Rail to Digital automated up to autonomous train operation

D23.4 – Proposal on TSI202x, SS147

Due date of deliverable: 31/07/2024

Actual submission date: 07/07/2025

Leader/Responsible of this Deliverable: Roelle, H.; SMO

Reviewed: Y

Document status		
Revision	Date	Description
01	19/08/2024	Creation of document with SS-147 v1.0.0 content
02	31/10/2024	Version for WP internal review
03	08/11/2024	Version for TMT review. Aligned with all WP23 members on 07/11/24
04	12/12/2024	Improved version after TMT review.
05	01/02/2025	Added SFTP for bulk data after discussion with TCMS experts group
06	07/07/2025	Incorporation of Joint Undertaking and System Pillar review comments

Project funded from the European Union's Horizon Europe research and innovation programme		
Dissemination Level		
PU	Public	X
SEN	Sensitiv – limited under the conditions of the Grant Agreement	

Start date: 01/12/2022 Duration: 20 months

ACKNOWLEDGEMENTS

This project has received funding from the Europe's Rail Joint Undertaking (ERJU) under the Grant Agreement no. 101102001. The JU receives support from the European Union's Horizon Europe research and innovation programme and the Europe's Rail JU members other than the Union.

REPORT CONTRIBUTORS

Name	Company	Details of Contribution
Abbati, L.	FSI	Second opinion, review
Ahmed, Z.	DB	Elaboration, second opinion, review
Schuerch, S.	SBB	Elaboration, second opinion, review
Rahn, K.	SMO	Second opinion, review
Roelle, H.	SMO	Elaboration, second opinion, review
Roullier, S.	SNCF	Second opinion, review
Rozijn, P.	NS	Second opinion, review

EXECUTIVE SUMMARY

A modular and upgradeable next-generation automatic train control (ATC) system demands seamless communication among on-train domains, a goal that the new on-board communication network (also known as One Common Bus) will facilitate. This new on-board communication network, initiated in the ERA TWG Modular Architecture, will offer further separated logical domains for TCMS and the operator to use the same physical network. This work has led to the incorporation of SUBSET-147 [1] into the current TSI 2023 release.

The deliverable D23.4, titled "Proposal on TSI202x, SS147," serves as the primary document in a series of deliverables that delineate the foundational elements necessary to formulate a proposal for the subsequent TSI 202x release (following the dissemination of the aforementioned deliverable). This proposal is intended to establish the framework for a shared on-board communication network, as outlined in SUBSET-147 [1], in the forthcoming iterations of TSI 202x.

In the task T23.4 related to this deliverable D23.4 various candidates of existing communication technologies on the OSI Layers 3 to 6 and partly on the safety layer were investigated. The pre-selected solution candidates of the deliverable “D23.3 – List of Solution candiates” [2] were jointly assessed on the requirements defined in the deliverable “D23.2 – List of system requirements for the Onboard Communication Network” [3].

First DDS/RTPS was ruled out for further proceedings, leaving the Internet Approach represented by TRDP and the Integrated Approach represented by OPC UA for further examination.

On the coverage of the technical requirements, neither OPC UA nor TRDP deliver full coverage, but OPC UA has a visible advantage over TRDP on the technical side. On the other hand, there is a clear market wise advantage for TRDP. But the discovered shortcomings from the technical requirements analysis are still needed to be closed before the Internet Approach (containing TRDP) could be chosen as the future EU Rail standard. Overall, neither TRDP nor OPC UA was a clear “winner”. Therefore, WP23 continued as follows:

- According to WP23’s results, the Internet Approach with TRDP was the more preferred solution.
- To finally judge on the feasibility, the technical weaknesses of the Internet Approach were assesed and concrete improvements and additions were selected in the following work areas:
  - Stream data, including audio and video
  - Request/Reply and bulk data communication
  - Security

As most gaps could be closed by selecting appropriate technologies, this document is based on the Internet Approach and presents results in form of a starting proposal for the next TSI SUBSET-147.

This final conclusion of the assessment was jointly elaborated and carefully aligned among all members of the workpackage.

ABBREVIATIONS AND ACRONYMS

AMQP	Advanced Message Queuing Protocol
ATC	Automatic Train Control
ATO	Automatic Train Operation
CCS	Control, Command and Signalling
CIP	Common Industrial Protocol
COTS	Commercial off-the-shelf
DDS	Data Distribution Service
ECN	Ethernet Consist Network
ERA	European Railway Agency
ERJU	Europe's Rail Joint Undertaking
ERTMS	European Rail Traffic Management System
ETB	Ethernet Train Backbone
ETCS	European Train Control System
FRMCS	Future Rail Mobile Communication System
HW	Hardware
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
MAC	Media Access Control
MQTT	Message Queuing Telemetry Transport
MVP	Minimum Viable Product
OCORA	Open CCS On-board Reference Architecture
ODVA	Open DeviceNet Vendors Association
OMS	Online Monitoring System
OPC UA	Open Platform Communications Unified Architecture
ORD	On-board Recording Device
OSI	Open Systems Interconnection
PROFINET	Process Field Network
PoC	Proof of Concept
QoS	Quality of Service

R2DATO	Rail to Digital automated up to autonomous train operation
RFC	Request for Comments
ROS	Robot Operating System
RPC	Remote Procedure Call
RTPS	Real-Time Publish Subscribe
SDT	Safe Data Transmission
SIL	Safety Integrity Level
SOME/IP	Scalable Service-Oriented Middleware over IP
SW	Software
TCMS	Train Control and Management System
TCN	Train Communication Network
TCP	Transmission Control Protocol
TRDP	Train Real-Time Protocol
TRL	Technical Readiness Level
TSI	Technical Specification of Interoperability
TWG	Topical Working Group
UDP	User Datagram Protocol
WP	Work Package

TABLE OF CONTENTS

1 PREFACE

The present document constitutes the Deliverable D23.4 “Proposal on TSI202x, SS147” in the framework of ERJU’s Innovation Pillar Flagship Project R2DATO WP23 T23.4.

A modular and upgradeable next-generation automatic train control (ATC) asks for a seamless communication among on-train domains. The new on-board communication network (also known as One Common Bus), as started in the ERA TWG Modular Architecture, will be a big step forward in that direction. Starting from the CCS and FRMCS systems, it will offer further separated logical domains for TCMS and the operator to use the same (physical) network.

The work of the ERA TWG Modular Architecture resulted in the SUBSET-147 v1.0.0 [1] being part of the current TSI 2023 release. It specifies the future harmonised communication backbone for the on-board CCS subsystems (like ETCS on-board, ATO on-board, FRMCS, etc.). The first stage of the specification of the communication backbone contains the definition of OSI-layers 1 and 2 in the SUBSET-147 v1.0.0 [1]. A common Ethernet CCS consist network has to be established in newly developed vehicles. For the higher OSI-layers 3 to 6 the three possible communication technology protocols TRDP, OPC-UA and PROFINET (incl. the implicitly defined network and transport layers) are currently specified.

In the first phase of EU-RAIL, the focus is on foundations for the onboard communication network building upon and substantially extending the prior work from CONNECTA and OCORA beyond TCMS and CCS and also toward higher protocol layers. Overall the project strives for a TRL of 4/5 (technology validated in a lab setup that represents practical train deployments). For higher TRLs the later phases of the projects will be used.

The aim of the work package WP23 is to specify a dedicated set of protocols on the OSI-layers 3 to 6 for the next TSI revision. With this specification the future onboard communication backbone is harmonized which paves the way for future modularization and upgradability of the CCS and other domains.

The deliverable is the main document of a series of deliverables containing the proposal for the next TSI 202x (after the release of that deliverable) for the future common onboard communication network.

