FP5TRANS4M-R

Transforming Europe's Rail Freight

D3.3

Digital & Data Reference System Architecture FDFT

Project acronym:	FP5-TRANS4M-R
Starting date:	2022-07-01
Duration (in months):	45
Call (part) identifier:	HORIZON-ER-JU-2022-01 (Topic: HORIZON-ER-JU-2022-FA5-01)
Grant agreement no:	101102009
Due date of deliverable:	Month 18
Actual submission date:	2024-10-02
Responsible/Author:	Wolfgang Windolf (SMO)
Dissemination level:	PU - Public
Deliverable Type:	R – Document, Report
Doc Version & Status:	V1.1 |Revised

Reviewed: (Yes)

"Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the Europe's Rail Joint Undertaking. Neither the European Union nor the granting authority can be held responsible for them."
"The project is supported by the Europe's Rail Joint Undertaking and its members."

Document history		
Revision	*Date*	*Description*
-	2024-03-26	*First draft*
1	2024-04-09	After input from review workshop
2	2024-04-15	Review
V1.1	2024-07-18	Chapters 2, 4.1, 5.4, 5.5, 5.7.2, 5.8, 7 amended after MCP meeting

Report contributors		
Name	Beneficiary Short Name	Details of contribution
Dr. Christoph Lackhove	DB	Contributor
Asa-Adzei Müller	VT	Contributor
Denes Der	AT	Contributor
Gernot Hans	AT	Contributor
Stefan Schultheis	RCA	Contributor
Ines Bachkönig	RCA	Reviewer
Andreas Schaefer-Enkeler	SMO	Author
Wolfgang Windolf	SMO	Responsible author

Reviewers		
Name	*Beneficiary Short Name*	*Details of contribution*
Dr. Markus Klohr	AT	Official Review and Feedback
Joachim Tiedemann	SMO	Official Review and Feedback

Table of Contents

List of Figures

List of Tables

1 Executive Summary

This document constitutes "Deliverable 3.3 Digital/Data reference system architecture FDFT" of ER JU Flagship Area 5 project FP5-TRANS4M-R. This document reports results from task 3.2 **FDFT reference system architecture**.

The objective of this document is to provide the Digital/Data reference system architecture and requirements based on deliverable D3.1 Functional system architecture FDFT and D3.2 Physical Reference System Architecture, in conjunction with the deliverable D2.2 User requirements of WP2 of ER JU FP5 TRANS4M-R. The Digital/Data reference system architecture will define the basis for the development of the innovations for WP5-WP12. It describes the **target of full automation** of the freight sector, as well as a subset based on the agreed technical enablers in FP5-TRANS4M-R.

The Digital/Data architectural requirements are followed by the **Digital/Data reference system architecture** including an overview as well as the logical blocks required in FDFT traction units and FDFT wagons. To allow un-restrained innovations to be used, when designing the technical enablers in FP5-TRANS4M-R, the document focusses at the Digital/Data related requirements in an open way, as much as possible.

Keywords: Digital/Data System Requirements; Digital/Data Reference System Architecture; Full Automation; Technical Enabler

2 Abbreviations & Acronyms

Abbreviation / Acronym	Description
ALG	Application Layer Gateway
ASO	Automatic Shunting Operation
ATO	Automatic Train Operation
ATP	Automatic Train Protection
CCL	Consist Control Unit
CCU	Compiled Consist List list, order, orientation of consists in a train
CONNECTA	Europe's Rail shift2Rail project "CONtributing to Shift2Rail's NExt generation of high Capable and safe TCMS and brAkes"
DAC	Digital Automatic Coupler
DAC CU	Digital Automatic Coupler Control Unit
Demo II	Due to concentration of project resources on train functions (as described in amendment #2) WP11 is focused now on the development of DAC uncoupling via push-button. Therefore, all features regarding the so-called Demo II trains are abandoned. For future purposes these features are considered in the system architecture as Demo II functions without further description."
ECN	Ethernet Consist Network
EDDP	European DAC Delivery Programme
ERA	European Railway Agency
ER JU	Europe's Rail Joint Undertaking
F-ETB	Freight Ethernet Train Backbone
F-ETBN	Freight Ethernet Train Backbone Node
FDFT	Full digital freight train
FDFTO	Full digital freight train Operation
F-TCN	Freight Train Communication network based on F-ETB, acc. to IEC 61375, 10BASE-T1L
FPSE	Flagship Project System Engineers
GCG	Ground Communication Gateway
GFM	Ground Fault Monitor
GNSS	Global Navigation Satellite System
HMI	Human Machine Interface for controlling and monitoring of a system (e.g.: lever, indicator, button, lamps, keyboard, display)
I/F	Interface
LAC	Last Active Consist

LCU	Locomotive Control Unit (i.e. CCU installed on a traction unit); term is defined to distinguish from CCU
MCG	Mobile Communication Gateway
MD	Mobile Device connectivity (e.g. FDFT Link to FDFT Backend)
MNO	Mobile Network Operator
NMEA	Nation Marine Electronics Association
NSAs	National Safety Authorities
OPEID	ID of activity as used in /WP2 D2.1/ Preliminary Operational Procedures
PB	Parking Brake
PDL	Power Distribution Line
RSL	Remote Safety Loop
RSLM	Remote Safety Loop Monitor
SL	Security Level
tbd.	To be defined
TCMS	Train Control & Management System
TPMS 2.0	Trusted Platform Module acc. to IEC 11889-1-4:2015
TSI	Technical Specifications for Interoperability
TUPSS	Traction Unit Power Supply System
UTC	Universal Time Coordinated
WGC	Wayside Communication Gateway
WP	Working package
WPSS	Wagon Power Supply System
X2RAIL	Europe's Rail shift2Rail project "Start-up activities for Advanced Signalling and Automation Systems"

3 Background

The present document constitutes the Deliverable D3.3 “Digital / Data reference system architecture FDFT” in the framework of the Flagship Project FP5- TRANS4M-R as described in the EU-RAIL MAWP and contributes as well to the Flagship Project FP5 TRANS4M-R.

The project aims to boost innovation for the European rail freight sector, concretely by developing, validating, and demonstrating TRANS4M-R technical enablers. The work to reach this level of TRL is complex and thus divided into several work packages highly dependent on each other. See WP structure in Figure 1 below

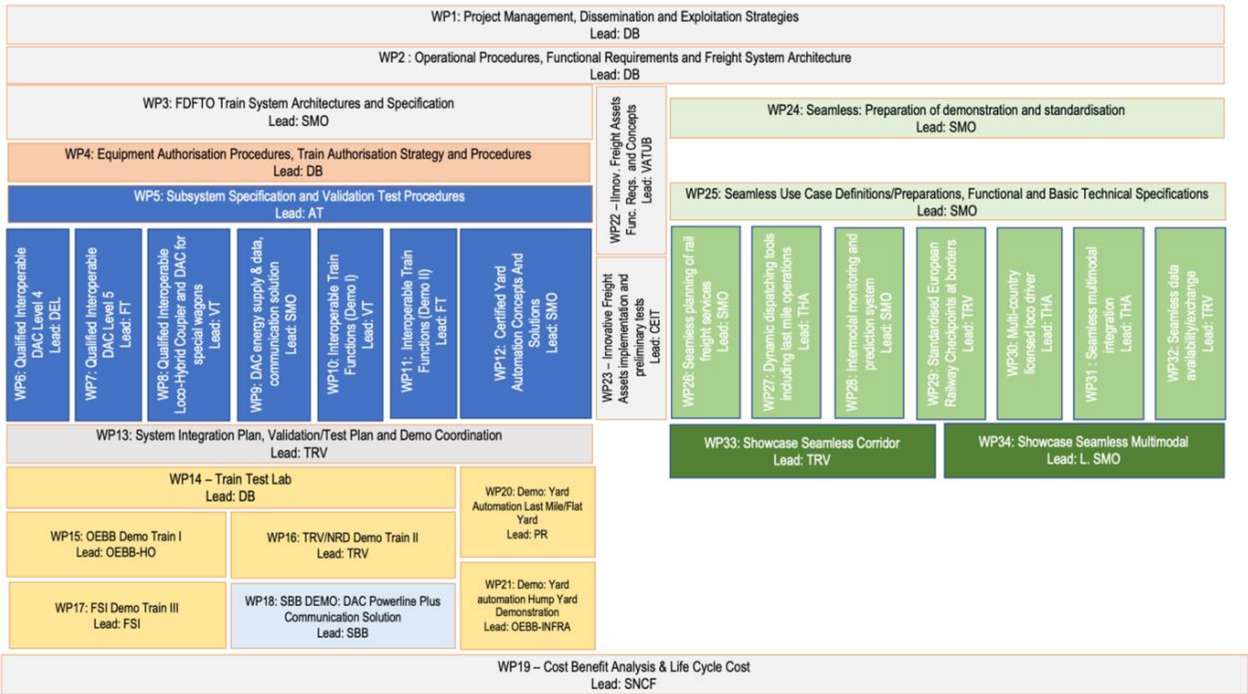

Figure 1: WP Structure in TRANS4M-R.

In WP3 the FDFTO train system architecture is defined based on various inputs either from operational requirements or from the specifications of the technical enablers for the FDFTO train.

4 Objective/Aim

The objective of this document is to provide a physical reference freight architecture FDFT concept as basis for the future work in FP5. It will be based on the functional reference system architecture concept, outlined in /WP3 D3.1/ and contains a description and specification for a physical reference system of rolling stock and the interfaces to the infrastructure.

4.1 Task Description

Task 3.3 started in month seven and the outputs of the task are included in this document as well as its sister document /WP3 D3.2/.

For the work a core team was established with experts for the relevant technical enablers. The team met after finishing /WP3 D3.1/ once a week to provide the relevant input to the document and to check if the input provided fits to the overall architectural concept.

Another group of experts, consisting of experts from other WPs was set up to ensure a continuous review process of the work done by the core team. This so-called review team met once a month with the core team to discuss the preliminary results. The purpose of these joint meetings was to disseminate the working progress and to get early feedback from the experts of the other WPs. The draft versions of this deliverable have been available at any time in the FP5 ProjectPlace to all members of all WPs. After discussion and agreement in the WP3 core group, the feedback has been incorporated into the deliverable.

Additionally, a mid-term on-site workshop was held for the alignment of the work done so far and the closure of open points.

The following table gives the direct match of the task definition from the grant agreement with the output. According to the task description a description and specification of the reference system (wagon/locomotive/infrastructure) is required. The infrastructure part is not in the scope of this deliverable because it is covered in WP2. However, the interfaces between rolling stock and infrastructure are covered in this deliverable. The deliverable shall serve as basis for implementation design of every wagon. The scope of the deliverables is extended to traction units because they play a significant role in FDFTO.

	Task definition from proposal	Output of WP3
Task 3.3	Based on the outcomes of Task 3.2 a base system will be designed. A description and specification for a physical (wagon/locomotive/infrastructure) reference system as basis for implementation-design of every wagon and a specification for a digital/data (applications) reference system architecture.	Deliverable D3.2: Physical reference system architecture FDFT Deliverable D3.3: Data reference system architecture FDFT

5 Digital/Data reference system architecture FDFT

5.1 System of interest

The system of interest is sketched in the following diagram. The two areas are denoted as “landside” and “trainside”. The trainside is covered in this document whereas the “landside” is covered by WP2.

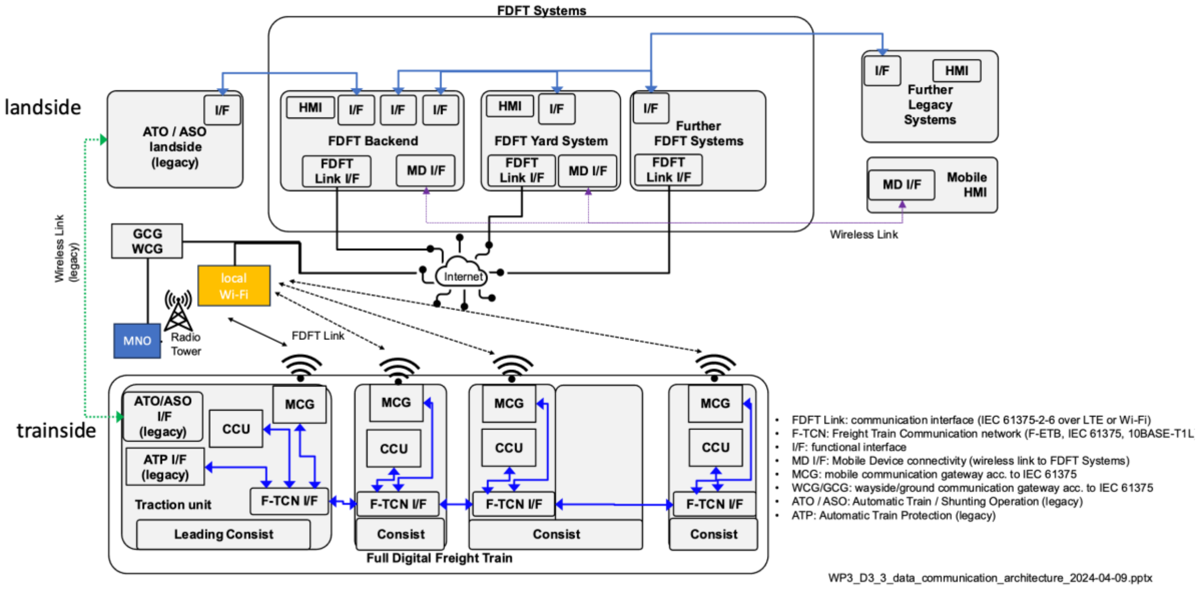

Figure 2: Overview of FDFTO System

5.2 New functional requirements

When deriving the data/digital reference system architecture from existing functional requirements (D3.1 functional system architecture) and D2.2 User requirements, new functional requirements might result. These new functional requirements are captured in this chapter.

e.g.: The management of the underlying communication network and / or wireless FDFT-Link to the landside FDFT-systems imposes new requirements to the CCU.

5.2.1 Management interface of MCG

The management of the MCG to control the settings for the wireless FDFT-Link, requires an out-of-band interface between the CCU and the MCG. This interface and the digital & data interface to be used is supplier specific.

