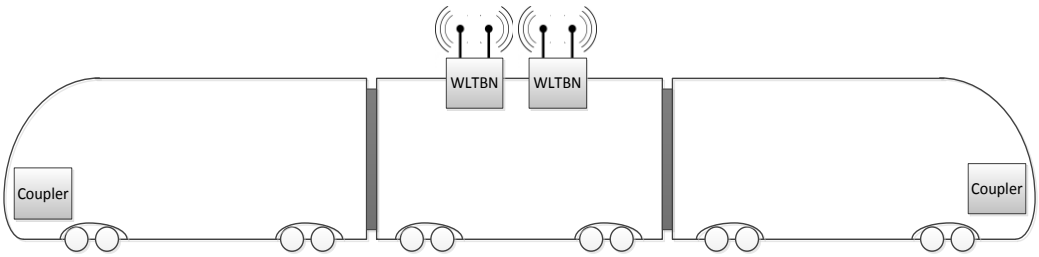


Figure 76: Redundant WLTBN with directional antennas

3.5 SECURITY

As already described in Figure 48 the train backbone communication for the safety related TCMS domain is separated from the OOS domain by using its own train backbone. All data transferred for the TCMS domain via WLTB has to be encrypted (see also chapter 4.3.1). This is needed to avoid that data transferred via WLTB can be used to get information about train operation. Same is needed for OOS train backbone for sensitive OOS data. Since LTE provides encryption mechanisms by design it can be used for both train backbones.
For safety related data safe data transmission has to be used additionally (see chapter 3.1.4).

3.6 FREQUENCY BAND, BANDWIDTH AND COVERAGE

The IEEE 802.16 standards mentioned in the previous chapters are characterized by different used frequencies bands, duplex modes (FDD, TDD) and possible transfer rates.
Since here only the technology will be evaluated, a choice of one or more (for the use of frequency diversity against jamming attacks) frequency bands will be not yet done.
Even the LTE bandwidth is still a bit below 100Mbit/s, the technology is interesting for the rolling stock use case since we will see an increase of the bandwidth in the coming years. Thus LTE as a train backbone gets even more interesting for the OOS and COS domain.
The recommendation for absolute and relative speed out of [69] still needs to be verified.
To avoid interferences with the telecommunication LTE bands in future, it would make sense to reserve at least in Europe a dedicated band for the railways.

3.7 WLTB ANTENNAS

Due to the use of an additional element (Coupler) to ensure consist to consist safety functions (orientation, identification), the location and antenna installation doesn't need to consider the directions of a train backbone signal has been received (see also Figure 77 and Figure 78).

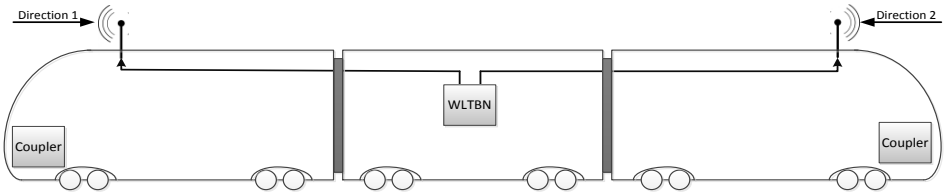


Figure 77: Architecture using 2 directional Antennas

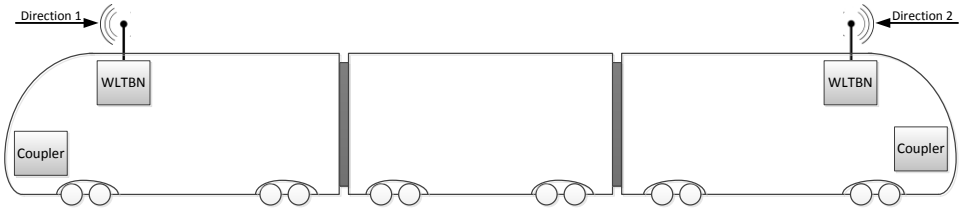


Figure 78: Architecture using 2 WLTBN

Therefore the antenna can be installed at one place of the consist. Due to the fact that LTE is able to cover transmission distances more than the worst case length of a train, one omnidirectional antenna per consist fits to the communication needs (see Figure 79).

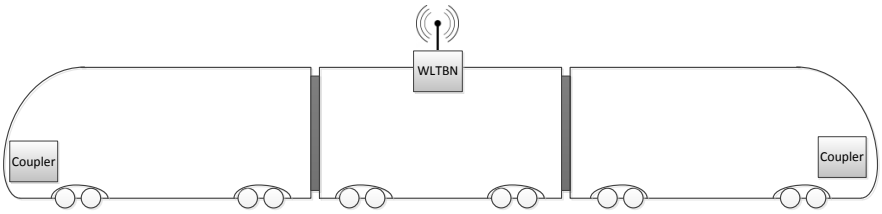


Figure 79: Omnidirectional antenna

In order to reduce the transmission power for the LTE and minimize wireless connections from consists located in nearby racks, it would be possible to think about using 2 directional antennas instead of Omnidirectional antenna (see Figure 80).

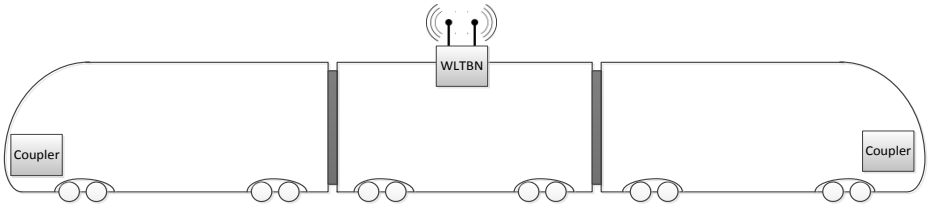


Figure 80: Directive antennas

But, finally, the use of directional antennas has been discarded due to:

- Suppliers of Radio components are the ones to design and implement the suitable solution to minimize power transmission, selecting the best transmission profile at any time for each solution.

- The use of couplers provides, in addition to orientation resolution, identification of consists, so this removes the need to minimize wireless connections from consists located in nearby racks. In fact, directive antennas would only partially mitigate that situation, as the lobe radiation angle of the antenna would have had to be at least wide enough to allow communications in curves, limiting the effectiveness of that measure.

4 WIRELESS ARCHITECTURE FOR INSIDE CONSIST COMMUNICATIONS

This chapter deals with the communication architecture inside of a consist. Nevertheless most of the perceptions in this chapter are also valid for a single vehicles in a consist. If not specially mentioned the following information is valid for a consist as well as for a vehicle.

4.1 FUNCTIONAL DOMAINS

All functions in a vehicle or consists and thus the related communication demand inside of a consist and from one consist to another consist can be grouped in 3 domains:

- Train Control and Monitoring System (TCMS)
- Operator oriented Services (OOS)
- Customer oriented Services (COS)

A special group of vehicle functions are the safety related functions (SIL2) which are located in the TCMS area only.
Typically the predominant communication demand is inside the domains. But there is also need for an inter-domain communication to exchange data. An assignment of the different vehicle functions to the domains has already been evaluated in chapter 2.2.

A special group of vehicle functions are the safety related functions. But this group is totally included in the TCMS domain. This group does not need a separate communication domain because the safety functions are implemented in such a way that a safe communication channel is not needed. Instead the normal non-safe TCMS domain communication channel is used and the communication is secured by a special transmission protocol (see chapter 2.3.2.1).
In order to ensure a separation between the domains and to ensure the proper category of transmission system according to the EN 50159 [70] standard (see chapter 2.3.2.3) a separation between the domains is necessary. Inter-domain communication is needed between TCMS and OOS on one side and OOS and COS on the other side. A direct communication between TCMS and COS is normally not needed. This leads to the principle network structure in Figure 81.

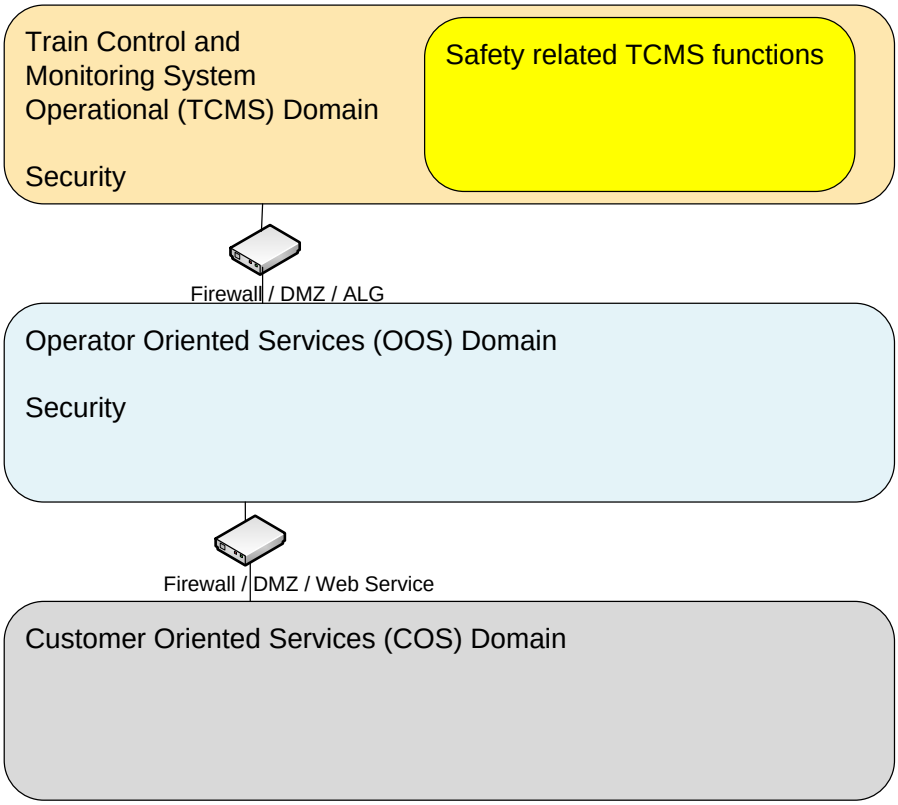


Figure 81: Function domains in a consist network

The separation between the 3 domains can be realized by either

- Physically separated networks which are interconnected by gateways which ensure the required separation regarding security between the networks (as shown in Figure 81)
- Logically separated networks which ensure the required separation by techniques like VLAN (see chapter 2.5.5) and end to end encryption and signature (see [57]). Additional counter measures like QoS (see chapter 2.3.6) are needed to ensure predictable behaviour especially for the TCMS domain.

The latter one is not considered in this document. It has to be further investigated whether e.g. end to end encryption does not have to high demands on the performance of the devices in the system. Another open question is if such a solution will be accepted by the authorities because of uncertain impact on the safety of the consist/vehicle.
In a pre-study [81] Wireless LAN (WLAN) according to IEEE 802.11 standard has been selected as appropriate solution for a wireless consist network. WLAN as standard technology is capable to manage any IP based traffic. So it's easy to integrate into existing ECN solutions. WLAN according

802.11 is a proven in use technology. Devices are available from a wide range of manufactures. The technology is open and no special licence agreements are necessary for the WLCN.

4.2 REDUNDANCY

This chapter depicts redundancy properties of the wireless TCMS consist network infrastructure. Redundancy aspects of WLEDs are not covered. Also not covered is the redundancy aspect for wired devices if the proposed network architecture does include a wired network part (see e.g. chapter 4.8.1).
As shown in chapter 4.6 the WLAN architecture includes 2 hierarchy levels: The Distribution System (DS) to interconnect the different Access Points and the Access Point with the WLEDs as second level.
In the case of ECN as Distribution System (DS, see chapter 4.6) redundancy is covered by the redundancy of the ECN ring structure and well known. All APs can share the same SSID and thus building an ESS. Thus it's possible that a WLEDs is able to associate to any AP in the ESS. Thus the distance between the APs should be selected in such a way that each WLED is in the communication range of at least 2 APs. If one AP fails the associated WLEDs are able to connect to another AP. Maybe signal strength of the new AP is lower. Thus the capacity (speed) of the channel to the new AP may be smaller. But the communication is not interrupted and the network is self-healing.
In a mesh network as described e.g. in 4.8.2 the Distribution System itself is a wireless network. From principle the Mesh Network is a two dimensional architecture. Implementation in a consist is more or less a special case in form of a line. All MSTA are arranged in a chain. Thus distance between the MSTAs must be short enough that the outage of one MSTA can be compensated by a direct communication of the neighbours. Depending on the distance between the two remaining MSTAs the performance may be lower. But communication is interrupted only shortly. The network traffic between the failed MSTA and its associated WLEDs will be spread between the 2 remaining MSTAs. Thus the mesh network is also self-healing.

4.3 SECURITY

Eavesdropping in conventional wired networks requires physical access to the wire or to the network devices. These are typically hidden behind cover panels or installed in cable conduits or placed in closed cabinets. Thus there is a mechanical protection against unauthorized access.
This is in contrast to the wireless technology. Here the air is a shared media and anybody who owns a corresponding equipment and stays within reach of the radio waves can have access to the network. Physical presence is no longer needed.
Suitable countermeasures are encryption and access control. Access control is handled in chapter 4.3.2. A proper encryption and authentication can bring a wireless network to the same level of confidence as a wired network. This is important to apply the same argumentation e.g. regarding closed network to the wireless network.
Another topic to be addressed in the security area in order to support the closed network principle is the separation of the different domains. This is addressed in chapter 4.3.4.

4.3.1 Encryption

At the beginning of IEEE 802.11 WLAN there was no authorization or encryption foreseen in the standard. This defect was closed by the introduction of the WEP extension. But it turned out that this technique has severe flaws. So WEP was replaced by WPA and later WPA2.
WPA was introduced by the alliance of the manufacturers of wireless device as short time reaction on the disaster with WEP.

In parallel IEEE 802.11i was standardized which was also a reaction on the WEP problem. The WPA manufacturer consortium took over major results from 802.11i and published this as WPA2 standard. But WPA2 is not identical to 802.11i[7].
WPA is using TKIP (Temporal Key Integrity Protocol) as encryption standard while WPA2 is using AES (AES Encryption Standard) for message encryption. AES is currently assumed as secure while TKIP is not recommended any more since 2009.
Conclusion is that WPA2 is currently the recommended access method for IEEE 802.11 wireless LANs.

4.3.2 Authentication

Authentication in a wireless network is necessary to identify Wireless End Devices (WLED) and grant them access to the wireless network.
Trustee in a IEEE 802.11 WLAN network is typically an Access Point (AP). Every WLED must authenticate himself at an AP and this AP grants access to the wireless network after a successful validation of the WLED. Mainly tree authentication methods are in place.

Pre-Shared-Key

Using of a shared key (“Password”) is an authentication method supported by all methods described in chapter 4.3.1. This shared key is used for authentication as well as for later encrypting of the messages. A weakness of this shared key approach is that the key must be stored in each WLED and in the AP. So there is a high probability that this key becomes known by unauthorized persons. This probability increases by the number of involved persons and WLEDs. That’s the reason why this approach is used only in the private area or in small companies. In order to handle rail vehicle fleets by vehicle manufacturers and vehicle operators this approach is not recommended.
Another authentication method was introduced mainly for the consumer sector in order to ease up or avoid the direct handling with the Pre-Shared-Keys. In order to have an optimal encryption these keys should be long and complex. But this impedes on the other side an easy setup of the WLEDs.

WiFi Protected Setup WPS

WPS was introduced to ease the setup of wireless devices regarding mutual authorization of Access Points (AP) and wireless devices. The main difficulty in this authorization process is bring the Pre-Shared Key (“WLAN Password”) of the AP to the wireless device. WPS provides an automatism for this key exchange.
There are 2 methods available:

- Authentication by a push button
  The authentication procedure is started by pressing a button at the AP or by enabling the WPS mode e.g. in the administration software of the AP. The first wireless device which tries to connect to the AP will receive the password for the Pre-Shared Key authorization.
- Authentication by PIN
  Here the authentication is done by entering of an 8-digit PIN on WLAN client side. This PIN is provided by the AP and the PIN is used for a multistep authentication procedure.

Both methods have pros and cons. Main problem of the 1st method is that the network communication is not encrypted during the time between pressing the WPS button and the successful authentication. A hacker could use this time slot for an attack. In private or office environments this procedure is not started very often. So the potential security gab is not very big in this case. But during commissioning of a consist this procedure has to be repeated for every wireless device again. Each time there is the vulnerability of the network.

[7] All topics covered by the amendments to IEEE 802-11-2007 (IEEE 802.11i is one of them) are incorporated in IEEE 802.11-2012

At first glance the PIN method seems to be more secure. But here a display is needed at the AP to provide a onetime PIN for the actual authentication. This display is often not available. Instead a static PIN is used. This makes this authentication method also vulnerable. In addition the wireless device must provide a mechanism to enter the PIN. This is often available in consumer products (e.g. mobile phones) but not in in products for automation.
So both WPS methods are not appropriate for railway applications.

IEEE 802.1x Authentication

This method is used for WPA2 (but also used in general for IEEE 802 networks) and in this scope it's often called WPA2-Enterprise or WPA2/802.1x.
Key component of IEEE 802.1x is the Extensible Authentication Protocol (EAP). IEEE 802.1x describes how EAP datagrams are embedded into Ethernet frames. So authentication according to IEE 802.1x is performed on OSI layer 2.
Often RADIUS (Remote Authentication Dial-In User Service) is used in the context of IEEE 802.1x. A RADIUS Server can take over the role of a central Authentication Server. RADIUS is not mandatory in IEEE 802.1x but often used. RADIUS is utilized in a wide range of professional applications from small companies up to the big players in the mobile phone and internet business.
In the IEEE 802.1x with RADIUS authentication process 3 parties are involved (Figure 82):

- Supplicant
- Authenticator
- Authentication Server

In wireless TCMS the WLED is the Supplicant. The Access Point is the Authenticator. The Authenticator can either handle the WLED authentication by himself or forward the request to a central authentication server (e.g. RADIUS). The RADIUS server is only available once in a consist and can be located on any (wired) ED or switch in the consist network. The RADIUS server can be used by all Authenticators (APs) in the consist.