To shape and guide the technical specification of WP23 and later WP24, WP23 takes a top-down approach first. This means:

- The WP’s work starts from the application and stakeholder perspective to first define scope and cornerstones of the future work (top level view). Main deliverable here is as a comprehensive set of user stories (see deliverable WP23-D23.1).
- Based on the user stories as guiding input, a set of system requirements for the communication functionality has been derived (see deliverable WP23-D23.2 [3]).
- In the task T23.3 various candidates of existing communication technologies on the OSI Layers 3 to 6 and corresponding safety layer were investigated and roughly checked against the core requirements. As a conclusion of the first investigation three solution candidates were defined. They all fulfill the core requirements and are most promising to fulfill the residual system requirements as well (see deliverable WP23-D23.3 [2]).

- The solution candidates were assessed in detail requirement by requirement. Based on this detailed assessment a harmonized solution proposal for communication backbone was elaborated in this deliverable “D23.4 – Proposal on TSI202x, SS147”.

WP23 proposes here, to make a partial amendment of WP24, to drive further the specification of SUBSET-147 using selected user stories from WP24. Later WP24 will improve the solution proposal on a lower level of detail. Taking the user stories from the first WP23 deliverable into account WP24 will concentrate on the technical management functionality and associated processes. By using the common user stories both WP23 and WP24 share the same scope, thus leading to matching specifications.

1.1 HINTS ON DOCUMENT STRUCTURE AND USAGE

This document consists of two main parts:

1. This preface and following a detailed explanation of the choice of the "Internet Approach". Ultimately, this segment is not intended to be incorporated into the TSI specification, as it serves merely as preparatory work for the TSI. A thorough elaboration on the selection of the "Internet Approach" is beyond the scope of the TSI specification.

   The TSI itself should prioritize the technical specification, without delving into the rationales behind specific technological decisions. The initial segment of this document constitutes the foundational work that culminates in the TSI specification.

2. An initial version of the next revision of the SUBSET-147.

The split into two parts was made to enable to start with the original content and structure of the current SUBSET-147. This allows for easier comparison of the new proposal with the current revision of SUBSET-147

2 PROCESS OF TECHNOLOGY SELECTION

2.1 STARTING POINT: DELIVERABLE WP23-D23.3

The first investigation (see deliverable WP23-D23.3 [4]) on different higher layer protocols resulted in the following solution candidates:

- TRDP according to IEC/EN 61375-2-3 [5]
- OPC UA PubSub according to IEC 62541 [6]
- DDS/RTPS according to DDSI-RTPS [7]

These three solution candidates were assessed in detail requirement by requirement, see appendix A.

As a result of the detailed assessment, it can be seen that none of the protocols fulfills every requirement. To select one of the solution candidates as the one standard solution a simple or even weighted counting of the fulfilled requirements would not be a fair approach. The investigated solution candidates with their capabilities are fundamentally different. They can be classified into the following two main cathegories:

- Internet Approach: TRDP
- Integrated Approach: OPC UA & DDS/RTPS

TRDP constitutes a special protocol especially designed for a special use case. This protocol suits into a bunch of existing protocols following the so called “Internet Approach” where every problem has its dedicated protocol. Good examples for this approach are the TCP, UDP or IP protocols defined e.g. in an RFC standard.

Whereas OPC UA and DDS/RTPS follow the “Integrated Approach”. In this approach a protocol includes a toolbox of different subprotocols for different purposes. All communication entities normally use a subprotocol of the toolbox. The different subprotocols are designed to match certain common requirements building the Integrated Approach. Every integrated solution like OPC UA or DDS/RTPS is built based on a common information model.

In the assessment of the three solution candidates on the detailed requirements a major disadvantage of DDS/RTPS was discovered. This concerns two of the core requirements already defined in previous deliverable “D23.3 – List of Solution Candidates” [4]. The core requirements were basically assessed in the previous step. Now a major disadvantage on safety and openness was discovered, as there is no dedicated safety layer for DDS available where the specification as well as the implementation are open. There are dedicated safety layers available for some not open implementations of DDS/RTPS. Also, these safety layers are neither open nor assumed to be interoperable between each other or between different implementations. Generally, it is possible to use another safety protocol on top of DDS/RTPS like e.g. SDTv2 defined in IEC 61375-2-3 [5]. But in such a case some of the main features of the Integrated Approach like the common information model would be lost. DDS/RTPS is not designed for exchanging already compiled binary data packets with an included safety trailer. So, using any open safety layer on top of DDS/RTPS is not an option.

Therefore, DDS/RTPS was excluded from the list of solution candidates because of the detailed requirements assessment. The two remaining solution candidates following two different approaches were:

- TRDP according to IEC/EN 61375-2-3 [5] following the Internet Approach
- OPC UA PubSub according to IEC 62541 [6] following the Integrated Approach

These two protocols were further investigated to make the final decision.

2.2 SECOND ASSESSMENT OF THE REMAINING CANDIDATES

While the previous chapter has shown the differences of TRDP and OPC UA with regards to the more technical criteria, there is more to investigate on a strategic level to conclude on which candidate to choose for further standardisation.

As the rolling stock domain is no longer an encapsulated regional market and to achieve attractive price points for supplied subsystems for rolling stock vehicles, one should also consider the situation in other regions outside the European market. Therefore, **market diffusion** of a certain communication technology and **technical requirements from other regional markets** shall be considered.

In addition, supplier industries for rolling stock historically have strong competencies in mechanics and electrics in their respective special field, but not those strong competencies in digitalization, machine-to-machine communication and software defined control. This fact must be considered. Hence, the **easy and cost efficient adaption** of a certain communication technology is a criterion as it influences effort and timelines in the supplier industry.

2.2.1 Market considerations

Judging on the market, one could differentiate between the rolling stock market and other markets, especially:

- Industry automation
- Automotive
- Avionics

Starting with the other markets, the following observations can be made:

- TRDP does not play a role in any other market than rolling stock, but is very strong there (see later)
- OPC UA is strong in industry automation, regardless of vendors. But looking at the automation pyramid, the role of OPC UA however does not go down to the shopfloor level at the time of writing, thus limiting the reuse potential for the rolling stock domain. The shopfloor level still is dominated by vendor specific technologies like ProfiNet, EtherCAT etc. Moreover, a complete data model would have to be developed for the railway onboard needs.
- Currently, OPC UA is considered for parts of future trackside railway domain (highly equivalent to data centers) as part of the EULYNX standards. The trackside railway domain is dominated by a few big market players. Therefore, neither the market participants nor the technological boundary condition of the onboard domain is comparable to railway trackside domain.

- Automotive and avionics both have their separate eco-systems, neither TRDP nor OPC UA play a predominant role there.

Examining the rolling stock specific markets, one should have a close look at different world regions:

- China:

  The Chinese rolling stock market has a clear preference for TRDP. Many tenders, independent from the segment, explicitly require TRDP. Consequently, subsystem vendors mostly support TRDP.

  OPC UA has no visible presence on the Chinese rolling stock market.

- India:

  While the number of tenders where Ethernet based designs are required is rising, the explicit requirement for TRDP depends on the market segment. In the mainline sector, most tenders are still solution agnostic, while in the metro business many tenders explicitly require TRDP, especially lead tenders like metro Mumbay.

  As a consequence there is a growing share of TRDP support in the supplier industry. OPC UA is not explicitly visible in India rolling stock market.

- USA:

  In cases where ethernet technology is required, this is often coupled with explicitly requiring TRDP (e.g. in light rail and metro segment).

  OPC UA has no visible presence on the US rolling stock market.

- Europe:

  While the European market is more solution agnostic compared to other markets, TRDP still has visible presence. By the acquisition of Bombardier, Alstom has become the owner of the inventor of and important driver behind TRDP and seems to be willing to apply TRDP in favour of other technologies.