5.3 Update of functional reference architecture

When deriving the physical architecture from existing functional reference system architecture /WP3 D3.1/, new functional blocks might become necessary. These new functional blocks are captured in this chapter.

No additional functional blocks are identified so far.

.

5.4 FDFTO Wagon Digital / Data Reference System architecture

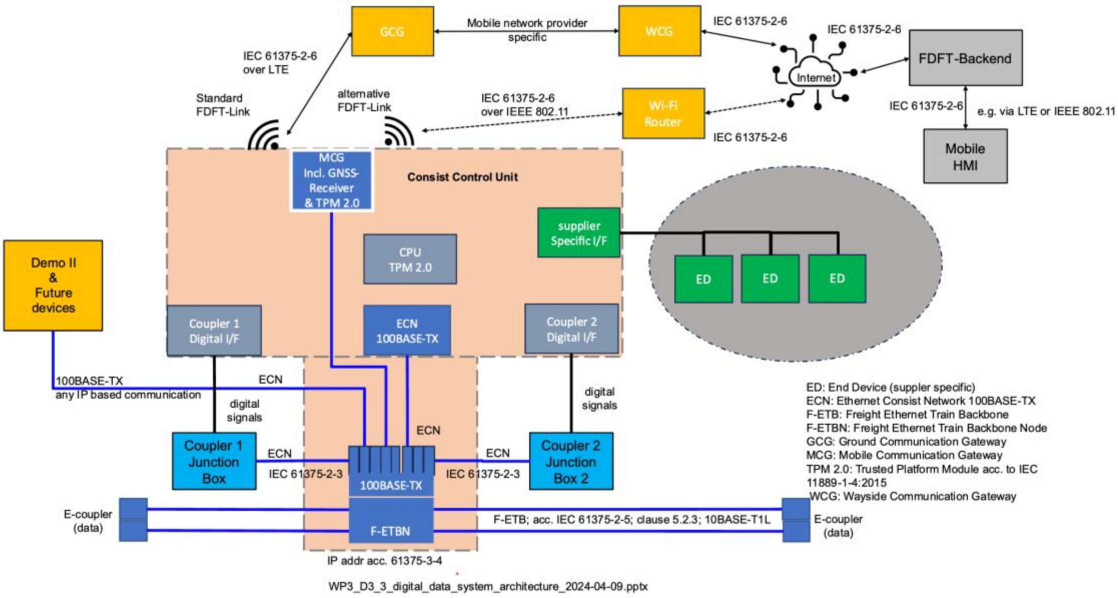

Figure 3: FDFTO Wagon Digital / Data Reference System Architecture

In the diagram above, the FDFT wagon digital/data reference system architecture is shown. This wagon digital/data reference system architecture shall support all functional requirements as described in /WP3 D3.1/, user requirements as described in /WP2 D2.2/ and requirements resulting from specification of the physical reference system architecture /WP3 D3.2/ by specifying a consist internal communication system, a train-wide-communication system (F-TCN) and a wireless FDFT-Link for information exchange with the landside FDFT systems.

In addition to the message-based data communication, the necessary digital interface protocols are specified (e.g.: passive consist detection, wake-up interface, digital interface to the coupler, push button-based control of coupler …).

The standardization of interfaces is restricted to those between the three domains (Coupler, Communication, CCU). All other interfaces can be implemented on a supplier specific approach, although the still following the general requirements as stipulated in chapter 5.7.

The requirements to the standardized interfaces are described hereinafter.

5.4.1 Coupler System

5.4.1.1 M-Coupler

This topic is covered in detail in /WP5 D5.2/ and described in the document covering the so-called coupler domain. There exists no direct interface with FDFT but indirectly via the coupler domain – CCU I/F.

5.4.1.2 E-Coupler

This topic is covered in detail in the deliverable /WP5 D5.2/. All aspects of mechanical layout, contacts selected, cover lid, ... are transparent to the digital / data reference system architecture.

5.4.1.3 Interface CCU – Coupler domain

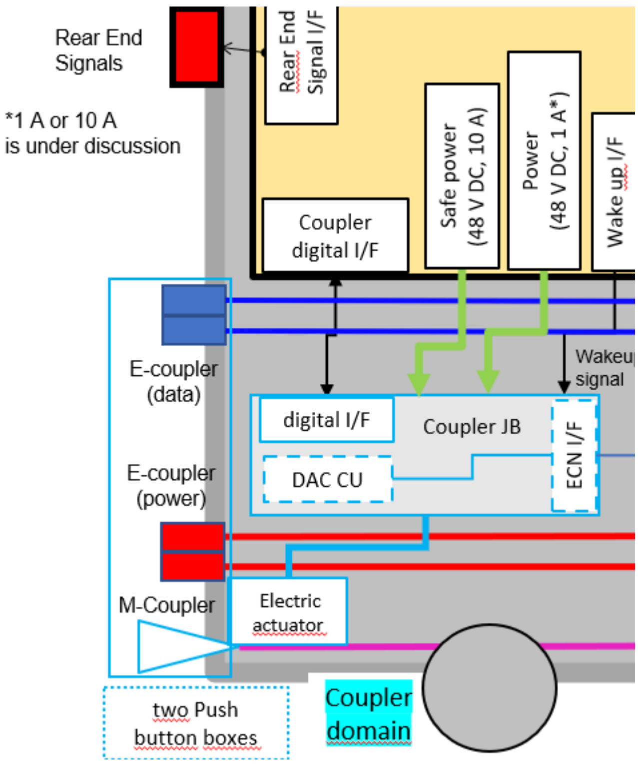

Figure 4: CCU - Coupler Interface

In the diagram above, the required interfaces between CCU domain (see /WP3 D3.2/ for details) and coupler domain are shown. As of now, two different interfaces (digital discrete vs. network based) shall be supported by the CCU to maintain the project time schedule for the so-called demo trains.

Both options will be developed and tested in parallel. Based on the outcome of these tests a final decision for one concept (either digital or network based) will be taken after field tests have been performed.

5.4.2. Consist Control Unit

The consist control unit of the wagon hosts the train functions, which are defined in deliverable /WP5 D5.1/.

The communication between other consist control units in a train, shall be performed solely via the F-ETB.

5.4.3. Wagon Power Supply System

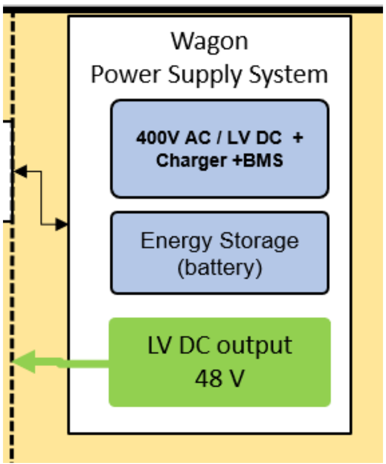

Figure 5: Wagon Power Supply System

The wagon power supply system is part of the CCU domain (see /WP3 D3.2/ for details) and thus is handled supplier specific.

5.4.3.1 Power Management Control Interface

This interface is supplier specific.

5.4.3.2 Power Management

The power management is supplier specific. The functional requirements from deliverable /WP3 D3.1/ shall be fulfilled.

The messages used for controlling the maximum power a WPS can take from the Power Distribution Line (PDL) shall be exchanged with the CCU using the IEC 61375-2-6 based protocol.

The messages containing information about the WPS shall be provided by the CCU using the IEC 61375-2-6 based protocol.

The detailed protocol requirements to control & monitor the WPS shall be described in deliverable /WP5 D5.4/

5.4.4 Brake System

All interfaces between CCU and brake components will be supplier specific and are not defined in this document.

All information, which needs to be exchanged between consists in the same train, shall be exchanged via the F-ETB, complying with the requirements out of chapter 5.6.2. Communication System

The protocol to be used shall be based on IEC 61372-2-6.

The protocol details (detailed message format) shall be defined in /WP5 D5.1/.

The number and type of independent data elements shall allow to reach the safety level prescribed respectively by /WP4 D4.2/ and an accuracy suitable for the use of this function described in /WP5 D5.1/.

5.4.4.1. Brake Pipe monitoring

This section provides the list of requirements for the digital & data reference architecture components which will enable the monitoring of the Brake Pipe on each consist, as requested in section 9.3.17 of /WP3 D3.1/.

Since the Brake Pipe pressure remains the input for the distributors (even in case of the future EP-brake implementation), it is one of the main parameters to be checked to perform the diagnostics of the brake system.

The monitoring of Brake Pipe can be used also in the context of ABT for:

- Brake Pipe continuity check and (directly measuring the Brake Pipe pressure on each wagon along the train, besides checking the consequent state of the brakes)
- Leakage test (providing multiple points of measure instead of just the one on the Traction Unit)

Rationale:

The Brake Pipe monitoring data is considered interchangeable, although the number and type of pressure transducers can be chosen by the suppliers as long as the above requirements are fulfilled.

5.4.4.2. Automated Brake Test

A master – slave approach is considered, where the CCU of each consist is the slave electronic unit providing the information to the Master of ABT (e.g. CCU on Traction Unit) about the different states of brake system.

The number and type of independent data elements shall allow to reach the safety level prescribed respectively by /WP4 D4.2/ and an accuracy suitable for the use of this function described in /WP5 D5.1/.

5.4.4.3. Automated Parking Brake Requirements

This topic is not more in scope of this document because the functionality has been moved to Demo II. The chapter will be updated when the requirements will have been defined.

5.4.4.4. Network based EP-Brake Requirements

This topic is not more in scope of this document because the functionality has been moved to Demo II. The chapter will be updated when the requirements will have been defined.

5.5 FDFTO Traction Unit Digital / Data Reference System architecture

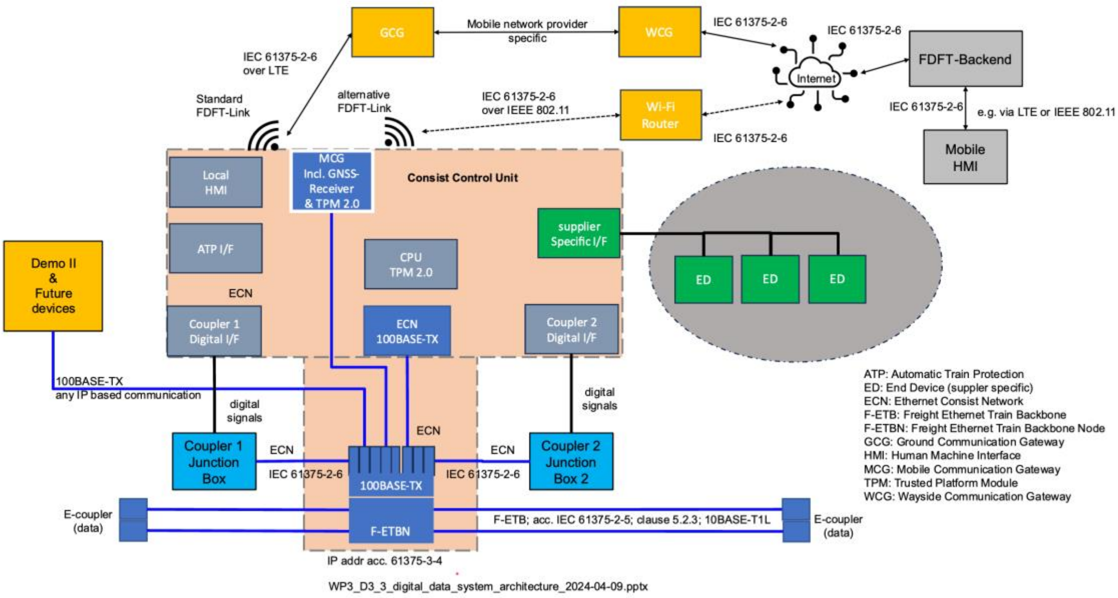

Figure 6: FDFTO Traction Unit Digital / Data Reference System Architecture

In the diagram above, the FDFT traction unit base system digital/data reference architecture is shown. This FDFT traction unit base system shall support all functional requirements as described in /WP3 D3.1/ by providing a consist internal communication system, a train-wide-communication system (the F-ETB), and a FDFT-Link (via MCG) for wireless information exchange with the landside FDFT systems.

In addition to communication, the power supply and the traction unit related further requirements are defined.

The standardization of interfaces is restricted to those between the three domains (Coupler, Communication, CCU). All other interfaces can be implemented on a supplier specific approach, although the still following the general requirements as stipulated in chapter 5.7.

The requirements to the standardized interfaces are described hereinafter.

5.5.1. Coupler System

5.5.1.1. M-Coupler

This topic is covered in detail in /WP5 D5.2/ and described in document covering the so-called coupler domain. There exists no direct interface with FDFT but indirectly via the coupler domain – CCU I/F.

The so-called hybrid coupler is not considered in this document: We consider only the DAC-part of this hybrid coupler, which shall behave identically to the DAC.

The hybrid coupler is described in /WP5 D5.2/.

5.5.1.2. E-Coupler

This topic is covered in detail by the /WP5 D5.2/. All aspects of mechanical layout, contacts selected, cover lid, … are transparent to the digital/data system architecture.

For the digital/data system architecture, the E-coupler is providing the means of interconnecting the F-ETBN between the consists.

5.5.2 Traction Unit Control Unit

The consist control unit of the traction unit shall host the train functions, which are defined in /WP5 D5.1/.

5.5.3 Traction Unit Power Supply System

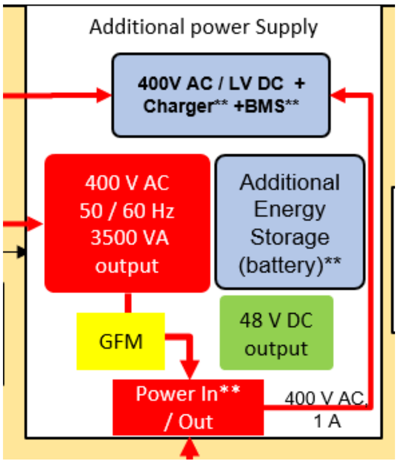

Figure 7: Traction Unit Power Supply System

The Traction Unit Power Supply System (TUPSS) is part of the CCU domain (see /WP3 D3.2/ for details) and thus is handled supplier specific. The “Power In** / Out” switch is under discussion and will be defined after the open topics, “dead” loco has been closed.

