ERTMS Data Applications

FFFIS part:

CCS Consist Network Communication Layers

REF : SUBSET-147

ISSUE : 1.0.0

DATE : 05/07/2023

Company	Technical Approval	Management approval
ALSTOM		
AZD		
CAF		
HITACHI RAIL STS		
MERMEC		
SIEMENS		
THALES		

1. MODIFICATION HISTORY

Issue Number Date	Section Number	Modification / Description	Author
pre-version 18-07-2020	all	Draft for extension of S-143 for S-119 lower layers; agreed comments of EECT #64 have been already considered	F. Bitsch
0.0.1 06-11-2020	all	First issue of the document	F. Bitsch
0.0.2 16-11-2020	all	Changes according to the review meeting in the UNIFE MG On-board Architecture at 16.11.2020	F. Bitsch
0.0.3 23-11-2020	all	Changes according to the review meeting in the UNIFE MG On-board Architecture at 23.11.2020	F. Bitsch
0.1.0 24-11-2020	Chapter 1	Draft version for distribution in the ERA TWG ARCHI	F. Bitsch
0.1.1 11-04-2021	all	Changes according to the review in the TWG Archi Meeting #5 and discussion with ATO WP	F. Bitsch
0.1.2 17-04-2021	5.1.1.4, 5.2, 9.2.3.1, 10.1.1.14	Alignement with Subset-139	F. Bitsch
0.1.3 19-05-2021	10.1, 10.2	Alignement with Subset-139	F. Bitsch
0.1.4 06-09-2021	Title page, 9.1, 9.2	Changes according to further received comments in the UNIFE MG On-board Architecture	F. Bitsch
0.1.5f 25-02-2022	13	New chapter on UTC time service has been added	F. Bitsch / F. Kaiser
0.1.5 25-02-2022	12	New chapter on One common bus has been added	Harald Roelle
0.1.6 17-03-2022	12	Revised based on review feedback	H. Roelle
0.1.7 22-03-2022	12	Addition review comments in chapter 12	H. Roelle
0.1.8 12-05-2022	all	EECT review 03-05-2022	F. Bitsch
0.1.9 08-06-2022	all	EECT review 25-05-2022	F. Bitsch

0.1.10 30-06-2022	6.3.1.1, 8.4.9.1, 9.1.1.2, 9.2.1.2, 9.2.2.4, and 10.1.1.6	EECT review 30-06-2022	F. Bitsch
0.2.0 17-02-2023	-	Formal update for the B4R1 pre-release version; watermark removed	F. Bitsch
1.0.0 05-07-2023	-	Baseline 4 1st release version; reference to S-146 corrected	F. Bitsch

2. INTRODUCTION

2.1 Table of Contents

2.2 Table of Figures

2.3 List of Tables

2.4 Abbreviations

2.4.1.1 For ATO related abbreviations see ERTMS/ATO Glossary [Ref 1]. (I)

2.4.1.2 For ETCS related abbreviations see SUBSET-023 [Ref 3]. (I)

API	Application Programming Interface
CAN	Controller Area Network
CCS	Control, Command and Signalling CCS means the subsystems on-board CCS and trackside CCS as defined in the EU directive 2016/797 and described in the technical specifications for interoperability for the control, command and signalling subsystems.
CN	Network/bus connecting equipment within a consist.
DHCP	Dynamic Host Configuration Protocol
DST	Daylight Saving Time
ED	End Device
ECN	Ethernet Consist Network as per IEC 61375-3-4
EMD	Electrical Middle Distance Bus
ESD+	Electrical Short Distance Bus
FRMCS	Future Railway Mobile Communication System
HW	Hardware
(I)	The statements made in this Subset are assigned to the following categories: (I) or (R) I = Informative (indicated by ‘(I)’ at the end of the clause). This is not a requirement. It is only for better understanding of the specification.
NTP	Network Time Protocol
OCCB	One common on-board CCS bus: A platform for the communication networks internal and external to the on-board CCS subsystem.
OMS	Online Monitoring System
MAC	Medium Access Control, subfunction on OSI layer 2
MVB	Multifunction Vehicle Bus
OSI	Open Systems Interconnection

PCP	Priority Code Point
Realtime data	Data that needs to be communicated within a certain upper time limit.
RPC	Remote Procedure Call
RST	Rolling Stock
(R)	The statements made in this Subset are assigned to the following categories: (I) or (R) R = Requirement (indicated by '(R)' at the end of the clause). This paragraph is a requirement and it is mandatory for the on-board CCS subsystem on newly developed vehicles designs requiring a first authorization and for the Interoperability Constituent ETCS On-board (independent from its specific application). For all vehicles, which do not fall under the definition "newly developed vehicles designs", its application is voluntary at the discretion of the system integrator.
SW	Software
TP	Time Protocol (RFC 868, [Ref 23])
TTLS	Train Time and Location Service
UTC	Coordinated Universal Time
Zone	Logical part of the on-train system architecture. In alignment with the security concepts the typical zones are: FRMCS, CCS, Rolling Stock, TOS, Passenger Network

Table 2-1: Abbreviations

2.5 Definitions

2.5.1.1 For ATO related definitions see ERTMS/ATO Glossary [Ref 1]. (I)

2.5.1.2 For ETCS related definitions see SUBSET-023 [Ref 3]. (I)

2.6 Scope and purpose of the document

2.6.1.1 This document defines the standard for the network technology being used for the on-board CCS subsystem to establish communication on the interfaces internal to the subsystem among different applications (e.g. ETCS on-board, ATO on-board) and on the interfaces to the subsystem rolling stock. It does not define a standard network technology for other subsystems (e.g. the rolling stock). Consequently, the rolling stock subsystem provides train interfaces and an interface for the ORD to the on-board CCS subsystem compliant to this document (either through a gateway or a rolling stock network technology compliant to this document). The communication technology used for other functions or interfaces on the rolling stock subsystem are out of scope of this document. (I)

2.6.1.2 The purpose of this document is to allow an economic design based on a fully standardized and state-of-the art solution for the communication among the various functional building blocks within the on-board CCS subsystem and to other subsystems. This will reduce the complexity and bring more flexibility for vehicle owners, if they want to scale the on-board CCS subsystem or change to another supplier. (I)

2.6.1.3 For the abstractions of different layers of the network technology this standard makes use of the layers defined by the OSI (Open System Interconnection) model. (I)

2.6.1.4 The abstraction of the layers as used in this document is shown in Figure 2-1.

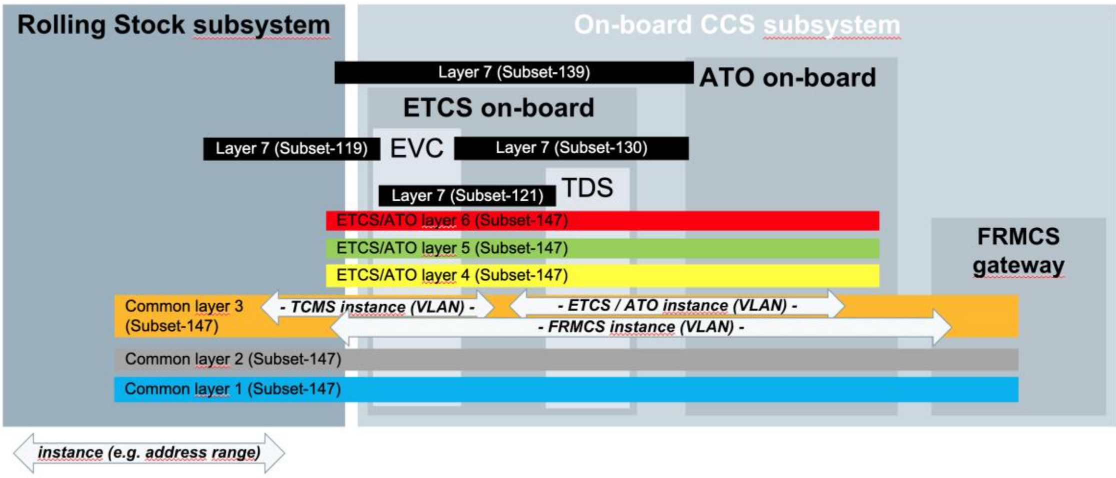

Figure 2-1: Levels of abstraction for the layers according to the OSI model

2.6.1.5 This document provides firstly a collection of all existing communication network technologies, including the ones which were included in previous versions of subsets (e.g. Subset-119 and -121) and in addition technology currently used by the suppliers. Hence, it freezes the current state of play of these technologies. (I)