  European funded project Shift2Rail/Connecta showed the general applicability of both TRDP and OPC UA for rolling stock application. From the perspective of European standardization, both TRDP and OPC UA are allowed as of TSI 2023 SS-147 [1].

- Worldwide by international standards:

  TRDP is the standard protocol for the Ethernet Train Backbone (ETB) as of IEC61375-2-3.

  IEC61375-3-4 for the Ethernet Consist Network (ECN), which is the category the Common Onboard Network of WP23 falls into, does not define a mandatory communication technology on higher layers like TRDP or OPC UA.

Summarizing the rolling stock market, as of today:

- TRDP has a significant momentum in the worldwide rolling stock industry already. However, this is only true for the communication protocol TRDP for process and message communication. Neither for information models, nor for communication needs apart from process and message communication, there is a common sense in the industry.

On the one hand, OPC UA plays no visible role in any of the rolling stock markets, but it‘s also not explicitly prohibited, at least where no other concrete technology is enforced.

- Markets beside rolling stock do not influence the decision between TRDP and OPC UA.

2.2.2 Effort and cost of technical adaption

With the remaining two technologies under consideration, each of them represents a different characteristic approach: TRDP represents the Internet Approach, OPC UA represents the Integrated Approach. The characteristics of these two approaches not only have a technological impact but also influence effort and cost of their implementation.

With the Internet Approach the overall functionality is built up by composition of individual parts and (sub-)technologies. E.g. for process data communication, TRDP is used, while for Request/Reply (RPC) communication e.g. HTTPS could be used. For a component supplier, this gives the opportunity to have a stepwise adoption to a standard made out of the Internet Approach. E.g. in a first minimum viable product (MVP), standard compliant process data communication could be released, while in a second MVP/release standard compliant Request/Reply (RPC) could be added. This means, that investments in adopting the standard also could be made step wise and spread over the time, while already releasing intermediate products. In addition, each step by itself would consist of smaller technology parts which could be easier achieved skill wise in a stand-alone and step by step manner. Due to the step-by-step manner, risk can be spread better and therefore controlled better.

In contrast, the Integrated Technology approach requires one big step up front. The strengths of the integrated parts can only be leveraged when the whole stack is implemented. The advantage is, that after the big upfront step, the complete functionality is available as a big bang. The downside here is, that skill wise every aspect of the Integrated Technology needs to be mastered at once. Consequently, the investment for implementing needs to be made completely before gaining market visibility. Risk wise, all risk is in the big upfront step and is hard to mitigate.

Considering a typical (sub-)system supplier for the railway industry, it is obvious that the Internet Approach’s step-by-step way of adopting new standards fits much better than the big bang approach of an Integrated Technology.

2.3 SELECTING THE INTERNET APPROACH FOR SUBSET-147

On the coverage of the technical requirements, neither OPC UA nor TRDP deliver full coverage, but OPC UA has a visible advantage over TRDP on the technical side. Therefore, for both candidates, individual additions need to be defined to deliver an acceptable coverage of the technical requirements.

Market wise, there is a clear advantage for TRDP, meaning TRDP as such but not for the Internet Approach as a whole. This in turn means that the discovered shortcomings from the technical requirements analysis still needs to be closed before the Internet Approach (containing TRDP) can be chosen as the future EU Rail standard (no matter what the current market status is). In contrast, OPC UA is not remarkably present in the rolling stock market by today and its advantage of availability in industry automation is weakened as devices on shopfloor level (which would be of interest for rolling stock) are not included.

The fit of TRDP to the structure and typical abilities of subsystem vendors is better than the one of OPC UA, giving TRDP an advantage here.

Overall, neither TRDP nor OPC UA is a clear “winner”. Therefore, WP23 continued as follows:

- In WP23’s opinion, the Internet Approach with TRDP was the more preferred solution.
- To finally judge on the feasibility, the technical weaknesses of the Internet Approach were assesed and concrete improvements and additions were selected in the following work areas:
    - Stream data, including audio and video
    - Request/Reply and bulk data communication
    - Security

As most gaps could be closed by selecting appropriate technologies, this document is based on the Internet Approach and presents results in form of a starting proposal for the next TSI SUBSET-147.

This final conclusion of the assessment was jointly elaborated and carefully aligned among all members of the workpackage.

3 STATUS OF THE PROPOSAL FOR SUBSET-147

The enclosed proposal cannot and doesn't want to deliver a complete, "ready to sign off" version of the next SUBSET-147. Instead, it is meant as a starting point for further detailing but with the inclusion of WP23's current results. Therefore, the proposal delivers:

- Proposal on new structure of SUBSET-147 (with minimizing the amount of rework in existing chapters)
- Definition of technologies to use for various communication patterns
- Proposal on chapters to remove from SUBSET-147
- Proposal on chapters to move to different subsets
- Identification of parts to be reworked
- Identification of new parts that need further elaboration
- Inside the proposal, comments on the required action are marked in magenta.

Especially, on the newly introduced technologies, the need for further clarifications has been identified:

- Open topics in process data communication include:
  - Maximum frame size / fragmented frames in TRDP
  - Definition of a security layer for TRDP
  - Aggregation of data for multiple receiver into one datagram
  - Weaknesses in specification of information model, e.g. bit-fields
  - Alignment with evolution of IEC 61375-2-3
- Open topics in Event based Communication include:
  - Information model.
  - Message format/encoding of AMQP message content.
  - Addressing: AMQP message hierarchy/structure, a.k.a. topic tree.
  - Service discovery: "How do I find the broker". By fixed DNS name, by bonjour/zeroconf, by ssd/upnp, by … ?
- Open topics in RPC communication include:
  - Upper layer, methodologies, or frameworks to specify and standardise the API interfaces, e.g. Web of Things (WoT).
  - Addressing: URL format/scheme.
  - Service discovery.

WP23 proposes here, to make a partial amendment of WP24, to drive further the specification of SUBSET-147 using selected user stories from WP24.

REFERENCES

[1] ERTMS/ETCS SUBSET-147: CCS Consist Network Communication Layers, Version 1.0.0

[2] CONNECTA, CTA-T3.5-D-BTD-002-12: Drive-by-Data Architecture Specification, 14/09/2018

[3] ERJU Innovation Pillar R2DATO D23.2: List of System Requirements, v1.1

[4] ERJU Innovation Pillar R2DATO D23.3: List of Solution Candidates, v1.0

[5] IEC 61375-2-3: Railway Applications – Electronic railway equipment – Train communication network (TCN) – Part 2-3: TCN communication profile, 2015

[6] IEC 62541-14: OPC Unified architecture – Part 14: PubSub, 2020

[7] The Real-time Publish-Subscribe Protocol DDS Interoperability Wire Protocol (DDSI-RTPS) Specification, Version 2.5, 2021

[8] ISO/IEC 19464: Information technology -- Advanced Message Queuing Protocol (AMQP) v1.0 specification, 2014

APPENDIX A: PROCESS DATA TECHNOLOGIES' REQUIREMENTS FULFILLMENT

The first investigation (see deliverable WP23-D23.3 [4]) on different higher layer protocols resulted in the following solution candidates:

- TRDP according to IEC/EN 61375-2-3 [5]
- OPC UA PubSub according to IEC 62541 [6]
- DDS/RTPS according to DDSI-RTPS [7]

These three solution candidates are subsequently assessed in detail requirement by requirement. The table shows a detailed analysis of how the intermediary solution candidates TRDP, OPC UA and DDS/RTPS satisfy each requirement.

The tables structure is organized in an easy and streightforward manner. Each requirement is attributed with a unique requirement id and a category. To present a consice requirement text, the requirement part common to each requirement is located in the third table column heading. When reading a requirement, the common requirement part must preceed the individual requirement part, e.g. "The Communication Infrastructure Technology Stack shall... ...enable consist-local communication.". Where appropriate, the requirement text is followed by a rationale or comment for each requirement. The last three table columns depict the actual assessment of how the solutions candidates satisfy each requirement.