5.5.3.1. Power Management Control Interface

This interface between the CCU and the TUPSS is supplier specific and thus not described in this document.

5.5.3.2. Power Management

The power management is supplier specific. The functional requirements from /WP3 D3.1/ shall be fulfilled.

5.5.3.3. Input 400 V AC

This interface is supplier specific and thus not described here.

The TUPSS shall be able to accept more power from the PDL upon remote request (for future use).

The protocol for negotiation of higher power input shall be based on IEC 61375-2-6.

Rationale: This functionality gives the opportunity to recharge batteries faster, when more power for each consist is available (e.g.: traction unit hauling less than 50 consists).

Remark: The provisioning of electrical power is restricted to 50 consists (wagons) electrically connected to one traction unit, whereas the system limit for communication between consists is defined to be 104 vehicles (4 traction units, 100 wagons).

The detailed requirements to the TUPSS will be defined in /WP5 D5.4/.

The additional application specific protocol elements shall be defined in /WP5 D5.1/.

5.5.3.4 Battery Management System (BMS)

This component and its interface to the CCU is supplier specific.

The BMS shall provide overall diagnostics (e.g. state of charge) upon request via the CCU to the requesting entity (e.g. traction unit, FDFT backend). The detailed requirements will be defined in /WP5 D5.4/.

5.5.3.5 Power Distribution Line monitoring

The PDL shall be monitored by a circuit to detect contact issues on the E-Coupler (power) insulation or ground faults. The implementation is supplier specific and thus not described in this document.

The diagnostic messages contents related to contact monitoring shall be defined in /WP5 D5.4/.

5.5.4 Brake System

All interfaces between CCU and brake components will be supplier specific and are not defined in this document.

All information, which needs to be exchanged between consists in the same train, shall be exchanged via the F-ETB, complying with the requirements out of chapter 5.6.2. Communication System

The protocol to be used shall be based on IEC 61372-2-6.

The protocol details (detailed message format) shall be defined in /WP5 D5.1/.

The number and type of independent data elements shall allow to reach the safety level prescribed respectively by /WP4 D4.2/ and an accuracy suitable for the use of this function described in /WP5 D5.1/.

5.5.4.1 Brake Pipe Monitoring

This section provides the list of requirements for the digital & data reference architecture components which will enable the monitoring of the Brake Pipe on each consist, as requested in section 9.3.17 of /WP3 D3.1/.

Since the Brake Pipe pressure remains the input for the distributors (even in case of the future EP-brake implementation), it is one of the main parameters to be checked to perform the diagnostics of the brake system.

The monitoring of Brake Pipe can be used also in the context of ABT for:

- Brake Pipe continuity check and (directly measuring the Brake Pipe pressure on each wagon along the train, besides checking the consequent state of the brakes)
- Leakage test (providing multiple points of measure instead of just the one on the Traction Unit)

Remark: in the future, when EP-brake will be implemented during Demo II, it will heavily rely on this measurement. Moreover, in the future extended brake monitoring functionalities can also make use of the BP monitoring (e.g. brake diagnostics during running condition).

Rationale:

The Brake Pipe monitoring data is considered interchangeable, although the number and type of pressure transducers can be chosen by the suppliers as long as the above requirements are fulfilled.

5.5.4.2 Automated Brake Test

A master – slave approach is considered, where the CCU of each consist is the slave electronic unit providing the information to the Master of ABT (e.g. CCU on Traction Unit) about the different states of brake system.

The number and type of independent data elements shall allow to reach the safety level prescribed respectively by /WP4 D4.2/ and an accuracy suitable for the use of this function described in /WP5 D5.1/.

5.5.4.3 Automated Parking Brake Requirements

This topic is not more in scope of this document because the functionality has been moved to Demo II. The chapter will be updated when the requirements will have been defined.

5.5.4.4 Network based EP-Brake Requirements

This topic is not more in scope of this document because the functionality has been moved to Demo II. The chapter will be updated when the requirements will have been defined.

5.5.5. CCU – ATP I/F

The interface shall be used for forwarding the information with respect to the train length and train integrity from the CCU to the ATP (ERTMS) device at high safety level.

Rationale: The ATP device shall provide train length information to the ground with SIL 4 and train integrity information with SIL 2. This requirement is based on the proposal from ER JU FA5 System Pillar WP3.1 FDFTO/ERTMS - Train Integrity and Train Length.

This interface between CCU and ATP will be supplier specific and not described here in detail but is assumed to be Ethernet based message exchange.

5.6 Common Interfaces

These interfaces are defined commonly for all consists (i.e. wagons as well as for traction units).

5.6.1 Coupler domain – CCU

The CCU shall support two interface approaches for communicating with the DAC coupler. This has been agreed to gather experience in upcoming field trials before the final decision for one of both interface approaches will be taken.

5.6.1.1 Network-based interface

The network-based interface shall use the ECN in order exchange information as mentioned below.

The data bus signals that shall be supported by the CCU and the DAC CU are listed in Table 1: Data Message Signals.
Remark: The table is based on the input from the work packages WP6 – WP8 and reflects the current status as of 2024-02-29.

The detailed description of the data bus signals to be used will be in /WP5 D5.1/.

Parameters:

- Commands: to be defined in /WP5 D5.1/
- Responses: to be defined in /WP5 D5.1/
- Diagnostics, error messages: to be defined in /WP5 D5.1/

Table 1: Data Message Signals

Data message	Safety Signal	Values	Sender	Receiver	Size data type	PD	MD	Period TX	Period RX
Train Mode	Yes	Shunting Train Run	CCU	DAC CU	BOOL	X		100 ms	100 ms
Decoupling	Yes	Activated Not Activated	CCU	DAC CU	BOOL	X		100 ms	100 ms
Prevent Coupling	Yes	Activated Released	CCU	DAC CU	BOOL	X		100 ms	100 ms
Heartbeat DAC CU	Yes	Milliseconds Counter	DAC CU	CCU (RSL)	Unsigned 32	X		100 ms	100 ms

Heartbeat CCU (RSL)	Yes	Milliseconds Counter	CCU (RSL)	DAC CU	Unsigned 32	X		100 ms	100 ms
Errors RSL	Yes	TBD	CCU (RSL)	DAC CU	TBD	X		100 ms	100 ms
Errors DAC CU	Yes	TBD	DAC CU	CCU (RSL)	TBD	X		100 ms	100 ms
Safe Power Supply 48 VDC	Yes	Enabled Disabled	CCU (RSL)	DAC CU	BOOL	X		100 ms	100 ms
Battery voltage status	No	TBD	PMM	CCU / DAC CU	STRUCTURE (Operating and charge status)	X		100 ms	100 ms
Coupler Status (Position of locking mechanis m)	Yes	Coupled Decoupled Ready to couple. Prevent Coupling Unknown	DAC CU	CCU	ENUMERAT ION	X		100 ms	100 ms
Time	No	TCN Time	CCU	DAC CU	TIMEDATE4 8 (IEC 61375-1)		X		
Couple partner	Yes	Detected Not Detected	DAC CU	CCU	BOOL	X		100 ms	100 ms
UIC Wagon number		Number of the Wagon	CCU	DAC CU	Unsigned 32		X		
GPS Position		GPS Position of the Wagon	CCU	DAC CU	TBD	X		500 ms	500 ms
Wagon Speed		Actual speed of the Wagon	CCU	DAC CU	Unsigned 32	X		500 ms	500 ms

5.6.1.2. Digital signal-based interface

All digital signals as listed in "Table 2: DAC 5 Digital Interface Connections" shall be exchanged between the CCU and the coupler junction box.
Remark: The table is based on the input from the work packages WP6 – WP8 and reflects the current status as of 2024-02-29.

The interface signals that shall be supported by the CCU and the coupler section are listed in Table 2: DAC 5 Digital Interface Connections.

The detailed description of the signals and the signalling pulses are to be defined in /WP5 D5.1/.

Table 2: DAC 5 Digital Interface Connections

Interface signals \ cases	Pin count	connector	remark
Transit lines through the electrical coupler:			
4* SPE incl. neighbour detection	4	X5	
4* Power Line 400VAC	4	X9	
Reserve signals needed?	?		Tbd.
Interface signals and energy supply at each coupler:			
Electrical Power 48 VDC input (power save mode dependent)	1	X8	
Electrical GND input	1	X8	
Safe Power 48 VDC input - decoupling actuation	1	X6	
Safe GND input - decoupling actuation	1	X6	

Monitoring mechanically coupled (2 x signal, 2 x power)	4	X6	
Monitoring mechanically (uncoupled and) ready to couple position (2 x signal, power will be taken from signal above)	2	X6	
Reserve sensor (2 x signal, power will be taken from signal above)	2	X6	
Monitoring Hybrid coupler position (not used on wagons) UIC mode (2 x signal, 2 x power)	4	X6	only for hybrid coupler
Monitoring Hybrid coupler position (not used on wagons) DAC mode (2 x signal, power will be taken from signal above)	2	X6	only for hybrid coupler
Monitoring Hybrid locked (2 x signal, power will be taken from signal above)	2	X6	only for hybrid coupler
Activation of coupler actuator to decouple + prevent coupling	2	X8	
Activation of coupler actuator to ready to couple position	2	X8	
Ethernet Consist Network (100BASE-TX)	4 +	X7	+ Shielding required
Push-Button Box (2 push buttons antivalent) input	6	X4	Out of scope
Permanent power 48 VDC input	2	X8	Tbd.

5.6.2. Communication System

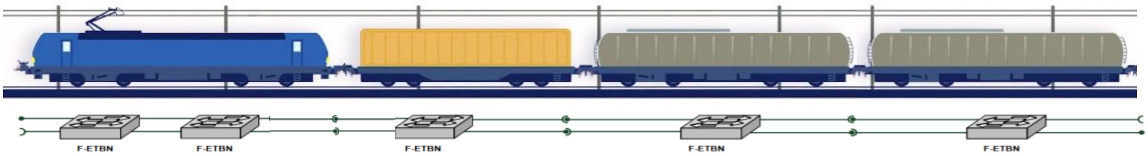

Figure 8: Freight Ethernet Train Backbone (acc. to IEC 61375-1)

5.6.2.1. Reference architecture

A reference architecture of a freight wagon communication subsystem is shown in Figure 10: F-ETBN* Interfaces. Central component is the F-ETBN, which connects the consist network with the train communication backbone (F-ETB). Consist local subsystems are interconnected via the consist network. The Consist Control Unit (CCU) hosts the train functions and controls the F-ETBN.

A list of all components, which together establish the communication system, is presented in.

Note that the communication system architecture in locomotives might be different. Reason is that many locomotives have already a control infrastructure, and the F-ETB is an add-on which needs to be integrated with the existing control system. As this is a special case highly dependent on the locomotive type this is not further detailed here. Nevertheless, the interfaces and functions defined herein are valid for locomotives as well, independent from the architecture.

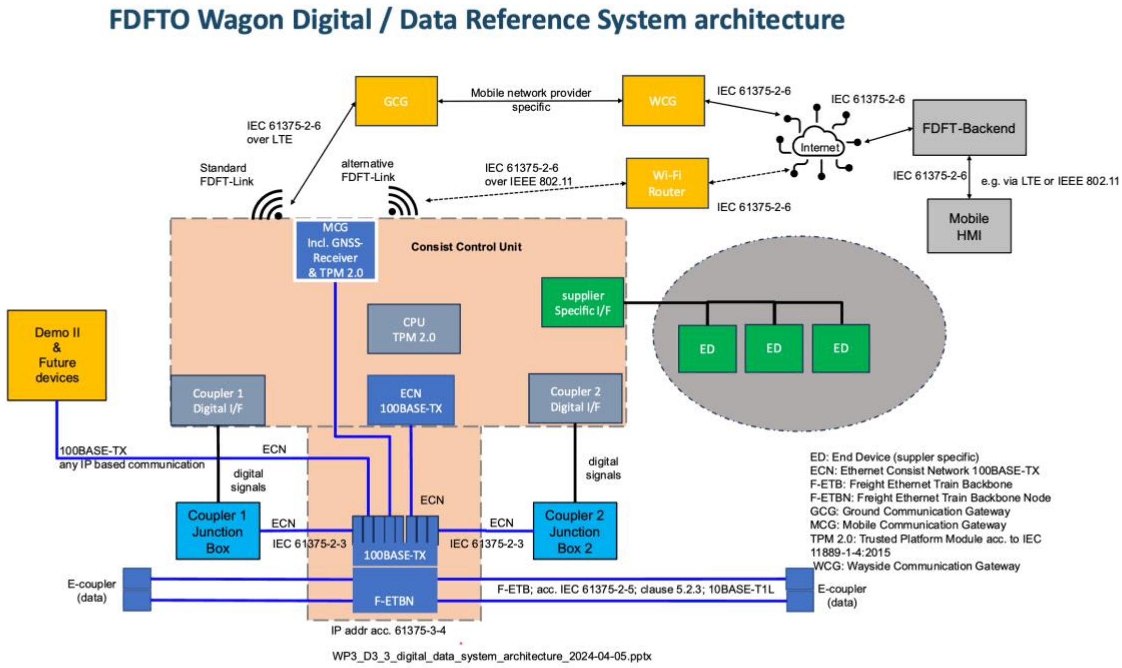

Figure 9: FDFTO Wagon / Digital / Data Reference System Architecture

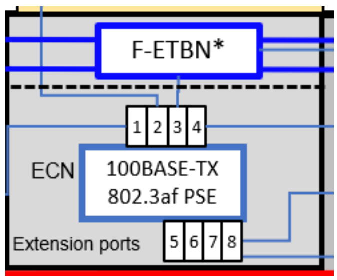

Figure 10: F-ETBN Interfaces*

The F-ETBN* interfaces consist of:
(remark: * denotes that the F-ETBN features are part of IEC 61375-2-3 ED2 that is planned to be published in summer 2024). The relevant additions are stipulated here:

- New subclause 6.9: wakeup process
- New subclause 6.10: passive wagon detection process
- New Annex part E.3.5: CCU-ETBN Interface for Wakeup control
- New Annex part E.3.6: CCU-ETBN Interface for passive wagon detection control
- New Annex part E.6.5: CCU-ETBN Interface for inserting a TLV packet (which itself is defined in Annex J) into HELLO frames
- New Annex part E.6.6: CCU-ETBN Interface for reading a TLV packet (which itself is defined in Annex J) inserted into received HELLO frames
- Annex J: Background information about freight trains, specification of automatic decoupling process

Table 3: Communication System Components

Component	Description
F-ETB	Freight Ethernet Train Backbone with cables and connectors.
F-ETBN	The Freight Ethernet Train Backbone Node (F-ETBN) connects the onboard devices and subsystems to the SPE-based Ethernet Train Backbone (F-ETB). Basic functions of the F-ETBN are: • Train Network Discovery as defined in IEC 61375-2-5 • Forwarding of Ethernet frames along the F-ETB (IEEE 802.1Q bridging) • Bypass in case of defective F-ETBN or powerless consist (passive consist) • IP packet routing between ECN and F-ETB • Train Composition Detection as defined in IEC 61375-2-3 including: o Set/reset "leading" o Train composition confirmation o Train composition correction o TTDB computation • Support of wake-up function • Support of passive consist detection • Optional: IP packet filtering (firewall)
Consist Network (ECN)	Consist local Ethernet network compliant to IEC 61375-3-4 (100BASE-TX).
CCU (Consist Control Unit)	Processing unit for train functions (list not exhaustive): ▪ train composition validation ▪ control of passive consist detection ▪ train integrity supervision ▪ train length determination ▪ control of wake-up function ▪ automatic brake test ▪ automated uncoupling ▪ …
MCG	Mobile Communication Gateway for train-to-ground communication
Junction Box	Box for providing a standardized E-coupler interface.
DAC	E-Coupler
DAC CU	DAC Control Unit.