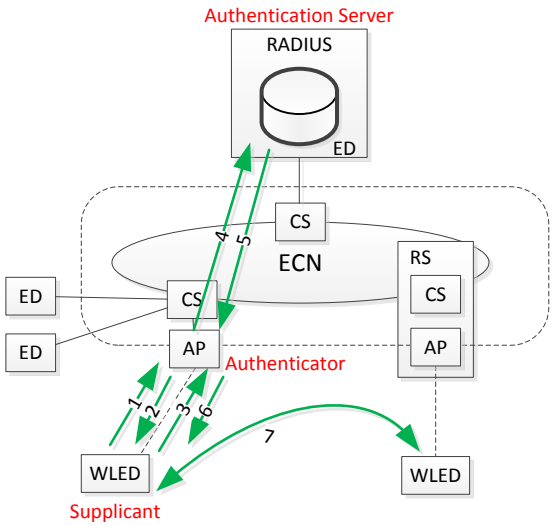


Figure 82: Authentication Process via RADIUS

The authentication process in the wire TCMS can be split into 7 steps:

1. The WLED (supplicant) sends his logon request to the AP (authenticator)
2. The Authenticator send back an authorisation request (e.g. user-name and password) back to the Supplicant
3. The Supplicant sends back the login credentials to the Authenticator.

4. The Authenticator forwards the credentials to the RADIUS server (Authentication Server)
5. The Authentication server checks the credentials and sends back the authentication result to the Authenticator.
6. In the case of a positive authentication the Authenticator enables WLAN access for the Supplicant and sends the necessary network parameters to the Supplicant.
7. The Supplicant connects to the WLAN. Access to other WLEDs is now enabled.

Besides authentication 802.1x can also be used for

- Authorisation
- Accounting
- Assignment of bandwidth (QoS)

Especially authorisation may be useful in the railways sector, e.g. granting access for applications to resources or for a maintenance access. Assignment of bandwidth can be used to restrict the network load of certain WLED (see also chapters 2.3.6 and 4.4).

Remarks:

1. The RADIUS server must not necessarily manage authentication by himself. He can delegate this in a further step to another service.
2. The RADIUS server can act as a RADIUS-proxy. That means there is another (central) RADIUS server in the system. Such a central RADIUS server could be located on the wayside in the operators or manufacturers network. RADIUS server and proxy can be synchronized e.g. vie MCG.
3. Instead of authentication by credentials, e.g. user-name and password, a MAC-based authentication is also possible. But this approach is not recommended. The MAC address can easily be investigated or guessed. This could provoke a security issue.
4. The RADIUS server can also be used for authorisation/authentication of portable devices, e.g. of maintenance staff.
5. Authentication must be done per consist. That prevents devices from connecting to another consist and thus also a direct connection from wireless end devices in different consists. This kind of communication must always be done via WLTB.

For the communication between Supplicant and Authenticator the Extensible Authentication Protocol (EAP) according RFC 3748 is used (Figure 83). Instead of designing a new cryptographic protocol for the EAP communication the authentication part of TLS is used. The secured protocol is called EAP-TLS. For security reasons pure EAP is not used for the wireless TCMS.

Remark: Besides this protocol other standardized protocols (e.g. EAP-MD5, EAP-OTP) as well as vendor specific protocols (e.g. LEAP (Cisco)) are in place.

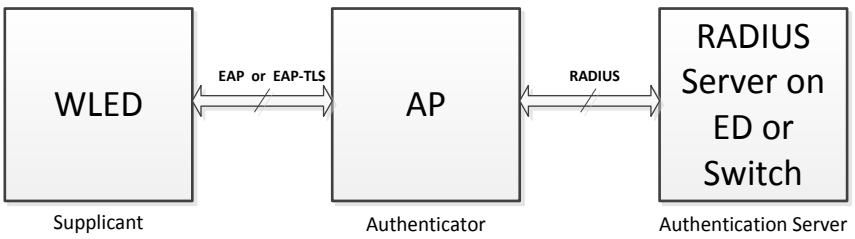


Figure 83: Used Protocols during Authentication

For communication between Authenticator and Authentication Server the RADIUS protocol according to RFC 2865 is used.

4.3.3 Authentication in WLAN Mesh Networks

In chapter 4.3.2 it has been shown how authentication between WLED and an Access Point (AP) is implemented. In this chapter authentication between Mesh Stations (MSTAs) is described.
A WLAN mesh network is a self-organizing network of equal notes (MSTAs). There are no clients and no servers. That means that a centralized authentication as described in the previous chapter with a RADIUS authentication server is not possible here.
Adequate peer-to-peer protocols have to be used for authentication instead. Any peer must be able to initiate an authentication at any time even two peers at the same time.
IEEE 802.11s defines authentication in mesh networks using the “Simultaneous Authentication of Equals” (SAE) protocol. This protocol is password based and used for authentication and encryption key generation.
Password based authentication has a big disadvantage. If the password becomes compromised the network must be assumed as not secure. Another disadvantage is that the password must be stored (and changed if necessary) in all participants of the mesh network.
On the other side the mesh network in the proposed architecture is used only as distribution system (DS). All WLEDs are connected to APs and these APs are then connected to the mesh network. Thus WLED authentication can be done by the mechanism as described in chapter 4.3.2. MSTA authentication could be done by a shared password because these credentials are not needed e.g. for service access.
This point must be investigated further. But caused by this security vulnerability a mesh network is not recommended for network with safety related traffic (e.g. TCMS domain).

4.3.4 Domain separation

As already discussed in chapter 2.5.6 routers and application level gateways (ALG) together with firewalls are appropriate and state of the art measures to separate the different domains from each other. The MCG in the OOS domain which connects the consist with a ground network can be seen as ALG.

4.4 QoS Quality of Service

QoS has many aspects. This document considers management of available bandwidth on OSI Level 2 (Data Link Layer) and robustness against imponderability of the physical media (OSI Layer 1). QoS can also be implemented on the higher level of the OSI layer. But this is then more application specific and not considered here.
As already explained in chapter 2.3.6 WLAN according to IEEE 802.11 did not include any QoS provisions from the beginning. Later on in IEEE 802.11e an enhancement for time sensitive applications was introduced. 802.11e optimizes scheduling of data packets by (a) a prioritization with different levels (EDCA) and (b) a coordination of the transmission (HCCA) so that packet collisions are avoided. EDCA optimizes inside of a device and HCCA optimizes between different devices. WLCN devices shall support IEEE 802.11e.
WLAN uses a shared media. So disturbances are to be expectable and have to be considered.
Source of these disturbances can be:

- Other WLAN systems nearby using the same or a neighbour frequency channel (or other systems like Bluetooth depending on the selected frequency band)
- Field propagation because of obstacles or reflections
- Intentional disturbances (jamming)

One countermeasure which can be helpful for all of these kind of disturbances is OFDM (Orthogonal Frequency-Division Multiplexing). This is a multicarrier modulation technique where the available frequency segment is used by several (orthogonal) sub-carriers. The transport data stream will be split into several sub-streams. Each of the sub-streams is then transmitted by one of the sub-carriers. If one of the sub-carriers is disturbed the data for the related sub-stream is moved to the other sub-streams. So disturbances can reduce the performance. But communication is not

totally interrupted. For intentional disturbances (jamming) this is only valid if the attacker does not use the same technology.
OFDM is only implemented in the IEEE 802.11a and 802.11g, 802.11n and 802.11ac standards (newer standards e.g. 802.11ad, ax are not considered here). 802.11a is not allowed in Europe and Japan because of other services in the used 5GHz band. Here specific variants have been established: 802.11h and 802.11j.
For WLCN one of the standards IEEE 802.11g,n,h or 802.11ac should be used. 802.11h is interesting because of another aspect. This standard describes two additional features which could improve robustness against disturbances. Dynamic Frequency Selection (DFS) allows a dynamic change of the used frequency channel. Transmit Power Control (TPC) allows an automatic change of the transmission power.

4.5 Frequency Band, Bandwidth and Coverage

The different IEEE 802.11 standards mentioned in the previous chapters are characterized by the used frequencies bands and possible transfer rates. Directly coupled to the used frequency band is the possible range between the network participants. In general the possible range is smaller if the frequency is higher. The following table gives a rough overview about the different standards.

Table 9: Overview IEEE 802.11 Standard

Standard	Freq. Band [GHz]			Max. Data Rate[8]	Coverage (indoor)
	2,4	5	60		
802.11 a	☐	☒	☐	54 Mbit/s	35
802.11 b	☒	☐	☐	11 Mbit/s	35
802.11 g	☒	☐	☐	54 Mbit/s	38
802.11 h	☐	☒	☐	54 Mbit/s	35
802.11 n	☒	☒	☐	150 Mbit/s	70
802.11 ac	☐	☒	☐	867 Mbit/s	35

Conclusion of chapter 4.4 was to use either IEEE 802.11 g,h,n or 802.11ac.
The required data according to the Requirement Specification is primarily determined by the needed data rate for video streaming in the OOS domain. The worst case assumption is 64 cameras with 8 Mbit/s for each of them. This means the required bandwidth is approx. 500Mbit/s. Such a bandwidth is only possible with WLAN according IEEE 802.11ac.
For the TCMS domain the required bandwidth of 10Mbit/s is much smaller. WLAN according 802.11n or even 802.11g would be sufficient.
The recommendation for absolute and relative speed out of [69] still needs to be verified.

4.6 Introduction To the Standard IEEE 802.11-2012 LAN (WLAN)

This chapter gives an introduction and an overview about the IEEE 802.11 LAN (WLAN) concepts and entities insofar as needed to understand the presented WLAN usage inside of a consist in the chapters 4.7 and 4.8 . A more detailed overview is given in [81].
The fundamental architectural entity is a Station (STA) which is an addressable instance of a medium access control (MAC) and physical layer (PHY) interface to the wireless medium. The STA represents no more than the message origin and destination. Every 802.11 WLED contains a STA.
The IEEE 802.11 architecture consists of several entities whose interaction provides transparent STA mobility to upper layer. The basic building block of IEEE 802.11 is the Basic Service Set (BSS). The BSS is defined as a set of successfully synchronised STAs. The synchronisation is a process supporting selection of a communication peer in the context of authentication process. The BSS's membership is dynamic (STAs can come within the range or go out of the range). An

[8] Gross bandwidth without consideration of any MIMO (Multiple Input Multiple Output) technique

infrastructure BSS consist of single Access Point (AP) and one or more STAs associated with that AP. The AP acts as a master controlling all STAs in the BSS. The STAs can communicate only via AP. The AP also provides the access to the Distribution System (DS) for all associated STAs. To ensure the required functionality the AP comprises the STA and the interface to the DS.
The DS is a logical architectural entity used to interconnect infrastructure BSSs. The Distribution System Medium and the Wireless Medium, which is the medium used by STAs and AP for their mutual communication, are logically separated. Each logical medium is used for different purposes, by a different entity of the architecture. The logical separation of Wireless Medium (WM) and Distribution System Medium (DSM) is considered to be the key for the flexibility of IEEE 802.11 architecture. The connection of BSSs via DS allows for creating WLANs of arbitrary complexity and increasing coverage.
The connection of BSSs by DS leads to the new level of network hierarchy - Extended Service Set (ESS), which is the union of BSS with the same Service Set Identifier (SSID). In the entire ESS the STAs may communicate and move between BSSs transparently to the LLC (Logical Link Control).
The standard doesn't prescribe any constraint of relative BSSs physical locations. Examples of relative locations are:

- The BSSs are collocated. This relative location can be used for redundancy.
- The BSSs are partially overlapped. This relative location can be used to increase WLAN coverage.
- The BSSs have no intersection.
- More than one ESS can be on the same location.

For the purpose of the integration of 802.11 LAN and non-802.11 LAN (e.g. 802.3 LAN) the logical architecture entity a Portal is defined. All data from non-802.11 LAN enter the 802.11 architecture via a Portal. It is possible for one device to offer both the functions of an AP and a Portal.

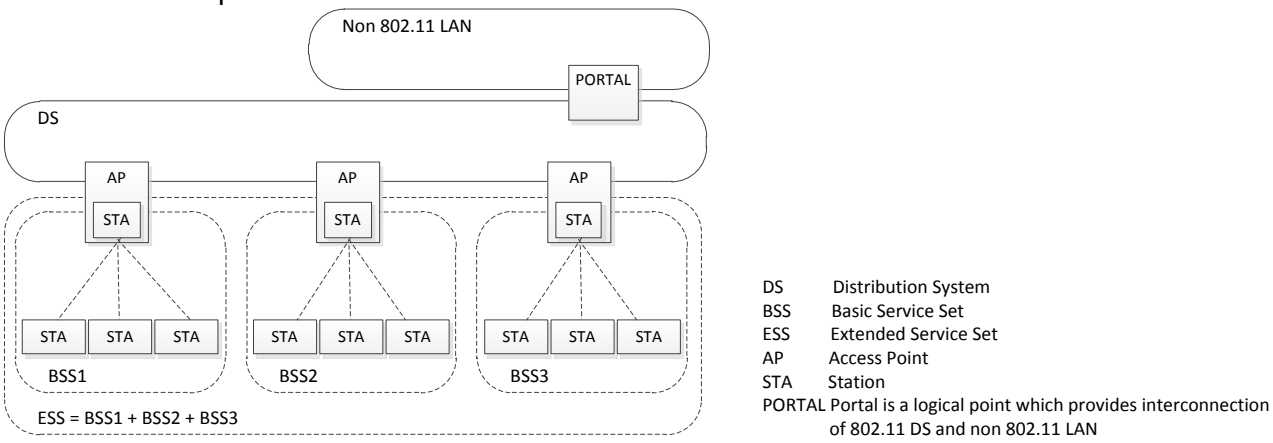


Figure 84: WLAN architecture – infrastructure BSSs

The standard IEEE 802.11 does not specify how the DS should be implemented. Instead, it specifies services. There are two categories of 802.11 services.

- Station Services (SS) – the services that shall be provided by any conformant STA. Authentication, De-authentication, Data confidentiality, MAC Service Data Units (MSDU) delivery, QoS traffic scheduling, Radio measurement are SS, to name just a few.
- Distribution System Services (DSS) - the services that shall be provided by DS, i.e. by PORTALs and APs to forward a data message to the right AP or PORTAL via DS medium. For the message delivery (the task of Distribution service) the DS needs to know which AP provides access to which STA. This kind of information is provided by the association services (Association, Re-association, and Disassociation). The successful association of a STA with the AP is a necessary condition for the STA to send data via that AP. If the distribution service recognises that the message recipient is not associated with any AP, the message is sent to a PORTAL. The messages distributed via PORTAL invoke

Integration service which is responsible for message delivery between a 802.11 DS and a non-802.11 LAN.

The services of both categories are used by the 802.11 MAC sublayer.
An AP shall implement both SS and DSS, a PORTAL only DSS.
The most common implementation of a DS uses 802.3 LAN (Ethernet). Figure 85 shows this option.

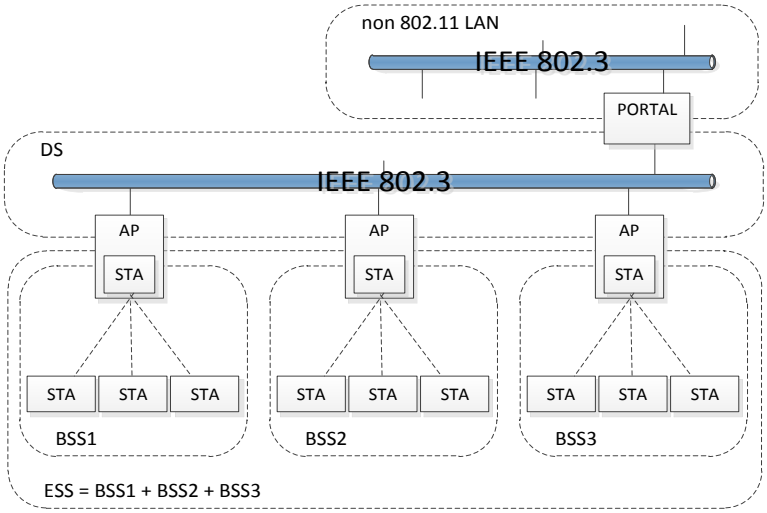


Figure 85: DS implemented as 802.3 LAN

The following 2 subchapters will present 2 alternatives for the distribution system adapted to the already available solutions in the wired TCMS and a new approach based on a wireless hierarchical distribution system.

4.6.1 BSS connected to ECN

This chapter describes the architecture of the network in which the infrastructure BSSs are connected to an ECN. The APs are connected via consist switch (CS) to the ECN, the ECN acts as 802.11 DS. The AP is connected to the CS by wire or the CS and the AP can be collocated in one device, denoted here as Relay Station (RS).
Figure 86 presents two solutions:

- The 802.11 DS shares the same physical medium with the ECN. The implementation of the portal function in each AP is required. A hybrid architecture where wired and wireless EDs are connected to the same ECN is possible.
- The 802.11 DS does not share the same physical medium with the ECN. The main difference from the previous solution is that the portal function is not implemented in each AP. The Portal is here shown as a standalone device acting as interface between 802.11 DS and non 802.11 LAN.

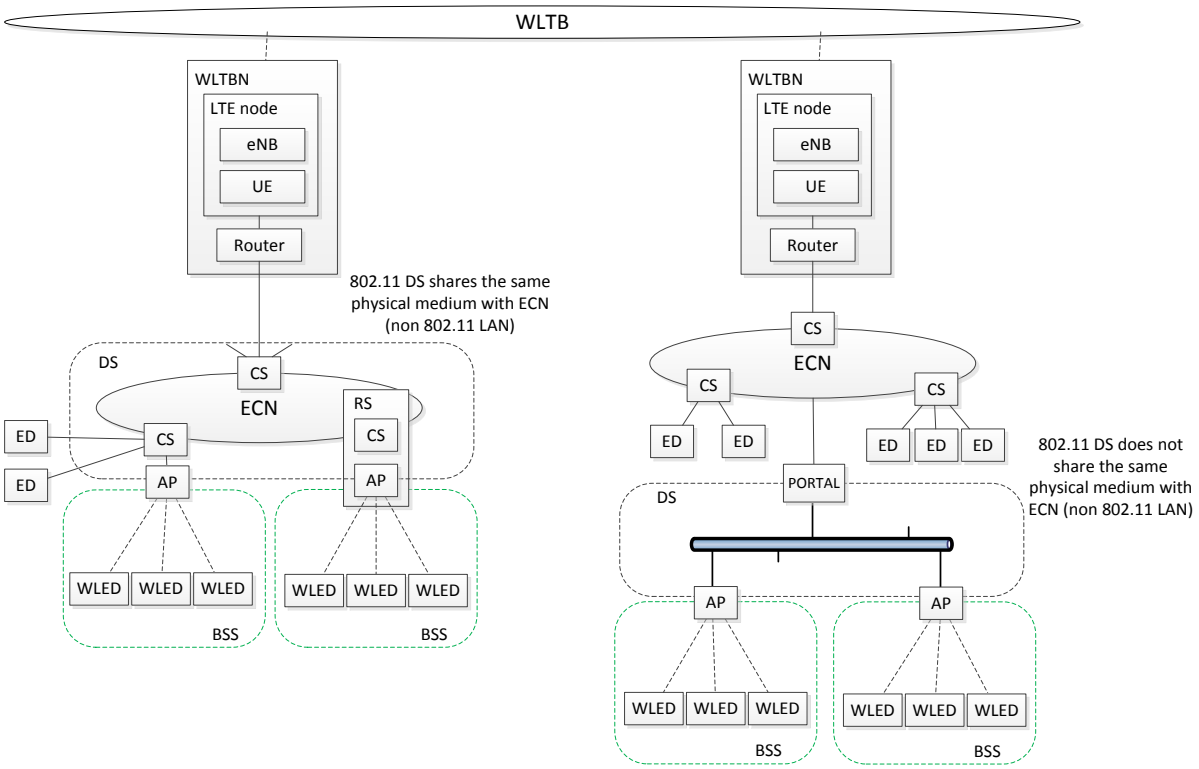


Figure 86: BSSs connected to ECN

Both solutions are predestined for vehicle architectures where WLCN is used in parallel to a wired consist network, e.g. in a transition phase if not all devices connected to the network are available as wireless device.