2.6.1.6 Secondly, this document provides the requirements for the Ethernet CCS Consist Network, which will be the future harmonised communication platform for the on-board CCS subsystem on basis of which functional building blocks of the on-board CCS subsystem (ETCS on-board, ATO on-board, FRMCS, etc.) will communicated with each other. The first stage to this communication platform is the definition of layers 1 and 2. For the layers 3 to 6 it is specified which communication technologies are allowed to use. A specific definition of these layers will follow at a later stage. (I)

2.6.1.7 This approach creates an abstraction of the application layer from the communication, which led to more stable application layer specifications and to more stable implementation of the application layer. Furthermore, it fixes a set of optional legacy technology for the transition period at discretion of the system integrator (normally the vehicle manufacturer). This removes the risk of introducing new technology which will become obsolete shortly with the target harmonised communication platform (Ethernet CCS Consist Network). The definition of layers 1 and 2 of the Ethernet CCS Consist Network will allow vehicle manufacturers to prepare newly developed vehicles designs for this future technology. (I)

2.6.1.8 According to the levels of abstraction used by this standard, the communication layers are layer 1 (physical layer) up to layer 5 (session layer)/layer 6 (presentation layer)[1], see Figure 8-1, which are used by ETCS on-board and ATO on-board for communication to other on-board equipment/subsystems in the Consist Network (CN), see the overview Figure 2-2. The interfaces of ETCS on-board, ATO on-board and of other on-board equipment to the On-board FRMCS will use only the layers 1 up to 3. (I)

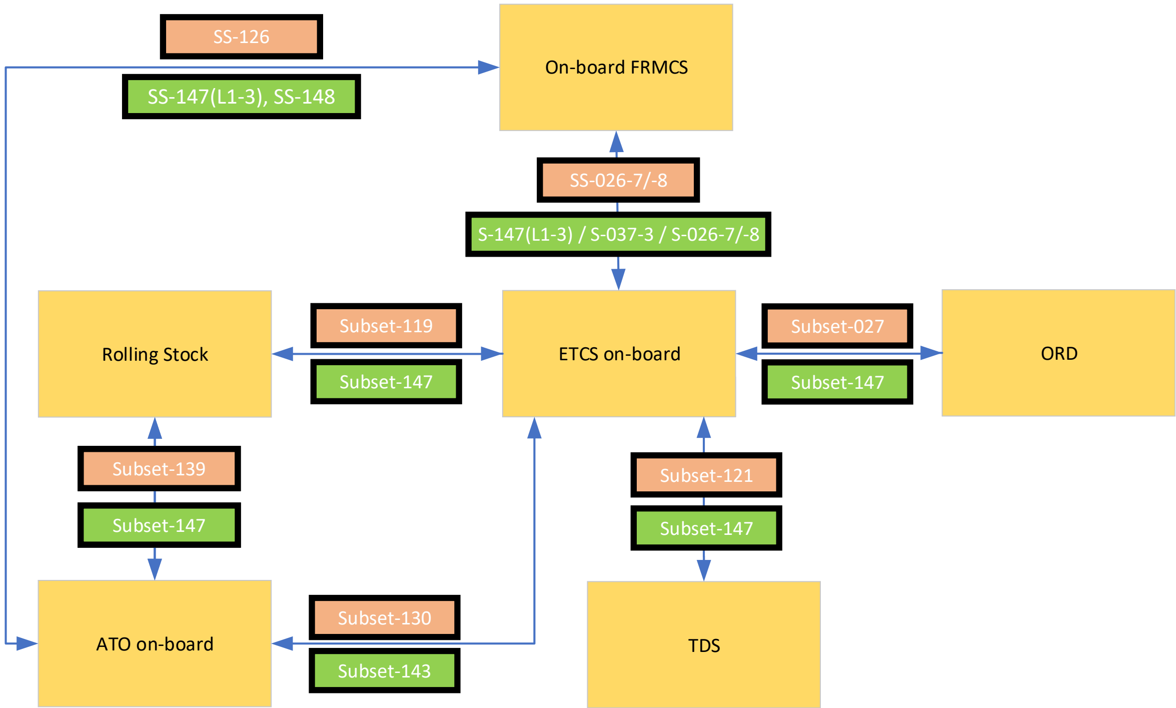

Figure 2-2: Interfaces and related specifications for ETCS & ATO on-board and Rolling Stock

[1] Some parts of the OSI reference model in layer 6, such as some syntax and semantics definition are defined in the current Subset-147 but exported to the Application Layer subsets where they are implemented.

2.6.1.9 Table 2-2 gives an overview on the application of Subset-147. (I)

Entity 1	Entity 2	Reference	Local Serial Communication	Service Class, see §8.4.4.1.1
ATO on-board	ETCS on-board	SS-130	SS-143	5
ATO on-board	On-board FRMCS	SS-126	SS-147(L1-2) and SS-148	5
ATO on-board	RST	SS-139	SS-147	5
ETCS on-board	ORD	SS-027	SS-147	5
ETCS on-board	TDS	SS-121	SS-147	5
ETCS on-board	RST	SS-119	SS-147	5
ETCS on-board	On-board FRMCS	SS-026-7/-8	SS-147(L1-2), SS-037-3 and SS-026-7/-8	5
ATO on-board	OMS	SS-149	SS-147	5
ETCS on-board	OMS	SS-149	SS-147	5

Table 2-2: Overview on several applications of Subset-147[2]

2.6.1.10 The overall goal of the CCS Consist Network is to allow to integrate components within the CCS-subsystem without any change to these components (interchangeability) in the future. This will avoid multiple logical and physical adapters between the systems in scope. In addition this document defines the train time and location service which provides information to be distributed via the CCS Consist Network. (I)

2.6.1.11 The application layer is not part of this document and is defined in Subsets application layer documents (e.g. Subset-119 or Subset-139, see Figure 2-2). (I)

2.6.1.12 In case of the interfaces of the ATO on-board it is possible to use Subset-143 [Ref 16] as alternative to Subset-147. But also in case of using Subset-143 the layers 1 and 2 as defined in chapter 8 and the time and location service as specified in chapter 9 shall be applied, see also 3.1.1.6. (R)

2.6.1.13 The chapters 7, 8, and 9 are applicable only for 'newly developed vehicle designs' requiring a first authorisation as defined in Article 14 of Commission Implementing Regulation 2018/545 and for the Interoperability Constituent ETCS On-board (independent from its specific application). (R)

[2] The applications are only mandatory, if the "reference" document is specified in a technical specification for interoperability as a basic parameter.

2.7 Reference documents

Ref. N°	Title	Reference	Author
[Ref 1]	ERTMS/ATO Glossary	13E154	EEIG ERTMS Users Group
[Ref 2]	ERTMS/ATO System Requirements Specification	SUBSET-125	UNISIG
[Ref 3]	Glossary of Terms and Abbreviations	SUBSET-023	ERA, UNISIG, EEIG ERTMS Users Group
[Ref 4]	System Requirements Specification	SUBSET-026	ERA, UNISIG, EEIG ERTMS Users Group
[Ref 5]	Electronic railway equipment – Train communication network (TCN) – Part 3-4: Ethernet Consist Network (ECN)	IEC 61375-3-4:2014	International Electrotechnical Commission
[Ref 6]	Train Communication Network – Communication Profile	IEC61375-2-3:2015 TCN	International Electrotechnical Commission
[Ref 7]	Train Communication Network – MVB	IEC61375-3-1:2012 TCN	International Electrotechnical Commission
[Ref 8]	Train Communication Network – CAN	IEC61375-3-3:2012 TCN	International Electrotechnical Commission
[Ref 9]	Serie Profinet	IEC61158-1:2019 / 61158-5-10 :2020 / 61158-6-10:2019	International Electrotechnical Commission
[Ref 10]	Profisafe	IEC61784-2:2019/ -3-3:2021	International Electrotechnical Commission
[Ref 11]	Train Communication Network – Train Communication Network – WTB	IEC61375-2-1:2012 TCN	International Electrotechnical Commission
[Ref 12]	Open Platform Communications Unified Architecture (OPC-UA)	IEC62541-1/-2:2016 / -3 – -14:2020 / -100:2015	International Electrotechnical Commission
[Ref 13]	Performance Requirements for Interoperability	SUBSET-041	UNISIG
[Ref 14]	Performance Requirements for STMs	SUBSET-059	UNISIG
[Ref 15]	TDS / ETCS On-board DMI-EVC Interface FFFIS	SUBSET-121	UNISIG