5.6.2.2. F-ETB (Freight Ethernet Train Backbone)

5.6.2.2.1 General

This section defines the in-train communication system which is responsible for interoperable data exchange between consists over Freight Ethernet Train Backbone (F-ETB) based on Single Pair Ethernet (SPE) technology. It does not specify consist local functions and consist local interfaces which don't affect the interoperable F-ETB data communication as for example interfaces to local subsystems or IO devices. The latter should be subject of the related consist communication subsystem specification (WP5).

The Freight Ethernet Train Backbone (F-ETB) is the connection of Freight Ethernet Train Backbone Nodes (F-ETBN) based on switched technology using a redundant, aggregated transmission media as defined in IEC 61375-1 (Figure 8: Freight Ethernet Train Backbone (acc. to IEC 61375-1)). Each consist contains at least one F-ETBN. Critical consists like leading locomotives could host 2 F-ETBN for improved availability. A minimum of one and a maximum of 127 F-ETBN shall be supported.

5.6.2.2.3 Addressing

The IP address map is defined as following:

- IEC 61375-2-5 and IEC 61375-3-4 define:

  - Train subnet: 00001010.1bbsssss.sshhhhhh.hhhhhhhh/18

  - Consist Network: 10.0.0.0/9, train-wide addressable (R-NAT): 10.0.0.0/18

- All train-wide addressable ED receive a source IP address in range 10.0.0.0/18

  - This local range can be mapped to train global range (train subnet) via R-NAT.

- 10.0.0.0/18 range needs to be subdivided for the different VLANs.

- Other local networks, which don’t require train-wide access, could also use other ranges, like local private networks 192.168.0.0/16, 172.16.0.0/12 or 169.254.0.0/16 [RFC3972], but also addresses from the 10.0.0.0/9 range except those reserved for train-wide addressability.

- e.g. for service access

- MAR has to ‘NAT’ (port forwarding) between the global wayside address and the local address

NOTE:
IEC 61375-2-5 allows more than one train subnet ('sssssss') per consist. This possibility shall not be used here.

5.6.2.2.4 Interfaces

To support consist interoperability and component exchangeability, a set of generic, well-defined interfaces must be specified and standardized. Besides those generic interfaces there might be local interfaces, typically for connecting subsystems or sensors/actuators, which are CCU design specific.

A list of generic interfaces is provided in Table 4: Generic Communication System Interfaces.

Table 4: Generic Communication System Interfaces

Interface	Description
F-ETB Interface	Physically, the F-ETB interface defines the interface between the F-ETBN and the F-ETB. Logically, it defines the interface between consists. For consist interoperability, mechanical detachability, electrical connectivity, and data communication connectivity have to be ensured. Data connectivity is specified with IEC61375-2-5 and IEC61375-2-3 for the communication layers (lower OSI layers). Application data itself are specified with freight train specific application profiles. Only the specification of the communication layers is in F-TCN scope.
E-Coupler Head Interface	This is the mechanical interface between E-couplers
Junction Box interface	Interface to sensors within the junction box (e.g., current sensors for the forked power line).
DAC-CU Interface	This interface is used to read sensor data like coupling state or to drive actuators like the actuator used for safe decoupling.
Subsystem Interface	Interface to local subsystems (optional)
I/O Interface	Local IO channels (optional)

5.6.2.2.5 Functions

There are a set of functions which the communication system has to provide or to support. Those functions are listed in Table 5:

Table 5: Communication System Functions

Function	Description
Support Ethernet Communication	Basic network function for propagating Ethernet frames within a OSI Layer 2 network (like F-ETB or F-ECN). This function is based on IEEE 802.1Q and deals with: ▪ frame relaying and forwarding ▪ link aggregation ▪ Quality of Service (QoS) ▪ Unicast/multicast ▪ Virtual LAN
Support F-ETB Bypass	F-ETBN shall be automatically bypassed in case of power-fail or a device defect.
Provide power to ED	Power over Ethernet (PoE, IEEE 802.3af/at) and Power over Dataline (PoDL, IEEE 802.3bu) is a feature which can be used to provide power to local end devices like sensors or actuators over the Ethernet cable.
Train Network Topology discovery	The function "Train Network Topology Discovery" is that part of the train inauguration which discovers the F-ETB topology as a sequence of F-ETBN devices and related consists. The Train Network Topology Discovery is specified in IEC 61375-2-5. The train inauguration protocol defined in this standard works as follows: Neighbourhood of F-ETBNs is discovered by exchange of HELLO frames between adjacent F-ETBNs, and the discovery result, together with the information of the consist the F-ETBN belongs to (identified by the cstUUID value), is communicated to all other F-ETBN with TOPOLOGY frames. Each F-ETBN, after having received TOPOLOGY frames from all (active) F-ETBN, is able to determine the sequence and orientation of all F-ETBN and related consists along the F-ETB. This information is stored in the Train Network Directory (TND) and is constantly kept up-to-date. With this information, F-ETBNs are able to configure their IP routes for application data exchange between ECN and F-ETB. After the Train Network Topology Discovery, train wide communication based on IP (and IP addresses) is possible.

Function	Description
Support IP communication	The function "support IP communication" shall ensure that end devices and network devices connected to F-TCN are able to exchange data using protocols which are based on IP as defined in RFC791. IP based protocols, which are important for the F-TCN, are the transport layer protocols UDP and TCP, the redundancy protocol VRRP, the group management protocol IGMP and application layer protocols like NTP, DHCP and TRDP. Also, DNS, which is used to resolve 'names' to IP addresses, is itself based on IP. This function supports all that what is needed for IP communication, starting with addressing of IP datagrams, the protocol itself, and routing of IP datagrams between different (V)LANs. For data transfer within the different (V)LANs, IP datagrams are encapsulated in Ethernet frames. Furthermore, the transport layer with its protocols UDP and TCP is specified.
Support Train Composition Detection	The function "Support Train Composition Detection" intends to provide information about the actual train composition to end devices application software. A train composition is determined by the following parameters: ▪ the number of consists (parameter 'numConsistsInTrain') ▪ the sequence number of each consist in the train (parameter "trnCstNo') ▪ the orientation of each consist in the train with respect to the train reference direction (parameter 'Orientation') ▪ the consists static properties (id, owner, type, supported functions, ...) ▪ the consists dynamic properties (e.g. "leading") The actual train composition information is kept in an internal database, where it can be retrieved from users by using respective interface protocols. The train inauguration function, which is responsible to determine the train composition, can be split into three sub-functions, which are related to the computation of the TTDB and the notification of a train topology change. These three functions are: • Train network topology discovery as defined above • Train directory computation (as specified in IEC 61375-2-3)

Function	Description
	• Operational train directory computation (as specified in IEC 61375-2-3
Support end device IP configuration	Function to configure connected end device location specific. Implemented with DHCP as specified in IETF RFC 2131 with options defined in IETF RFC 2132.
Support name-based addressing	Function to support the train wide addressing with Universal Resource Identifiers (URI). A train specific URI schema is defined in IEC 61375-2-3. Name based addressing is using a Domain Name System (DNS) server as specified in IETF RFC 1034/1035.
Handle Date and Time	Distribution of date and time information received from a time source like the MCG using Network Time Protocol (NTP) as specified in IETF RFC 5905.
Support F-ETB Control	These are functions for train inauguration control like: • Leading request • Confirmation/Correction • Train inauguration inhibition • Retrieve F-ETB status information. • Retrieve train composition information. • Wakeup request • Passive consist detection control These functions are specified in IEC 61375-2-3 Annex E.
Support online monitoring and diagnostics	Read status and statistic information from network devices. Can be used for network diagnosis. Protocols to be used are SNMP (IETF RFC 3410) and NetConf (IETF RFC 6241).

5.6.2.2.6 Virtualized reference architecture and IP address map

The virtualized reference architecture defines the subnetting of the physical LANs into a set of VLANs. The motivation behind is to have a further separation of mixed-criticality data. More in detail, a separation is done in the following manner:

- ECN: VLAN separation for application, network device service access and maintenance access
- IEC 61375-2-5 considers only one F-ETB VLAN per F-ETB
  - Used for application and network device service access
  - Further F-ETB VLAN could be used for T2G

All the VLANs with their characteristics are described underneath.

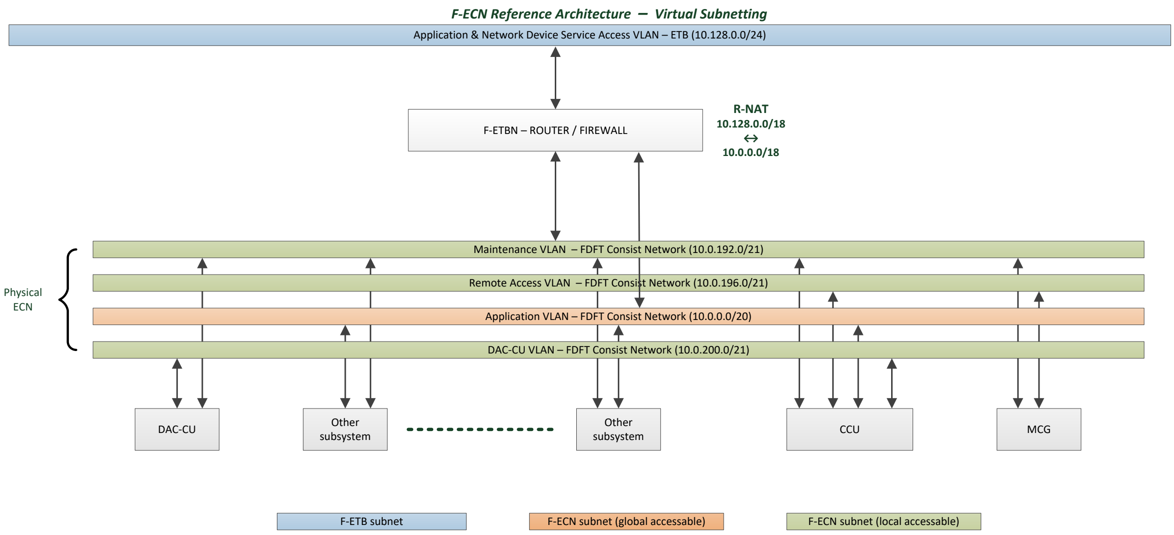

Figure 11: Virtual LANs

Virtual Subnet	Description	IP address range	VLAN ID
Application & Network Device Service Access Subnet – F-ETB	Train wide subnet for inter-consist communication. IEC 51375-2-3 defines one subnet; therefore, this subnet is used for TCMS and PACIS application and maybe used for train-wide service access.	10.128.0.0/24	n/a
ECN - Application Subnet	ECN subnet for application data exchange between ECN connected devices. Also used for transfer of inter-consist application data by connecting to the F-ETB via the F-ETBN.	10.0.0.0/20	111
ECN - Maintenance Connection Subnet	ECN subnet for maintenance connection. This subnet is used for maintenance of ECN network devices (software download, configuration, diagnostics).	10.0.192.0/21	121
ECN - Network Device Service Access Subnet	ECN subnet for connection of a service device (e.g. service laptop). This is a very localized subnet just connecting the service Ethernet port with the SGTW.	10.0.196.0/21	122
ECN – DAC-CU Subnet	ECN subnet for connecting to the DAC-CU	10.0.200.0/21	123

5.6.2.2.7 Redundancy management

Redundancy of network components shall prevent a network outage in case of a single network failure. Network failures to be covered are:

- Ethernet link loss (disruption of cable, transceiver failure, E-coupler connector failure)
- Network device failure

These topics are discussed in the next sections.

5.6.2.2.7.1 F-ETB Link redundancy

As Ethernet is a segmented network and no bus, a single F-ETB link failure will affect only one Ethernet segment. Multiple F-ETB faults will not lead to a communication loss as long as not both F-ETB lines of one Ethernet segment are disturbed.

Link redundancy of one Ethernet segment shall be handled by using link aggregation as defined in IEEE 802.1AX.

5.6.2.2.7.2 F-ETBN redundancy

Presently not planned to use redundant F-ETBN.

5.6.2.2.8 Performance

An important aspect of the communication system are requirements related to quantities and performance values. Quantities of the communication system are listed in Table 6, timing performance values in Table 7: Communication System Performance.

Table 6: Communication System Quantities

Parameter	Value	Comment
Maximal number of consists	104	100 wagons + 4 traction units
Maximal number of F-ETBN	127	Some traction units/wagons may have 2 F-ETBN for redundancy
Maximal number of subsequent passive consists to be detectable	10	Limited by technical constraints of the passive consist detection applied.
Maximal number of IP source addresses per consist for train-wide addressing.	16	Limited to restrict the size of CSTINFO telegram (see IEC 61375-2-3) to one Ethernet frame. With this, IP fragmentation can be avoided which

Parameter	Value	Comment
		increases robustness of train inauguration. Number of consist-local IP addresses is virtually unlimited.