4.6.2 BSS in WLCN

To fulfil the requirement on the maximum replacement of wired medium the solution shown in Figure 86 can be used. This solution relies on the hierarchical arrangement of 802.11 infrastructure BSSs. The presented architecture has two level of the BSS hierarchy. The first level BSS forms the WLCN, its AP can be connected to the WLTBN by wire or can be collocated in it. The second level BSSs connect WLEDs to the consist network. Figure 87 shows also the collocation of the first level STA and the second level AP in one device – Relay Station (RS), which is depicted in detail in Figure 88.

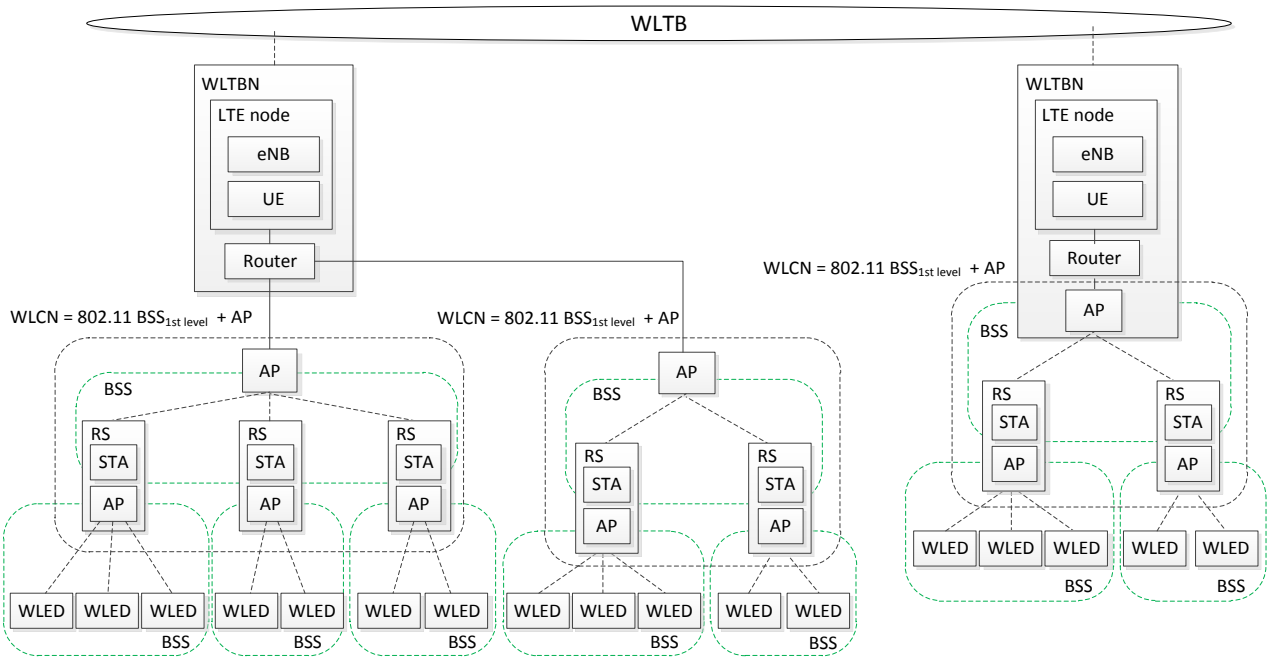


Figure 87: 802.11 BSS in WLCN

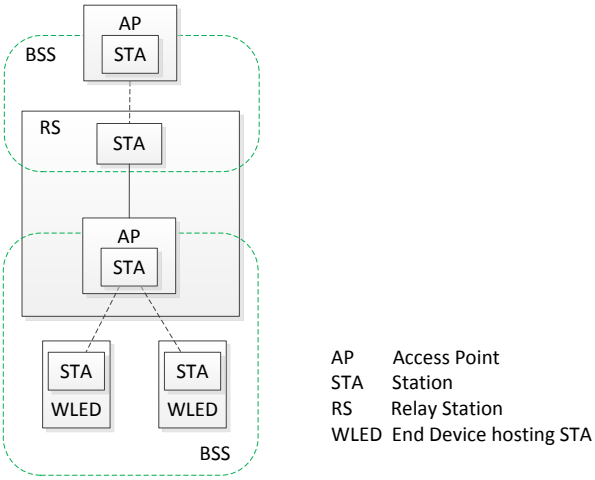


Figure 88: The detail of Relay Station in the hierarchical arrangement of the BSSs

The presented solution has at least the following disadvantage:

- Communication inefficiency when WLEDs from different BSSs of the second level are communicating. Each message will be forwarded via first level AP in this case.

Also, there is a question whether the first level BSS can act as 802.11 DS for the second level BSSs. The 802.11 gives no implementation constraints as far as the DS is concerned, but the implementations of DS are usually based on the assumption that DS medium behaves as a broadcast medium.

4.6.3 MBSS in WLCN

This chapter deals with the use of Mesh Basic Service Set (MBSS) as a wireless DSM (Distribution System Medium). The Mesh Basic Service Set (MBSS) differs from the infrastructure BSS mainly in that that it has no master station like AP. The MBSS is composed of mesh stations (MSTA) which establish wireless mesh links to the mesh STAs in their neighbourhood, thus forming mesh

path from a source MSTA to a destination MSTA (there can be more paths, of which one is selected). All MSTAs can be a message source, sink or propagator. The MBSS transports MAC Service Data Unit (MSDU) between source and destination MSTAs over potentially multiple hops of the wireless medium without leaving the MAC layer at intermediate MSTAs.
Figure 89 shows the so called Infrastructure/Backbone Wireless Mesh Network architecture [82] and indicates how it can be applied in a train (red labels). The infrastructure for clients comprises mesh routers which form self-configuring and self-healing connections among themselves. This infrastructure can be integrated with Wi-Fi networks via mesh routers with gateway/bridge functionalities. The mesh infrastructure shown in the figure can be implemented using different wireless technologies (WLAN, WiMAX). For WLAN: mesh router = MSTA, mesh router with gateway/bridge = MSTA + MGATE.

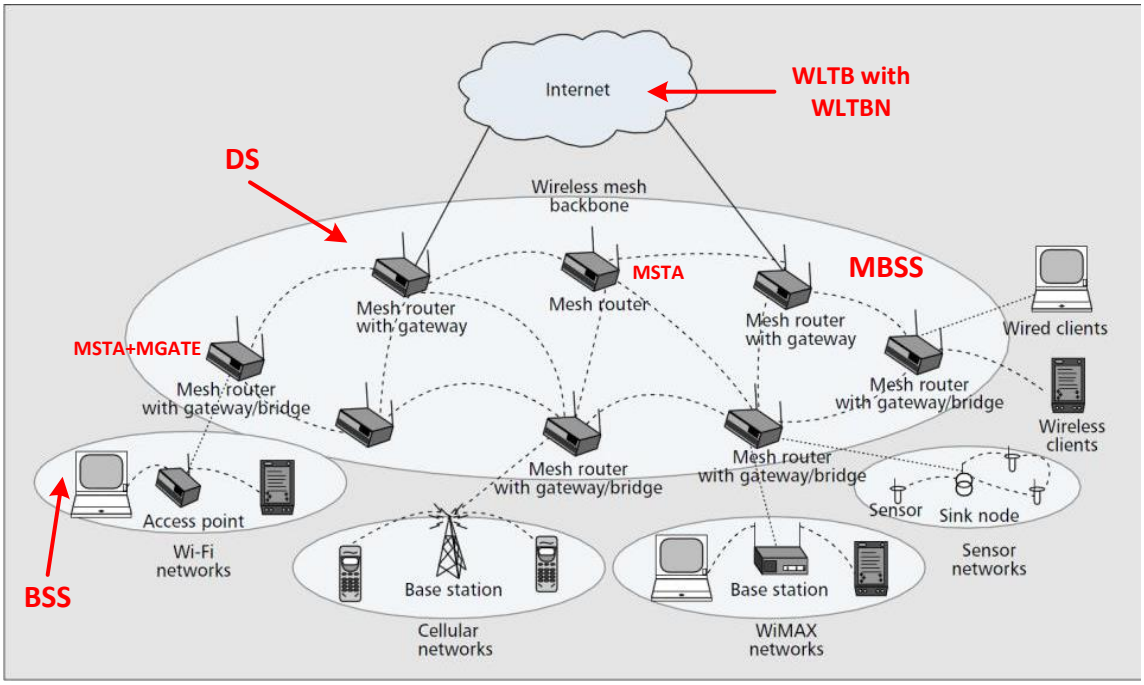


Figure 89: Infrastructure/Backbone WMS [82]

The MBSS, a self-contained network of MSTAs, can be connected to a DS through the logical interface denoted as Mesh Gate (MGATE). The integration of MGATE and AP allows using the MBSS as a DS medium and as such the MBSS is hidden and transparent for non-mesh STAs (WLEDs). As in the infrastructure BSS also in the MBSS the PORTAL integrates non 802.11 LAN and 802.11 DS. In the architecture shown in Figure 90 the PORTAL acts as the interface to the WLTBN. The PORTAL, the MGATE and MSTA can be collocated in a WLTBN.

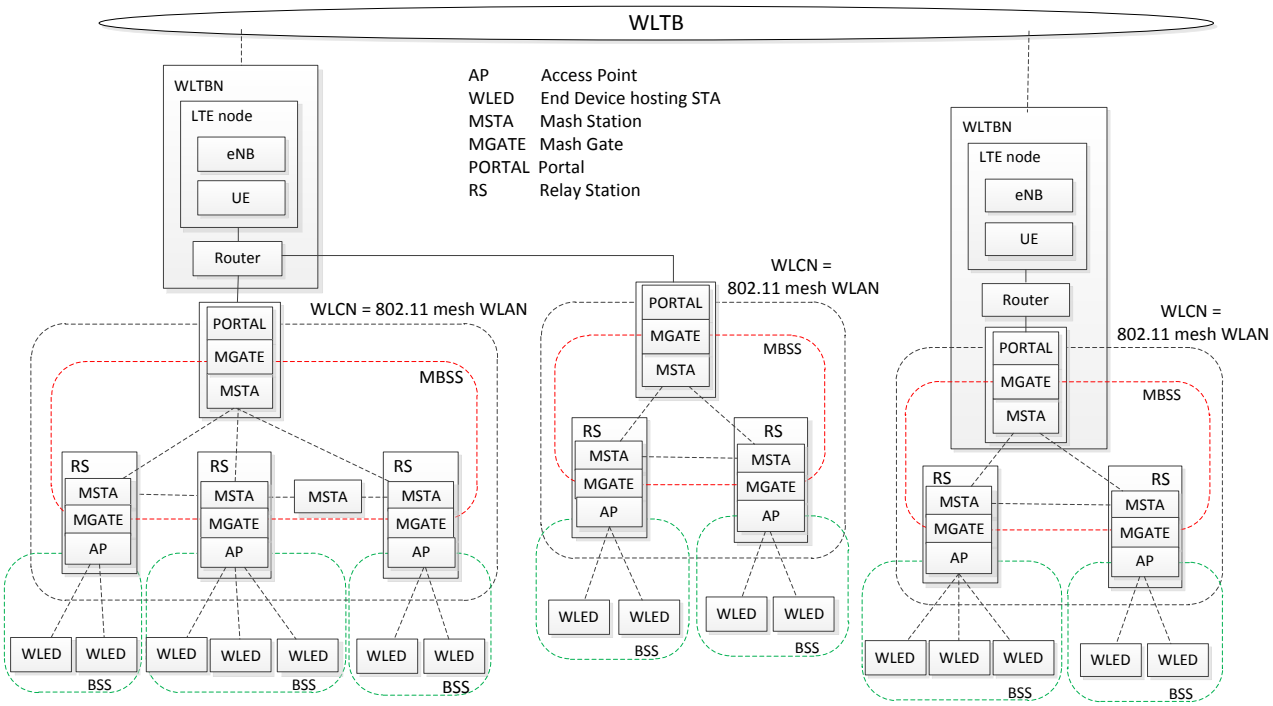


Figure 90: MBSS in WLCN

The Figure 91 shows in detail the interface between the MBSS and BSS. The MSTA, the MGATE and the AP are collocated in one device, denoted here as Relay Station (RS).

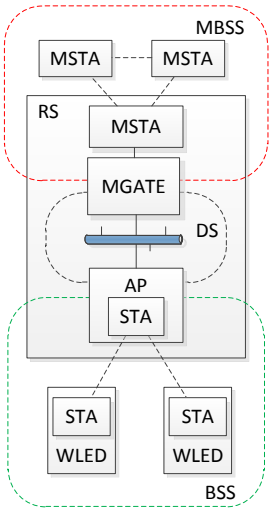


Figure 91: Relay Station between BSS and MBSS

High flexibility of WLAN architecture is illustrated in Figure 92 and Figure 93. Here the consist network combines wired and wireless parts. In one case the WLTBN is connected to the wireless part (Figure 92), in the other to the wired part (Figure 93).