Ref. N°	Title	Reference	Author
[Ref 16]	ERTMS/ATO: Interface Specification Communication Layers for On-board Communication	SUBSET-143	UNISIG
[Ref 17]	Network Time Protocol Version 4: Protocol and Algorithms Specification	RFC 5905: 2010	Internet Engineering Task Force (IETF)
[Ref 18]	DHCP Options and BOOTP Vendor Extensions	RFC 2132: 1997	Network Working Group
[Ref 19]	Electronic railway equipment - On board driving data recording system - Part 1: System specification	IEC 62625-1:2013	International Electrotechnical Commission
[Ref 20]	ERTMS End-to-End Security Layer	SUBSET-146	UNISIG
[Ref 21]	ATO-OB / Rolling Stock FFFIS Application Layer	SUBSET-139	UNISIG
[Ref 22]	TSI LOC&PAS	1302/2014	European Commission Regulation
[Ref 23]	Time Protocol	RFC 868: 1983	Network Working Group
[Ref 24]	Industrial communication networks - Network and system security – Part 3-3: System security requirements and security levels	IEC 62443-3-3: 2013	International Electrotechnical Commission
[Ref 25]	IEEE Standard for Local and Metropolitan Area Networks–Bridges and Bridged Networks	IEEE 802.1Q-2018	IEEE
[Ref 26]	FRMCS FFFIS – Form Fit Functional Interface Specification	FRMCS FFFIS-7950	UIC
[Ref 27]	EuroRadio FIS - FRMCS Communication Functional Module	Subset-037-3	UNISIG
[Ref 28]	ERTMS/ATO System Requirement Specification	Subset-125	UNISIG
[Ref 29]	ATO-OB / ATO-TS FFFIS Application Layer	Subset-126	UNISIG
[Ref 30]	ATO-OB / ATO-TS Interface Specification - Transport and Security Layers	Subset-148	UNISIG

Table 2-3: Reference Documents

3. GENERAL REQUIREMENTS

3.1.1.1 This specification includes the solutions regarding the Ethernet, MVB and CAN based on [Ref 5], [Ref 7], and [Ref 8]. (I)

3.1.1.2 The communication between ATO on-board and other on-board equipment / subsystems shall be based on Ethernet. The MVB and CAN solutions are not needed for ATO. (R)

3.1.1.3 The communication between FRMCS on-board entities and other on-board equipment / subsystems shall be based on Ethernet. The MVB and CAN solutions are not needed for FRMCS on-board entities. (R)

3.1.1.4 The communication between the TDS (Train Display System according to [Ref 15]) and the ETCS on-board shall be based on Ethernet or on MVB. The CAN solution shall not be applied for this interface. (R)

3.1.1.5 For 'newly developed vehicle designs' only Ethernet CCS Consist Network lower layers defined according to chapter 11 shall be applicable. (R)

3.1.1.6 The communication technologies PROFINET [Ref 9] (incl. PROFIsafe [Ref 10]), TRDP [Ref 6], OPC-UA [Ref 12], and Subset-143 [Ref 16] are supplementary protocols for the application of Ethernet. (R)

3.1.1.6.1 Exception: In case of the communication of FRMCS on-board entities the corresponding specifications shall be applied (e.g. Subset-037-3 [Ref 27] and Subset-026-7/-8 [Ref 4] for ETCS or Subset-148 [Ref 30], -126 [Ref 30] and -125 [Ref 28] for ATO). (R)

3.1.1.7 This document provides a precise specification of the communication principles (possible communication protocols) used for the communication between the ETCS on-board, the ATO on-board and other on-board equipment / subsystems. [Ref 4] explains the architecture of the ETCS on-board and the interfaces to other equipment and [Ref 2] explains the architecture of ERTMS/ATO and the interfaces to other equipment. (I)

3.1.1.8 Usually the interface description on FFFIS layer is divided into two parts:
(i) Application layer interface describing all the functionalities and data exchanged between the communication parties and
(ii) the lower levels of communication.
This document describes part (ii), whereas some constraints and restrictions are addressed towards part (i) (see section 6). (I)

3.1.1.9 Optionally the Rolling Stock (for ORD also in case of newly designed vehicles) can integrate a gateway to adapt to the bus/network type defined by the ERTMS/ETCS on-board or ATO on-board in order to avoid touching an MVB or CAN based Rolling Stock, but enabling upgradeability on the CCS, see Figure 3-1. (I)

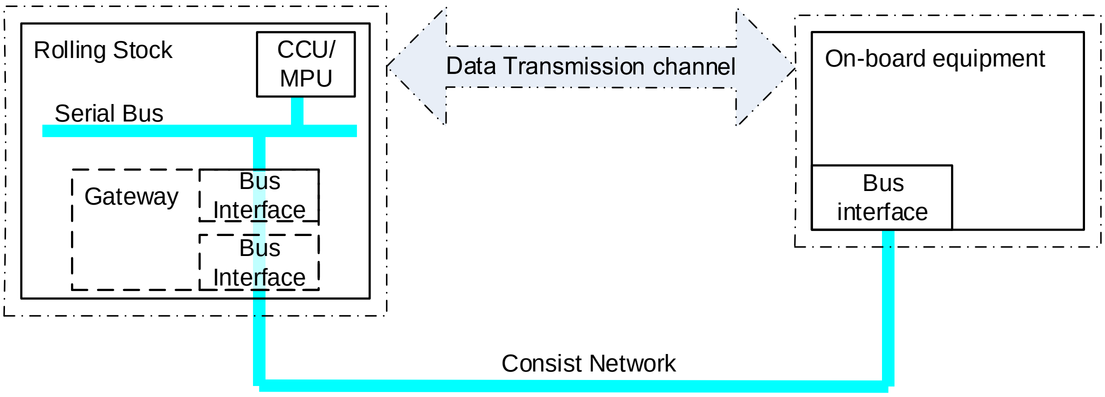

Figure 3-1: Rolling Stock can integrate a gateway to adapt to the bus/network type defined by the ERTMS/ETCS on-board or ATO on-board

4. MVB

4.1.1.1 The physical layer is ESD+ or EMD. (I)

4.1.1.2 The interface should be implemented in accordance with IEC61375-3-1 [Ref 7] – class 2 for process data and message data. (I)

5. CAN

5.1.1.1 The interface should be implemented in accordance with [Ref 8]. (I)

6. RULES TO APPLICATION LAYER DOCUMENTS

6.1 Introduction

6.1.1.1 This chapter contains rules for the application layer in order to have a harmonised handling of variables and packets in the application layer documents. (I)

6.2 Definition of the Variables

6.2.1.1 Variables are used to encode single data values. Variables cannot be split into smaller units. The whole variable has one type (meaning). (R)

6.2.1.2 Variables may have special values which are related to the basic meaning of the variable. (R)

6.2.1.3 Special values which are not spare, have always the highest values in a variable (e.g. 32767 = “unknown”). (R)

6.2.1.4 Spare values are located between the normal and special values in the variable range except where justified. (R)

6.2.1.5 If bitsets are used, the variables shall be defined starting from the lowest bit position, i.e. at offset zero as defined in IEC61375-2-1 [Ref 11], §6.4.4.3. (R)

6.2.1.6 Names of variables are unique. A variable is used in context with the meaning as described in the variable definition. Variables with different meanings have different names. (R)

6.2.1.7 If signed values are used, the negative values shall be encoded as 2’s complement. (R)

6.2.1.8 One bit variables (Boolean) always use 0 for false and 1 for true. (R)

6.2.1.9 Offsets for numerical values are avoided (0 is used for 0, 1 for 1, etc.) except where justified. (R)

6.2.1.10 The variable’s length shall be multiple of a byte unless otherwise specified. (R)

6.2.1.11 If a variable is shorter than a byte in length, the variable is part of a bitset whose length is multiple of a byte. (R)

6.2.1.12 The transmission order shall respect the order of variables listed in the packet format (from top to bottom). (R)

6.2.1.13 The signal types are defined in IEC61375-2-1 [Ref 11], table 19 (INT# can be used for INTEGER# and UINT# for UNSIGNED#). (R)