For a comfortable and easy-to-use comparison between the solution candidates, a visual aid is introduced in the form of color-coded table cells:

- ***Green:*** *requirement is fully satisfied by the solution candidate.*
- ***Orange:*** *requirement is partially satisfied by the solution candidate. This usually implies limitations within the implementation of the solution candidate. Additional improvements or technological rework is needed for full compliance. Please refer to the comment associated with the assessment for further detail.*
- ***Red:*** *requirement is not satisfied by the solution candidate. Please refer to the comment associated with the assessment for further detail.*
- ***Grey:*** *requirement is already fully covered by lower protocol layers, is out of scope or not assessable for the solution candidate.*

Each table cell may optionally introduce a comment regarding the fulfilment of a requirement by the respective solution candidate. These comments, especially longer ones, are used sparingly to keep a short and concise comparison table but still provide just the right amount of additional detail to give background information on how the assessment has been reached.

ID	Category	Requirement: "The Communication Infrastructure Technology Stack shall…"	Rationale / Comment	TRDP	OPC UA	DDS/RTPS
ComStackReq-Func-01	Scope	… enable consist-local communication.	Driven by EN 61375-3. Could be later extended to also cover inter-consist communication.			
ComStackReq-Func-02	Scope	... define a communication model.	Main purpose for communication technology. Defining - communicating partners - communication mechanisms - syntax and semantics of protocol data structures and exchange formats on their respective OSI layers. Requirement is related to OSI layers 1 to 6. Implicit model already covered in SUBSET-147. Must be made explicit/eventually expanded.	- communication partners and mechanisms are well-defined - exchange format and encoding for data structures exists, but mapping is vague		
ComStackReq-Func-03	Scope	… NOT take passenger entertainment/passenger internet access in scope.	Motivated by security, bandwidth and operational considerations; not to be confused with passenger information systems.	Not assessable		
ComStackReq-Func-04	Communication Patterns	... support 1-to-1 communication patterns.				
ComStackReq-Func-05	Communication Patterns	... support 1-to-many communication patterns.	Especially for process data communication this pattern is useful. Preferably realized on lower layers to avoid high load towards application layer. Makes higher layer protocols simpler if already available on lower layers, saves performance and is also more efficient in hardware use.		with OPC UA PubSub	PubSub
ComStackReq-Func-06	Power Supply Functions	… support the possibility to transmit power over the communication bus to the devices.	Reduce cabling. Using the bus supplied power must not be mandatory but optionally possible. Main driver to make it optional is to avoid unnecessary cost from having all switch ports to supply power.		based on Ethernet, Power over Ethernet (PoE) possible	
ComStackReq-Func-07	Communication Functions	... enable train-local real-time data exchange for process data.	Overall interpretation of real-time: Motion-control quality is NOT intended. (See also non-functional requirements)			
ComStackReq-Func-08	Communication Functions	... enable train-local non-real-time data exchange.				

ID	Category	Requirement: "The Communication Infrastructure Technology Stack shall…"	Rationale / Comment	TRDP	OPC UA	DDS/RTPS
ComStackReq-Func-09	Communication Functions	… not prevent realization of future remote real-time data exchange for process data.	Very likely needed for higher GoA levels (e.g., for remote train operation).	Not assessable		
ComStackReq-Func-10	Communication Functions	... enable remote non-real-time data exchange.	Needed for today's non-CCS-specific train/wayside connectivity (e.g., remote software updates, remote diagnostics, FRMCS services, etc.)	diagnostics possible via Message Data (MD), no bulk data support	build-in support for diagnostic events and data access, message chunking enables to split up big data payloads	Example are already available i.e. for OTA updates, Fragmentation of big data payloads available on DDS level
ComStackReq-Func-11	Communication Functions	... enable train-local process data communication.	Perspective of a generic use-case. Typically, with a cyclic communication pattern.			
ComStackReq-Func-12	Communication Functions	… enable train-local message data communication.	Perspective of a generic use-case. Typically, with a spontaneous/event driven/acyclic communication pattern.			
ComStackReq-Func-13	Communication Functions	... enable train-local stream data communication.	E.g., audio and camera streams (not only for CCTV, also for higher GoA levels). Perspective of a generic use-case.	out of scope of these protocols		
ComStackReq-Func-14	Communication Functions	... enable train-local bulk data communication.	E.g., file transfer. Perspective of a generic use-case.	MD payload size is restricted due to missing fragmentation/chunk support	message chunking enables to split up big data payloads	Fragmentation of big data payloads available on DDS level
ComStackReq-Func-15	Communication Functions	... enable train-local RPC communication.	Especially for network- and application-management functions. Especially to relief applications from relating request to replies.	only preconfigured request/reply communication possible with Message Data		DDS-RPC
ComStackReq-Func-16	Communication Functions	… allow/not prevent the realization of remote process data communication.	This is a "heads-up" requirement to remind of implications on remote communication, esp. for OSI layers >2	No prevention of functionality, strongly architecture-dependent, depends on security requirements and realization (e.g., gateway), for general support see requirements above		
ComStackReq-Func-17	Communication Functions	… allow/not prevent the realization of remote message data communication.	This is a "heads-up" requirement to remind of implications on remote communication, esp. for OSI layers >2			

ID	Category	Requirement: "The Communication Infrastructure Technology Stack shall…"	Rationale / Comment	TRDP	OPC UA	DDS/RTPS
ComStackReq-Func-18	Communication Functions	… allow/not prevent the realization of remote stream data communication.	This is a "heads-up" requirement to remind of implications on remote communication, esp. for OSI layers >2			
ComStackReq-Func-19	Communication Functions	… allow/not prevent the realization of remote bulk data communication.	This is a "heads-up" requirement to remind of implications on remote communication, esp. for OSI layers >2			
ComStackReq-Func-20	Communication Functions	… allow/not prevent the realization of remote execution communication.	This is a "heads-up" requirement to remind of implications on remote communication, esp. for OSI layers >2			
ComStackReq-Func-21	Consolidation	... enable the consolidation of today's physical on-board communication networks into logical communication networks on a shared physical infrastructure.	Purpose of the "OneCommonBus" approach, reduce the number and variety of physical networks on a train.			
ComStackReq-Func-22	Consolidation	... enable the consolidation of distinct zones of differing criticality on a shared physical infrastructure.	Purpose of the "OneCommonBus" approach, reduce the number and variety of physical networks on a train.	Already fully covered by lower layers definition in SUBSET-147 v1.0.0		
ComStackReq-Func-23	Consolidation	… provide appropriate separation mechanisms for consolidated (=former physically separated) on-train communication networks/zones.	Basic prerequisite for any consolidation is to realize an equivalent level of separation			
ComStackReq-Func-24	Consolidation	… provide means to manage and configure QoS classes. Each class defines a set of typical QoS parameters such as bandwidth, delay and jitter.		Not assessable		
ComStackReq-Func-25	Consolidation	… provide prioritization/QoS mechanisms based on the QoS class that is assigned to a given application or service.		TRDP allows to set the PCP value of layer 2 directly.	OPC UA allows to set the DSCP value of layer 3.	QoS mechanisms in DDS/RTPS available. But mapping down to DSCP value on layer 3 or even PCP value on layer 2 unknown.
ComStackReq-Func-26	Consolidation	… be able to consolidate FRMCS and CCS zones on the same on-train	Zones serve here as an example, also number not limited	Already fully covered by lower layers definition in SUBSET-147 v1.0.0		