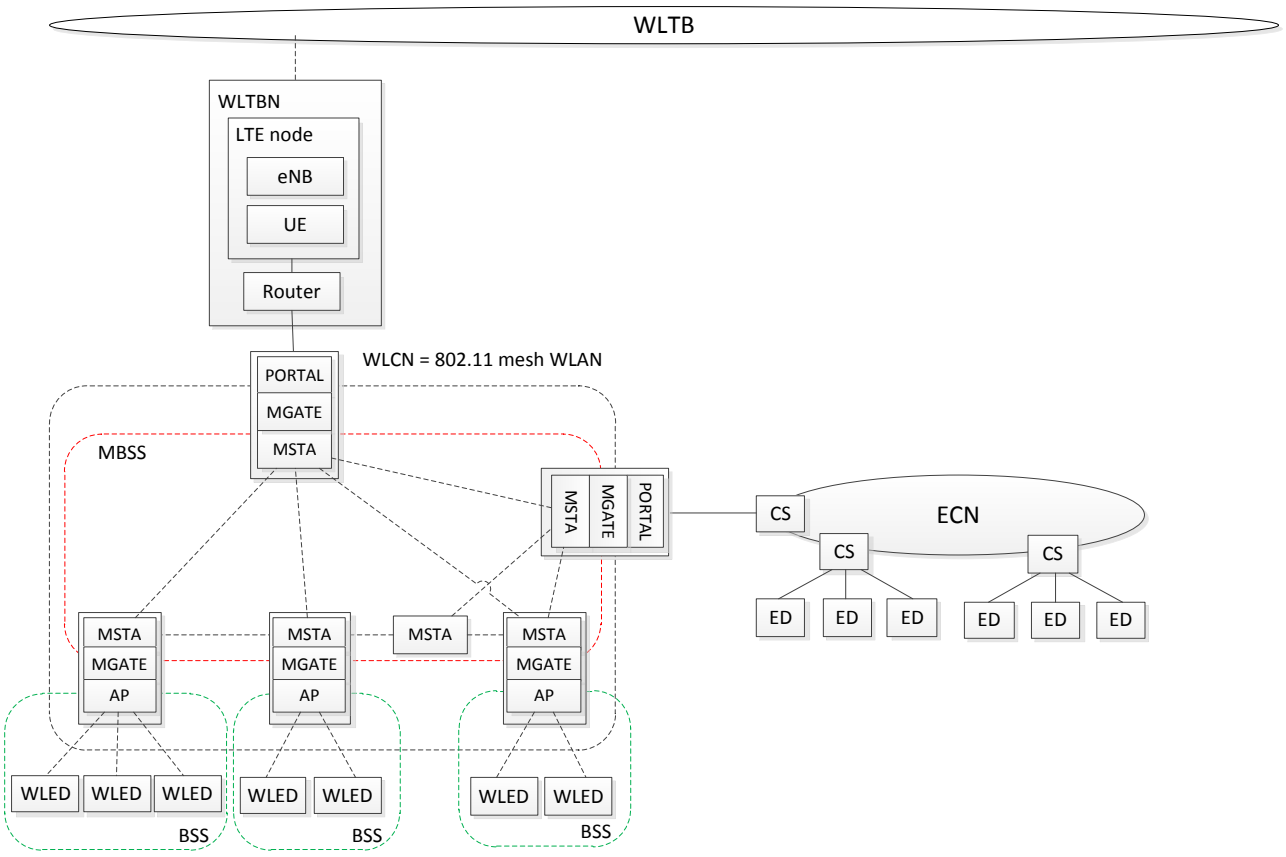


Figure 92: Hybrid consist network I

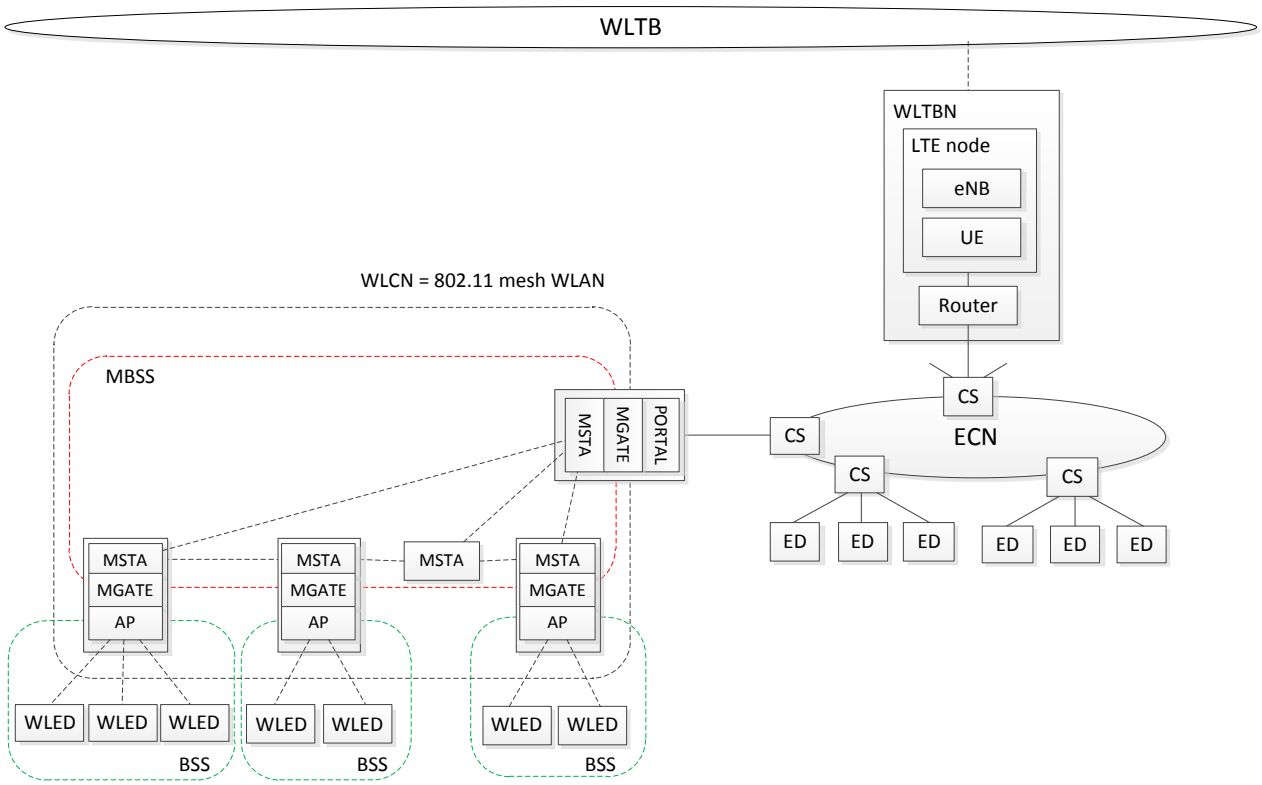


Figure 93: Hybrid consist network II

4.7 RECOMMENDATION FOR WIRELESS COMMUNICATION ARCHITECTURE INSIDE CONSISTS AND VEHICLES

After presentation of several wireless architectures derived from the standard some architecture details for implementation of the wireless link in the vehicle are presented.
Wireless communication inside a consist using a radio link is highly influenced by the physical mechanism of the wave propagation. In the chapters 2.3.1 and 2.3.5 the main aspects have been described. Several technical methods to reduce these effects and improve the communication performance have also been explained. Most of the methods have to be implemented inside the communication devices and can't be influenced by the vehicle architecture. Thus these counter measures are not in the scope of this document.
Nevertheless it's possible to improve the wireless communication inside the vehicle by some architecture and design measures.
For a proper working of the wireless communication inside of a vehicle a stable radio wave propagation is essential. Best would be a line of sight between the involved communication partners (see chapter 2.1). But for sure this is not always possible. E.g. in a locomotive there are a lot of metallic surfaces which leads to very complicated pattern of the reflections. In a multiple vehicle consist it's not the rule that there is a free passage between the vehicles. But even if this free passage is available the line of sight assumption may be wrong, e.g. inside of curves. These constraints can be avoided by a suitable selection of the communication architecture and integration in the vehicle design. In the example in Figure 94 802.3 Ethernet (e.g. ECN) is used as distribution media (see chapter 4.6.1). Here only one AP is used per vehicle. If the vehicle design is more complex (e.g. compartments in the vehicle) and causes difficult wave propagation the number of AP can be increased (e.g. one AP per compartment) to ensure that the direct link between AP and associated WLEDs provides a higher signal strength than the indirect link caused by reflections.

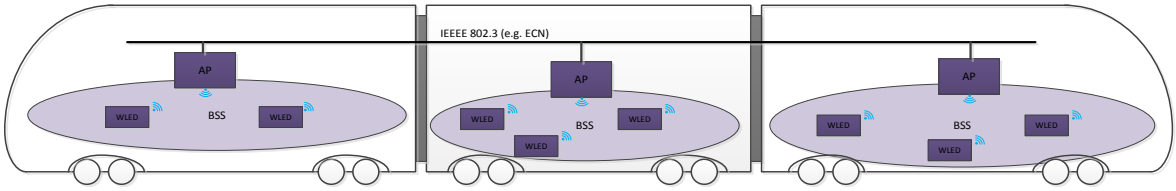


Figure 94: Consist network solution based on a combination of a wired and a wireless part

Disadvantage of this solution is that still a wired connection between the vehicles of a consist is needed. A mesh solution as described in chapter 4.8.2 does not need such a wired part.
While the wired connection between the vehicles of a consist is typically realized in a coupler the connection between the vehicles in the case of a mesh network must be considered separately. The problem here is that the two interacting passage mesh stations (pMTSA), which are realising the passage from one vehicle to the other must have a wireless link to the other MSTAs of the own vehicle as well to the other pMSTA of the other vehicle. That must be ensured by the design of the consist. In the case of a multiple vehicle consist with free passage between the vehicles this is not a problem. If there are constraints or requirements regarding e.g fire protection or costs which lead to a design without a free passage between the vehicles of the consist either special measures are necessary (e.g. non-transparent non-metallic windows on the opposite positions of both vehicles) or the use of the wireless mesh network is even not possible. That must be decided case by case and must not be in contradiction to any other requirements, e.g. fire protection.

4.8 RECOMMENDATION FOR WIRELESS COMMUNICATION INSIDE CONSISTS AND VEHICLES

As described in chapter 2.4 the consist network has to support the logical and technical separation between

- Train Control and Monitoring System (TCMS) and the
- Operator oriented Services (OOS) and the
- Customer oriented Services (COS)

domains.
For each of the domains one of the architectures described in chapter 4.6 can be used. The selection of the concrete technology must be based on the consist requirements and design.
The domains TCMS and OOS on one side and OOS and COS on the other side are interconnected by routers or gateways which ensure a secure separation of the domains which are assumed as security zones. This is state of the art. Precondition is a proper configuration of these devices which have to be ensured by specific security related application conditions.

4.8.1 TCMS Domain

Communication between end devices in the TCMS domain is mission critical. One of the most obvious function of the TCMS network is the safe and secure communication between the end devices to ensure safe functions of the vehicle/consist like safe inauguration and door control. Safe communication can only be ensured if the communication is deterministic with predefined maximum delays. This is difficult to ensure by wireless communication.
More problematic is to ensure the necessary availability requested by mission critical and safety critical functions because the wireless communication can be disturbed by other systems on the track using the same communication channel or even by criminal intent. Due to encryption the safe communication can't be compromised directly but the underlying supervision mechanisms will cause a safe state which means e.g. an emergency stop with negative effect on the availability of the vehicle. There are different possibilities to make the communication system less sensitive for this disturbances (e.g. specific railway frequency band, frequency diversity, refer to 2.3.1). The availability for the different wireless communication technologies, the effectiveness and costs of these solutions need to be evaluated more in detail.
End devices in the TCMS domain are often located in closed metallic cabinets and mounted on the roof and underfloor. This cumbers wireless communication as general communication channel. In some applications it may be adequate to use isolated wireless applications which are connected to the wired TCMS. Safe devices shouldn't be inside this isolated application. Intersection between wired TCMS and wireless TCMS can be realised by

- APs connected to or integrated in a wired ring switch (RS) (see Figure 86) or
- APs integrated in the WLTBN (see Figure 87 and Figure 95)

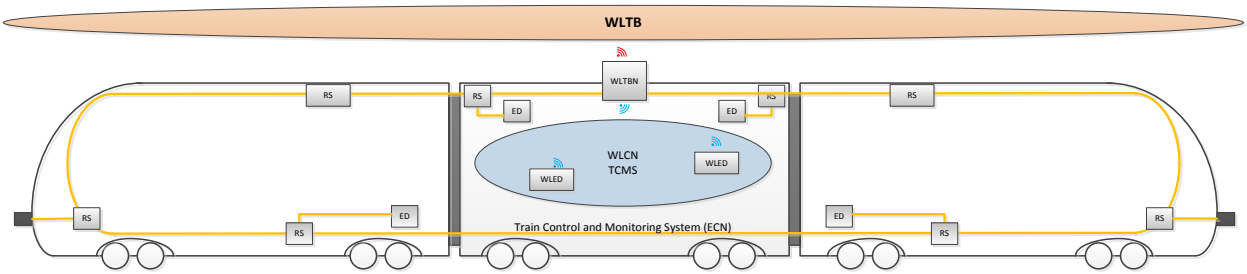


Figure 95: Wired TCMS solution with isolated wireless application in the middle vehicle

Based on the considerations above a hybrid wired/wireless approach is proposed for the TCMS domain. Mission and safety critical EDs (ED-S) as well as EDs not reachable by WLAN because of the vehicle design are connected to the wired consist ring. All other EDs can be connected either

to the wired consist ring or to the wireless network. Later this hybrid approach can be revisited if new developments in the wireless area ensures a disturbance free communication.
The wired consist ring acts as DS for the AP(s) of the WLCN. Authentication of the WLEDs is done by a RADIUS server which can be located in one of the wired end devices, in one of the ring switches or in the WLTBN. The RADIUS server can also be used to authenticate e.g. a PC or portable device which is used e.g. for service access. Due to the usage of a RADIUS server there is no need for a vulnerable common password/key for all network participants. Together with usage of strong encryption according to WPA2 standard the same level of confidence as for a pure wired network can be assumed. Access from the OOS domain is very restricted by a state of the art router/gateway.
In order to allow portable devices (e.g. service PC) to connect even from outside the vehicle (e.g. in the workshop) related measures must be considered in the vehicle design phase (e.g. antennas outside).
The used APs must be able to manage connections with up to 510 WLED. From layer 2 perspective there is no restriction on the number of vehicles in a consist.

4.8.2 OOS Domain

Communication in the OOS domain is not directly mission critical. Thus typical restrictions of the wireless approach as described in the previous chapter are acceptable.
In order to have a maximum effect e.g. on weight and cabling a complete wireless approach in form of a mesh network is obvious. Chapter 5 provides a study for the possible savings in terms of number of devices, cabling and installation costs but also in the fields engineering, commissioning and supply management.
The wireless mesh network is shown in the upper part of the consist in Figure 96. The mesh network covers the complete consist.
A relay station RS includes a mesh station MSTA, a mesh gateway MGATE and an AP. In each vehicle of the consist such a RS is used to connect the mesh network with the WLEDs. Topologies with more than one RS are possible too if one RS can't cover all WLEDs. Between the left and the middle vehicle two mesh stations MSTAs are used to realize the passage between the two vehicles. Between the middle and the right vehicle this is not necessary (e.g. free passage between the vehicles).

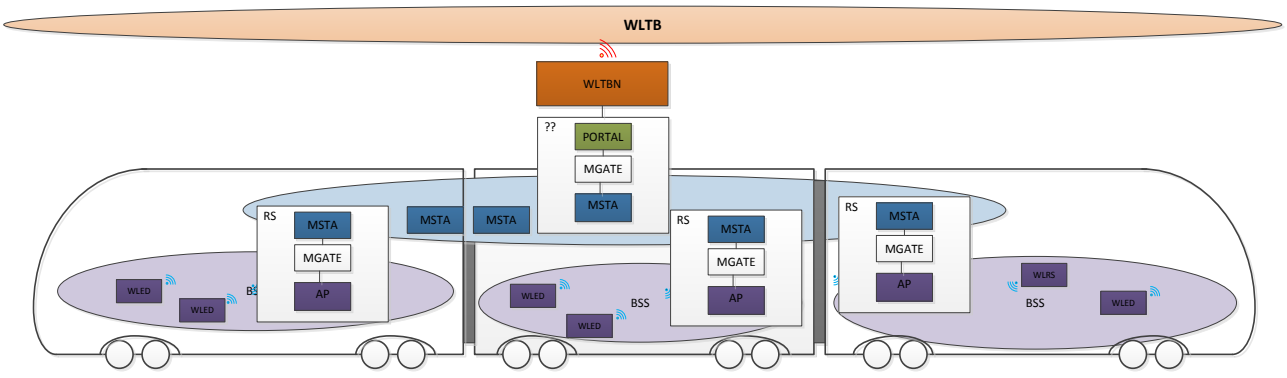


Figure 96: Mesh consist network

Authentication of the WLEDs is done by a RADIUS server which can be located in one of the Mesh Stations (MSTA) or in the device which connects the mesh network to the WLBTN. Disadvantage of this architecture is that authentication of the WLED can only be done after successful establishment of the mesh network.

Authentication for service access can also be done by the RADIUS server. In order to allow portable devices (e.g. service PC) to connect even from outside the vehicle (e.g. in the workshop) related measures must be considered in the vehicle design phase (e.g. antennas outside).
Together with the usage of strong encryption for the mesh network and for the wireless infrastructure connection between WLEDs and APs according to WPA2 standard the same level of confidence as for a wired network can be assumed. Access from the COS domain is very restricted by a state of the art router/gateway.
The used APs must be able to manage connections with up to 510 WLED. From layer 2 perspective there is no restriction on the number of vehicles in a consist.
As described in chapter 4.3.3 all mesh stations are using the same password. This is a potential vulnerability. But the mesh network is not used for service access. So there is no need that the password is shared between several users (especially service and maintenance staff). The password are stored once during commissioning inside the devices. Thus the password can be protected by process instructions.

4.8.3 Combined approach for TCMS and OOS

For cost sensitive vehicles an alternative to the approach to have separated networks for TCMS and OOS could be considered. Here only one ECN for both domains is used. That means that traffic of both domains is sharing the same ring. Nevertheless a logical separation between both domains is vital for security reasons. This can be done by virtual LANs (VLAN). The VLAN concept is switch related. That means that ED are not involved in this concept. In a WLAN network a shared media is used. Thus a VLAN concept can only be implemented if the devices of the different domains are connected to different APs with unequal SSIDs and channels and login.

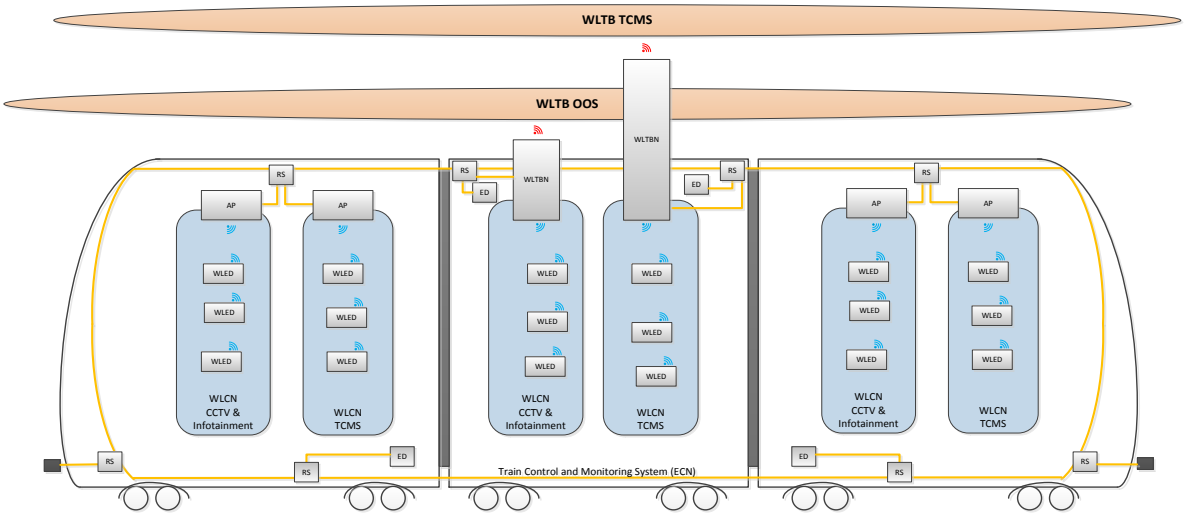


Figure 97: One ring two access points architecture

Besides security the topic QOS must be considered in particular because the required bandwidth for the OOS domain is much higher as for the TCMS domain. And there is a risk that heavy load for the OOS domain may suppress TMCS traffic.

4.8.4 COS Domain

The same chain of ideas for the network structure as used for the OOS can be applied here. The COS domain is also not mission critical and so a mesh network is also appropriate in this case.
In this domain public internet access for passengers is realized by a MCG which is also a WLED. No customer traffic is routed to the OOS domain. But nevertheless the gateway to the OOS

domain must be always state of the art and must be hardened against attacks from the COS domain. This must be ensured also after delivery of the consist.
The used APs must be able to manage connections with up to 510 WLED. From layer 2 perspective there is no restriction on the number of vehicles in a consist.

5 STUDY ON POSSIBLE SAVINGS

5.1 INTRODUCTION

The goal of this chapter is to give some ideas about material and engineering costs in current projects for the function domain OOS and possible savings while using a wireless communication instead of a wired network.

First of all, a summary of OOS functions are given, which are analysed in this document.

Secondly, current solutions for the function domains TCMS and OOS for the communication levels inside vehicle and inside consist are presented.

Thirdly, a wireless architecture for the function domain OOS for the communication levels inside vehicle and inside consist is defined.

Fourthly, engineering and material costs of a “standard” project for both architectures and technologies are presented.

Finally, a conclusion has been added to summarize the results.

5.2 ANALYZED FUNCTIONS OF OOS

Today, following functions are part of the function domain OOS:

- Passenger Information System (PIS)
  - Audio equipment for announcements and intercom
  - Visual equipment for announcements (internal and external)
  - Infotainment displays
- Closed Circuit Television (CCTV)
  - CAM: IP Camera
  - NVR: Network Video Recorder
  - VDU: Video Display Unit

Also part of the OOS domain but not considered in this study are:

- Passenger Counting System
- Seat Reservation System
- LED:
  - LEDF: Frontal LED Display
  - LEDI: Interior LED Display
  - DRM: Dynamic Route Map LED Display

Of course there are also other functions in the OOS domain but this document analyses only the functions PIS and CCTV. It considers the communication levels inside vehicle and inside consist, but not the function level consist to consist.

5.3.1 Current architecture

Two types of network architectures are used in most of current projects:

- 1 wired network for TCMS and OOS together.
- 2 wired networks for TCMS and OOS, 1 network for each function domain. The networks are interconnected via a gateway.

If a mobile crew handheld is required, a wireless network only for this function is added.

The current projects use following technologies:

- Cameras are connected via IP/PoE switch
- Audio components are connected via IP switch
- Displays are connected via IP switch. Daisy chains up to five displays are used.
- Other PIS and CCTV related units are connected via IP switch (not shown in Figure 98).