6.3 Definition of the Packets and Data Structures

6.3.1 General

6.3.1.1 The definition of data structures could be focused on the specification of packets like in the context of the existing FFFIS but might also use formal methods for data modelling. (I)

6.3.1.2 Packets are multiple variables grouped into a single unit, with a defined internal structure. (R)

6.3.1.3 In case of application for ATO interfaces the following applies: For all Data Classes Message Data and Process Data the same header structure shall be used. They payload data consists of a header, followed by the application specific data. (R)

6.3.2 ATO Header Definition

6.3.2.1 The following table lists the header used on ATO application layer. (R)

Payload Header				
Item	**Variable Name**	**Description**	**Data Type**	**Resolution/Formula**
1	NID_PACKET	ATO Packet number.	UINT8	Numbers 0 .. 30: Slot 1 31 .. 60: Slot 2 61 .. 90: Slot 3 91 .. 120: Slot 4 121 .. 150: Slot 5 151 .. 180: Slot 6 181 .. 210: Slot 7 211 .. 240: Slot 8 241 .. 255: reserved Each application layer interface shall select one slot only. It needs to be made sure that the slots are not reused elsewhere.
2	L_PACKET	Length of Header + User Data length.	UINT16	**Minimum:** 7 **Maximum:** Process Data: 1468 Message Data: 65524 **Resolution:** 1 byte
3	T_TIMESTAMP	Timestamp in milliseconds since start-up. The timestamp will be set at the moment the telegram is issued.	UINT32	**Resolution:** 1 ms

Table 6-1: Header Structure used on ATO Application Layer

6.4 User Data

6.4.1.1 The definition of User Data is out of scope of this document. It should be defined in the application layer documents, see 2.6.1.8. (I)

7. PERFORMANCE REQUIREMENTS

7.1.1.1 The Performance Requirements are valid for the Ethernet CCS Consist Network which means that the On-board Core Network and End Devices are in the scope (equipment). (R)

7.1.1.2 The communication channel (EndToEnd on application level, see 7.1.1.1) shall transmit the data related to the application layer within 50 ms (for 95% of samples) for Ethernet CCS Consist Network. (R)

7.1.1.3 The communication channel (EndToEnd on application level, see 7.1.1.1) transmits the data related to the application layer within 0.35 s (for 95% of samples) for CAN and MVB. (I)

7.1.1.4 Justification for CAN and MVB: [Ref 13] and [Ref 14] define for specified events a maximum reaction time of 1.5 s for a transmission path in one direction and a maximum reaction time of 2.0 s for a bidirectional transmission. Assuming a registration time of 0.1 s and a processing time of 0.4 s for both bus participants, the remaining time value is assigned to the communication channel. (I)

7.1.1.5 See [Ref 14] §3.2 (Measurements) for a definition of start and stop events on the STM interface in this case. (I)

7.1.1.6 For Ethernet CCS Consist Network at least a network/bus cycle time of the source device of 20 ms shall be supported. (R)

7.1.1.7 For CAN and MVB at least a cycle time of the source device of 128 ms is supported. (I)

7.1.1.8 In case the Rolling Stock integrates a gateway to adapt to the bus type defined by the ERTMS/ETCS on-board or ATO on-board the additional transfer delay introduced due the implementation of the gateway shall be below 50ms (worst case) (this relates to communication channel which is EndToEnd on application level, see 7.1.1.1). (R)

8. ETHERNET CCS CONSIST NETWORK

8.1 Introduction

8.1.1.1 This protocol specification is divided into separate layers. Figure 8-1 shows the representation of the different layers according to the Open Systems Interconnection (OSI) model. (I)

(7) Application
(6) Presentation
(5) Session
(4) Transport
(3) Network
(2) Data Link
(1) Physical

Figure 8-1: OSI Layers

8.1.1.2 Both communication parties the ETCS on-board, the ATO on-board and other on-board equipment / subsystems shall be compliant to the End Device Interface characteristics as specified in IEC 61375-3-4 [Ref 5]. (R)

8.2 Principles

8.2.1 Strategy of specification

8.2.1.1 The definition of the lower layers of Ethernet CCS Consist Network (**One Common Bus lower layers)** is one of the high priority tasks leading to the introduction of the envisaged One Common Bus. (I)

8.3 Scope of Ethernet CCS Consist Network Lower Layers

8.3.1.1 The concept for the evolution of the on-board CCS architecture is based on the introduction of a standard network based on Ethernet as per [Ref 5] for the interfaces among the elements for the full OSI layer stack (OSI layers 1 to 7) on the long-term.[3] (I)

[3] With IEC61375-3-4 being an important base for this specification, the relations to this standard will be explained explicitly at important places. To improve readability, this will be done in footnotes.

8.3.1.2 This network for a future vehicle on-board communication will be referred to as the Ethernet CCS Consist Network, also called **One Common Bus** in this specification. (I)

8.3.1.3 The following chapters will provide definitions for the layers 1 and 2 according to the OSI model (see Figure 8-1: OSI Layers) of the Ethernet CCS Consist Network. (I)

8.3.1.4 The focus lies on the OSI layers 1 and 2 to allow the provision of hardware interfaces in order to prepare for the future introduction of the Ethernet CCS Consist Network for the vehicle on-board communication. (I)

8.3.1.5 The following specification clearly distinguishes between the following categories:

- The **On-board Core Network**: Made of **Network Devices**[4] which are interconnected and build up an ECN.
- **End Devices in scope**: Devices not being part of the On-board Core Network but connected to the On-board Core Network and which are in scope of this specification (see 8.3.2.3). From here, the term **End Device** is used as a short form for "End Device in scope".[5]

(End) devices connected to the On-board Core Network which are out of scope of this specification (see 8.3.2.3). (I)

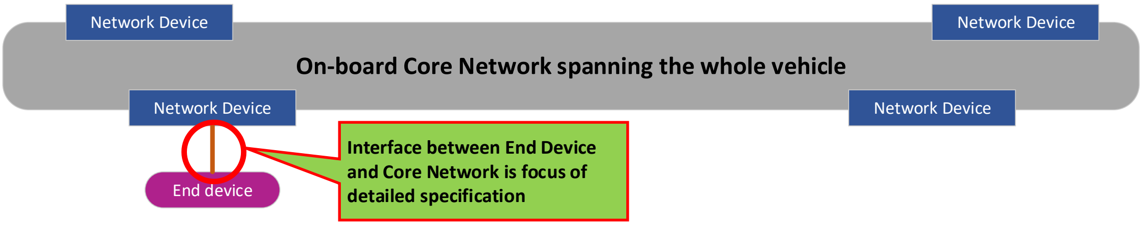

Figure 8-2: Separation of On-board Core Network and End Devices

8.3.1.6 The specification defines the **End Device Interface** between the On-board Core Network of the Ethernet CCS Consist Network and the End Devices in scope connected to it, thus leaving freedom for the design and architecture of the network core itself. This implies that there is no preferred solution provided for e.g., the topology of the network, being ring, ladder or a combination of these, or concepts/architectural patterns to offer redundancy within the network. For details, esp. on devices with multiple links, see 8.4.1.3. (I)

---

[4] As of IEC61375-3-4 chapter 4.2.4: Network Device types "repeater" and "consist switch"

[5] For clarification: Regarding IEC61375-3-4 chapter 4.2.3, this specification addresses End Device types of Temporary Devices and Standard Devices, as long as they belong to scoping of this chapter (see chapter 8.3.2.3).