ID	Category	Requirement: "The Communication Infrastructure Technology Stack shall…"	Rationale / Comment	TRDP	OPC UA	DDS/RTPS
		communication network on a shared physical infrastructure.				
ComStackReq-Func-27	Consolidation	… be able to consolidate TCMS zone and OMTS zone on same on-train communication network on a shared physical infrastructure.	Zones serve here as an example, also number not limited. OMTS = Onboard Multimedia and Telematic Subsystem (new term from IEC 62580)			
ComStackReq-Func-28	Consolidation	… enable building vehicles with a single on-train communication network consist over multiple cars.	Explicitly leave the vehicle architecture open for vendors to enable cost efficient designs. Be able to build up multiple car consists.			
ComStackReq-Func-29	Interoperability	… allow/not prevent the interoperability of end devices of different vendors.	This shall be achieved by unambiguous specifications and possibly by establishing conformance tests. This includes the interoperability between end device and network device because w/o that interoperability the end-to-end communication wouldn't be possible.	compliance testing from one company available, XML configuration (IEC 61375-2-3, Annex C) with basic data types is informatively specified, partially incomplete (bitsets), application profiles helpful (in accordance to IEC 61375-2-4)	compliance testing and definition of companion specifications are central to OPC UA, application profiles helpful (in accordance to IEC 61375-2-4)	In general, it doesn't prevent interoperability however conformance testing of DDS is currently unknown. There are gateways available as well.
ComStackReq-Func-30	Interoperability	… allow/not prevent the interoperability of end devices of different product generations.	This shall be achieved by downward compatible evolution of standards and suitable version management. This includes the interoperability between end device and network device because w/o that interoperability the end-to-end communication wouldn't be possible. The usage of legacy end devices might require gateway functionality.	Enough stability on L3-6, for application layer, mechanisms for up/down compatibility need additional specification. Overall concept missing anyway.	Enough stability on L3-6, for application layer, in general some base mechanisms available by _dynamic_ information model and conformance testing. Overall concept missing anyway.	Change in specification or relinking is required in DDS which requires recompilation

ID	Category	Requirement: "The Communication Infrastructure Technology Stack shall…"	Rationale / Comment	TRDP	OPC UA	DDS/RTPS
ComStackReq-Func-31	Interoperability	… allow/not prevent the interoperability of network devices of different vendors.	This shall be achieved by unambiguous specifications of network device capabilities and possibly by establishing conformance tests.	Not in scope, profiles must be provided		
ComStackReq-Func-32	Interoperability	… allow/not prevent the interoperability of network devices of different product generations.	This shall be achieved by downward compatible evolution of standards and suitable version management and possibly by establishing conformance tests.			
ComStackReq-NonFunc-01	Interoperability	… come with compliance testing and certification processes in a lightweight way.	Foster interchangeability and second source approach. Lightweight means, that that testing procedures shall be available from external sources (paid or unpaid) and applying them shall cause no significant extra effort in development, e.g. by implementing extra test cases during development.	compliance testing from one company available	compliance testing and certification available	not known
ComStackReq-NonFunc-02	Maintainability	…ease failure detection for maintenance activities.	Improve defect handling and maintenance. Stems from maintenance scenarios where identifying a fault situation should be as easy as possible. Applies to end-devices and border-network-devices.	Requirements not in scope of higher-layer protocols		
ComStackReq-NonFunc-03	Maintainability	… support an exchange of devices with low configuration effort. Low configuration effort means that no other end-device shall be affected, and configuration activities shall be made centrally.	Improve defect handling and maintenance. Stems from maintenance scenarios where exchanging a faulty asset should be as easy as possible (e.g., no dependency on device MAC addresses). Applies to end-devices and border-network-devices.			
ComStackReq-NonFunc-04	Compatibility	… provide mechanisms to enable / support compatibility management for any given set of functionalities.	Allow for future extension of protocol stacks or even hardware upgrades. Example: protocol version negotiation during the TLS handshake or 10/100/1000 MBit/s capabilities of Ethernet ports. Preserve compatibility while enabling innovation			
ComStackReq-NonFunc-05	Portability	… be platform independent (HW from SW). There shall be no dependency to a specific CPU model or platform or specific ethernet hardware.	Decoupling and flexibility in hard- and software.			
ComStackReq-NonFunc-06	Portability	… support different physical topologies such as star, ring, ladder and hybrids of these	Enable adequate topologies for different vehicle architectures	Already fully covered by lower layers definition in SUBSET-147 v1.0.0		

ID	Category	Requirement: "The Communication Infrastructure Technology Stack shall…"	Rationale / Comment	TRDP	OPC UA	DDS/RTPS
ComStackReq-NonFunc-07	Portability	… support at least links over copper cables.	Serves as the common base for interoperability.			
ComStackReq-NonFunc-08	Portability	… support links over fibre.	Openness for future technologies.			
ComStackReq-NonFunc-09	Portability	… use standardized physical connectors for devices.	Refers to a typical real-world problem. Solution shall refer to a standard like IEC etc.			
ComStackReq-NonFunc-10	Adaptability	… not imply the use of a specific programming language/environment.	Leave the flexibility to realize cost effective solutions and enable innovation.			Available for multiple enviornments and in multiple languages.
ComStackReq-NonFunc-11	Adaptability	… not enforce a specific operating system.	Leave the flexibility to realize cost effective solutions and enable innovation.			
ComStackReq-NonFunc-12	Adaptability	… not imply specific types of hardware technology on components (e.g., CPU family).	Leave the flexibility to realize cost effective solutions and enable innovation.			
ComStackReq-NonFunc-13	Adaptability	… be deployable and usable on a variety of (component) device classes, from low-end microcontrollers to high-end computing devices.	Leave the flexibility to realize cost effective solutions and enable innovation, especially for simple end devices like sensors.ee	low resource footprint	provides profiles for different device classes in OPC UA Part 7, chapter 6 => should be proven in the lab-demonstrator	Examples available for STM32
ComStackReq-NonFunc-14	Safety	… support different levels of safety concurrently without forcing all entities to follow the highest safety level.	Enable cost effective solutions. Avoid unnecessary complexity for applications that only need lower safety levels.	optional safety layer SDTv2 is specified and implemented	optional safety layer for up to SIL 4 is specified, implementation ongoing	
ComStackReq-NonFunc-15	Safety	... support the implementation of safety layers for functions with safety requirements up to SIL 4.	Typically, such implementations involve the safety requirements of EN 50159:2010 for railway safety applications.	SDTv2 for functions up to SIL 2 standardized, implemented and approved. SDTv4 for functions up to SIL 4 defined and implemented.	safety layer for up to SIL 4 is specified, implementation ongoing.	Implementations available for ISO 26262 but not yet Rail Safe. The specifications and implementations of safety layers are not open.