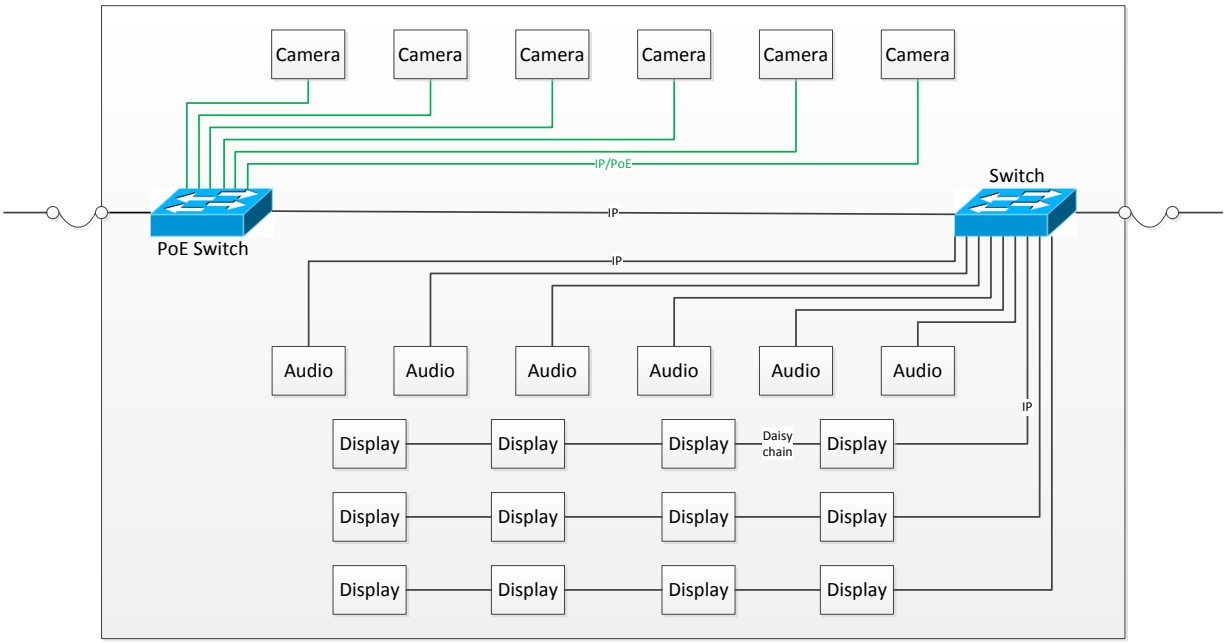


Figure 98: Current OOS Architecture of a car

Explanation:

- Camera = Indoor, front, rear view and pantograph cameras
- Audio = Controllers, amplifiers, passenger & crew communication units
- Display = External front, external side, internal or infotainment displays or dynamic route maps

IP/PoE cameras have only IP connection, no separate power supply connection.

Switches and other IP components have additional, separate power connections (not shown in Figure 98).

Remark: The train level communication architecture (ETB and related cabling) is not shown in Figure 98 but considered later in the calculations.

5.3.2 New Architecture

Supplier and architecture selection is mainly driven by the supplier component costs. The internal engineering effort is not sufficient considered.

Actual projects show that the costs for engineering especially in the area of physical integration is much higher than planned. Cable and harness related updates are big cost drivers.

Therefore a task was started to analyse actual PIS and CCTV related costs of an average project (see Figure 98), which contains:

- 6 cameras per car
- 6 audio components per car
- 12 displays per car
- Additional PIS and CCTV equipment in cab cars (not shown in Figure 98)

This architecture shall be compared with a solution based on wireless network (shown in Figure 99):

- Each car contains 1 MSTA
- MSTA connects all WLEDs (cameras, audio and displays).

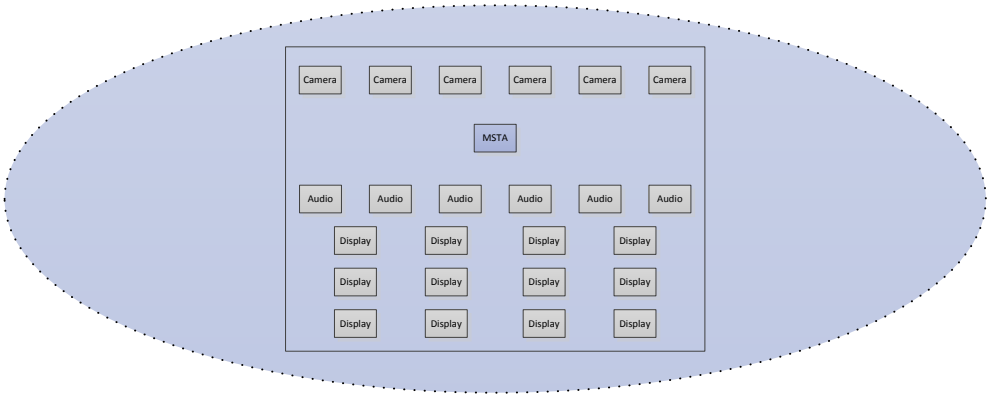


Figure 99: Mesh OOS Architecture of a car

A car is logically interconnected with the neighbour cars of a vehicle via Mesh WLANs.

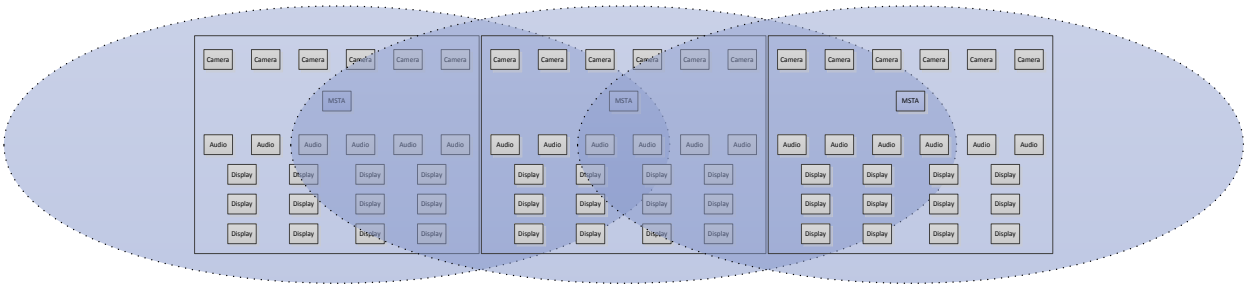


Figure 100: Mesh WLAN in a vehicle of 3 cars

The OOS has following interfaces:

1. To TCMS
   - Driver HMI, to visualize CCTV and PIS data to the driver
   - Train diagnosis, to collect status and diagnostic data

- Train control, to receive train status data for PIS state machine transitions

2. To Wayside:
   - PIS maintenance, to get PIS configuration data
   - PIS connection server, to get real-time PIS data
   - Wayside HMI, to visualize CCTV and PIS data to the operator

Remark: The train level communication architecture (WLTB including accessories) is not shown in Figure 98 but considered later in the calculations.

5.4 PROJECT ANALYSIS - MATERIAL

5.4.1 General

Some projects were analysed and a “standard” car and vehicle composition with average components per car were defined, which is used in the following sections.

5.4.2 Components

5.4.2.1 List of components – wired network

The components of the “standard” composition for the current wired network are shown in Table 10.

Table 10: OOS components – wired network

Type	Cab car	Intermediate car	Cab car
Train Switch	1	0	1
Camera	7	6	7
Audio	8	6	8
Display	13	12	13
Switch	4	3	4
Other unit	3	-	3
Total	36	27	36

Other unit = Control unit, T2W and DVR

Total components = 99

5.4.2.2 List of components – wireless network

The components of the “standard” composition for a future wireless network are shown in Table 11.

Table 11: OOS components – wireless network

Type	Cab car	Intermediate car	Cab car
WLTBN	0	1	0
Camera	7	6	7
Audio	8	6	8
Display	13	12	13
MSTA	1	1	1
Other unit	3	-	3

Total	32	26	32

Other unit = Control unit, T2W and DVR

Total components = 90

5.4.3 Cables

5.4.3.1 List of cables – wired network

Each end device has one related IP connection.

The IP-ring cables were assigned to the IP-ring switches.

The IP-ring cabling for a 3-cars vehicle is shown Figure 101.

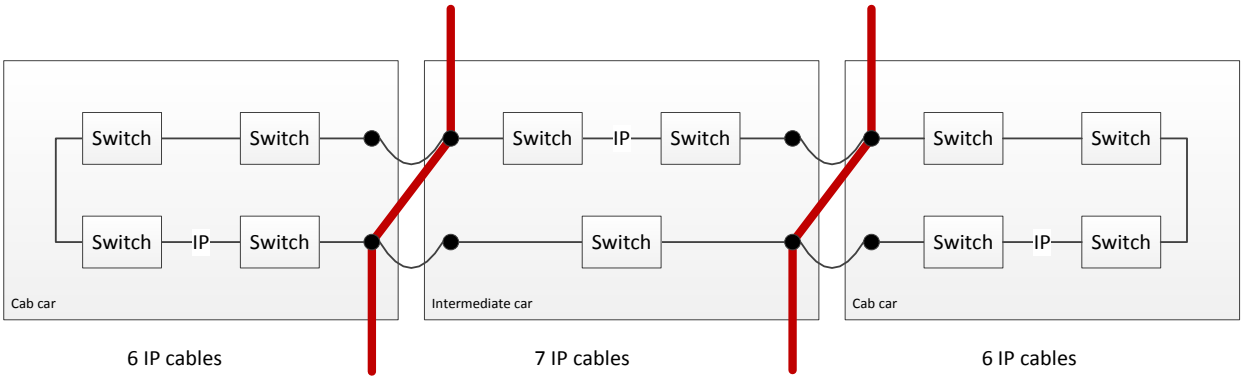


Figure 101: IP-ring network[9]

The IP cables of the “standard” composition for the current wired network are shown in Table 12.

Table 12: IP cables –wired network

Type	Cab car	Intermediate car	Cab car
Train Switch	1+4[10]	0+4	1+4
Camera	7	6	7
Audio	8	6	8
Display	13	12	13
Switch	6	7	6
Other unit	3	-	3
Total	42	35	42

Other unit = Control unit, T2W and DVR

Total IP cables = 119

The power cables of the “standard” composition for the current wired network are shown in Table 13.

[9] The red lines are defining the border to which car the cables are assigned

[10] X+Y means: Y is the number of cables to connect the TS to a ring switch, Y cover the ETB cabling inside the vehicle

Table 13: Power cables –wired network

Type	Cab car	Intermediate car	Cab car
Train Switch	1	-	1
Camera	-	-	-
Audio	8	6	8
Display	13	12	13
Switch	4	3	4
Other unit	3	-	3
Total	29	21	29

Other unit = Control unit, T2W and DVR

Total Power cables = 79

5.4.3.2 List of cables – wireless network

The power cables of the "standard" composition for a future wireless network are shown in Table 14.

Table 14: Power cables – wireless network

Type	Cab car	Intermediate car	Cab car
WLTBN	-	1	-
Camera	7	6	7
Audio	8	6	8
Display	13	12	13
MSTA	1	1	1
Other unit	3	-	3
Total	32	25	32

Others = Control unit, T2W and DVR

Total Power cables = 89

5.4.4 Comparison

The summary for components and cables of the above sections are shown in Table 15.

Table 15: Component and cable comparison

Item	Wired network	Wireless network	Variation
Components	99	90	-9%
IP cable	119	-	-100%
Power cable	79	89	+13%
Total cables	181	89	-49%

With the proposed wireless solution the amount of components and therefore component costs are only little reduced.

But, as expected, the number of cables is halved for the wireless solution. More than the reduction of cabling, important is that the more expensive IP cables are reduced. That means that from material cost point of view the reduction is much more than 50%.

Pre-assembled cubicles are used in some vehicle type. IP cables and power cables are connected to a plug adapter which is the interface of the cubicle (see Figure 102).

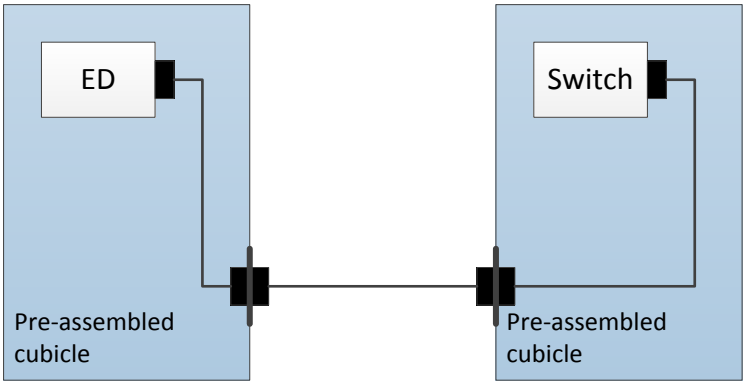


Figure 102: Cabling for pre-assembled cubicles

Worst case contain connections 3 parts of cables. Because the cost driver of cables are the connectors, pre-assembly increases the total costs of cabling dramatically.

5.5 PROJECT ANALYSIS - ENGINEERING

5.5.1 Mechanical and Electrical Integration

5.5.1.1 Vehicle documentation

Each project uses 1 central database to document the mechanical and electrical design of the vehicle. This database serves special exports and views for specialists and activities, e.g.:

- Supply management (e.g. for suppliers)
- Pre-assembly (e.g. equipment cabinet, driver´s desk)
- End-assembly (cable bundles)
- Commissioning
- Certification
- Trouble-shooting
- Stored in PDM and LN project database

The exports were used electronically or paper-based everywhere in the project. After database updates these exports have also to be updated.

Each of the work packages will decrease because of the reduced amount of devices and cables, connectors etc. Not all of them will be quantified in this study.

5.5.1.2 Component documentation

Each component is defined in the vehicle documentation by:

- Component 2D / 3D drawings
- Component circuit diagram including wiring information
- Component parts list including mounting tools

The engineering effort for components is depending on:

- Amount of component types
- Amount of components

- Amount of connectors per component

The wireless network has less amount of components (see section 5.4.4). Therefore the mechanical and electrical engineering effort is less.

5.5.1.3 Cable documentation

Each cable is defined in the vehicle documentation by:

- Cable circuit diagram (connections between connector pins and wires), including assembly rules
- Cable parts list (connector type, length, labelling)
- Cable layout
- Harness, cable is belonging to

The engineering effort for cables is depending on:

- Amount of cable types
- Amount of cables
- Amount of wires per cable
- Complexity factor of cable assembly

The wireless network has less amount of cable types (only power cables) and less amount of cables (see section 5.4.4). Therefore the mechanical and electrical engineering effort is much less.

5.5.2 Physical Integration and Commissioning

5.5.2.1 Component integration

During the physical integration and commissioning following activities per component are executed:

- Component installation including component fixing
- Component download and configuration
- Component commissioning and testing on train
- Component pre-series for the first 3 – 10 vehicles: change to series afterwards
- Component labelling (preparation, labelling)

The wireless network has less amount of components (see section 5.4.4). Therefore the physical engineering effort is less.

5.5.2.2 Cable integration

During the physical integration and commissioning following activities per cable are executed:

- Cable installation, including cable fixing
- Cable commissioning and testing on train
- Cable pre-series for the first 3 – 10 vehicles: Assembly on-board (exact cable length unknown)
- Cable series: Pre-assembly
- Cable labelling (preparation, labelling)

The wireless network has less amount of cable types (only power cables), less amount of cables and a much less complexity factor of cable assembly (see section 5.4.4). Therefore the physical engineering effort is much less.

5.6 SUPPLY MANAGEMENT

The analysis of the supply management activities and effort is not part of this document. But it is obvious, that also the supply management effort is depending on the amount of components and cables.

5.7 PRODUCTION

The production of components and cables is similar depending as described for mechanical and electrical integration in section 5.5.1.

The costs are directly depending on:

- Amount of components
- Amount of cables

Production costs for the future wireless network are much lower than for the current wired network.

Note: The development costs for the wireless device are not included.

5.8 MAINTENANCE COSTS

Not only during the engineering phase and the production phase a wireless TCMS can contribute to cost savings:

- Problems with cabling and connectors can be reduced and are limited e.g to the power supply
- The maintenance staff does not need to go inside the trains. Access is possible from outside the trains

5.9 WEIGHT

Based on the components and cables the reduction of weight is calculated. For connectors the M12 connector is assumed.

Data from projects and supply management:

Cable weight reduction minimal (direct connected):

- Average IP cable length 9m
- Cable weight (without connectors, 1m) 0,081kg
- Cable weight (without connectors, 9m) 0,729kg
- 1 Connector 0,18kg
- 2 connectors (1 cable) 0,36kg
- 2 connectors (2 units) 0,36kg
- Cable weight (4 connectors, 9m) 1,45kg

Cable weight reduction maximal (2 intermediate plug adapters):

- Average IP cable length 12m
- Cable weight (without connectors, 1m) 0,081kg

- Cable weight (without connectors, 12m) 0,972kg
- 1 Connector 0,18kg
- 6 connectors (3 cables) 1,08kg
- 2 connectors (2 units) 0,36kg
- Cable weight (8 connectors, 12m) 2,41kg

The weight for a component is assumed with 5kg including mounting parts.

Table 16: Weight reduction

Item	Wired network	Wireless network	Reduction [units]	Reduction min [kg]	Reduction max [kg]
Components / 3-cars	99	90	9	45	45
IP cable / 3-cars	119	-			
Power cable / 3-cars	79	89			
Cables / 3-cars	198	89	109	158,0	262,7
Total / 3-cars				203.0	307,7
Total / 1 car				67,7	102,6

5.10 SUMMARY AND CONCLUSION OF THE STUDY

The advantages of a wireless network are:

- Less mechanical and electrical integration effort
- Less physical integration effort
- Less procurement effort
- Less storage capacity needed
- Less component and cable production costs
- Less update effort
- Less weight
- Cable quality no longer an issue
- Simple bus extension, because only power cable needed

On the other side following additional work has to be covered:

- Development of the MSTA
- Development of WLED
- Development of security and safety functions for WMN
- Adapted interior design
- Additional effort for wireless commissioning

A wireless network will simplify the engineering work a lot of and will save both time and money.

6 CONCLUSIONS

The Roll2Rail project covers different rolling stock topics. The goal of the WP2 is to make research on technologies and architectures to provide fundamentals for the building of a train communication system based on wireless transmission which is to be used by Train Control and Monitoring System (TCMS) and other on-board electronic systems.