8.3.1.7 Any port of any Network Device of the On-board Core Network (e.g. the port of a switch), where an End Device in scope is connected to, will be named **On-board Core Network Port**. (I)

8.3.2 Logical Zones and End Devices

8.3.2.1 Logical Zones

8.3.2.1.1 A Logical Zone is an area of the network including End Devices. The definition is based on grouping of certain overall functionality on the vehicle. The concept stems from security concepts, where a zone represents an area that shares the same level of protection. (I)

8.3.2.1.2 Today, Logical Zones are often represented by a physical network, e.g., for CCS functions, for communication functions etc. As the Ethernet CCS Consist Network has the goal to consolidate those separated networks, the concept of Logical Zones is introduced to make these distinct areas of protection still visible and usable. (I)

8.3.2.1.3 In Shift2Rail Project CONNECTA 3 the concept of “domains” is equivalent to Logical Zones. (I)

8.3.2.1.4 The Ethernet CCS Consist Network may carry also logical zones not in scope. Interfaces to devices residing in those zones are out of scope. (I)

8.3.2.2 Scoping of Logical Zones (R)

8.3.2.2.1 Logical Zones in scope of this specification are:

- FRMCS: Contains devices realising FRMCS functionality.
- CCS: Contains devices of CCS domain apart from FRMCS

8.3.2.2.2 Logical Zones explicitly not in scope:

- Rolling Stock: Devices of the Train Control System
- OOS (Operator Oriented Services)
- Passenger network or COS (Customer Oriented Services)
- Any other Logical Zone not explicitly mentioned in the Logical Zones in scope

8.3.2.3 Scoping of End Devices (R)

8.3.2.3.1 End Devices in scope:

- End Devices fully inside the On-board CCS Subsystem
- Gateway devices are in scope as of chapter 8.4.1.3 ff
- Examples include:

- On-Board FRMCS Cab Radio
- ETCS on-board
- ATO on-board

8.3.2.3.2 End Devices explicitly not in scope:

- Class B Systems
- Any device not visible at the edge of the On-board Core Network
- Any device not associated with the Logical Zones in scope
- Devices associated with the Logical Zones in scope but are directly related with individual designs or implementations of applications in the respective Logical Zones (e.g., I/O components, sensors, actuators etc.)
- Any other device not addressed by the End Devices in scope

8.3.3 Relations to security

8.3.3.1 Ethernet CCS Consist Network lower layer security functions

8.3.3.1.1 The security for the lower layers is supported by the network separation / segmentation function to ensure non-inference between logical separate communications (e.g., vital communication and non-vital communication) and authentication / authorization of End Devices at the On-board Core Network (I)

8.3.3.1.2 Additional security functions are expected on higher layers to ensure end-to-end security (e.g., direct end-to-end trust relationship of communication partners by authentication, integrity protection of messages, and confidentiality, if required by application). An example, how this can be achieved, is defined in [Ref 20]. (I)

8.3.3.2 CCS application layer security functions

8.3.3.2.1 The application layer is not part of this specification. This section is provided for better understanding of the overall security concept. (I)

8.3.3.2.2 [Ref 20] defines secured communication, as well as certificate management for ETCS, ATO and KMC. (R)

8.4 Definition of requirements

8.4.1 Base technology

8.4.1.1 The basic idea of the Ethernet CCS Consist Network is to share the same physical network infrastructure among multiple Logical Zones and applications therein, without replicating On-board Core Network Devices (e.g., switches) and their inter-connection (e.g., cables) for each of the Logical Zones or applications.[6] (I)

8.4.1.2 Any occurrence of the terms End Device and Logical Zone, even if not explicitly mentioned, are limited to the scope defined in chapter 8.3.2. (I)

8.4.1.3 Network architecture

8.4.1.3.1 No definition for the topology of the On-board Core Network is provided. This is left open to implementation of the actual onboard network to provide freedom of choice.[7] (I)

8.4.1.3.2 No specific technology or devices, especially Ethernet sub-standards, are prescribed for the On-board Core Network itself to provide freedom of choice. However, the interface technology towards End Devices specified in this chapter, implicitly poses some technical requirements on the On-board Core Network. (I)

8.4.1.3.3 Although the intention of this specification is to leave open the technical specification as much as possible to a specific vehicle design, some minimal cornerstones are defined to support modularity and upgradeability and to avoid unnecessary effort in upgrade and refurbishment. For example, cabling for the on-board core network is specified to give an opportunity to later upgrade to higher network speeds without the costly necessity to replace cabling. (I)

8.4.1.3.4 This chapter provides definitions for End Devices in scope on how to interface with the On-board Core Network on OSI layers 1 and 2. (I)

8.4.1.3.5 An End Device in scope may be related to Logical Zones in scope as of one of the following cases (I)

- An End Device residing in a single Logical Zone in scope
- An End Device in multiple Logical Zones (at least one of them in scope) of the Ethernet CCS Consist Network, either working as device being visible in multiple Logical Zones with internal separation of Logical Zones or acting as a gateway above layers 1 and 2 between Logical Zones.
- An End Device providing connectivity to different physical networks on layers above OSI layer 1 or 2, thus acting as a gateway to at least one of the Logical Zones in scope.

---

[6] Some basics mechanisms, e.g., VLANs, are mentioned already in IEC61375-3-4. This specification goes beyond, thus improving interchangeability and modularity. In addition, security aspects are addressed.

[7] In alignment with IEC61375-3-4 chapter 4.2.2

8.4.1.4 On-board Core Network characteristics

8.4.1.4.1 The base technology for the Ethernet CCS Consist Network is switched Ethernet.[8][9] (R)

8.4.1.4.2 The On-board Core Network shall allow at least transmission with a rate of 1Gbit/s. It shall apply 1000BASE-T (IEEE802.3ab of category 5e und 6) or better. (R)

8.4.1.4.3 On-board Core Network Ports for interfacing towards End Devices shall support 100BASE-TX (IEEE802.3 Clause 25) and 1000BASE-T (IEEE802.3ab of category 5e und 6) and better. (R)

8.4.1.5 End Device characteristics

8.4.1.5.1 End Devices connected to the network shall support at least 100BASE-TX (IEEE802.3 Clause 25). (R)

8.4.2 OSI layer 1: Physical layer

8.4.2.1 Cabling

8.4.2.1.1 To ease exchangeability of network components and upgradeability to higher speed classes inside the On-board Core Network, cabling used inside (connecting devices like switches together) the On-board Core Network shall be of CAT-6A (ISO/IEC 11801 2nd Ed. (2002)) or of a higher performance category. (R)

8.4.2.1.2 Optionally, fibre optic cables may be used inside the On-board Core Network. (I)

8.4.2.1.3 Cabling used for connecting End Devices to the network shall be of CAT-6 or of a higher performance category. (R)

8.4.2.2 Connectors

8.4.2.2.1 A standardised connector of type M12 with coding X-Code (IEC 61076-2-109) shall be used for connecting both ends of the cable in case of

- Connecting an End Devices to the On-board Core Network
- Inter-connections of On-board Core Network devices. (R)

8.4.2.2.2 Alternatively, a standardised connector of type M12 with coding D-Code (IEC 61076-2-101) can be used only at the end of an End Device when connecting to the On-board Core Network by 100BASE-TX. (R)

---

[8] In alignment with IEC61375-3-4 chapter 4.2.1

[9] Wireless technologies may be added to future revisions

8.4.2.2.3 Pinout of any cable shall be assembled as a straight-through cable. Crossed cables must not be used. (R)

8.4.2.3 Power supply over network cable

8.4.2.3.1 Using Power-over-Ethernet (PoE) (e.g., PoE: IEEE 802.3af-2003; PoE+: IEEE 802.3at-2009; PoE++: IEEE 802.3bt-2018) for End Devices is explicitly allowed optionally. Therefore, End Devices may use PoE if provided by the On-board Core Network but must not rely on it. If PoE is not available, End Devices must have the capability of getting external power supply. Using switch-independent PoE-injectors may serve as external power supply. (R)

8.4.3 OSI layer 2: Aspect of separation / segmentation

8.4.3.1 Separation/segmentation of traffic inside the On-board Core Network

8.4.3.1.1 The On-board Core Network shall be capable of appropriately separating traffic of different Logical Zones. Because of different Logical Zones sharing the same physical network, the On-board Core Network shall provide measures for logical segregation between the traffic, so that requirements regarding network segmentation from IEC 62443-3-3 SR 5.1, [Ref 24] can be fulfilled. (R)

8.4.3.1.2 In the sense of leaving the concrete On-board Core Network implementation up to the vehicle implementation, no further specification is done here. (I)

8.4.3.1.3 See also the chapter 8.4.5 on bandwidth limitation. (R)

8.4.3.2 Separation/segmentation of traffic towards End Devices

8.4.3.2.1 OSI layer 2 shall provide separation and segmentation based on VLANs as of IEEE802.1Q[10] [Ref 25], as the Ethernet CCS Consist Network targets to share one physical medium. (R)

8.4.3.2.2 A single physical link towards an End Device may carry traffic from a single Logical Zone or multiple Logical Zones. (I)

8.4.3.2.3 In case of traffic for a single Logical Zone, the link may use untagged or tagged traffic. Tagged frames may be used to fulfil QoS requirements. The tag used must match the VLAN ID the respective On-board Core Network Port is configured for. Any frames tagged differently shall be dropped at the On-board Core Network Port. (R)