ID	Category	Requirement: "The Communication Infrastructure Technology Stack shall…"	Rationale / Comment	TRDP	OPC UA	DDS/RTPS
				SDTv4 is currently in standardization.		
ComStackReq-NonFunc-16	Security	... support authentication of communication entities.	Only allow authorized devices. Base for authorization. Parts already addressed in TSI2023 SS147.	security is not in scope of TRDP, additional mechanisms required	built-in for Client/Server and PubSub	Authentication Service Plugin
ComStackReq-NonFunc-17	Security	... support the auditing of communication activities.	Allow to build trace infrastructure on usage of illegal/offending devices		built-in for Client/Server	Logging Service Plugin
ComStackReq-NonFunc-18	Security	... provide optional encryption functionality towards the application layer to allow for data confidentiality. The necessary encryption functionality shall be available for all communication patterns and functions.			built-in for Client/Server and PubSub	Cryptographic Service Plugin
ComStackReq-NonFunc-19	Security	... provide optional disclosure of intentional data integrity violations towards the application layer. The necessary integrity checking functionality shall be available for all communication patterns and functions.	Prevent attacks based on data manipulation, man-in-the-middle attacks, replay etc. This requirement is independent from any checks to disclose unintentional changes e.g. by bit errors.		built-in for Client/Server and PubSub	Data Tagging Service Plugin
ComStackReq-NonFunc-20	Security	... support integrated authorization of communication activities.	Even if authorization decisions as such are made on higher layers, the enforcement of those decisions (esp. negative ones) shall be supported on the lower layers. Parts of this concept are already addressed in TSI2023 SS147. More details on this requirement are expected from ERJU System Pillar.		built-in for Client/Server	AccessControl Service Plugin
ComStackReq-NonFunc-21	Security	… ease and support the management (distribution, renewal, revocation …) of authentication credentials (e.g., certificates)			supported via Global Discover Server (GDS)	
ComStackReq-NonFunc-22	Security	… be resilient to (D)DoS attacks.	Base for consolidation		mitigations listed in OPC UA Part 2, 5.1.2	has no broker

ID	Category	Requirement: "The Communication Infrastructure Technology Stack shall…"	Rationale / Comment	TRDP	OPC UA	DDS/RTPS
ComStackReq-NonFunc-23	Security	… support different levels of security concurrently without forcing all entities to follow the highest security level.	Enable cost effective solutions. Avoid unnecessary complexity for application that only need lower security levels.		security is optional and configurable	
ComStackReq-NonFunc-24	Openness	… be based on publicly available and open standards, developed by a transparent and standardized process.	Should be aligned with European Standardization Policies. Base for interoperability	specification and development by TCN Open Interests Group, standardized in IEC 61375	specification and development by OPC Foundation, standardized in IEC 62541, currently not in rail-specific standards	made availble by Object Management Group (OMG) but not standardized yet in Rail
ComStackReq-NonFunc-25	Cost	… avoid any unnecessary cost (e.g., royalties for standards).	Enable cost efficient solutions	(Note: Product certification may be a paid service.)	(Note: Product certification may be a paid service.)	(Note: Product certification may be a paid service.) Have to pay for vendor specific safety standard/implementation
ComStackReq-NonFunc-26	Adaptability	… able to provide different stages of features to enable cost effective, "fit-to-the problem" solutions.	Enable cost efficient solutions and/or application-specific feature profiles.	low footprint, however additional mechanisms are required to address all requirements (e.g., security)	provides profiles with different functionality sets	by core and extensions
ComStackReq-NonFunc-27	Availability	… provide redundancy mechanisms to bypass failures of components of the on-train communication network component/link.	Realizing availability solely by component MTBFs would be very costly. Therefore, redundancy mechanisms shall be available. Partially handled by TSI2023 SS147.	Not in scope, partly covered by lower layers definition in SUBSET-147 v1.0.0		
ComStackReq-NonFunc-28	Availability	… define a typical upper limit for acceptable communication outage time (e.g., by redundancy switchover).	Needed by the application layer to provide mechanisms to cope with the downtime.			
ComStackReq-NonFunc-29	Latency	… provide latency low enough to enable clock synchronization with an accuracy of 1ms between end devices (local consist scope!).	Typical use case in CCS applications; latency related.			

ID	Category	Requirement: "The Communication Infrastructure Technology Stack shall…"	Rationale / Comment	TRDP	OPC UA	DDS/RTPS
ComStackReq-NonFunc-30	Latency	… provide latency limited to max 10 ms for process data (local consist scope!).	Typical use case in CCS applications; latency related.			
ComStackReq-NonFunc-31	Latency	… provide latency limited to max 100 ms for spontaneous/event-driven communication (local consist scope!).	Typical use case in CCS applications; latency related.			
ComStackReq-NonFunc-32	Jitter	… provide jitter low enough to enable clock synchronization with an accuracy of 1 ms between end devices (local consist scope!).	Typical use case in CCS applications; jitter related.			
ComStackReq-NonFunc-33	Jitter	… provide jitter limited to max 10 ms for process data (local consist scope!).	Typical use case in CCS applications; jitter related.			
ComStackReq-NonFunc-34	Bandwidth	… support a minimum link speed of 1 GBit/s on all shared links.	1GBit/s is current sweet spot of capacity/flexibility vs. Cost. 100 Mbit/s too slow for shared links.			
ComStackReq-NonFunc-35	Bandwidth	… allow link speeds of 100 MBit/s for end devices, full and half duplex.	Enable migration of existing devices			
ComStackReq-NonFunc-36	Bandwidth	… use cabling that is prepared for 10 GBit/s link speeds.	Cabling hard to change but (almost) at same price as for 1 Gbit/s			
ComStackReq-NonFunc-37	Bandwidth	… use (passive) coupling devices (connector between coaches/cars) that are prepared for 5 GBit/s link speeds.	Couplers major cost drivers. Cost wise 5 GBit/s << 10 GBit/s, with 5 GBits/s likely to be sufficient for next five years. Topic not yet addressed in TSI.			
ComStackReq-NonFunc-38	Bandwidth	… shall provide different link speeds towards end devices.	Migration scenarios. Forward/backward compatibility			
ComStackReq-NonFunc-39	Scalability	… support at least 500 nodes on one consist-local network.	Mostly TCMS-related requirement. CCS has a comparably low number of nodes.			
ComStackReq-NonFunc-40	Scalability	… allow at least a physical distance between two nodes of 100 m.				
ComStackReq-NonFunc-41	Scalability	… allow at least a total extent of a single consist (from leftmost to rightmost node) of 500 m.				

ID	Category	Requirement: "The Communication Infrastructure Technology Stack shall…"	Rationale / Comment	TRDP	OPC UA	DDS/RTPS
ComStackReq-NonFunc-42	Maturity	… make use of functionality that is available on the market.	Avoid getting trapped by vaporware or delayed realization of standards. Example for a standard not being available on the market for now 10 years: 802.1X-2010	railway market only	widespread on various markets, but not in railway market	even openDDS is available
ComStackReq-NonFunc-43	Maturity	… make use of solutions that are available from multiple vendors.	No vendor lock in. Attractive price points.	one open-source stack available (TCNOpen, written in C), commercial extensions of TCNOpen	implementations available from numerous vendors	Adlink, eProsima, RTI, Thales are some examples
ComStackReq-NonFunc-44	Maturity	… make use of proven technology.	Required base for reliable vehicles. Proof can come from a TRL-7+ either from the rail sector or a comparable level from a different sector.	proven in railway sector	proven in multiple sectors	examples available from multiple sectors incl. aerospace and automotive
ComStackReq-NonFunc-45	Maturity	… use components that are available in significant quantities.	Kind of heads-up requirement. Need to at least estimate market available quantities. Supply chain availability. Attractive price points.	Not assessable		
ComStackReq-NonFunc-46	Maturity	… be supported by a community approach.	Quality in use rises with support being available	forums are TCN Open Interests Group and IEC standardization activities	forum is OPC Foundation	support available in dev forums
ComStackReq-NonFunc-47	Maturity	… be supported by commercial consulting services.	Quality in use rises with support being available	strongly limited to railway domain	expertise widely available including academic sources	services available from RTI, Adlink, eProsima etc.