This deliverable describes proposals for suitable architectures including redundancies, and interfaces of the new wireless networks for inter consist and intra consist communications. The three functional domains -TCMS domain, Operator Oriented Services (OOS) domain and Customer Oriented Services (COS) domain, which have been defined in the Wireless TCMS Requirements Specification, D2.1 [69], have become the basic building blocks of the functional architecture with distinct communication networks in each of them due to different requirements put on these networks. It is also important to note that On Board Multimedia and Telematics (OMTS) [84] approach has been considered in transversal way for services that need to be provided in each functional domain.

The reasons for the splitting of train communication network into two hierarchical levels, are given in IEC 61375 standard series (TCN), have been recognized as generally valid. That is why this architectural decision has been also taken for the wireless TCN. For each functional domain there can be a train backbone level with Wireless Train Backbone (WLTB) for consist to consist communications and a consist network level with Wireless Consist Networks (WLCN) for inside consist communications. Although the proposed architecture allows for various combinations of wireless and wired (as specified in IEC 61375) communications the wireless technologies are in focus. The important network element in the two-level TCN is a gateway through which there is communication between both network levels. That element connecting consist networks to the Wireless Train Backbone is called Wireless Train Backbone Node (WLTBN) and its functionality goes far beyond routing data traffic. It is to be stressed that in the case of consist to consist communication the communication must always go through the local WLTBN even if the wireless end device would be able to establish direct wireless connection to the target consist.

The communication can be safety related or not safety related. Due to the fact that a train has a dynamic network (consists can be operationally coupled or decoupled) the train integrity has to be ensured before the end devices are able to communicate to each other and has to be permanently supervised. In D2.5, train integrity is achieved in two steps. In a first step, the train discovery establishes the communication network. In the second step, the safe train inauguration is performed. This second step is safety related because it retrieves the safety relevant orientation and sequence of vehicles. Because the number of consists in the train (train length) cannot be safely detected by these steps (e.g. unpowered consist at the train end), the train length has to be confirmed by another mechanism, e.g. by the driver. Each change of the safety relevant train parameters (sequence, orientation, number of vehicles) has to be detected.

Going further into detail, although different strategies for train discovery have been proposed, as it can be seen in Table 8, the most suitable solution has been adopted, as it is also summarized in chapter 3.1.1.5. This solution will be the basis for the safe train inauguration function and it will be implemented using RFID and a secondary/redundant safe channel (e.g. pneumatic brake pipes will imply that consists still will need to be mechanically coupled to fulfil required safety levels).This fact leaves open the possibility for the future for an improved solution, if virtually coupled[11] consist concept needs to be realized. For the moment, Release 8&9 of LTE and Standard Data Path Mode has been selected. Further details of this selection will be collected and explained in D2.7 deliverable.

Regarding safe data transmission between end-devices, once the train has been successfully inaugurated, different aspects have be to taken into account. Safe end devices have to use a

[11] Virtual Coupling (Shit2Rail TD 2.8) aims to enable 'virtually coupled trains' to operate much closer to one another (within their absolute braking distance) and dynamically modify their own composition on the move (virtual coupling/uncoupling of train convoys), while ensuring at least the same level of safety as is currently provided.

safety layer (e.g. SDT) to safely communicate with another safe end device (ED-S). Regular end devices are not allowed to use a safety layer. This is valid for intra consist as well as for train backbone communication. In D2.5, safety functions up to safety integrity level SIL2 are considered. Higher safety integrity levels may be reached by implementing additional mechanisms in parallel (e.g. train lines) [12]. Therefore, the architecture has been left somehow flexible: train lines, wired consist networks (e.g.: ECN, MVB, CAN) and wireless networks (based on WiFi Mesh Technology) will be allowed for the implementation. Within this deliverable a concrete solution has been provided for several train functions in order to meet the goals defined in D2.1 deliverable [69] – see traceability matrix in Appendix III, chapter 9 -. Nevertheless, from safety and security point of view, the complete technical detail analysis and its results will be available in D2.4 confidential deliverable [83].
Furthermore, a brief study of proposed architecture feasibility from LCC point of view has been also done. This study is documented in chapter 5.
Moreover, the train inauguration procedure for wireless train backbone proposed in this deliverable will be detailed in D2.8 [85], implemented and its validation tests will be specified and executed. The laboratory validation test setup, to be sufficiently representative, will represent at least three consists. The follow-up tests (also addressed in D2.8 [85]) shall validate the end device to end device data exchange over the wireless consist to consist communication. The successful pass of these tests will strongly indicate that TCMS systems that follow the architecture proposed here will be able to satisfy the requirements on WTCMS as they have been stated in D2.1 [69].
This deliverable has strived to address all topics which an architecture document is expected to cover. For the purpose of giving evidence that these expectations have been fulfilled the traceability matrix to the system requirements has been provided in the Appendix III. This matrix maps the sections in this deliverable to the system requirements, given in D2.1 [69], which were identified as architecturally significant ones. Of course, there are still steps beyond that need to be carried out, such as a complete analysis for each train function and its allocation to wired network, wireless network or train line approach of the combined Wireless TCMS solution proposed within this deliverable.
Additionally, as it is already foreseen within CONNECTA and X2RAIL projects from Shift2Rail, a close collaboration between TCMS and the Signalling Systems will be needed in order to achieve the unique/combined solution of a Virtually Coupled Consists Concept. For sure, this should be based on future evolutions of LTE technology, such as LTE-Advance Pro (one of the commercial names for LTE Release 13&14), where latencies around 2-3ms are expected [86] or Evolved LTE (more commonly known as 5G for LTE Releases 15&16), where availability figures up to 99,999% year are expected.

[12] For more details about assumptions see chapter 3.1.1.

7 APPENDIX I – ACRONYMS AND DEFINITIONS

AES	Advanced Encryption Standard
ALG	Application Layer Gateway
AP	Access Point (WLAN IEEE 802.11)
AVB	Audio Video Bridging
AWGN	Additive White Gaussian Noise
BER	Bit Error Rate
BSS	Basic Service Set
CBTC	Communication-Based Train Control
CCA	Clear Channel Assessment
CCTV	Closed Circuit Television
CDMA	Code Division Multiple Access
COS	Customer Oriented Services
CR	Cognitive Radio
CSMA	Carrier Sense Multiple Access
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
DFS	Dynamic Frequency Selection (WLAN IEEE802.11h)
DS	Distribution System (see WLAN IEEE 802.11)
DSM	Distribution System Medium
DVR	Digital Video Recorder
EAP	Extensible Authentication Protocol
ECN	Ethernet Consist Network
ECR	Ethernet Consist Ring
ED	End Device
ED-S	Safe End Device
EDCA	Enhanced Distributed Channel Access (WLAN 802.11e)
EMF	Electromagnetic Field
eNodeB	LTE Base Station
EPC	Evolved Packet Core
ESS	Extended Service Set (WLAN IEEE 802.11)
ETB	Ethernet Train Backbone
ETBN	Ethernet Train Backbone Node
FDMA	Frequency Division Multiple Access
FIFO	First In First Out
FRTS	Future Request To Send
HCCA	Hybrid Communication Channel Access (WLAN 802.11e)
IP	Internet Protocol
LAN	Local Area Network
LTE	Long Term Evolution
MAC	Medium Access Protocol
MBSS	Mesh Basic Service Set
MCG	Mobile Communication Gateway
MGATE	Mesh Gate
MME	Mobility Management Entity
MSDU	MAC Service Data Units
MSTA	Mesh Station
MVB	Multifunction Vehicle Bus
OFDM	Orthogonal Frequency-Division Multiplexing

OMTS	On-board Multimedia and Telematics Subsystem/Services
OOS	Operator Oriented Services
P-GW	Packet Data Network Gateway
PHR	Packet Header
PHY	Physical Interface
PIS	Passenger Information System
pMSTA	Passage Mesh Station, see also MSTA
PoE	Power over Ethernet
PRR	Packet Reception Rate
PSDU	Packet Service Data Unit
PTP	Precision Time Protocol
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RF	Radio Frequency
RFID	Radio Frequency IDentification
RS	Relay Station
RSSI	Received Signal Strength Indication
S-GW	Serving Gateway
SAE	Simultaneous Authentication of Equals (WLAN IEEE 802.11s)
Safely	Attribute for a function which has to be applied according to required SIL
SDMA	Space Division Multiple Access
SDR	Software Defined Radio
SHR	Synchronisation Header
SIL	Safety Integrity Level
SNR	Signal Noise Ratio
SRP	Stream Reservation Protocol
SSID	Service Set Identifier (WLAN IEEE 802.11)
STA	Station
T2W	Train to Wayside Communication
TCMS	Train Control and Monitoring System
TDMA	Time Division Multiple Access
TKIP	Temporal Key Integrity Protocol
TPC	Transmit Power Control (IEEE 802.11h)
TSMP	Time Synchronized Mesh Protocol
TSN	Time Sensitive Networking
UE	User Equipment
URI	Uniform Resource Identifier
VLAN	Virtual LAN
VTS	Virtual TDMA for Sensors
WCSC	Wireless Control Service Client
WEP	Wired Equivalent Privacy (WLAN IEEE 802.11)
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless LAN
WLTBN	Wireless Train Backbone Node
WLCN	Wireless Consist Network
WLED	Wireless End Device
WM	Wireless Medium
WMN	Wireless Mesh Network
WPA	Wi-Fi Protected Access (WLAN IEEE 802.11)
WPA2	Extension of WPA
WPS	WiFi Protected Setup (WLAN IEEE 802.11)
WSN	Wireless Sensor Networks

WTB	Wired Train Backbone

Train to Train (virtually coupled) – out scope of Roll2Rail by the moment
Consist to Consist (definition of the IEC 61375-2-5) - short distance / long distance
Inside consist (definition of the IEC 61375-3-4, .. 2-3)
Inside vehicle (definition of the IEC 61375-3-4, .. 2-3)
End Device (definition of the IEC 61375-3-4)

8 APPENDIX II – REFERENCES

[1] Wei Shen (2014), A Protocol Framework for Adaptive Real-Time Communication in Industrial Wireless Sensor and Actuator Network (Doctoral dissertation).

[2] P. Huang, L. Xiao, S. Soltani, M.W. Mutka and X. Ning, *"The evolution of MAC Protocols in Wireless Sensor Networks: A Survey,"* IEEE Communications Surveys & Tutorials, vol. 15, pp. 101-120, Apr. 2012.

[3] J. Polastre, J. Hill and D. Culler, "Versatile Low Power Media Access for Wireless Sensor Networks," in *Proc. SenSys*, 2004.

[4] P. Huang, C. Wang, L. Xiao, and H. Chen, "RC-MAC: A Receiver-Centric Medium Access Control Protocol for Wireless Sensor Networks," in *Proc. IWQoS*, 2010, pp. 1–9.

[5] L. Tang, Y. Sun, O. Gurewitz, and D. B. Johnson, "PW-MAC: An Energy-Efficient Predictive-Wakeup MAC Protocol for Wireless Sensor Networks," in *Proc. INFOCOM*, 2011, pp. 1305–1313.

[6] W. Ye, J. Heidemann, and D. Estrin, "An Energy-Efficient MAC Protocol for Wireless Sensor Networks," in *Proc. INFOCOM*, 2002, pp. 1567–1576.

[7] T. van Dam and K. Langendoen, "An Adaptive Energy-Efficient MAC Protocol for Wireless Sensor Networks," in *Proc. SenSys*, 2003, pp. 171–180.

[8] S. Du, A. K. Saha, and D. B. Johnson, "RMAC: A Routing-Enhanced Duty-Cycle MAC Protocol for Wireless Sensor Networks," in *Proc. INFOCOM*, 2007, pp. 1478–1486.

[9] Y. Sun, S. Du, O. Gurewitz, and D. B. Johnson, "DW-MAC: A Low Latency, Energy Efficient Demand-Wakeup MAC Protocol for Wireless Sensor Networks," in *Proc. MobiHoc*, 2008, pp. 53–62.

[10] G. Lu, B. Krishnamachari, and C. S. Raghavendra, "An Adaptive Energy-Efficient and Low-Latency MAC for Data Gathering in Wireless Sensor Networks," in *Proc. IPDPS*, 2004.

[11] W. Ye, F. Silva, and J. Heidemann, "Ultra-Low Duty Cycle MAC with Scheduled Channel Polling," in *Proc. SenSys*, 2006, pp. 321–334.

[12] S. Marinkovic, E. Popovici, C. Spagnol, S. Faul, and W. Marnane, "Energy-Efficient Low Duty Cycle MAC Protocol for Wireless Body Area Networks," *IEEE Trans. Inf. Technol. Biomed.*, vol. 13, no. 6, pp. 915–925, 2009.

[13] I. Rhee, A. Warrier, M. Aia, and J. Min, "Z-MAC: A Hybrid MAC for Wireless Sensor Networks," in *Proc. SenSys*, 2005, pp. 90–101.

[14] V. Rajendran, K. Obraczka, and J. J. Garcia-Luna-Aceves, "Energy-Efficient Collision-Free Medium Access Control for Wireless Sensor Networks," in *Proc. SenSys*, 2003, pp. 181–192.

[15] W.-Z. Song, R. Huang, B. Shirazi, and R. LaHusen, "TreeMAC: Localized TDMA MAC Protocol for Real-Time High-Data-Rate Sensor Networks," in *Proc. PerCom*, 2009.

[16] G. P. Halkes and K. G. Langendoen, "Crankshaft: An Energy-Efficient MAC-Protocol for Dense Wireless Sensor Networks," in *Proc. EWSN*, 2007, pp. 228–244.

[17] T. Zheng, S. Radhakrishnan, and V. Sarangan, “PMAC: An Adaptive Energy-Efficient MAC Protocol for Wireless Sensor Networks,” in *Proc. IPDPS*, 2005.

[18] G. Zhou, C. Huang, T. Yan, T. He, J. A. Stankovic, and T. F. Abdelzaher, “MMSN: Multi-Frequency Media Access Control for Wireless Sensor Networks,” in *Proc. INFOCOM*, 2006, pp. 1–13.

[19] H. K. Le, D. Henriksson, and T. Abdelzaher, “A Practical Multi-Channel Media Access Control Protocol for Wireless Sensor Networks,” in *Proc. IPSN*, 2008, pp. 70–81.

[20] Y. Wu, J. A. Stankovic, T. He, J. Lu, and S. Lin, “Realistic and Efficient Multi-Channel Communications in Wireless Sensor Networks,” in *Proc. INFOCOM*, 2008, pp. 1193–1201.

[21] Q. Yu, J. Chen, Y. Fan, X. Shen, and Y. Sun, “Multi-Channel Assignment in Wireless Sensor Networks: a Game Theoretic Approach,” in *Proc. INFOCOM*, 2010, pp. 1127–1135.

[22] O. D. Incel, L. van Hoesel, P. Jansen, and P. Havinga, “MC-LMAC: A Multi-Channel MAC Protocol for Wireless Sensor Networks,” *Ad Hoc Netw.*, vol. 9, pp. 73–94, January 2011.

[23] Y. Kim, H. Shin, and H. Cha, “Y-MAC: An Energy-Efficient Multichannel MAC Protocol for Dense Wireless Sensor Networks,” in *Proc. IPSN*, 2008, pp. 53–63.

[24] J. Borms, K. Steenhaut, and B. Lemmens, “Low-Overhead Dynamic Multi-Channel MAC for Wireless Sensor Networks,” in *Proc. EWSN*, 2010, pp. 81–96.

[25] P. Suriyachai, U. Roedig, and A. Scott, “A Survey of MAC Protocols for Mission-Critical Applications in Wireless Sensor Networks,” *IEEE Commun. Surveys Tuts.*, vol. 14, no. 2, pp. 240–264, 2012.

[26] J. Kim, J. Lim, C. Pelczar and B. Jang, “RRMAC: A Sensor Network MAC for Real Time and Reliable Packet Transmission,” *Proceedings of International Symposium Consumer Electronics*, Vilamoura, 14-16 April 2008, pp. 1-4.

[27] Z. Teng and K. Kim, "A Survey on Real-Time MAC Protocols in Wireless Sensor Networks," *Communications and Network*, Vol. 2 No. 2, 2010, pp. 104-112.

[28] T. Watteyne, I. Augé-Blum and S. Ubéda, “Dual-Mode Real-Time MAC Protocol for Wireless Sensor Networks: A Validation/Simulation Approach,” *Proceedings of the 1st International Conference on Integrated As Hoc and Sensor Network*, Nice, 30-31 May 2006.

[29] A. Krohn, M. Beigl, C, Decker and T. Zimmer, “TOMAC- Real-Time Message Ordering in Wireless Sensor Net-works Using the MAC Layer,” *Proceedings of 2nd International Workshop on Networked Sensing Systems*, San Diego, 27-28 June 2005.

[30] K. Karenos and V. Kalogeraki, “Real-Time Traffic Man-agement in Sensor Networks,” *Proceedings of IEEE In-ternational Real-Time System Symposium*, Rio de Janeiro, 5-8 December 2006, pp. 422-434.

[31] E. Egea-López, J. Vales-Alonso, A. S. Martínez-Sala, J. García-Haro, P. Pavón-Mariño and M. V. B. Delgado, “A Wireless Sensor Networks MAC Protocol for Real- Time Applications,” *Personal and Ubiquitous Computing*, Vol. 12, No. 2, February 2008, pp. 111-122.

[32] H. Li, P. Shenoy and K. Ramamritham, “Scheduling Messages with Deadlines in Multi-Hop Real-Time Sensor Networks,” *Proceedings of IEEE Real Time and Embed-ded Technology and Applications Symposium*, 7-10 March 2005, pp. 415-425.

[33] J. A. Afonso, L. A. Rocha, H. R. Silva and J. H. Correia, “MAC Protocol for Low-Power Real-Time Wireless Sensing and Actuation,” *Proceedings of the 11th IEEE International Conference on Electronics, Circuits and Systems*, Nice, 10-13 December 2006, pp. 1248-1251.

[34] S. Munir, S. Lin, E. Hoque, S. M. S. Nirjon, J. A. Stankovic, and K. Whitehouse, “Addressing Burstiness for Reliable Communication and Latency Bound Generationin

Wireless Sensor Networks," in *Proc. 9th ACM/IEEE Int. Conf. InformationProcessing in Sensor Networks (IPSN '10)*, 2010, pp. 303–314.

[35] P. Suriyachai, J. Brown, and U. Roedig, "Time-critical data delivery in wireless sensor networks," in *Proc. 6th IEEE Int. Conf. Distributed Computing in Sensor Systems (DCOSS'10)*, 2010, pp. 216–229.

[36] O. Durmaz, A. Ghosh and B. Krishnamachari (2011). Scheduling Algorithms for Tree-Based Data Collection in Wireless Sensor Networks, *Theoretical Aspects of Distributed Computing in Sensor Networks*, (pp 407-445). Springer Berlin Heidelberg.