8.4.3.2.4 Any untagged frames sent by an End Device shall be tagged by the On-board Core Network Port on per-port basis before being forwarded. (R)

[10] Compliant with IEC61375-3-4

8.4.3.2.5 For links carrying traffic of multiple Logical Zones, tagged frames as described in IEEE802.1Q [Ref 25] shall be used. (R)

8.4.3.2.6 The On-board Core Network Port shall only forward those VLANs in the interest of the connected End Device. (R)

8.4.3.2.7 The On-board Core Network Port shall drop incoming frames carrying any VLAN tags outside the set of configured VLANs for the respective port. (R)

8.4.3.2.8 The assignment of actual VLAN IDs to zones / applications is beyond this specification and is a matter of project configuration. (I)

8.4.3.3 Authentication / Authorization of End Devices

8.4.3.3.1 For authentication of End Devices at the On-board Core Network IEEE 802.1X-2004 EAP-TLS and later versions shall be used. The End Device shall act as supplicant, the On-board Core Network (e.g., a switch) shall act as authenticator. It is mandatory for the On-board Core Network (e.g., a switch) to authenticate the End Device, while an End Device optionally also may authenticate the On-board Core Network. (R)

8.4.3.3.2 The authentication shall be done on a port base. On links with multiple VLANs configured, a successful authentication on port level is sufficient to enable access to all VLANs the respective On-board Core Network Port is configured for. (R)

8.4.3.3.3 For existing End Devices without 802.1X support, MAC-based port security at the On-board Core Network Port may be used. (I)

8.4.3.3.4 An appropriate risk analysis is strongly recommended and therefrom derived additional security measures may be applied. (I)

8.4.3.3.5 Distribution of credentials and access policies are beyond this specification and are a matter of project configuration. (I)

8.4.4 OSI layer 2: Aspect of Quality-of-Service

8.4.4.1 Quality-of-Service in general

8.4.4.1.1 Quality-of-service in the lower layers is targeted on OSI layer 2 by using Priority Code Points as of IEEE 802.1Q-2014 (sometimes referred as IEEE P802.1p, also known as VLAN priority). (R)

8.4.4.1.2 To leverage the capabilities of prioritising traffic inside a VLAN, the Ethernet CCS Consist Network specifies its own rail-specific, vehicle-onboard interpretation of the Priority Code Points (PCP) (R):[11][12]

Priority	PCP value	Service Class	Typ. total band-width[13] [Mbit/s]	Typ. max delay[14] [ms]	Typ. usage example
0 (low)	0	Best effort	-	-	Default Mass data transport (e.g., memory dumps, S/W update data)
1	1	Broadband stream data	500	200	CCTV Video stream
2	2	Preferred stream data	150	150	PIS display Non-crit. outside display Passenger counting
3	3	Sporadic management data	50	100	IEC61375-3-4: "Message Data" CCS message data (e.g., diagnostics) SNMP HTTP switch management Netconf
4	4	Time-critical stream data	50	100	Cab radio audio stream
5	5	Ordinary process data	100	5	IEC61375-3-4: "Process Data" CCS process data

[11] PCPs given here are a refinement of data classes of IEC61375-3-4 chapter 4.3

[12] The table does not contain a maximum jitter by intention. Tests with a 1Gbit On-board Core Network (as required by this specification) based on Strict Priority Queuing have shown, that any jitter occurring is at least one magnitude lower than the maximum delay. Therefore, being sufficient for the respective applications.

[13] IEC61375-3-4 chapter 4.3 does not make a statement on bandwidth distribution.

[14] The delay values fulfil IEC61375-3-4 chapter 4.3. In fact, they are stricter here.

Priority	PCP value	Service Class	Typ. total band-width[13] [Mbit/s]	Typ. max delay[14] [ms]	Typ. usage example
6	6	Time-critical process data	50	1	IEC61375-3-4: "Supervisory Data" Appl. level time synchronization
7 (high)	7	Network control	1	1	Spanning tree Redundancy protocols NOT network management

Table 8-1: Service Class overview

8.4.4.1.3 The table shows the bandwidth distribution for 1 Gbit link speed. For other link speeds the bandwidth distribution should be adapted proportionally. (I)

8.4.4.1.4 Although this specification is limited to the scope of Logical Zones FRMCS and CCS, some typical examples in the above table from other zones are given to illustrate the intended use of the Service Classes. (I)

8.4.4.1.5 The above data on bandwidth and delay are meant as typical maximum values. It's the network provider's duty to keep those limits in the On-board Core Network by appropriate static and dynamic network management provisions. (R)

8.4.4.2 Quality-of-Service inside the On-board Core Network

8.4.4.2.1 In order to leave the actual On-board Core Network implementation up to the vehicle implementation, no further specifications on technical details for appropriate static and dynamic network management provisions are done here. (I)

8.4.4.2.2 Strict Priority Queuing may be used to realise the specified Service Classes. (I)

8.4.4.3 Quality-of-Service towards End Devices

8.4.4.3.1 In case of using tagged frames (for either single or multiple VLANs on the link), an End-Device may use PCP tagging to inform the On-board Core Network on the individual priority of a frame. (I)

8.4.4.3.2 In case of untagged frames, the On-board Core Networks decides on the QoS class of the traffic. (I)

8.4.4.3.3 The decision on trustworthiness of PCP tagging is in the responsibility of the On-board Core Network and is beyond this specification (open item). (I)

8.4.4.3.4 To improve compatibility to existing devices and to avoid unnecessary complexity, the interface to the End Devices in scope must not require the End Device to send certain frames precisely at a pre-planned point in time, e.g., to make use of Time-Aware Scheduling as specified in IEEE 802.1Qbv. (R)

8.4.4.3.5 End Devices must not expect to receive frames with minimal jitter, but with a guaranteed maximum delay. (R)

8.4.4.3.6 Any other mechanisms requiring a microsecond or even sub-microsecond time synchronization between an End Device and the On-board Core Network cannot be expected from the interface to the End Device. (R)

8.4.5 OSI layer 2: Aspect of Bandwidth limitation

8.4.5.1 Using VLANs with PCP as of IEEE 802.1Q serves as a basis for QoS marking. Inside the On-board Core Network, that should be combined with other mechanism for quality-of-service realization and security. The concrete technologies remain up to the vehicle implementation, no further specifications on technical details for appropriate static and dynamic network management provisions are done here. (I)

8.4.5.2 Especially for traffic segregation between zones and traffic classes, ingress policing and shaping may be considered. Per-Stream Filtering and Policing (PSFP) as of IEEE 802.1Qci may serve as a basis. (I)

8.4.5.3 Although multicast communication is a matter of the layers above OSI layer 2, the On-board Core Network shall support multicast communication in sense of limiting traffic to a necessary extent. This means that sending multicast traffic to receivers shall not only be realised by flooding the network, but IGMP-Snooping (or a similar mechanism) shall be available to limit traffic to On-board Core Network Ports where there is in fact a multicast receiver connected. (R)

8.4.6 OSI layer 2: Aspect of Availability / Redundancy

8.4.6.1 Availability is an important non-functional property to be fulfilled by the Ethernet CCS Consist Network. Redundancy is one of the most common concepts in improving availability. (I)

8.4.6.2 This chapter only addresses redundancy on network level. Functional redundancy e.g., by redundant End Devices is not covered here and needs to be specified on an application basis. (I)

8.4.6.3 Redundancy in the On-board Core Network

8.4.6.3.1 This specification makes no assumption on how redundancy is realised inside the on-board core network. (I)

8.4.6.3.2 Like the On-board Core Network's topology intentionally is left open, consequently the same applies to redundancy technologies and their respective redundancy protocols. (I)

8.4.6.3.3 The service class "Network control" shall be used for redundancy protocols. (R)

8.4.6.3.4 Any redundancy mechanisms and technologies shall not make implications on the End Devices. Especially specific redundancy protocols shall be transparent to End Devices. (R)

8.4.6.4 Redundancy in connecting End Devices

8.4.6.4.1 An End Device may have multiple redundant links to the On-board Core Network. These may go to different On-board Core Network Devices. (R)

8.4.6.4.2 An End Device with multiple links to the On-board Core Network must not act as a switch between those links, i.e., any forwarding of frames between redundant links by the End Device is forbidden. (R)