Proposal to TSI202x SUBSET-147

1 MODIFICATION HISTORY

Issue Number Date	Section Number	Modification / Description	Author
1.0.0 2023-07-05	-	Released version as part of TSI 2023	F. Bitsch
1.0.1	all	First version of restructuring and importing new content	Z. Ahmed H. Roelle S. Schuerch
1.1	all	First proposal on V2	ERJU WP 23

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 [4] [5]. (I)

2.4.1.2 For ETCS related abbreviations see SUBSET-023 [6]. (I)

AMQP	Advanced Message Queuing Protocol
API	Application Programming Interface
ATC	Automatic Train Control
ATO	Automatic Train Operation
CAN	Controller Area Network
CCS	Control, Command and Signalling
CIP	Common Industrial Protocol
COTS	Commercial off-the-shelf
DDS	Data Distribution Service
DHCP	Dynamic Host Configuration Protocol
DST	Daylight Saving Time
ED	End Device
ECN	Ethernet Consist Network
EMD	Electrical Middle Distance Bus
ERA	European Railway Agency
ERJU	Europe’s Rail Joint Undertaking
ESD+	Electrical Short Distance Bus
ERTMS	European Rail Traffic Management System
ETB	Ethernet Train Backbone
ETCS	European Train Control System
FRMCS	Future Rail Mobile Communication System
HMI	Human Machine Display
HW	Hardware
(I)	Informative
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
MAC	Media Access Control

MD	Message Data
MQTT	Message Queuing Telemetry Transport
MVB	Multifunction Vehicle Bus
NTP	Network Time Protocol
OCORA	Open CCS On-board Reference Architecture
OMS	Online Monitoring System
ODVA	Open DeviceNet Vendors Association
OPC UA	Open Platform Communications Unified Architecture
ORD	On-board Recording Device
OSI	Open Systems Interconnection
PCP	Priority Code Point
PROFINET	Process Field Network
PoC	Proof of Concept
QoS	Quality of Service
(R)	Requirement
R2DATO	Rail to Digital automated up to autonomous train operation
RFC	Request for Comments
Realtimedata	Data that needs to be communicated within a certain upper time limit.
RMI	Remote Method Invocation
ROS	Robot Operating System
RPC	Remote Procedure Call
RST	Rolling Stock
RTPS	Real-Time Publish Subscribe
SDT	Safe Data Transmission
SIL	Safety Integrity Level
SOME/IP	Scalable Service-Oriented Middleware over IP
SW	Software
TCMS	Train Control and Management System
TCN	Train Communication Network
TCP	Transmission Control Protocol
TOS	Train Operator System
TRDP	Train Real-Time Protocol
TRL	Technical Readiness Level

TSI	Technical Specification of Interoperability
TTLS	Train Time and Location Service
TWG	Topical Working Group
UDP	User Datagram Protocol
UTC	Coordinated Universal Time
WP	Work Package
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.

2.5 DEFINITIONS

2.5.1.1 For ATO related definitions see ERTMS/ATO Glossary [4]. (I)

2.5.1.2 For ETCS related definitions see SUBSET-023 [6]. (I)

2.5.1.3 The statements made in this Subset are assigned to the following categories: (I)

- 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.
- 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.

2.6 SCOPE AND PURPOSE

TODO: REVIEW AND REWORK NEEDED

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 1.

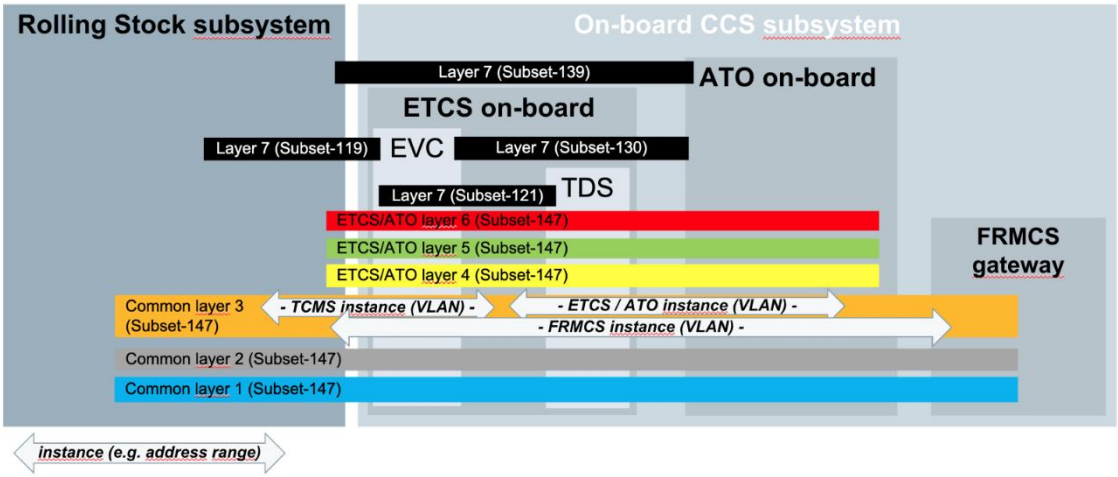

Figure 1: Levels of abstraction for the layers according to the OSI model

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 communicate 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 be used. 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 4, 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. 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)

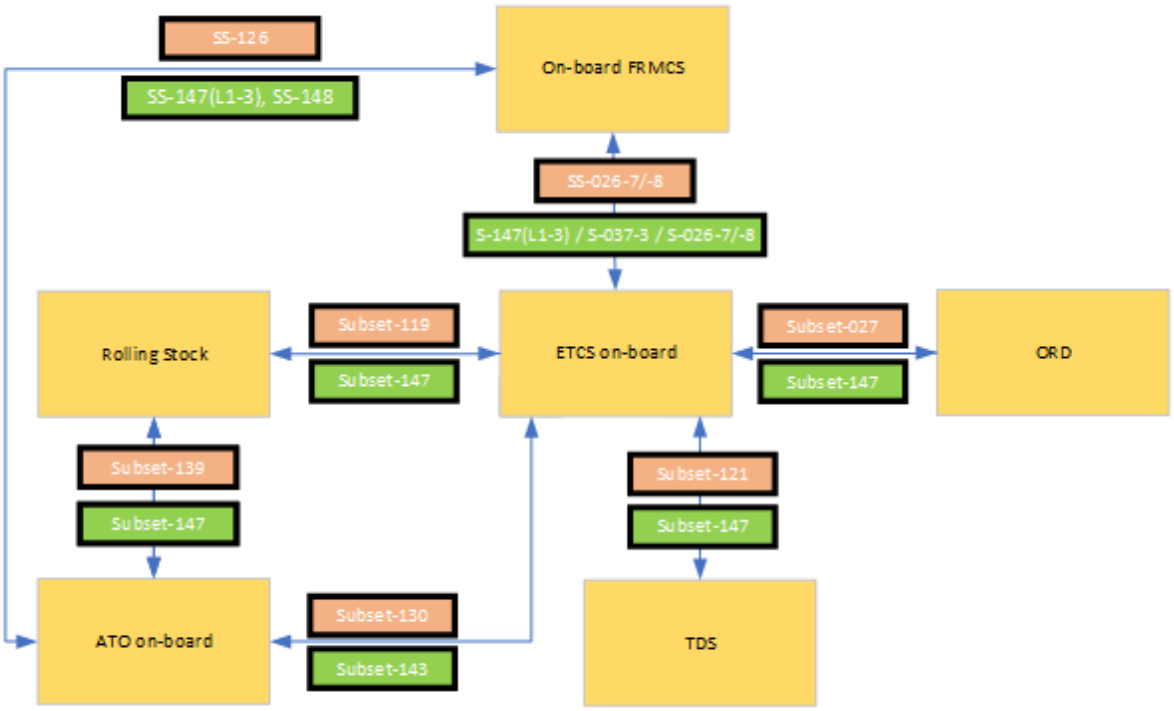

Figure 2:Interfaces and related specifications for ETCS & ATO on-board and Rolling Stock

[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 1 gives an overview on the application of SUBSET-147. (I)

Entity 1	Entity 2	Reference	Local Serial Communication	Service Class, See 9.4.1.1
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	5
ATO on-board	OMS	SS-149	SS-147	5
ETCS on-board	OMS	SS-149	SS-147	5

Table 1: 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 in implementation (some configuration may be applied though) to these components (interchangeability) in the future. This will avoid multiple logical and physical adapters between the systems in scope. (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). (I)

2.6.1.12 In case of the interfaces of the ATO on-board it is possible to use SUBSET-143 [7] as alternative to SUBSET-147. But also, in case of using SUBSET-143 the layers 1 and 2 as defined in chapter 8 shall be applied, see also 3.1.1.6. (R)

2.6.1.13 The chapters 7 and 8 are applicable only for ‘newly developed vehicle designs’ requiring a first authorization 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

[1] UNISIG, *ERTMS Data Applications - CCS Consist Network Communication Layers,* SUBSET-147 1.0.0.