[37] P. Wolf-Bastian, S. Hans, J. Brown, U. Roedig and L. Wolf, "Constructing Schedules for Time-Critical Data Delivery in Wireless Sensor Networks," ACM Transactions on Sensor Networks, 2014.

[38] Cui, S., Madan, R., Goldsmith, A., Lall, S, "Energy-delay tradeoffs for data collection in tdmabased sensor networks," in *ICC '05*, vol. 5, pp. 3278–3284 vol. 5 (2005)

[39] Pan, M., Tseng, Y., "Quick convergecast in zigbee beacon-enabled tree-based wireless sensor networks," *Computer Communications* 31(5), 999–1011 (2008)

[40] Revah, Y., Segal, M., "Improved lower bounds for data-gathering time in sensor networks," in *ICNS '07*, p. 76. IEEE Computer Society, Washington, DC, USA (2007). DOI http://dx.doi.org/10.1109/ICNS.2007.71

[41] Florens, C., Franceschetti, M., McEliece, R., "Lower bounds on data collection time in sensory networks," *IEEE Journal on Selected Areas in Communications* vol. 22(6), pp. 1110–1120 (2004)

[42] P. Suriyachai, U. Roedig and A. Scott, "A Survey of MAC Protocols for Mission-Critical Applications in Wireless Sensor Networks," *IEEE Communications Surveys & Tutorials*, vol. 14, pp. 240-264, Mar. 2011.

[43] A. Rowe, R. Mangharam, and R. Rajkumar, "RT-Link: A Time-Synchronized Link Protocol for Energy-Constrained Multi-hop Wireless Networks," in *Proc. 3rd Annu. IEEE Communications Society Conf. Sensor, Mesh and Ad Hoc Communications and Networks*, Reston, VA, USA, 2006, vol. 2, pp. 402-411.

[44] S. C. Ergen, and P. Varaiya, "PEDAMACS: Power Efficient and Delay Aware Medium Access Protocol for Sensor Networks," *IEEE Trans. Mobile Comput.*, vol. 5, pp. 920-930, Jul. 2006.

[45] M. Salajegheh, H. Soroush, and A. Kalis, "HyMAC: Hybrid TDMA/FDMA Medium Access Control Protocol for Wireless Sensor Networks," in *Proc. 18th IEEE Int. Symp. Personal, Indoor and Mobile Radio Communications*, Athens, Greece, 2007, pp. 1-5.

[46] E. Felemban, C.-G. Lee, and E. Ekici, "MMSPEED: Multipath Multi-SPEED Protocol for QoS Guarantee of Reliability and Timeliness in Wireless Sensor Networks*," IEEE Trans. Mobile Comput.*, vol. 5, pp. 738-754, Jun. 2006.

[47] HART Communication Foundation, "WirelessHART Technology,"[Online]. Available: http://www.hartcomm.org/protocol/wihart/ wireless_technology.html, Dec. 2009.

[48] K.S.J. Pister, and L. Doherty, "TSMP: time sychronized mesh protocol," in *Proc. IASTED Symp. Parallel and Distributed Computing andSystems*, Orlando, FL, USA, 2008.

[49] Z. N. Chen, Antennas for Portable Devices, Chichester, UK: John Wiley & Sons, 2007.

[50] A. Vander Vorst, A. Rosen, and Y. Kotsuka, RF/Microwave Interaction with Biological Tissues, Hoboken, NJ: John Wiley & Sons, 2006.

[51] Council Recommendation of 12 July 1999 on the limitation of exposure of the general public to electromagnetic fields (0 Hz to 300 GHz): http://ec.europa.eu/health/electromagnetic_fields/docs/emf_rec519_en.pdf

[52] K. Fujimoto and J. R. James, Mobile Antenna Systems Handbook, London: Artech House, 2001.

[53] ICNIRP, "Guidelines for limiting exposure to time-varying electric, magnetic and electromagnetic fields (up to 300 GHz)," 1998.

[54] ANSI/IEEE, "IEEE standard for safety levels with respect to human exposure to radio frequency fields 3 kHz to 300 GHz," 1992.

[55] IEEE, "Recommended Practice for Determining the Peak Spatial-Average Specific Absorption Rate (SAR) in the Human Head from Wireless Communications Devices: Measurement Techniques (Std 1528-2003)," 2003.

[56] K. Ito, "Phantoms for evaluation of interactions between antennas and the human body," in Course on Antennas and Propagation for Body-Centric Wireless Communications, Queen Mary, University of London, 2009.

[57] R2R-T2.4-D-CAF-012, RAMS and Security Analysis Report

[58] Peter Stavroulakis, Interference Analysis and Reduction for Wireless Systems. Artech House, London. 2003.

[59] Texas Instruments. Understanding and Enhancing Sensitivity in Receivers for Wireless Applications. 1999. Available at: http://www.ti.com/lit/an/swra030/swra030.pdf

[60] T. Jorgensen, “How to design the ideal digital cordless phone”

[61] A. F. Molisch, *Wireless Communications 2nd Edition,* Wiley, 2010.

[62] J. Fuhl, A. F. Molisch, and E. Bonek, “Unified channel model for mobile radio systems with smart antennas”, *IEE Proc. Radar, Sonar Navigation*, 145, 32-41 (1998)

[63] P. Erätuuli and E. Bonek, “Diversity arrangements for internal handset antennas”, *8th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC’97)*, Helsinki, Finland, pp. 589-593 (1997)

[64] J. H. Winters, “Optimum combining in digital mobile radio with cochannel interference”, *IEEE JSAC*, 2, 528-538 (1984).

[65] *AVR2021: AT86RF231 Antenna Diversity*, Atmel Application Note

[66] M. Burns and T. Starr, “Implementing ‘Diversity’ Using Low Power Radios”, AN085 Application Note

[67] Moxa: http://www.moxa.com/newsletter/connection/2013/03/feat_01.htm

[68] F. Casado, R. Torrego, P. Rodríguez, A. Arriola and I. Val, “Reconfigurable Antenna and Dynamic Spectrum Access Algorithm: Integration in a Cognitive Radio Platform for Reliable Communications,” *Journal of Signal Processing Systems*, vol. 78, pp. 267-274, Mar. 2015.

[69] R2R-T2.1-D-TRI-053-10, D2.1 – Specification of Wireless TCMS

[70] Safety related communication in transmission systems, EN 50159 - 2010

[71] TTTech, “IEEE TSN (Time-Sensitive Networking): A Deterministic Ethernet Standard,” pp. 1–9, 2015.

[72] “The Deterministic Ethernet Guide.” [Online]. Available: http://www.deterministicethernet.com/#!time-sensitive-networking--tsn-/o4zg4.

[73] M. J. Teener, “A Time-Sensitive Networking Primer?: Putting It All Together,” in 2015 International IEEE Symposium on Precision Clock Synchronization for Measurement, Control and Communication, 2015, pp. 1–49.

[74] G. Pitcher, “Deterministic data developments,” New electronics, no. March, pp. 29–30, 2016.

[75] M. D. J. Teener, “IEEE 802 Time-Sensitive Networking?: Extending Beyond AVB,” in IEEE-SA Ethernet & IP @ Automotive Technology Day, 2013, pp. 1–30.

[76] R2R-T2.5-T-BTD-006-04 – D2.5 - Device Location Table

[77] IEC 61375-2-3 TCN Communication Profile, Edition 1.0

[78] IEC 61375-2-5 Ethernet Train Backbone, Edition 1.0

[79] IEC 61375-1 Train Communication Network (TCN) – Part 1: TCN General Architecture, 2012

[80] R2R-WP02-B-CAF-072-01 - WP2 – 4th Quarterly Meeting – Technology Selection

[81] R2R-T2.5-T-UNC-069-02 WLAN In WTCN

[82] A Survey on Wireless Mesh Networks, Ian F. Akyildiz, Georgia Institute of Technology, Xudong Wang, Kiyon, Inc, IEEE Radio Communications September 2005 page s23-s80.

[83] R2R-T2.4-D-CAF-012-09 RAMS and Security Analysis Report

[84] IEC 62580-1:2015, On-board multimedia and telematics subsystems for railways – Part 1: General architecture

[85] R2R-T2.8-D-IK4-009-05 – D2.8 – Validation Report

[86] LTE-Advanced Pro - Pushing LTE capabilities towards 5G - http://resources.alcatel-lucent.com/asset/200176

[87] Wi-Fi Capacity Analysis for 802.11ac and 802.11n: Theory & Practice; Timo Vanhatupa, Ph.D. Senior Research Scientist, Ekahau, 2013

[88] Wireless LANs: 802.11-WLAN-Technologie und praktische Umsetzung im Detail; Joerg Rech, 2012

9 APPENDIX III - REQUIREMENT TRACEABILITY

Table 17: Traceability of Requirements [69]

REQ ID	OBJ	SHORT TITLE	WTCMS / WTCN	Traceability - Chapter from D2.5
SRWTCMS_001	Req	ARCH_DEFINITION	WTCMS	2.5 - Interfaces
SRWTCMS_002	Inf	N/A	N/A	N/A
SRWTCMS_003	Req	ARCH_DEFINITION_WTCN_VS_TCN	WTCN	2.5 - Interfaces
SRWTCMS_004	Req	ARCH_DEFINITION_WLCN_VS_ECN	WTCN	2.5 - Interfaces
SRWTCMS_005	Req	ARCH_DEFINITION_BACKWARD_COMPATIBILITY	WTCMS	2.5 - Interfaces
SRWTCMS_006	Req	ARCH_DEFINITION_COMPATIBILITY_WLTB_VS_ALL	WTCN	2.5 - Interfaces

REQ ID	OBJ	SHORT TITLE	WTCMS / WTCN	Traceability - Chapter from D2.5
SRWTCMS_007	Req	ARCH_DEFINITION_COMPATIBILITY_WLCN_VS_ETB	WTCN	2.5 - Interfaces
SRWTCMS_008	Req	ARCH_DEFINITION_COMPATIBILITY_WLCN_VS_WLTB	WTCN	2.5 - Interfaces
SRWTCMS_009	Req	ARCH_DEFINITION_COMPATIBILITY_WLTB_VS_ALL	WTCN	2.5 - Interfaces
SRWTCMS_010	Req	ARCH_DEFINITION_COMPATIBILITY_WLTB_VS_ALL	WTCN	2.5 - Interfaces
SRWTCMS_011	Req	ARCH_DEFINITION_WLTB_&_ETB_COMBINATION	WTCN	2.5 - Interfaces
SRWTCMS_012	Req	ARCH_DEFINITION_WITH_WLTB	WTCN	2.5 - Interfaces
SRWTCMS_013	Req	ARCH_DEFINITION_WITHOUT_WLTB	WTCN	2.5 - Interfaces
SRWTCMS_014	Req	ARCH_DEFINITION_WLTB_NUM_CERO	WTCMS	3 Wireless Architecture for Consist to Consist Communications
SRWTCMS_015	Req	ARCH_DEFINITION_COMPATIBILITY_VS_OTHER_CONSISTS	WTCN	3.1.1 - Train Discovery
SRWTCMS_016	Inf	N/A	N/A	N/A
SRWTCMS_017	Req	ARCH_DEFINITION_COMPATIBILITY_VS_INAUGURATION	WTCN	3.1.7 Train Inauguration Inhibit
SRWTCMS_018	Req	ARCH_DEFINITION_PORTABLE_DEVICES_ACCESS	WTCMS	4.3.2 Authentication 4.8.1 TCMS Domain
SRWTCMS_019	Inf	N/A	N/A	N/A
SRWTCMS_020	Req	ARCH_DEFINITION_WLCN_INSIDE_CONSIST	WTCN	4 Wireless Architecture for Inside Consist Communications
SRWTCMS_021	Req	ARCH_MAX_WLTB	WTCN	2.4 Basic architecture concepts
SRWTCMS_022	Req	ARCH_MAX_WLTBN_VS_WLCN	WTCN	2.4 Basic architecture concepts
SRWTCMS_023	Req	ARCH_MAX_WLTBN_VS_WLTB_VS_TRAIN.	WTCN	2.4 Basic architecture concepts
SRWTCMS_024	Req	ARCH_MAX_WLTBN_VS_WLTB_VS_CONSIST	WTCN	2.4 Basic architecture concepts
SRWTCMS_025	Inf	N/A	N/A	N/A
SRWTCMS_026	Req	ARCH_MAX_CONSIST_NETWORK_VS_WLTB_VS_TRAIN	WTCN	2.4 Basic architecture concepts
SRWTCMS_027	Req	ARCH_MAX_CONSIST_NETWORK_VS_WLTB_VS_CONSIST	WTCN	2.4 Basic architecture concepts
SRWTCMS_028	Req	ARCH_MAX_WLCN_VS_VEHICLES	WTCN	2.4 Basic architecture concepts
SRWTCMS_029	Req	ARCH_MAX_WED_VS_WLCN	WTCN	2.4 Basic architecture concepts 4.8.1 - TCMS Domain 4.8.2 - OOS Domain 4.8.3 - Combined approach for TCMS and OOS 4.8.4 - COS Domain
SRWTCMS_030	Req	ARCH_MAX_IPV4_MULTICAST_ROUTES	WTCN	3.2.1.1 Regular Communication between End Devices in different Consists
SRWTCMS_031	Req	ARCH_MAX_DISTANCE_WLTB	WTCN	3 - Wireless Architecture for Consist to Consist Communications
SRWTCMS_033	Req	ARCH_COMMS_BETWEEN_WLED	WTCN	2.4 Basic architecture concepts
SRWTCMS_034	Req	ARCH_COMMS_WLTBN_VS_WLED	WTCN	3 Wireless Architecture for Consist to Consist Communications
SRWTCMS_035	Req	ARCH_COMMS_WLTBN_VS_WLED_REDUNDANCY	WTCMS	3 Wireless Architecture for Consist to Consist Communications

REQ ID	OBJ	SHORT TITLE	WTCMS / WTCN	Traceability - Chapter from D2.5
SRWTCMS_036	Req	ARCH_COMMS_RELATION_WLCN_VS_WLTB	WTCN	2.4 Basic architecture concepts
SRWTCMS_037	Req	ARCH_COMMS_RELATION_WLTB_VS_WLCN	WTCN	2.4 Basic architecture concepts
SRWTCMS_038	Req	ARCH_COMMS_CONTROL_INTERFACE	WTCN	3.1.1Train Discovery
SRWTCMS_039	Req	ARCH_COMMS_WLCN_VS_WECN	WTCN	2.5.4.5WLCN-ECN Interface
SRWTCMS_040	Req	OPMOD_TOPO_UPDATE_INAUG_COUPLING	WTCN	3.1.1.1.5 Lengthening/Shortening detection
SRWTCMS_041	Req	OPMOD_TOPO_UPDATE_INAUG_WLTBN_LOST	WTCN	3.1.2 Safe Train Inauguration (Distribution of Train Inauguration Results)
SRWTCMS_043	Req	OPMOD_ORIENTATION_CONFIGURABLE	WTCN	3.1.2 Safe Train Inauguration (Distribution of Train Inauguration Results)
SRWTCMS_044	Inf	N/A	N/A	N/A
SRWTCMS_045	Req	OPMOD_INAUG_ORIENTATION_DETECT	WTCN	3.1.2 Safe Train Inauguration (Distribution of Train Inauguration Results)
SRWTCMS_046	Req	OPMOD_INAUG_ORDER_DETECT	WTCN	3.1.2 Safe Train Inauguration (Distribution of Train Inauguration Results)
SRWTCMS_047	Inf	N/A	N/A	N/A
SRWTCMS_048	Req	OPMOD_INAUG_APP_INHIBIT	WTCN	3.1.7 Train Inauguration Inhibit
SRWTCMS_049	Inf	N/A	N/A	N/A
SRWTCMS_050	Req	OPMOD_INAUG_INHIBIT_IGNORE_NEW_TOPO	WTCN	3.1.7 Train Inauguration Inhibit
SRWTCMS_051	Req	OPMOD_INAUG_HOT_COUPLING_MAX_TIME	WTCN	3.1.1 Train Discovery 3.1.2- Safe Train Inauguration (Distribution of Train Inauguration Results)
SRWTCMS_052	Req	OPMOD_INAUG_COLD_COUPLING_MAX_TIME	WTCN	3.1.2 - Safe Train Inauguration (Distribution of Train Inauguration Results)
SRWTCMS_053	Req	OPMOD_INAUG_SERVICES_POWER_UP_MAX_TIME	WTCMS	3.1.2 - Safe Train Inauguration (Distribution of Train Inauguration Results)
SRWTCMS_054	Req	OPMOD_INAUG_UPDATE_IPV4_ROUTES_MAX_TIME	WTCN	3.1.2 - Safe Train Inauguration (Distribution of Train Inauguration Results)
SRWTCMS_055	Inf	N/A	N/A	N/A
SRWTCMS_056	Req	OPMOD_INAUG_COMM_INTERRUPT_MAX_TIME	WTCMS	3.1.2 - Safe Train Inauguration (Distribution of Train Inauguration Results)
SRWTCMS_057	Req	OPMOD_INAUG_APP_CONFIRMATION	WTCN	3.1.2 - Safe Train Inauguration (Distribution of Train Inauguration Results)
SRWTCMS_058	Req	COMM_IP_QOS_PRIO_QUEUES_BACKBONE	WTCMS	2.5.5 - Protocols
SRWTCMS_059	Req	COMM_IP_QOS_PRIO_QUEUES_CONSIST	WTCMS	2.5.5 - Protocols
SRWTCMS_060	Req	COMM_IP_TRAFFIC_SHAPING	WTCN	2.5.5 - Protocols
SRWTCMS_061	Inf	N/A	N/A	N/A
SRWTCMS_062	Req	COMM_VLAN_MIN_NUMBER	WTCMS	2.5.5 - Protocols
SRWTCMS_063	Req	COMM_VLAN_ACT_PERFOMANCE	WTCMS	2.5.5 - Protocols