Table 7: Communication System Performance

Parameter	Value	Description
F-ETB link interruption recovery time	≤ 0.25 s	An Ethernet link interruption may lead to a temporary communication interruption until all traffic is transferred to the redundant Ethernet link.
F-ETBN failure recovery time	≤ 1.3 s	In case of an F-ETBN failure bypass needs to be enabled and the new Ethernet links between the now directly connected neighbour F-ETBN needs to be setup. During that time F-ETB communication is interrupted.
F-ETBN fail-over time	≤ 1.3 s	Consists with redundant F-ETBN only: time from one F-ETBN failing until the redundant F-ETBN took over and data communication is restored.
Control/Status process datagram payload size	256 octets	Size of the application dataset within the process data (TRDP-PD) control/status frame cyclically sent by all consists with high priority
Control/Status process datagram cycle time	100 ms	
F-ETB Frame Error Probability (FEP)	$\leq 10^{-3}$	Probability that an Ethernet frame is corrupted.
Maximal F-ETB Control/Status process datagram latency time	0.2 s	Maximal F-ETB transfer time when F-ETB is fully loaded with lower priority traffic, no frame pre-emption. Time measured from Ethernet frame ingressing the source F-ETBN until the frame egresses the destination F-ETBN. Assumption: TRDP-PD dataset size of 256 octets

5.6.3.2 FDFT Link Gateway

5.6.3.2.1 Basic design and hardware

A physical Mobile Communications Gateway (MCG) shall be implemented on each consist (see /WP3 D3.2/). The support of redundant implementation of MCGs on a consist is not required.

The redundancy functionality between MCGs in a train is not required.

The concept of Train to ground communications shall follow IEC 61375-2-6. If there are options in this normative, either a recommendation or a decision on the way to follow the normative is given in this document.

The MCG shall allow to communicate with other devices in the consist using the Ethernet Consist network (ECN).

The GNSS module shall support the output of the protocol GNSS NMEA (at least version 4.0 shall be supported).

The specific data that shall be provided by the GNSS module to a user (CCU) isn't yet defined and needs to be specified by WP5 (train functions).

Description	Reference to IEC 61375	Justification / Rationale
A Mobile Communications Gateway (MCG) shall be implemented on each consist to provide FDFT Link functionality.		To provide the functionality of the Wireless FDFT-Link, a physical FDFT-Link Gateway shall be provided. It shall be called Mobile Communications Gateway (MCG).
The MCG sub-system shall meet the elements shown in IEC 61375-2-6, chapter 4.4.3, table 3.		
The MCG shall be able to negotiate the power class acc. to (IEEE 802.3af) with the network port of the Ethernet Train Backbone Node (F-ETBN).		In case the device is physically a separate device, it shall support the protocol acc. to 802.3af as a so-called

		powered device (PD).
The MCG shall support the VLAN tagging acc. to IEEE 802.1q for communications with device being connected to the ECN (Ethernet Consist Network) for in consist communications.		VLANs are used to separate communication profiles.
For Train to ground communication the requirements shown in IEC 61375-2-6, chapter 4.2, table 1 shall be met. Exceptions to table 1 are noted in the reference to this requirement.	<X1>	
No redundancy through another MCG located on another consist in the same train shall be considered, as mentioned in IEC 61375-2-6, chapter 4.2, table 1, row 6.	As a reference see <X1>	IEC 61375-2-6 chapter 4.2, table 1, row 6 states a redundancy option using a MCG located in another consist.
Multiple MCGs shall not be considered as mentioned in IEC 61375-2-6, chapter 4.2, table 1, row 5.	As a reference see <X1>	IEC 61375-2-6, chapter 4.2, table 1, row 5 states a redundancy option, which is not required. MCG is neither required for redundancy nor for load balancing as most other components are not redundant either. To save costs.
A trusted platform module (TPM) that is included in the MCG hardware shall be used to securely store authentication keys.		
The TPM technology shall support at least TPM 2.0.		

5.5.4.3.2 FDFT Link Mobile Communication

The MCG shall support the protocols to allow connectivity via Public Mobile Communications Network or Wireless LAN (bearers) to wayside systems, herein referred as Ground Communications Gateway (GCG) and Wayside Communications Gateway (WCG), to provide connectivity to FDFT Backend systems.

The MCG shall meet all the requirements from bearers.

The MCG shall support the functionality to select a specific mobile network selector service to always manage the active communication channel when more mobile communication network options are available.

The services provided by the MCG shall be always available to the FTFD backend systems via the FDFT link, therefore the FDFT Link shall be available at any time.

The Train Wake-up shall be implemented to ensure communications and wake up at any time. The protocol to support this functionality shall be as defined in IEC 61375-2-3:2024 chapter 6.9 "Wake-up" Option

Description	Justification / Rationale
For the MCG a public cellular network (mobile network) shall be used to provide the data connection (bearer).	
A Wireless LAN (Wi-Fi network) shall be supported as addition to public cellular network (bearer).	
Wireless LAN shall be implemented according to standard IEEE 802.11.	2.4 GHz frequency as general option
The MCG shall only act as Wi-Fi Client in a Wireless LAN environment.	
The MCG shall <u>not</u> use wireless communication standards for railway communication and applications (GSM-R / LTE-R) .	MCG uses solely public mobile network or Wireless LAN instead.
The public cellular network technology shall be state-of-the-art.	Currently, this would mean LTE (4G, 4th generation) as a minimum requirement for cellular network.

	For future use 5G and evolving technologies shall be considered.
A substandard offering machine-to-machine (M2M) communication shall be supported by the MCG. Specifically, this means LTE-M (LTE Cat-M1) for 4G public cellular networks.	This is sufficient for low bandwidth requirements and has the effect of saving power.
If the public cellular network is capable of LTE Cat-M1, it shall be preferred by the MCG.	Prefer use of low power technology. LTE Cat-M1 offers bandwidth from 300 kbit/s up to 1 Mbit/s.
In 5G public cellular network, low power option shall be preferred (NB-IoT 5G or similar).	Prefer use of low power technology; the standard is still evolving
If 4G and 5G public cellular network are unavailable, an <u>option</u> should be provided to fall-back to 2G technology.	This is an <u>option</u> to provide better network coverage. 2G network will likely not play a big role beyond year 2027.
Each entity using the FDFT Link communication shall consider the available bandwidth for LTE Cat-M1 (bandwidth from 300 kbit/s up to 1 Mbit/s).	
Each entity using the FDFT Link communication shall consider the latency for LTE Cat-M1 (typical value of 10-20ms).	Source: 3GPP Release 13
An MCG Network Selector Service (NSS) shall be implemented according to IEC 61375-2-6, chapter 6.3.4.	If more than one bearer (public cellular network

	or Wi-Fi) is available, the selection of radio interface shall be implemented according to IEC 61375-2-6.
If no bearer is available, it must be ensured that a communication network on the wayside is set up by infrastructure operators.	informational; Wi-Fi network or negotiation with public cellular network operators.
The functionality of a SIM card for public cellular network authentication shall be included.	eSIM (embedded SIM card) is preferred
The SIM card shall provide data roaming capability for public cellular networks.	
The bearer shall provide an IPv4 address (IP address) used for communication.	A private IPv4 address is not considered a security feature but is likely to reduce access from the public Internet.
The IP address on the external interface of the MCG can be dynamically assigned and does not need to be public.	Mobile public network or Wi-Fi network
The FDFT Link shall support NAT (Network Address Translation).	The bearer may provide NAT (or Carrier Grade NAT, CGNAT) functionality, if a private IP address or a dedicated

	space is assigned to the external interface of the MCG. Eg. this is defined in IETF RFC 1918 and IETF RFC 6598.
IPv6 support shall be considered. The same rules apply to IPv6 as to IPv4 addresses.	
If IPv6 is used, a transition technology shall be implemented by the bearer to reach IPv4 endpoints if required.	An IPv4 endpoint could be the FDFT Link I/F of the FDFT Backend.
The services provided by MCG shall be always available to the FDFT backend systems via the FDFT link.	Even when consist is in energy saving mode.
An MCG Train Wake-up Service as described in IEC 61375-2-6, chapter 6.3.6 shall be implemented to ensure continuous communication capability and wake up.	Even when the consist is in energy saving mode.

5.6.3.3. FDFT Link Interface

IT security level 4 (SL 4) as defined in IEC 62443-3-3 applies.

Rationale:
SL 4 – Prevent the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with extended resources, IACS specific skills and high motivation.
Remark: In the current situation, SL4 is the expected required security level.

Every consist shall use a unique private key for authentication.

The FDFT link shall always be initiated by the MCG, as no incoming communication through public interfaces shall be available on the MCG for IT security reasons.

The MCG shall use DNS to initiate connections to wayside systems.

On wayside systems, the authentication information is challenged against a PKI (Public Key Infrastructure), which does not need to be publicly recognised, but must be known and trusted by all systems in the GCG/WCG participating in the authentication.

Description	Justification / Rationale
The Requirements for Board to Ground communication shall be fulfilled as described in DIN EN 61375-2-6 Chapter 4.2 Table 1.	Additional requirements or specifications are described below.
No IP Ports (TCP or UDP) shall be open on the MCG on the external interface of the MCG.	No services are offered on public interfaces of MCG.
All incoming connection requests on the external interface of the MCG shall be dropped.	No services are offered on public interfaces of MCG.
A connection for the FDFT Link shall only be initiated by the MCG.	A transaction in the FDFT Link can be connected in both directions.
FDFT Link connections shall be initiated using a DNS hostname (FQDN).	No static IP address shall be configured to allow change of service IP on the landside.
The requirements for the FDFT Link connection shall be met according to DIN IEC 62443-3-3.	
As the FDFT Link transmits safety related information and uses a public mobile radio network, the criteria for the FDFT Link shall comply with chapter 5.15 of IEC 62443-3-3.	
FDFT Link requires the protection according to SL 4 (security level 4) as defined in IEC 62443-3-3.	

The FDFT Link shall protect the integrity of information including cryptography according to IEC 62443-3-3, chapter 7.3.3.1	
Requirements for Identification and Authentication shall be considered based on IEC 62443-3-3, chapter 5.	SL to be defined based on the requirements of the application as described in the normative.
Keys for authentication shall be secured by a Trusted Platform Module as a hardware measure.	TPM 2.0 or better
Multifactor authentication is required by security level 4 (SL 4) in IEC 62443-3-3. The authentication key stored in TPM is one factor. An additional factor shall be chosen.	Eg. SIM card, ID of MCG (MAC), or any static identification.
To securely handle a large number of consists, the use of Public-Key-Infrastructure as described in IEC 62443-3-3, chapter 5.10 shall be implemented.	
A PKI (Public Key Infrastructure) shall be used to authenticate a large number of consists according to criteria explained in IEC 62443-3-3, chapter 5.11.	
Every consist requires a unique and genuine private key / account to authenticate against wayside systems.	For authentication against GCG/WCG.
The PKI parameters shall be set up and kept state-of-the art.	This included algorithms, key lengths, and other services like revocation.
The PKI or CA (Certificate Authority) does not require to be an internationally recognized root CA.	The PKI can be self-hosted / self-signed.

FDFT Link Data / MCG function

The MCG shall provide network connectivity and data services from and to the consist via Radio interfaces. It shall provide Firewall services and supports zones as described in IEC 62443-3-3.

The MCG shall provide basic services to subsystems on the consist, like time source and position information through a GNSS module.

Description	Justification / Rationale
The MCG shall support and provide shared communication (as a router/gateway) to be used as described in IEC 61375-2-6, chapter 4.6.1.2.	Communication by many devices on the (same) consist is possible
The MCG shall act as a firewall for all interfaces and zones to control and separate traffic flows as described in IEC 62443-3-3 chapter 9.4.	
The MCG's IT security architecture shall be aligned with the concepts defined in IEC 62443, especially IEC 62443 part 3-3.	
The MCG shall provide functionality of an Application Layer Gateway ("broker service architecture") as described in IEC 61375-2-6, chapter 5.2.	
The MCG shall provide access from subsystems on the consist, attached to the ECN to FDFT backend services.	E.g: from a telematics device to communicate with FDFT backend.
The MCG shall provide access from FDFT backend services to subsystems on the consist attached to the ECN.	
The MCG shall access subsystems on the consist via VLANs in the Ethernet Consist Network (ECN) through the Train Backbone Node (F-ETBN).	
Each transaction using FDFT Link communications shall classify to either use the MCG as an ALG or as a shared communication (router). See IEC 61375-2-6 for details.	Define for each application separately how to communicate
The GNSS receiver shall provide the following information as a minimum: • latitude & longitude • altitude • time • speed & direction	

• accuracy of position (accuracy value or error estimate, including when a satellite fix is obtained.)	
The MCG shall act as time source via the network using NTP (RFC5905) as protocol.	Based on time obtained through GNSS.
Proposal: The MCG shall synchronize itself to the UTC as received thru the GNSS receiver.	
The MCG shall share position data using standard protocols via network connection to other subsystems on the consist.	Either forward NMEA 0183 data or via gpsd (TCP/IP). For example used by a telematics device.
The MCG shall provide TLOS (Train Location Service) as described in chapter 6.3.2 of IEC 61375-2-6.	

FDFT Link Data / Requirements for GCG function

A GCG provides DNS services (among other services and functions). An MCG registers or updates it's consist address using DNS with the IP address assigned to the FTFT Link interface of the MCG. Services on the consist will be available to the FTFD backend through this registered address/hostname.

GCG also is a key part in the PKI (Public Key Infrastructure).