8.4.6.4.3 An End Device with redundant links cannot expect from the On-board Core Network to provide any switchover mechanisms between redundant links. Especially the management of those redundant links cannot be expected be incorporated into the On-board Core Network's management. (R)

8.4.6.4.4 The use of redundant links to the On-board Core Network is in the responsibility of the End Device and could involve higher layer protocols. For discovering the typical failure scenarios of cable failures and switch outages, the local interface link status may be used; for port failures of having flawed communication while the link being up, the local interface error statistics/indicators may be used. (I)

8.4.7 OSI layer 2: Aspect of Security

8.4.7.1 The security for the lower layers is focused on separating and segmenting network traffic to ensure non-interference between logical separate communications (see chapter 8.4.3). (I)

8.4.7.2 Confidentiality, Integrity and Authentication

8.4.7.2.1 OSI layers 1 and 2 alone are not able to completely address confidentiality and cryptographic protected integrity in an end-to-end perspective. (R)

8.4.7.2.2 Confidentiality and cryptographic protected integrity, as well as communication partner authentication must be addressed in higher protocol layers in an end-to-end security concept. This end-to-end security concept is out of scope of this specification. (R)

8.4.7.2.3 Subset 146 gives an example on specifying end-to-end security for specific applications. (I)

8.4.7.2.4 Potential technologies integrity and confidentiality protection in lower layers (as MACsec) were investigated. Due to failing the end-to-end security principle and current unavailability of the technology in network switches for the on-board environment, these technologies only may optionally be applied. Neither End Devices nor the On-board Core Network can expect those technologies to be available. (I)

8.4.8 OSI layer 2: Aspect of Safety

8.4.8.1 Safety provisions are a matter between end-to-end communication partners. Therefore, the OSI layers 1 and 2 have to be regarded as a black channel in the sense of safety. Consequently, safety has to be addressed on higher OSI layers (e.g., by an appropriate safety protocol) and is out of scope of this specification. (R)

8.4.9 OSI layers 3 to 6

8.4.9.1 For the application of Ethernet CCS Consist Network the communication technologies PROFINET (see IEC61158 [Ref 9]) (incl. PROFIsafe, see IEC61784-2/-3-3 [Ref 10]), TRDP (see IEC61375-2-3 [Ref 6]), and OPC-UA [Ref 12] are allowed. In case of the interface of the ATO on-board also the alternative described in clause 2.6.1.12 can be used for the application of Ethernet CCS Consist Network. (R)

8.4.9.1.1 Exception: In case of the communication of FRMCS on-board entities the corresponding specifications shall be applied (e.g. Subset-037-3 [Ref 27] and Subset-026-7/-8 [Ref 4] for ETCS or Subset-148 [Ref 30], -126 [Ref 30] and -125 [Ref 28] for ATO). (R)

8.4.9.2 The OSI layers 3 to 6 are implicitly defined by the chosen communication technology. (I)

8.4.9.3 The system integrator shall choose one of the communication technologies, to which he wants to comply. (R)

8.4.10 Other topics

8.4.10.1 This specification defines the usage functionality of the End Device Interface. Any management functionality is not part of the Ethernet Consist Network definition. (I)

8.4.10.2 Network configuration and management

8.4.10.2.1 Configuration procedures and interfaces for the on-board core network are beyond this specification and are a matter of project configuration. (I)

8.4.10.3 Authentication data provider

8.4.10.3.1 In addition to switches supporting IEEE 802.1X, an authentication data provider is required, e.g., by a RADIUS or DIAMETER service. As this involves considerations beyond the End Device's Interface on OSI layers above 1 and 2, this is out of scope of this specification. (I)

8.4.10.3.2 The configuration of the authentication data provider is out of scope of this specification. (I)

8.4.10.3.3 The specific configuration of MAC-based port security is out of scope of this specification. (I)

9. TRAIN TIME AND LOCATION SERVICE

9.1 General

9.1.1.1 The Train Time and Location Service (TTLS) shall provide a common reference time for all applications on the vehicle. It is defined as a service. The device, on which the service is running on, is out of scope of this Subset, and is project specific. (R)

9.1.1.2 It is assumed that the system integrator/vehicle manufacturer ensures that the time service for the on-board CCS subsystem and the ORD according to Subset-147 will be made available in each consist. (I)

9.2 Architecture

9.2.1.1 Using a high precision and battery buffered local clock, together with external time sources, the TTLS (marked blue in Figure 9-1) will provide a UTC time for distribution to all applications on the train that needs it. (I)

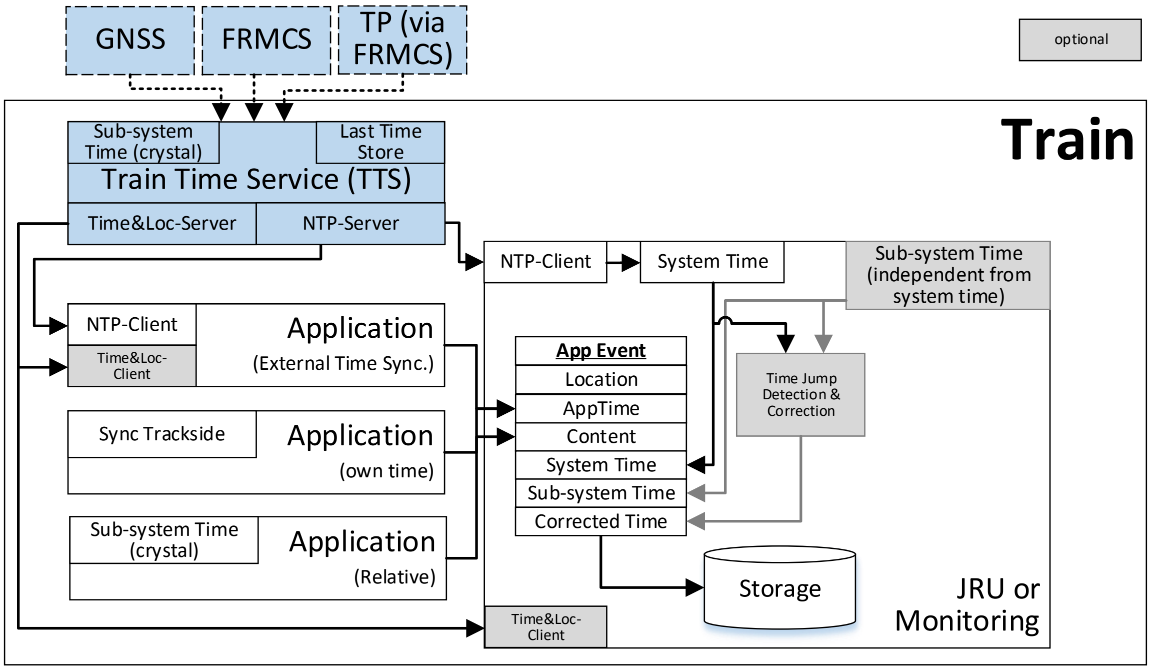

Figure 9-1: Embedding the time service into the system

9.2.1.2 The provided service as described in this chapter shall be used by all applications connected to the network which require a common reference time, for example by

- ATO for time-table related functions (calculation of energy efficient speed profile, dwell time calculation etc.),

- ETCS (e.g. time display on the screen or packet STM-177),
- Cab Radio,
- PKI communication,
- ORD or
- any monitoring or diagnosis system (on a voluntary basis) (R)

9.2.1.3 For a continuous time in the monitoring data, a detection and compensation (to make it monotonous and continuous) of time jumps can be foreseen in the time stamps to be stored (marked grey in Figure 9-1and see Figure 9-2). (I)

9.2.1.4 Monitoring starts with synchronization of the system time to the TTLS or, if the optional time correction specified in §9.2.1.3 is realised, after system start-up. (R)

9.2.1.5 Time jumps can be caused by leap seconds or transient effects for NTP synchronisation. (I)

9.2.1.6 "Compensation" means a apportioning of the time in steps of maximum 0.5 ms per second. (R)

9.2.1.7 "Applications (Own time)" means Applications with an internal time synchronisation between track and train (e.g. energy counter). (I)

9.2.1.8 "Applications (Relative)" means Applications that have no absolute time relationship. (I)