REQ ID	OBJ	SHORT TITLE	WTCMS / WTCN	Traceability - Chapter from D2.5
SRWTCMS_064	Req	COMM_UNICAST_ED	WTCN	2.5.5 - Protocols
SRWTCMS_065	Req	COMM_MULTICAST_BACKBONE	WTCN	2.5.5 - Protocols
SRWTCMS_066	Req	COMM_MULTICAST_CONSIST	WTCN	2.5.5 - Protocols
SRWTCMS_067	Rec	COMM_BROADCAST_CONSIST	WTCMS	2.5.5 - Protocols
SRWTCMS_068	Inf	N/A	N/A	N/A
SRWTCMS_069	Req	NORM_EN45545_2_COMPLIANT	WTCMS	Design Phase Related - Not Architectural
SRWTCMS_070	Req	NORM_EN50121_3_2_COMPLIANT	WTCMS	Design Phase Related - Not Architectural
SRWTCMS_071	Req	NORM_EN50125_1_COMPLIANT	WTCMS	Design Phase Related - Not Architectural
SRWTCMS_072	Req	NORM_EN50155_COMPLIANT	WTCMS	Design Phase Related - Not Architectural
SRWTCMS_073	Inf	N/A	N/A	N/A
SRWTCMS_074	Req	NORM_EN61373_COMPLIANT	WTCMS	Design Phase Related - Not Architectural
SRWTCMS_075	Req	NORM_EN50499_COMPLIANT	WTCMS	Design Phase Related - Not Architectural
SRWTCMS_076	Req	NORM_EN50500_COMPLIANT	WTCMS	Design Phase Related - Not Architectural
SRWTCMS_080	Req	LEGAL_FREQ_BANDS_LAWS_COMPLIANT	WTCMS	3.6/4.5 - Frequency Band, Bandwidth and Coverage
SRWTCMS_081	Req	MAINTAIN_DEVICE_DOWNLOAD_MIN_BANDWIDTH	WTCMS	4.5 - Frequency Band, Bandwidth and Coverage
SRWTCMS_082	Rec	MAINTAIN_LIFETIME_MIN	WTCMS	Design Phase Related - Not Architectural
SRWTCMS_083	Rec	TECH_MOUNT_DIN_RAIL	WTCMS	Design Phase Related - Not Architectural
SRWTCMS_084	Rec	TECH_MOUNT_ORIENTATION	WTCMS	Design Phase Related - Not Architectural
SRWTCMS_085	Rec	TECH_MOUNT_PLACEMENT_EMC	WTCMS	Design Phase Related - Not Architectural
SRWTCMS_086	Inf	N/A	N/A	N/A
SRWTCMS_087	Rec	TECH_TRANSMIT_POWER_AUTO_ADAPT	WTCMS	Design Phase Related - Not Architectural
SRWTCMS_088	Rec	TECH_TRANSMIT_POWER_EMISSION_MAX_DB	WTCMS	Design Phase Related - Not Architectural
SRWTCMS_089	Rec	TECH_TRANSMIT_POWER_DIR_ANT_MAX_DB	WTCMS	Design Phase Related - Not Architectural
SRWTCMS_090	Rec	TECH_IFACE_CONNECTORS	WTCMS	Design Phase Related - Not Architectural
SRWTCMS_091	Inf	N/A	N/A	N/A
SRWTCMS_092	Rec	TECH_IFACE_VISUAL_POWER_COMMS	WTCMS	Design Phase Related - Not Architectural
SRWTCMS_093	Rec	TECH_PROTECTION_IP_CLASS_INSIDE	WTCMS	Design Phase Related - Not Architectural
SRWTCMS_094	Rec	TECH_PROTECTION_IP_CLASS_OUTSIDE	WTCMS	Design Phase Related - Not Architectural
SRWTCMS_095	Inf	N/A	N/A	N/A
SRWTCMS_096	Rec	TECH_SPECS_WEIGHT_MAX	WTCMS	Design Phase Related - Not Architectural

REQ ID	OBJ	SHORT TITLE	WTCMS / WTCN	Traceability - Chapter from D2.5
SRWTCMS_097	Rec	TECH_SPECS_VOL_MAX	WTCMS	Design Phase Related - Not Architectural
SRWTCMS_098	Rec	TECH_SPECS_ENCAPSULATION	WTCMS	Design Phase Related - Not Architectural
SRWTCMS_099	Rec	TECH_SPECS_POWER_SUPPLY_MIN	WTCMS	Design Phase Related - Not Architectural
SRWTCMS_100	Rec	TECH_SPECS_ED_POWER_CONSUMPTION	WTCMS	Design Phase Related - Not Architectural
SRWTCMS_101	Rec	TECH_ANT_TYPE	WTCMS	Design Phase Related - Not Architectural
SRWTCMS_102	Rec	TECH_ANT_SIZE_MAX	WTCMS	Design Phase Related - Not Architectural
SRWTCMS_103	Rec	TECH_ANT_RADOME_GROUND_CONN	WTCMS	Design Phase Related - Not Architectural
SRWTCMS_104	Req	TECH_FREC_BANDS_WIRELESS_TECH	WTCMS	3.6/4.54.5 - Frequency Band, Bandwidth and Coverage
SRWTCMS_105	Req	TECH_FREC_BANDS_COMPATIBILITY	WTCMS	3.6/4.5 - Frequency Band, Bandwidth and Coverage
SRWTCMS_106	Req	TECH_INTERFERENCE_RADIO_PROTECTION	WTCMS	4.8.1 TCMS Domain
SRWTCMS_107	Inf	N/A	N/A	N/A
SRWTCMS_108	Req	PERF_WLTBN_QOS_MEASURE_PARAMS	WTCN	2.4 Basic architecture concepts
SRWTCMS_109	Req	PERF_WLCN_QOS_LATENCY_SPECS	WTCN	2.4 Basic architecture concepts
SRWTCMS_110	Req	PERF_WLTBN_QOS_LATENCY_SPECS	WTCN	2.4 Basic architecture concepts
SRWTCMS_111	Req	PERF_WLCN_TCMS_DATA_RATE	WTCN	4.5 - Frequency Band, Bandwidth and Coverage
SRWTCMS_112	Req	PERF_WLTB_TCMS_DATA_RATE	WTCN	3 - Wireless Architecture for Consist to Consist Communications
SRWTCMS_113	Req	PERF_WLCN_TCMS_DATA_SIZE	WTCN	2.5.3 Wireless TCN
SRWTCMS_114	Req	PERF_WLTB_TCMS_DATA_SIZE	WTCN	2.5.3 Wireless TCN
SRWTCMS_115	Req	PERF_WLCN_TCMS_DATA_CYCLE_TIME	WTCN	2.5.3 Wireless TCN
SRWTCMS_116	Req	PERF_WLTB_TCMS_DATA_CYCLE_TIME	WTCN	2.5.3 Wireless TCN
SRWTCMS_117	Req	PERF_WLCN_OMTS_DATA_RATE	WTCN	2.5.3 Wireless TCN
SRWTCMS_118	Req	PERF_WLTB_OMTS_DATA_RATE	WTCN	2.5.3 Wireless TCN

REQ ID	OBJ	SHORT TITLE	WTCMS / WTCN	Traceability - Chapter from D2.5
SRWTCMS_119	Req	PERF_WLCN_OMTS_DATA_SIZE	WTCN	2.5.3 Wireless TCN
SRWTCMS_120	Req	PERF_WLTB_OMTS_DATA_SIZE	WTCN	2.5.3 Wireless TCN
SRWTCMS_121	Req	PERF_WLCN_OMTS_DATA_CYCLE_TIME	WTCN	2.5.3 Wireless TCN
SRWTCMS_122	Req	PERF_WLTB_OMTS_DATA_CYCLE_TIME	WTCN	2.5.3 Wireless TCN
SRWTCMS_123	Req	PERF_WTCN_QOS_PRIORITY	WTCN	2.5.5 - Protocols
SRWTCMS_124	Req	RED_SWITCH_OVER_ED_MAX_TIME	WTCMS	4.2 - Redundancy
SRWTCMS_126	Inf	N/A	N/A	N/A
SRWTCMS_127	Req	SERV_SUPPORT_UNIQUE_IDEN_FLEET	WTCMS	2.4 Basic architecture concepts
SRWTCMS_128	Req	SERV_PROVIDE_TOPO_TRAIN	WTCMS	3.1.2 - Safe Train Inauguration (Distribution of Train Inauguration Results)
SRWTCMS_129	Req	EXT_IF_WLTB_ALLOW_IP_PROTOCOLS	WTCN	2.5.5 - Protocols
SRWTCMS_130	Req	EXT_IF_WLCN_ALLOW_IP_PROTOCOLS	WTCN	4.1 - Functional Domains
SRWTCMS_133	Req	EXT_IF_WTCMS_SUPPORT_DHCP_OPT_61	WTCN	2.5.3.2 - WLCN-WLED Interface
SRWTCMS_134	Req	LC_WLTB&WLCN_NO_USE_PROP_IF	WTCN	2.5 - Interfaces
SRWTCMS_135	Rec	LC_WLTB_TECH_EVO_COMPATIBLE	WTCN	Design Phase Related - Not Architectural
SRWTCMS_136	Rec	LC_WLCN_TECH_EVO_COMPATIBLE	WTCN	Design Phase Related - Not Architectural
SRWTCMS_137	Rec	LC_WTCMS_TECH_WIDE_USE	WTCMS	Design Phase Related - Not Architectural
SRWTCMS_138	Rec	LC_ED_DOCUMENTED	WTCMS	Design Phase Related - Not Architectural
SRWTCMS_139	Rec	LC_ED_BASED_ON_RECYCLED_MAT	WTCMS	Design Phase Related - Not Architectural
SRWTCMS_140	Rec	OTHER_COMM_TEST	WTCN	Design Phase Related - Not Architectural
SRWTCMS_141	Inf	N/A	N/A	N/A
SRWTCMS_142	Req	ARCH_DEFINITION_COMPATIBILITY_WLCN_VS_BACKBONE	WTCN	2.5 - Interfaces
SRWTCMS_143	Req	PERF_WLTBN_QOS_PRIORITIES_APP	WTCMS	4.4 - QoS Quality of Service
SRWTCMS_144	Req	ENV_COND_SCENARIOS	WTCMS	3.7 WLTB Antennas
SRWTCMS_145	Rec	ENV_COND_MANEUVERS	WTCMS	3.7 WLTB Antennas
SRWTCMS_146	Req	ENV_COND_MIN_CURVE_RADIUS	WTCMS	3.7 WLTB Antennas
SRWTCMS_147	Req	ENV_COND_REL_SPEED_RANGE	WTCMS	3.6/4.5 - Frequency Band, Bandwidth and Coverage
SRWTCMS_148	Req	ENV_COND_ABS_SPEED_RANGE	WTCMS	3.6/4.5 - Frequency Band, Bandwidth and Coverage

REQ ID	OBJ	SHORT TITLE	WTCMS / WTCN	Traceability - Chapter from D2.5
SRWTCMS_149	Req	ENV_COND_NUM_TRAINS_PER_SQUARE_KM	WTCMS	3.1.1.5 - Conclusion
SRWTCMS_150	Req	NORM_EN60721-3-5_COMPLIANT	WTCMS	Design Phase Related - Not Architectural
SRWTCMS_151	Rec	LC_ED_BASED_ON_RoHS_COMP	WTCMS	Design Phase Related - Not Architectural
SRWTCMS_152	Req	LEGAL_INTEROPERABILITY_DIRECTIVE	WTCMS	Design Phase Related - Not Architectural
SRWTCMS_153	Req	LEGAL_SAFETY_DIRECTIVE	WTCMS	Design Phase Related - Not Architectural
SRWTCMS_154	Rec	LEGAL_SAFETY_VERIFICATION_DIRECTIVE	WTCMS	Design Phase Related - Not Architectural
SRWTCMS_155	Req	NORM_EN50126_COMPLIANT	WTCMS	Design Phase Related - Not Architectural
SRWTCMS_156	Req	NORM_EN50128_COMPLIANT	WTCMS	Design Phase Related - Not Architectural
SRWTCMS_157	Req	NORM_EN50129_COMPLIANT	WTCMS	Design Phase Related - Not Architectural
SRWTCMS_158	Req	NORM_EN50159_COMPLIANT	WTCMS	Design Phase Related - Not Architectural
SRWTCMS_159	Req	MAINTAIN_DEVICE_UPDATE_MIN_BANDWIDTH	WTCMS	3.6/4.5 - Frequency Band, Bandwidth and Coverage
SRWTCMS_160	Req	COMM_MECHANISM_SEPARATE_DATA_FLOWS	WTCMS	2.5.3.2WLCN-WLED Interface
SRWTCMS_161	Rec	REL_WED_MTBF	WTCMS	RAMS D2.4 Related
SRWTCMS_162	Rec	REL_WLTBN_MTBF	WTCMS	RAMS D2.4 Related
SRWTCMS_163	Inf	N/A	N/A	N/A
SRWTCMS_164	Rec	REL_FUNC_INAUGURATION	WTCMS	RAMS D2.4 Related
SRWTCMS_165	Rec	REL_FUNC_DATA_TRANSMISSION	WTCMS	RAMS D2.4 Related
SRWTCMS_166	Rec	REL_CALCULATIONS	WTCMS	RAMS D2.4 Related
SRWTCMS_167	Inf	N/A	N/A	N/A
SRWTCMS_168	Inf	N/A	N/A	N/A
SRWTCMS_169	Rec	AVAIL_WLTB_TCMS	WTCMS	RAMS D2.4 Related
SRWTCMS_170	Inf	N/A	N/A	N/A
SRWTCMS_171	Rec	AVAIL_WLCN_TCMS	WTCMS	RAMS D2.4 Related
SRWTCMS_172	Inf	N/A	N/A	N/A
SRWTCMS_173	Rec	AVAIL_WLTB_OOS	WTCMS	RAMS D2.4 Related
SRWTCMS_174	Inf	N/A	N/A	N/A
SRWTCMS_175	Rec	AVAIL_WLCN_OOS	WTCMS	RAMS D2.4 Related
SRWTCMS_176	Inf	N/A	N/A	N/A
SRWTCMS_177	Rec	AVAIL_CALCULATIONS_MTTR	WTCMS	RAMS D2.4 Related
SRWTCMS_178	Inf	N/A	N/A	N/A
SRWTCMS_179	Rec	AVAIL_FLOODING_DETECTION	WTCMS	Design Phase Related - Not Architectural
SRWTCMS_180	Rec	AVAIL_JAMMING_DETECTION	WTCMS	Design Phase Related - Not Architectural
SRWTCMS_181	Rec	MAINTAIN_MODULAR_DESIGN	WTCMS	Design Phase Related - Not Architectural

REQ ID	OBJ	SHORT TITLE	WTCMS / WTCN	Traceability - Chapter from D2.5
SRWTCMS_182	Rec	MAINTAIN_MODULAR_UPGRADE_OF_WLCN	WTCMS	Design Phase Related - Not Architectural
SRWTCMS_183	Rec	MAINTAIN_MODULAR_UPGRADE_OF_ED_&_WED	WTCMS	Design Phase Related - Not Architectural
SRWTCMS_184	Rec	MAINTAIN_TIME_MINIMIZING_BY_DIF_DEV_TYPES	WTCMS	Design Phase Related - Not Architectural
SRWTCMS_185	Rec	MAINTAIN_TIME_MINIMIZING_BY_ACCESS_DEV	WTCMS	Design Phase Related - Not Architectural
SRWTCMS_186	Rec	MAINTAIN_HW_&_SW_EVOL_EASILY	WTCMS	Design Phase Related - Not Architectural
SRWTCMS_187	Rec	MAINTAIN_USED_SW_MINIMIZED	WTCMS	Design Phase Related - Not Architectural
SRWTCMS_188	Rec	MAINTAIN_LRU_BY_STANDARD_WEB_BROWSER	WTCMS	Design Phase Related - Not Architectural
SRWTCMS_189	Rec	MAINTAIN_LRU_PREVENT_&_PREDICT	WTCMS	Design Phase Related - Not Architectural
SRWTCMS_190	Rec	MAINTAIN_LRU_NOT_SCHED_ACT	WTCMS	Design Phase Related - Not Architectural
SRWTCMS_191	Rec	MAINTAIN_LRU_AUTODIAGNOSIS	WTCMS	Design Phase Related - Not Architectural
SRWTCMS_192	Rec	MAINTAIN_LRU_INTERCHANGEABILITY	WTCMS	Design Phase Related - Not Architectural
SRWTCMS_193	Rec	MAINTAIN_LRU_VS_RCM	WTCMS	Design Phase Related - Not Architectural
SRWTCMS_194	Rec	MAINTAIN_LRU_SW_UPDATE_BACKUP	WTCMS	Design Phase Related - Not Architectural
SRWTCMS_195	Req	SAF_FUNC_INAUGURATION_SIL	WTCMS	Design Phase Related - Not Architectural
SRWTCMS_196	Inf	N/A	N/A	N/A
SRWTCMS_197	Req	SAF_FUNC_DATA_TRANSMISSION_SIL	WTCMS	RAMS D2.4 Related
SRWTCMS_198	Rec	SAF_CALCULATIONS	WTCMS	RAMS D2.4 Related
SRWTCMS_199	Inf	N/A	N/A	N/A
SRWTCMS_200	Req	SAF_FUNC_INAUGURATION_FDRT	WTCMS	RAMS D2.4 Related
SRWTCMS_201	Req	SAF_FUNC_DATA_TRANSMISSION_FDRT	WTCMS	RAMS D2.4 Related
SRWTCMS_202	Inf	N/A	N/A	N/A
SRWTCMS_203	Req	SAF_STATE	WTCMS	RAMS D2.4 Related
SRWTCMS_204	Inf	N/A	N/A	N/A
SRWTCMS_205	Req	SAF_VS_RED	WTCMS	RAMS D2.4 Related
SRWTCMS_206	Inf	N/A	N/A	N/A
SRWTCMS_207	Req	RED_WLTB_PERSIST_SINGLE_FAILURE	WTCMS	3.4 Redundancy
SRWTCMS_208	Inf	N/A	N/A	N/A
SRWTCMS_209	Req	RED_WLCN_PERSIST_SINGLE_FAILURE	WTCMS	3.4 Redundancy
SRWTCMS_210	Inf	N/A	N/A	N/A
SRWTCMS_211	Req	RED_WLTBN	WTCMS	3.4 Redundancy
SRWTCMS_212	Req	RED_WLTBN_VS_TOPOLOGY	WTCMS	3.4 Redundancy 3.1.7 Train Inauguration Inhibit
SRWTCMS_213	Req	RED_WLTBN_SWITCH_OVER_MAX_TIME	WTCMS	3.4 Redundancy
SRWTCMS_214	Inf	N/A	N/A	N/A

REQ ID	OBJ	SHORT TITLE	WTCMS / WTCN	Traceability - Chapter from D2.5
SRWTCMS_215	Req	RED_DEAD_CAR	WTCMS	3.4 Redundancy
SRWTCMS_216	Rec	RED_DIVERSITY	WTCMS	3.4 Redundancy
SRWTCMS_217	Req	PERF_WTCMS_JITTER	WTCMS	2.4 Basic architecture concepts
SRWTCMS_218	Inf	N/A	N/A	N/A
SRWTCMS_219	Inf	N/A	N/A	N/A
SRWTCMS_220	Inf	N/A	N/A	N/A

Legend:

Abbreviations:

- Inf Informative comment
- Rec Recommendation
- Req Requirement
- N/A Not Applicable