Description	Justification / Rationale
The GCG shall be reachable via DNS FQDN.	The FQDN is statically configured in MCGs that use this GCG.
Every operator shall provide a FQDN for the GCG endpoint to be able to handle connections from their respective consists.	The FQDN is statically configured in MCGs that use

	this GCG.
The MCG shall update the ground DNS server to register its consist identification with the IP address assigned to the wireless interface according to IEC 61375-2-6, chapter 6.3.1.4.	The registration shall be done using nsupdate according to IEEE RFC 2136.
No address registration via DNS for Train Journey shall be implemented as suggested in IEC 61375-2-6, chapter 5.3.5.2.	Not required
The numbering of FQDN shall follow the recommendation in 61375-2-6, chapter 5.3.5.1.	An example for consist addressing via DNS: UIC318112345670 .tcndns.oebb.at for consist 31 81 1234 567-0
Each GCG shall know and trust each Root CA to which it must authenticate.	
Each GCG shall have access to revocation services.	Eg. CRL, OCSP or comparable.

5.6.3 Train Function related requirements

5.6.3.1. Overview

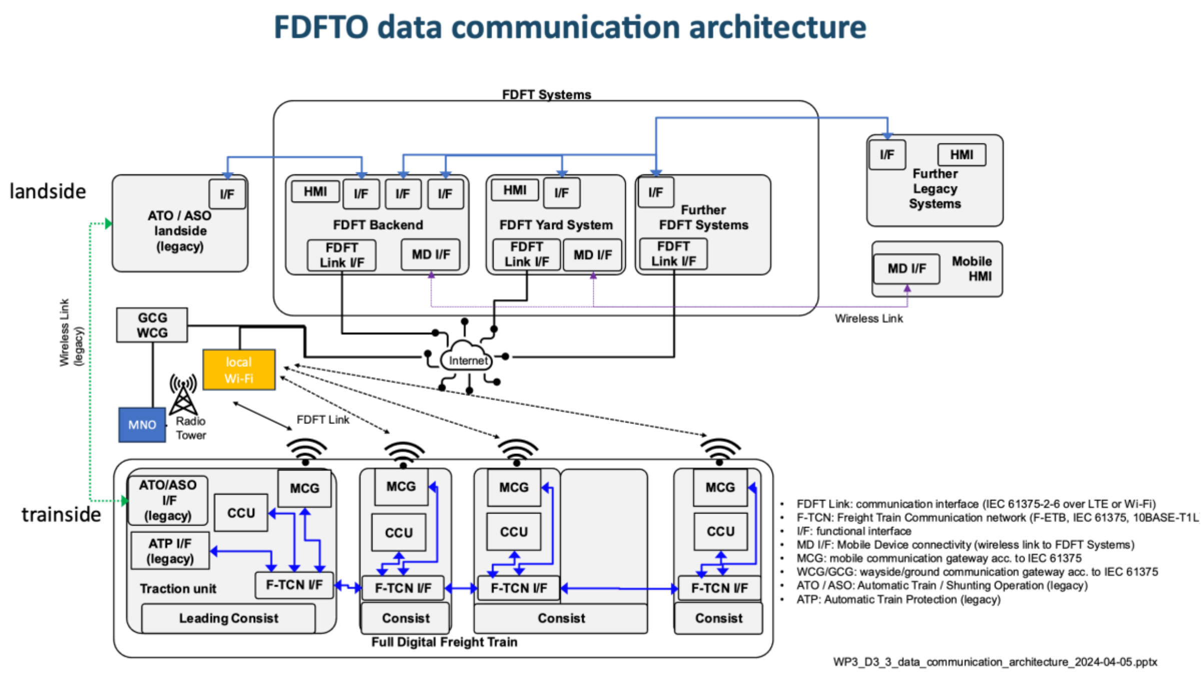

Figure 12: FDFTO Data Communication Architecture

Logical blocks - IPNs view - requirements

Impact paths are the relationships between components or logical blocks in a system architecture that can be affected by changes to one or more components. Understanding the impact paths of a system architecture helps to define the role of components, and the needed functionality they should provide.

When developing a new system architecture, understanding the potential impact paths is important in ensuring that the system meets safety requirements and other desired outcomes. This is particularly critical in areas where safety and reliability are essential.

Expert groups such as train functions and brake system experts provide valuable technical inputs for the design of the system architecture.

These requirements can then be used at the definition of subsystems and individual components requirements, ensuring that the system architecture is optimized for safety and functionality, which can ensure that the new system meets the needs and requirements of the operators, users, and use cases.

Identifying which subsystems are impacted by other subsystems, developers can define requirements for these subsystems that ensure they are optimized to work within the context of the overall system architecture.

Impact Paths are built up from Impact Nodes and a connection between them, building the IPGs (Impact Path Graphs).

Impact Path Nodes (IPNs) are logical blocks often represented by separate physical subsystems but does not necessarily means separated devices. Example given the DAC HMI (Human Machine Interface) can be an additional display in the locomotive, but in can also utilize one of the already installed displays on the locomotive in shared use, as long needed information is provided with the defined safety level. To stick to this example the mentioned HMI and HMIS (HMI Safe) can also be incorporated in one physical device as long the functional and safety requirements are fulfilled.

From requirement perspective for IPNs it is important, which role an IPN has when it is a part of an IPG, depending on its position in the IPG from signal or message aspect:

- as source/provider – which generates message to be sent via the IPG,
- pass-through – mostly passing only further the message, or
- receiver/user – receiving message from source for processing or execution of request

Train functions are clustered according /WP3 D3.1/ chapter 9.2 FDFT Traction unit Base System functional architecture heading structure and mapped to the Impact Path Graphs:

The following tables stipulate the principal messages to be exchanged between the CCUs of different consists (traction unit and wagons),although the detailed messages shall be defined in /WP5 D5.1/.

Message group	Topic
LF01	Communication system F-TCN interface in traction unit
LF02	Power Distribution line in traction unit
LF03	Brake Pipe in traction unit
LF04	Traction Unit power supply system (producer)
LF05	Traction Unit related functional blocks
LF05.1	Uncoupling control
LF05.2	Prevent coupling control
LF05.3	M-Coupler status monitoring system
LF06	Traction unit power supply system (consumer)
LF07	Traction unit local HMI device interface
LF08	FDFT-Link interface
LF09	Train integrity monitoring
LF10	Train composition detection support
LF11	Train length determination support
LF12	Train length determination voter
LF13	Last coupler detection support
LF14	Adjacent wagon detection support
LF15	FDFT functional check
LF16	ABT functions
LF17	Power Management Control // Monitoring
LF30	Rear End Signal
LF31	Rear End Signal Control

In the following chapters, only the principal messages are listed, which are required to be defined interoperable. The definitions shall be done in /WP5 D5.4/.

LF01 - Communication system F-TCN interface in traction unit

The FDFT base system shall have an Interface to the F-TCN, allowing the onboard devices to communicate with other network participants using the F-TCN.

REQ-ID	REQ	OPEID	NOTE
REQ-LF01-001	LF01 shall support 400V_OFF request sending from LCU to CCUs.	TU30.2	
REQ-LF01-002	LF01 shall support brake system status query from LCU to CCUs.	BE41.4 O41.4 O41.15 O41.4 O41.15 BE41.4 TU25.2	

REQ-LF01-003	LF01 shall support generating and sending compiled network node list to LCU	WWS32.2	
REQ-LF01-004	LF01 shall support PB APPLY request sending from LCU to CCUs.	TU25.2	
REQ-LF01-005	LF01 shall support PB_ENA request sending from RSLM to RSLs.	TU25.2	
REQ-LF01-006	LF01 shall support TIM (Train Integrity Monitoring) start request sending from LCU to LAC (Last Active Consist) CCU.	TU32.9 TU31.7 TU32.1	
REQ-LF01-007	LF01 shall support Train Operation Mode request sending from LCU to CCUs.	S4.10 BE4.10 TU4.9 TU30.3 TU31.2 O4.1 BE4.1	
REQ-LF01-008	LF01 shall support Train Operation Mode request sending from RSLM to RSLs.	BE4.1 S4.10 BE4.10 TU30.3 O4.1 TU31.2 TU4.9	
REQ-LF01-009	LF01 shall support Train Operation Mode status reporting sending from CCUs to LCU.	WWS31.4 WWS30.4 O4.1 BE4.1 TU31.7	
REQ-LF01-010	LF01 shall support Train Operation Mode status reporting sending from RSLs to RSLM.	O4.1 TU25.2 BE4.10 S4.10 BE4.1 WWS30.4 WWS31.4 TU4.9	

LF04LF04 - Traction Unit power supply system (producer)
The traction unit power supply system shall send the process & status data as captured by the traction unit base system itself or captured by the wagon / consist base systems via the F-TCN.

REQ-ID	REQ	OPEID	NOTE
REQ-LF04-001	LF04 shall support Authorized Operator request to switch ON/OFF 400V on HMI.	TU30.2	
REQ-LF04-002	LF04 shall be supported by broadcasting ON/OFF state of 400V from LCU to CCUs to allow short Train Integrity Monitoring preparation for change.	TU30.2	
REQ-LF04-003	LF04 shall support showing 400V status on HMI.	TU30.2	
REQ-LF04-004	LF04 shall support showing 400V status on HMIS.	TU30.2	
REQ-LF04-005	LF04 shall be supported by LCU and PSU to switch ON and OFF 400V.	TU30.2	
REQ-LF04-006	LF04 shall be supported by LCU and PSU to enable or disable 400V and 48V supply.	TU31.9	

LF07 - Traction unit local HMI device interface

The traction unit local HMI device interface allows access to the functionality of the traction unit base system via a local HMI. This allows e.g.: TU operator to make use of the functionality provided by the traction unit base system.

REQ-ID	REQ	OPEID	NOTE
REQ-LF07-001	LF07 shall support Authorized Operator in BPC (Brake Performance Calculation) data query on HMI.	O41.15	
REQ-LF07-002	LF07 shall support AUTHORISED OPERATOR in BPC (Brake Performance Calculation) validation on HMI.	O41.15	
REQ-LF07-003	LF07 shall support Authorized Operator in providing expected Consist Composition List	TU32.8	
REQ-LF07-004	LF07 shall support Authorized Operator in reporting train arrival.	S4.10	
REQ-LF07-005	LF07 shall support Authorized Operator in requesting 400 V ON/OFF on HMI.	TU30.2 TU31.9	
REQ-LF07-006	LF07 shall support Authorized Operator in requesting PB apply / release.	P25.1	
REQ-LF07-007	LF07 shall support Authorized Operator in requesting Train Operation Mode SH (Shunting)	P30.1	
REQ-LF07-008	LF07 shall support Authorized Operator in requesting Train Operation Mode TR (Train Run)	P31.1 O4.1	

LF08 - FDFT-Link interface

The traction unit <FDFT-Link interface> allows access to the functionality of the traction unit base system via the FDFT-Link. This allows any FDFT-System to initiate all activities as given by the operational procedures. In addition, the FDFT-Link interface allows the FDFT Base System of the TU to send the process & status data as captured by the traction unit base system itself or captured by the wagon / consist base systems and transferred via the F-TCN to the traction unit.

REQ-ID	REQ	OPEID
REQ-LF08-001	LF08 shall be able to transfer TIM (Train Integrity Monitoring) stop report to BE.(Backend)	TU32.1
REQ-LF08-002	LF08 shall be able to transfer Train Operation Mode status to BE.	TU31.5 TU30.5
REQ-LF08-003	LF08 shall support ATO reports about movement status to BE.	BE41.4
REQ-LF08-004	LF08 shall support BE approval to LCU for brake power calculation.	BE41.15
REQ-LF08-005	LF08 shall support BE report about train arrival to LCU.	TU4.9 BE4.10
REQ-LF08-006	LF08 shall support BE request to ATO for movement.	BE41.4
REQ-LF08-007	LF08 shall support BE request to LCU for brake power calculation.	BE41.13
REQ-LF08-008	LF08 shall support BE request to LCU for PB APPLY.	BE25.1
REQ-LF08-009	LF08 shall support BE request to LCU for Train Operation Mode switching.	BE31.1 BE30.1 BE4.1
REQ-LF08-010	LF08 shall be able to transfer 400V status to BE.	TU31.9
REQ-LF08-011	LF08 shall be able to transfer brake performance calculation data, changes, and results to BE.	BE41.14 BE41.15
REQ-LF08-012	LF08 shall be able to transfer detected consist composition list.	TU32.6
REQ-LF08-013	LF08 shall be able to transfer PB status to BE.	BE25.1 TU25.4
REQ-LF08-014	LF08 shall be able to support reporting from LCU to BE for the Train Operation Mode status.	BE31.6 TU30.8 BE4.1 BE4.10 S4.10 O4.13 BE31.1 BE30.1 TU4.9
REQ-LF08-015	LF08 shall be able to transfer train arrived to BE.	S4.10

LF09 - Train integrity monitoring

The traction unit <train integrity monitoring> collects information from all wagons / consists in train, foremost from the last wagon / consist in train, to perform the train integrity detection function. All messages shall be exchanges via the F-TCN.

REQ-ID	REQ	OPEID
REQ-LF09-001	LF09 shall be supported by CCUs reporting TIM (Train Integrity Monitoring) status to LCU.	TU31.7
REQ-LF09-002	LF09 shall be supported by LCU requesting TIM (Train Integrity Monitoring) start from CCUs.	TU31.7 TU32.9
REQ-LF09-003	LF09 shall be supported by LCU stopping TIM (Train Integrity Monitoring) function.	TU30.6 TU32.1
REQ-LF09-004	LF09 shall be supported by displaying the actual status of TIM (Train Integrity Monitoring) on HMI.	TU31.7
REQ-LF09-005	LF09 shall be supported by RSL of LAC sending the status for valid TIM (Train Integrity Monitoring) via ETBN to the RSLM.	TU31.7
REQ-LF09-006	LF09 shall be supported by the RSLM evaluating the status of valid TIM (Train Integrity Monitoring) from status provided by LCU and LAC RSL.	TU31.7
REQ-LF09-007	LF09 shall be supported by displaying the status of summarized valid TIM (Train Integrity Monitoring) on HMIS.	TU31.7

LF10 - Train composition detection support

The traction unit based <train composition detection> function collects information from all wagons / consists in the train to derive the actual train composition. All messages shall be exchanges via the F-TCN.