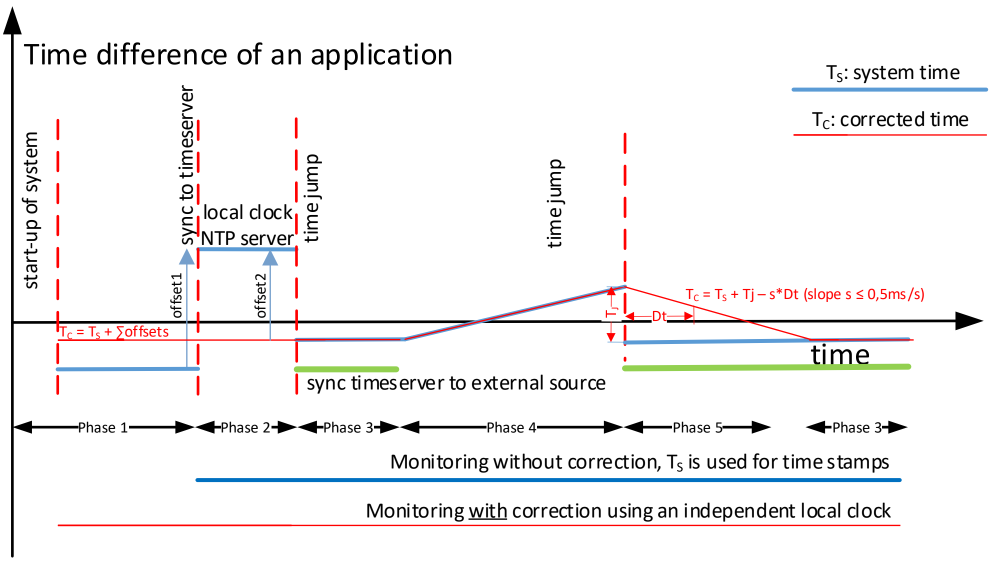

Figure 9-2: Compensation of time jumps

9.2.1.9 Note for explanation of Figure 9-2:

Phase 1: a sub-system starts with an own time

Phase 2: time is distributed via NTP but server is not synchronised to an external clock; no correction of time

Phase 3: NTP server is synchronised with external clock, no correction necessary

Phase 4: no external synchronisation which causes a drift

Phase 5: re-synchronisation to the external clock; drift is detected and apportioned over the time (I)

9.2.2 Correction of Timestamps in Monitoring Data

9.2.2.1 To have the possibility for correction the Monitoring can use a sub-system time which shall be independent from the system time. (R)

9.2.2.2 The sub-system time is specific for the respective application. The sub-system time is based on an independent local clock. System time is the time of the Operating System which is synchronised via NTP. (I)

9.2.2.3 As long as the Train Time and Location Service has no synchronisation to an external source, the monitoring system should store the sub-system time into the records in case the sub-system time is implemented, otherwise the records are stored without timestamp. (I)

9.2.2.4 After first synchronisation of the Train Time and Location Service to an external source (NTP Leap Indicator = “3” – clock not synchronised):

- The system time (synchronised via NTP) shall be used for time marking. (R)
- The offset between sub-system time and system time shall be calculated and used for correction of timestamps of all events which are to be stored. (R)
- For ORD the corrected time should be stored additionally to the system time. (I)
- Information that are used for time correction can be stored as meta data in the stream. (R)

9.2.2.5 Correction of the time stamps can be done in the background or at readout of the stream. (R)

9.2.2.6 Leap Indicator is a two-bit code warning of an impending leap second to be inserted in the NTP timescale, see RFC 5905 [Ref 17]. (I)

9.2.2.7 Additional time jumps occurring in the following time are detected by the NTP Leap Indicator and/or by comparing the sub-system time and the system time (controlled by

NTP). For correction of the time stamps, the time jump is apportioned, see Figure 9-2. (R)

9.2.2.8 Also, UTC leap seconds causes time jumps and shall be handled. They will be indicated by the Leap Indicator (value “1” or “2”). (R)

9.3 Requirements

9.3.1 General Requirements

9.3.1.1 There shall be only one centralised time service on a train used for all applications. (R)

9.3.1.2 Optionally several NTP Stratum 1 server can be used for error detection. (I)

9.3.1.3 For compatibility reasons bridges to other distribution or bus/networks should be possible. (I)

9.3.1.4 Unique and ascending start time: If external synchronisation fails then the sequence of recordings shall be preserved. A non-ascending start time indicates a problem with the real-time clock (e.g. batterie failure). (R)

9.3.1.5 For monitoring data (offline/stored data) a compensation of the time jumps should be done in order to achieve continuous time stamps. (I)

9.3.1.6 Time distribution shall be started earlier than 50s after power on. (R)

9.3.1.7 This is the time to start-up the NTP service and deliver the first time to set an application time. It should be lower with some margin than the 60s for JRU according to [IEC 62625-1]. (I)

9.3.2 Requirements on Time Sources

9.3.2.1 The NTP server shall work as Stratum 1 and time sources as Stratum 0. (R)

9.3.2.2 Which time sources are used is a developer’s choice. Possible sources are:

- Primary time source (a reference clock that defines and provides UTC time):
  - buffered local real-time clock (note: to be used as long as there is no time with higher precision available)
  - GNSS
- Secondary time source:
  - FRMCS (via auxiliary gateway function; for version 2 of FRMCS)
  - Time Protocol via FRMCS (RFC 868, [Ref 23]) (I)

9.3.3 Interface to Application

9.3.3.1 There shall be two interfaces to the application:

- Clock Synchronisation to UTC
- Time Stamp & Location (R)

9.3.3.2 Clock Synchronisation to UTC

9.3.3.2.1 The distribution of the UTC time shall take place via NTP protocol RFC 5905 [Ref 17]. (R)

9.3.3.2.2 The address of the time service shall be distributed by DHCP service according to RFC 2132 [Ref 18]. (R)

9.3.3.2.3 The distributed information shall contain:

- Leap indication; Leap Indicator = “11” if no trustable time is available (last time stamp > sub-system time)
- Precision as defined in RFC 5905 [Ref 21]
- Clock Reference Identifier
  - “XLOC”: no external synchronization (local clock only)
  - “XEXT”: external synchronization (e.g. GNSS) (R)

9.3.3.3 Time Stamp & Location

9.3.3.3.1 Distribution according to this subset, in intervals (≥1s) shall be defined by the client. (R)

9.3.3.3.2 The location shall be provided as GNSS coordinates and the time, the location is valid for. (R)

9.3.3.3.3 The delay between measuring on the GNSS device and receiving it at time service on the first NTP server shall be compensated. (R)

9.3.3.3.4 The distributed information shall contain: (R)

- UTC (time stamp) (format: resolution in ms)
- Precision as defined in RFC 5905 [Ref 17].
- DST Time Zone (optional information)
- Longitude (decimal -180.00000..180.00000)
- Latitude (decimal -90.00000..90.00000)
- Speed (format: resolution in km/h)

9.3.3.4 IANA time zone database is an example for implementation of DST Time Zone. (I)

9.3.3.5 The guarantied accuracy of the distributed time in relation to UTC shall be ±1s in the synchronised state which is the state in which the time is synchronised with an external time source. (R)

9.3.3.6 The distribution of time information shall be performed in realtime (following the UTC, time jumps are accepted and shall be handled by application). (R)

9.3.3.7 Time distribution in realtime means that the distributed time follows the current precision of the time reference. Time jumps (e.g. leap-seconds or re-synchronisation from GNSS) have to be handled by the application. (I)

9.3.4 Hardware Requirements

9.3.4.1 Reliability equivalent to ODR requirements according IEC 62625-1 [Ref 19], chap. 4.3.1.4; MTBF > 50.000 h. (R)

9.3.5 Security of the Train Time and Location Service

9.3.5.1 There are no applicable IT security requirements on the train time service. (I)

9.3.5.2 In future releases this statement has to be proven, especially in relation to the introduction of FRMCS. (I)

10. ITEMS FOR FURTHER STUDIES

10.1.1.1 Train Time and Location Service: Failure reactions could be added in case the service fails and is not available as e.g. indication to the driver or degraded modes. (I)

10.1.1.2 Strategy on conformance tests. (I)

10.1.1.3 Security contribution of S-147 has to be considered when new enhancements in relation to cyber security are proposed. (I)

10.1.1.4 The decision on trustworthiness of PCP tagging in the responsibility of the On-board Core Network. (I)

10.1.1.5 Higher layer protocol suits, their relation between communication models and protocols, information models and their technical representation. (I)

10.1.1.6 To define user data (message, packets, …) for distributed information (see §9.3.3.3.4) on application layer level.