REQ-ID	REQ	OPEID
REQ-LF10-001	LF10 shall be supported by BE that check Consist Composition List actual vs. expected.	BE32.7
REQ-LF10-002	LF10 shall be supported by display data belonging to Consist Composition List the option to validate it.	P32.7
REQ-LF10-003	LF10 shall be supported by display data belonging to Consist Composition List warning on changes.	D2
REQ-LF10-004	LF10 shall be supported by ETBN that collects compiled network node list.	WWS32.2
REQ-LF10-005	LF10 shall be supported by HMI showing the Consist Composition List: the actual and expected status.	TU32.6
REQ-LF10-006	LF10 shall be supported by LCU that it can build Consist Composition List.	TU32.5 WWS32.2 TU32.5

LF11 - Train length determination support

The TU based <train length determination support> provides the length of the TU and forwards this information to the requesting function (e.g., Train length determination voter). All messages shall be exchanges via the F-TCN.

REQ-ID	REQ	OPEID
REQ-LF11-001	LF11 shall be supported by CCUs by sending consist length data via ETBN to the LCU.	TU10.3
REQ-LF11-002	LF11 shall be supported by HMI by allowing Authorized Operator to initiate train composition data query.	P10.2
REQ-LF11-003	LF11 shall be supported by HMI by displaying summarized consist length, expected length data from LCU.	TU10.3
REQ-LF11-004	LF11 shall be supported by HMI by displaying deviations between expected and detected data from consists in train, and to support in more granular way to find place of deviation.	TU10.3
REQ-LF11-005	LF11 shall be supported by LCU by collecting and summarizing consist length data received via ETBN from the CCUs.	TU10.3

REQ-LF11-006	LF11 shall be supported by LCU in a way that it can accept a request from BE via LINK to determine all consist data (e.g., consist length).	BE10.2 TU10.3
REQ-LF11-007	LF11 shall be supported by LCU in a way that it can report to BE via LINK the requested collected consist data.	TU10.3

LF13 - Last coupler detection support

The TU based <last coupler detection support> provides information to the TU base system, if and which coupler of the train is the so called "last coupler" in a train. This function requires distinct means (e.g.: sensors) to determine the last coupler.

Additionally, the TU also shall monitor their second coupler which is called "front end coupler". From functional point of view is the "front end coupler" equal to the last coupler and must be monitored.

All messages shall be exchanges via the F-TCN.

REQ-ID	REQ	OPEID
REQ-LF13-001	LF13 shall be supported by LCU which detects via network inauguration the consists in train. Additionally, the consist orientation will be detected. The neighbour (adjacent) consist detection provides information about further coupled consists.	Not applicable
REQ-LF13-002	LF13 shall be supported by CCU of LAC that detects by network inauguration the consist orientation and periodically by the neighbour (adjacent) consist detection system that no further consist is coupled.	Not applicable
REQ-LF13-003	LF13 shall be supported by CCU that reports detected last coupler via ETBN to LCU.	Not applicable
REQ-LF13-004	LF13 shall be supported by LCU that collects detected last coupler via ETBN, stores and display it on HMI.	Not applicable

LF14 - Adjacent wagon detection support

The <adjacent wagon detection support> provides information to the TU base system if there exists an adjacent wagon / consist.

All messages shall be exchanges via the F-TCN.

REQ-ID	REQ	OPEID
REQ-LF14-001	LF14 shall be supported by consist equipment that provides neighbor consist detection to the CCU or LCU with the information about existing or missing connected neighbor consist.	TU32.4

REQ-LF14-002	LF14 shall be supported in a way that passive (battery exhausted) consists are also detected – even if there are multiple consecutive passive (battery exhausted) consists.	TU32.4

LF15 - FDFT functional check

The TU < FDFT functional check> provides information to the TU base system about the functional health state of the TU. This function requires a set of sensors allowing to derive the functional state of the TU, not yet specified.

This functional check becomes relevant only if the TU is part of a train in a passive way (i.e. behaving like a wagon).

The F-ETBN part of locomotive will behave like a wagon, so it will support train inauguration with neighbour detection and consist composition list build up.

All messages shall be exchanges via the F-TCN.

REQ-ID	REQ	OPEID
REQ-LF15-001	LF15 shall be supported by ETBN part of each TU providing functionality like wagons support the train inauguration, neighbour detection, and consist composition list build up.	Not applicable.
REQ-LF15-002	LF15 shall be supported by LCU providing information about state of each non-leading TU brake system (including pneumatic, electrical brake state and parking brake) and DAC power system to the leading consist.	Not applicable.
REQ-LF15-003	LF15 shall be supported by LCU of leading consist by collecting brake and DAC power system information from non-leading TU-s.	Not applicable.
REQ-LF15-004	LF15 shall be supported by HMI that displays TU specific brake system and DAC power system data for leading and non-leading TUs.	Not applicable.

LF16 - ABT functions

For ABT functions, a master – slave approach is considered, where the CCU of each consist is the “slave” unit providing the information to the master unit of the ABT (e.g. CCU on leading consist or LCU on Traction Unit) about the different states of brake system.

All messages shall be exchanges via the F-TCN.

REQ-ID	REQ	OPEID
REQ-LF16-001	LF16 shall be supported by BE providing brake test relevant data (in form of expected results) to LCU via LINK.	TU9.9 SD9.4

REQ-LF16-002	LF16 shall be supported by CCUs that collects the consist BRE status (applied / released pneumatic brake and PB, selected brake position (G/P), cut in/out) and reports it via ETBN to LCU.	TU9.15 SD9.14
REQ-LF16-003	LF16 shall be supported by HMI allowing AOP to initiate an ABT.	BO9.3
REQ-LF16-004	LF16 shall be supported by HMI displaying deviations from expected values during ABT warning the AOP and providing mitigation hints.	TU9.19 SD9.17
REQ-LF16-005	LF16 shall be supported by HMI displaying each step of ABT as list, showing actual running phase, and after closing given phase showing short summary (results optionally passed/fail/deviation status).	TP09
REQ-LF16-006	LF16 shall be supported by HMI that allows AOP to validate train composition with accepted brake system state of consists to start the ABT. AOP should have possibility to validate deviations on particular consists – e.g., brake non-available.	BO9.3
REQ-LF16-007	LF16 shall be supported by HMI that allows AOP to accepted ABT results.	BO9.26
REQ-LF16-008	LF16 shall be supported by LCU checking correct function of the BP control of loco (or test unit) involved in the ABT.	TU9.10 SD9.5
REQ-LF16-009	LF16 shall be supported by LCU checking those preconditions (train composition valid, only needed PB-s are applied, non-available consists brake system is accepted by AOP) are meat by correct state of all consists involved in the ABT.	TU9.10 SD9.5
REQ-LF16-010	LF16 shall be supported by LCU that collects from via ETBN all CCUs the consist BRE status and display it on HMI to AOP after each test phase.	D9.9 D9.11
REQ-LF16-011	LF16 shall be supported by LCU that reports ABT status (to be done / in progress / results (passed / failed / deviating / values) to BE via the LINK.	BE9.25
REQ-LF16-012	LF16 shall be supported by LCU that stores in non-volatile and safe memory (e.g., in JRU) the result of ABT. The data to be stored is as minimum the ABT timestamp + AOP ID + result.	BO9.26
REQ-LF16-012	LF16 shall be supported by LCU with access to BP control of TU (increase / hold / decrease BP pressure) and the BP pressure value.	TU9.11 TU9.12 TU9.13 TU9.20 TU9.23 SD9.6 SD9.7

		SD9.8 SD9.18 SD9.22

LF17 - Power Management Control & Monitoring

The traction unit-based <Power Management Control & Monitoring> function allows to control and monitor the traction unit power supply system, to allow operations as well as charging the Energy Storage (battery).

All messages shall be exchanges via the F-TCN.

REQ-ID	REQ	OPEID
REQ-LF17-001	LF17 shall be support Authorized Operator by HMI to select 400V ON/OFF on HMI	TU31.9
REQ-LF17-002	LF17 shall be support Authorized Operator by HMI to select 400V ON/OFF on HMIS	TU31.9
REQ-LF17-003	LF17 shall be supported by enable 400V by LCU that after preconditions are fulfilled PCU gets enabled (by enable electrical signal)	TU31.9
REQ-LF17-004	LF17 shall be supported by HMI to active status for 400V (ON/OFF).	TU31.9
REQ-LF17-005	LF17 shall be supported by HMI to show Authorized Operator that preconditions are fulfilled (or not) for 400V_ON.	TU31.9
REQ-LF17-006	LF17 shall be supported by HMIs to active status for 400V (ON/OFF).	TU31.9
REQ-LF17-007	LF17 shall be supported by LCU that reports 400V status to BE.	TU31.9
REQ-LF17-008	LF17 shall be supported enable 400V by RSLM that after preconditions are fulfilled - PCU gets enabled (by the enable electrical signal).	TU31.9

5.7. General requirements

5.7.1 Cybersecurity

5.7.1.1 Background

The adoption of digital technologies in the freight railway sector, as well as an increased demand for interconnectivity of train systems, have brought new cyber risks, such as malicious attacks, unauthorized intrusions, and system failures. These risks can have serious consequences, ranging from interruptions in train service, to human injury or exposure of train operator's internal information.

As of today, there is a lack of a comprehensive and universally accepted cybersecurity regulation specifically targeting the railway industry. National or local legislation regarding cybersecurity in the railway sector are still in its early stages and may vary greatly between different countries and regions. Therefore, the cybersecurity architecture which is subject of this document is based on generic cybersecurity standards and technical specifications such as the IEC 62443 series, CENELEC TS 50701 and the upcoming IEC 63452 standard.

The scope of this section is to determine basic cybersecurity countermeasures to implement on the FDFT. This work is inspired by cyber security investigations that have been executed in other Europe's Rail projects like CONNECTA or X2RAIL. While X2RAIL focus was on signalling systems, CONNECTA analysed threats for the Next Generation TCMS/TCN (NG-TCMS/NG-TCN), which in general are also valid for FDFT[1]. In ER JU FA5, System Pillar, a cybersecurity team is currently defining a comprehensive set of related documents.

When tackling cybersecurity, the following items need to be addressed which are in line with the cyber security process defined by IEC 62443:

- Description of the System under Consideration (SuC) and derived zoning model
- Detailed cyber security risk assessment
- Definition of the (target) cybersecurity level vector
- Definition of cybersecurity measures

These four items are addressed principally and preliminarily within the following sections but need still to be analysed in detail.

[1] CONNECTA had passenger trains in focus, but because the TCN architecture is mostly identical for passenger and freight trains, the cyber security measures defined by CONNECTA-3 can be adopted for FDFT.

5.6.1.2 Zone and conduit model

A basic architectural feature of F-TCN is the separation of a consist-level communication network (ECN), a train-level communication network (F-ETB) and the train-to-ground communication link (FDFT-Link).

ECN:	Mostly static network (static topology). It may only be changed in a workshop. Closed communication system acc. to EN 50159. Exception: local wired maintenance access by service personnel.
F-ETB:	Dynamic network, topology changes when freight wagons are coupled or uncoupled. Closed communication system acc. to EN 50159 because number of participants is restricted, and participants are known.
FDFT-Link:	Wireless connection to ground communication system, open communication system according to EN 50159.

From this, four basic zones and four conduits can be defined:

Zone	Description
Z1_ECN	Contains all network devices and end devices in a consist which are interconnected via the ECN. Zone is static.
Z2_ECN-LM	Local Maintenance zone. This zone contains the ECN Ethernet maintenance port(s) and the connected maintenance devices like service laptops.
Z3_ETB	Contains F-ETBN device, junction box and automatic coupler
Z4_F-Link	Contains MCG and radio access points

Conduit	Description
C1_ECN-ETB	Connects zones Z1_ECN and Z3_ETB
C2_ETB	Connects two consists zones Z3_ETB on F-ETB
C3_ECN-LM	Connects zones Z1_ECN and Z2_ECN-LM
C4_F-Link	Connects zones Z4_F-Link and Z1_ECN

5.7.1.3 Detailed risk analysis and cyber security level vector

The detailed risk analysis for the FDFT is still to be done. For the time being, and until there is a target cyber security level vector defined basing on the results of the FDFT detailed risk analysis, it is proposed to use the target cyber security level vector defined by CONNECTA for NG-TCMS:

SL–T := {3,3,3,3,2,3,7}

This vector defines the target level values for the 7 foundational requirements of IEC 62443-3-3:

FR 1 - Identification and authentication control (IAC)

FR 2 - Use control (UC)

FR 3 - System integrity (SI)

FR 4 - Data Confidentiality (DC)

FR 5 - Restricted data flow (RDF)

FR 6 - Timely response to events (TRE)

FR 7 - Resource availability (RA)

Related cybersecurity requirements are defined in IEC 62443-3-3 (system level) and IEC 62443-4-2 (component level).

5.7.1.4 Measures

Based on the required target cybersecurity level vector, a preliminary list of cybersecurity measures can be identified. Those measures are assigned to zones and conduits within the following tables.

Zone	Measures
Z1_ECN	Network devices (e.g., F-ETBN, MCG) and end devices shall support: • Tamper resistance • Secure boot (certified software, TPM module) of ND/ED • Use control for maintenance access The zone shall provide a RADIUS server.
Z2_ECN-LM	Maintenance devices like service laptop shall be dedicated for this purpose and shall be protected: • Up-to-date virus scanner • Only necessary software from trusted sources • User management (authorized personnel only)
Z3_ETB	See Z1_ECN
Z4_F-Link	MCG shall act as application layer gateway, see IEC 61375-2-6 ED2.

Conduit	Description
C1_ECN-ETB	F-ETBN shall support a Layer 3 firewall for filtering inbound IP data traffic F-ETBN shall support Layer 2 traffic policing and traffic filtering (IEEE 802.1Q) to prevent overload of F-ETB (e.g., prevention of denial-of-service attack)
C2_ETB	Two concepts possible (still open for investigation):

	i) Strict mutual authentication of consists, e.g., by using IEEE 802.1X EAP-TLS. If there is an untrusted consist, F-ETB communication disrupted. ii) Tolerable mutual authentication, e.g. by checking certificates after train inauguration. Non trusted consists will be detected, but they still remain connected to the F-ETB.
C3_ECN-LM	IEEE 802.1X based access control (maintenance device is supplicant, network device is authenticator).
C4_F-Link	Encrypted communication between MCG and ground station (e.g., via VPN tunnel) Mutual authentication. See IEC 61375-2-6 ED2 for details.

5.7.1.4 Intrusion detection notification

The CCU and the MCG shall send a notification about a detected intrusion to a registered destination.

5.7.1.5 Tampering detection notification

The CCU and the MCG shall send a notification about a detected tampering to a registered destination.

5.7.2 Safety-Related Requirements

In /WP4 D4.2/ “Risk assessment and harmonized safety architecture” the potential hazards that a DAC-fitted FDFT could lead to are identified and analysed. This process uses the results of /WP2 D.2.1/ “Preliminary operational procedures” as input. The result of this analysis being a HAZOP (Hazard and Operability) table that is an appendix of /WP4 D4.2/. The main results of this work are the safety related requirements impacting the digital / data architecture are given in the following table.

Table 8: Safety Requirements and related TFFRs

TFFR	Safety Requirement
10^{-9}	Unintended decoupling / train separation during the train run without opening the brake pipe must be prevented. If a local decoupling mechanism is introduced, the same safety requirement as for the central decoupling function applies. Unauthorized access must be prevented.
	Speed and brake distance related data must be provided correctly to ATP.
	Without trackside line occupied monitoring, decoupling / train separation without information to the ATP must be avoided.
	Without trackside line occupied monitoring, train length determination must be provided correctly.
10^{-7}	Unwanted decoupling, decoupling of wrong waggon in a protected area must be avoided. The brake percentage must be provided to the loco (on board channel) in a protected area.
10^{-6}	Don’t apply power if contacts are not coupled or covered.
	Indicate malfunction of coupling and exceedance of force limits to operator.
	Indicate “lost” consists to operator and / or ATP (automatic train protection).
	Switch on end of train signal at the end of the vehicle being at end of train.

Safety requirements are partially dependent on a specific design. In some cases, the responsibility is shared between an operational and a supervision channel. This means, that the requirements and even the hazard analysis must be checked and revised in respect to the final design.

Remark: The hazard log and who is in charge in resolving the consequences, e.g. EU agency if it is done by national safety authorities, or who is in charge, is currently discussed with the ERA and the NSAs.

The supervision aspect (vehicles and operations) is addressed by law to the NSAs. This shall be considered in upcoming releases of /WP4_D4.1/ and /WP4_D4.2/.

5.8 Open Topics

Some topics could not be finally closed for various reasons mainly due to missing input from various expert groups as well as postponed decisions in the project. These are:

- Interface coupler domain – CCU

  For the time being, two different concepts for the control of the DAC exist: concept 1 has an integrated intelligence in the coupler itself which communicates with the CCU via the ECN, whereas concept 2 is directly controlled from the CCU with a discrete wired interface. Both concepts shall be developed, deployed, and tested in the field for a final decision.
  The interface description will be updated by the DAC System Interface Clarification Group (part of WP5)

- Push buttons / signal lamps for manual operation of DAC

  The detailed architecture of the panel with push buttons and signal lamps for the manual operation of the DAC and the interface to the coupler and/or the CCU must be developed at a later phase within FP5 because operational procedures as well as detailed train functions for decoupling are still pending.
  The interface will be described in /WP5 D5.2/.

- Behaviour of a dead traction unit in a freight train

  The operational requirements for a dead traction unit running as wagon in FDFT must be harmonized with the constraints to install the necessary components for this purpose what will be done at a later phase within FP5 or in other future projects.
  The interface will be described in /WP5 D5.1/.

- Rear end signals requirements

  The requirements for rear end signal (e.g. taillights) in an automated environment must be defined before this topic can be considered in the digital / data reference system architecture.
  The interface will be described in /WP5 D5.2/.

- Reliability, availability, and maintainability

  These topics are currently under discussion so that the necessary input for the development of the digital / data reference system architecture is still pending.
  These topics will be handled by FP5 RAM working group.

- Cybersecurity (HW/SW aspects)

  The topic of cybersecurity is currently under discussion so that the final necessary input for the final development of the digital / data reference system architecture is still pending. In this document the chapter 5.7.1 Cybersecurity is covered preliminarily and just contained to give an overview about the general requirements

to be considered.
This topic will be covered by the European Group "Cybersecurity".

- Interchangeability

  Also, this topic is currently under discussion so that the necessary input for the development of the digital / data reference system architecture is still pending. This topic will be handled by the recently setup group of operators, vehicle keepers and suppliers.

6 Conclusion

This document constitutes deliverable D3.3 “Digital / Data reference system architecture FDFT” of ER JU Flagship Area 5 project FP5 TRANS4M-R. The project aims to boost innovation for the European rail freight sector, concretely by developing, validating, and demonstrating TRANS4M-R technical enablers.

The objective of this document is to provide the physical system architecture for rolling stock fitted with a DAC to enable the operation of full digital freight trains throughout Europe. The digital / data reference system architecture will serve – together with the functional reference system architecture described in /WP3 D3.1/ and the physical reference system architecture described in /WP3 D3.2/ - as foundation for authorisation of FDFTO and will define the basis for the development of the innovations for WP5-WP12.

The section Methodology explains how WP3 intensively aligned the various inputs from the different developments within the project.

While designing the architecture, open topics have been identified. The topics have to been solved in the future work within FP5 from other WP’s. Nevertheless, with this document the groundwork has been done for a common development of the FDFT. All other WPs can use this document as their foundation.

Based on the continuous development in TRANS4M-R, the feedback from the freight sector, new concepts, the system architecture will be developed further within FP5 and other projects to come.

7 References

reference	*Publication date*	*Description*
WP2 D2.1	2023-06-30	WP2 D2.1: Preliminary Operational Procedures_v1.0.pdf
WP3 D3.2	2024-04-30	WP3 D3.2: Physical reference system architecture FDFT
WP3 D3.3	2024-04-30	WP3 D3.3: Data reference system architecture FDFT
WP4 D4.1	2023-04-28	WP4 D4.1: Authorisation Strategy and Overall Safety Plan
WP4 D4.2	2023-11-15	WP4 D4.2: Risk assessment and harmonized safety architecture
WP5 D5.1	planned	D5.1: Functional Requirements Specification of Train Functions
WP5 D5.2	2023-12-20	D5.2: Technical Specifications of Wagon and Locomotive DAC up to Level 5
WP5 D5.4	planned	D5.4: Technical Specification of Wagon Power System and Communication System

8 Appendix

HMI (for DAC)

The purpose of an HMI (Human-Machine Interface) on a locomotive is to facilitate communication and interaction between the operator and the DAC control and monitoring systems of the locomotive.

The HMI allows the operator to access and control the DAC system, including the couplers, brakes, and various monitoring systems. It provides a graphical interface that displays real-Train Integrity Monitoring information about the status of the train DAC specific part, such as status of Train Operation Mode, couplers, and other status.

The HMI also provides warnings and alerts for important events, such as violation of train integrity, enforced Train Operation Mode-change, and other safety-related issues, allowing the operator to respond quickly and effectively.

Overall, the HMI on a locomotive serves as a critical tool for simplifying and streamlining the operation of the DAC system, while also ensuring safety and providing up-to-date information for the operator.

As mentioned in the introduction part the HMI for DAC is not necessarily a dedicated display, and can reuse the already existing display on loco, as long as requirements are met by shared display.

REQ-ID	REQ	OPEID
REQ-HMI-001	HMI shall provide brake power calculation data to the driver, request data from BE and display results	O41.15 BE41.13 BE41.14 BE41.15
REQ-HMI-002	HMI shall provide information train arrived at destination.	TU4.9 BE4.10
REQ-HMI-003	HMI shall provide information about TI process, Compiled Consist List (CCL), deviation, and validation status, with CRC.	P31.6 TU31.7 TU32.6 P32.7 TU32.8
REQ-HMI-004	HMI shall provide input for Train Operation Mode selection.	BE31.1 BE30.1 P30.1 P31.1 O4.1

REQ-HMI-005	HMI shall provide input to define expected Compiled Consist List.	TU32.8
REQ-HMI-006	HMI shall provide input to report train arrival.	S4.10
REQ-HMI-007	HMI shall provide output for BE requests (like start movement, request PB APPLY)	BE41.4 BE25.1
REQ-HMI-008	HMI shall provide status of train. Content: Train status: active Train Operation Mode, TIM (Train Integrity Monitoring), brakes in train: checked, PB, Power line: 400V, PSU and closing lid status[2]	P30.1 P31.1 TU25.2 TU25.4 P25.5 TU31.9 BE4.1 O4.1 TU30.2 O4.1 TU30.5 TU30.8 TU31.5 BE30.9 BE4.1 P25.1 TU31.9 BE4.10 S4.10 TU4.9 BE30.1 BE31.1 O41.4
REQ-HMI-009	HMI shall provide warning if train is shortened without RDC.	D2
REQ-HMI-010	HMI shall take 400V ON or OFF request.	TU30.2 TU31.9
REQ-HMI-011	HMI shall take request for PB APPLYlication or RELease on given consists.	P25.1

HMIS (HMI-Safe)

Provides a dedicated HMI-part for safety relevant operations – like Train Operation Mode (Train Operation Mode) change, 400V switch ON, PB (Park brake) release or RDC (Remote Decoupling).

[2] There is no safety related function allocated to lid status.

This IPN can be integrated to the HMI if it is compliant with the safety targets.

REQ-ID	REQ	OPEID
REQ-HMIS-001	HMIS shall allow Authorized Operator to APPly or RELease PB.	P25.1
REQ-HMIS-002	HMIS shall allow Authorized Operator to select 400V ON or OFF.	TU31.9
REQ-HMIS-003	HMIS shall allow Authorized Operator to select Train Operation Mode.	O4.1 P30.1 P31.1
REQ-HMIS-004	HMIS shall allow ATO to APPly or RELease PB.	BE25.1
REQ-HMIS-005	HMIS shall allow ATO to select Train Operation Mode.	BE30.1 BE31.1 BE4.1
REQ-HMIS-006	HMIS shall display PB status (APPlied / RELeased / unavailable) on train.	P25.1 TU25.2 TU25.4 P25.5
REQ-HMIS-007	HMIS shall display summarized Train Operation Mode status.	BE4.1 TU4.9 BE4.10 S4.10 O4.1 BE4.1 TU4.9
REQ-HMIS-008	HMIS shall display valid TIM (Train Integrity Monitoring) status.	TU31.7
REQ-HMIS-009	HMIS shall displays 400V status (ON or OFF).	TU31.9 TU30.2
REQ-HMIS-010	HMIS shall provide access for LCU to enforce safe Train Operation Mode.	TU4.9
REQ-HMIS-011	HMIS shall provide information to RSLM.	TU30.5 TU31.5 BE25.1

LCU

LCU (Locomotive Control Unit) is the central intelligence IPN for DAC system on locomotive level, and as leading consist also on train level. It is the locomotive specific extended CCU (Consist Control Unit).

Main tasks of LCU are:

- as central DAC communication node:
    - collect requests from Authorized Operator, BE, ATP via HMI and HMIS
    - display system status, feedback, provide help with train operation.
    - on train level: provide access to CCUs in train.
    - on locomotive level: provide access to TCMS.
- as leading consist - coordinate train functions, ensuring execution of them.

REQ-ID	REQ	OPEID
REQ-LCU-001	LCU shall be able to collect CCUs Train Operation Mode status	BE4.1 O4.1 WWS30.4 WWS31.4
REQ-LCU-002	LCU shall be able to display the Train Operation Mode status on HMI.	O4.1 TU4.9 BE4.10 S4.10 BE30.1 TU30.8 BE31.1
REQ-LCU-003	LCU shall be able to report the actual Train Operation Mode to BE via LINK.	BE4.1 TU4.9 BE4.10 S4.10 O4.13 BE30.1 BE31.1

REQ-LCU-004	LCU shall be able to request Train Operation Mode NL (Neutral) from CCUs.	TU4.9 BE4.10 BE4.10 S4.10 S4.10
REQ-LCU-005	LCU shall be able to request Train Operation Mode TR (Train Run) from CCUs.	BE4.1 O4.1
REQ-LCU-006	LCU shall be able to store Train Operation Mode in nonvolatile protected memory (like e.g., JRU).	TU4.9 TU30.7

CCU

CCU (Consist Control Unit) is the central intelligence IPN for DAC system on wagon level.

Main tasks of CCU are:

as central consist communication node:

- collect requests from LCU – later from PUB (Push Buttons)
- provide feedback to LCU – later to PUB HMI.
- on train level: support train inauguration, neighbour detection.
- on consist level: provide access to Coupler heads, BRE and Rear End Signal.

REQ-ID	REQ	OPEID
REQ-CCU-001	CCU shall report BRE status to LCU.	O41.4 O41.15 BE41.4
REQ-CCU-002	CCU shall accept request from LCU to switch to TOM_NL	BE4.10 S4.10 TU4.9
REQ-CCU-003	CCU shall accept request from LCU to switch to TOM_SH	TU30.3

REQ-CCU-004	CCU shall accept request from LCU to switch to TOM_TR	O4.1 TU31.2 BE4.1
REQ-CCU-005	CCU shall be able to request PB apply from BRE	WWS25.3
REQ-CCU-006	CCU shall have access to neighbour detection result.	WWS32.3
REQ-CCU-007	CCU shall process request of PB_APP from LCU	TU25.2
REQ-CCU-008	CCU shall process request of TIM start on LAC	TU32.9 TU31.7
REQ-CCU-009	CCU shall process request of TIM stop on LAC	TU32.1
REQ-CCU-010	CCU shall process warning of 400V_OFF from LCU	TU30.2
REQ-CCU-011	CCU shall query PB status from BRE	WWS25.3
REQ-CCU-012	CCU shall report PB status to LCU	TU25.2
REQ-CCU-013	CCU shall report TOM status to LCU	WWS31.4 WWS30.4 BE4.1 O4.1
REQ-CCU-014	CCU shall support BRE query by LCU.	BE41.4
REQ-CCU-015	CCU shall tunnel through RSL replies to RSLM	S4.10 BE4.10 S4.10 O4.1 BE4.1 TU25.2 WWS30.4 WWS31.4 TU4.9
REQ-CCU-016	CCU shall tunnel through RSLM messages to RSL	BE4.1 BE4.10 TU30.3 TU31.2 TU4.9 O4.1 TU25.2