[2] ERJU Innovation Pillar R2DATO, *D23.3: List of Solution Candidates,* V1.0.

[3] ERJU Innovation Pillar R2DATO, *D23.2: List of System Requirements,* V1.1.

[4] EEIG ERTMS Users Group, *ERTMS/ATO Glossary,* 13E154.

[5] ERA, UNISIG, EEIG ERTMS Users Group, *System Requirements Specification,* SUBSET-026.

[6] ERA, UNISIG, EEIG ERTMS Users Group, *Glossary of Terms and Abbreviations,* SUBSET-023.

[7] UNISIG, *ERTMS/ATO: Interface Specification Communication Layers for On-board Communication,* SUBSET-143.

[8] IEC, *Electronic railway equipment – Train communication network (TCN) – Part 3-4: Ethernet Consist Network (ECN),* IEC 61375-3-4:2014.

[9] IEC, *Train Communication Network – MVB,* IEC61375-3-1:2012 TCN.

[10] IEC, *Serie Profinet,* IEC61158-1:2019 / 61158-5-10 :2020 / 61158-6-10:2019.

[11] IEC, *Train Communication Network – CAN,* IEC61375-3-3:2012 TCN.

[12] UNISIG, *TDS / ETCS On-board DMI-EVC Interface FFFIS,* SUBSET-121.

[13] IEC, *Profisafe,* IEC61784-2:2019/ -3-3:2021.

[14] IEC, *Train Communication Network – Communication Profile,* IEC61375-2-3:2015 TCN.

[15] IEC, *Open Platform Communications Unified Architecture (OPC-UA),* IEC62541-1/-2:2016 / -3 – -14:2020 / -100:2015.

[16] UNISIG, *EuroRadio FIS - FRMCS Communication Functional Module,* Subset-037-3.

[17] UNISIG, *ATO-OB / ATO-TS Interface Specification - Transport and Security Layers,* Subset-148.

[18] UNISIG, *ATO-OB / ATO-TS FFFIS Application Layer,* Subset-126.

[19] UNISIG, *ERTMS/ATO System Requirements Specification,* Subset-125.

[20] UNISIG, *Performance Requirements for Interoperability,* SUBSET-041.

[21] UNISIG, *Performance Requirements for STMs,* SUBSET-059.

[22] UNISIG, *ERTMS End-to-End Security Layer,* SUBSET-146.

[23] IEC, *Industrial communication networks - Network and system security – Part 3-3: System security requirements and security levels,* IEC 62443-3-3: 2013.

[24] IEEE, *IEEE Standard for Local and Metropolitan Area Networks–Bridges and Bridged Networks,* IEEE 802.1Q-2018.

[25] IEC, *Train Communication Network – Train Communication Network – WTB,* IEC61375-2-1:2012 TCN.

[26] UNISIG, *ERTMS/ATO System Requirements Specification.*

3 GENERAL REQUIREMENTS

TODO: REVIEW AND REWORK NEEDED, especially remove references to MVB, CAN, PROFINET and OPC-UA.

3.1.1.1 This specification includes the solutions regarding the Ethernet, MVB and CAN based on [8], [9] and [10] [11]. (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 [12]) 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 9 shall be applicable. (R)

3.1.1.6 The communication technologies PROFINET [10] (incl. PROFIsafe [13]), TRDP [14], OPC-UA [15] and SUBSET-143 [7] 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 [16] and SUBSET-026-7/-8 [5] for ETCS or SUBSET-148 [17], -126 [18] and -125 [19] 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. [5] explains the architecture of the ETCS on-board and the interfaces to other equipment and [19] 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 4). (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. (I)

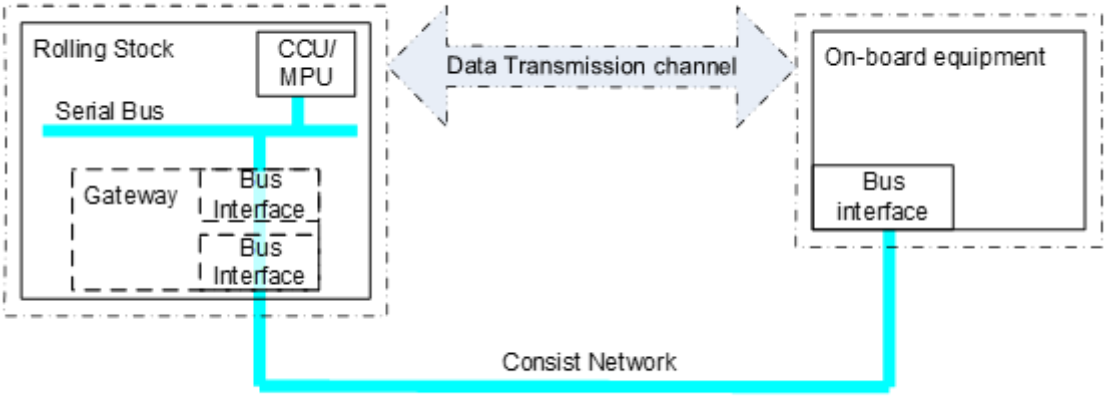

Figure 3:Rolling Stock can integrate a gateway to adapt to the bus/network type defined by the ERTMS/ETCS on-board or ATO on-board

~~4 MVB~~

<removed>

MVB is obsolete for Common On-Board Communication Network

~~5 CAN~~

<removed>

CAN is obsolete for Common On-Board Communication Network

~~6 RULES TO APPLICATION LAYER DOCUMENTS~~

<removed>

The former chapter was incomplete as it did not differentiate between the various types of communication presented in this new revision. It was also incomplete in the sense that didn't follow a clear distinction of communication model, information model and their application specific use.

Decision to be made:

- Either massively extend the chapter, thus addressing
  - The distinction of communication types
    - Process data
    - Event data
    - Bulk data
    - Stream data
  - The distinction of communication sub-models for each type
    - Information model, including marshalling to the specific technologies
    - Communication model
    - Organization model
- Alternatively shift the relevant content to Application Profiles.

7 PERFORMANCE REQUIREMENTS

TODO: REVIEW AND REWORK NEEDED

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: [20] and [21] 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 [21] §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

TODO: WHOLE §8 REVIEW AND ADAPTIONS WRT NEW MIDDLE LAYERS CONTENT

8.1 INTRODUCTION

8.1.1.1 This protocol specification is divided into separate layers. Figure 4 shows the representation of the different layers according to the Open Systems Interconnection (OSI) model. (I)

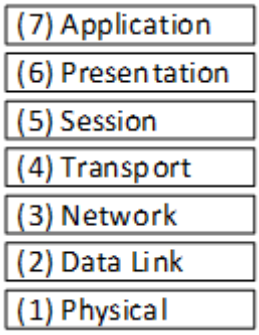

Figure 4: OSI Layers

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 [8]. (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

TODO: Clarify scoping for HMI devices, especially for HMIs being exclusively used by ETCS/CCS systems versus hybrid HMIs being used by ETCS and TCMS in parallel.

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 [8] [14] for the

interfaces among the elements for the full OSI layer stack (OSI layers 1 to 7) on the long-term.[3] (I)

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 4: 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)

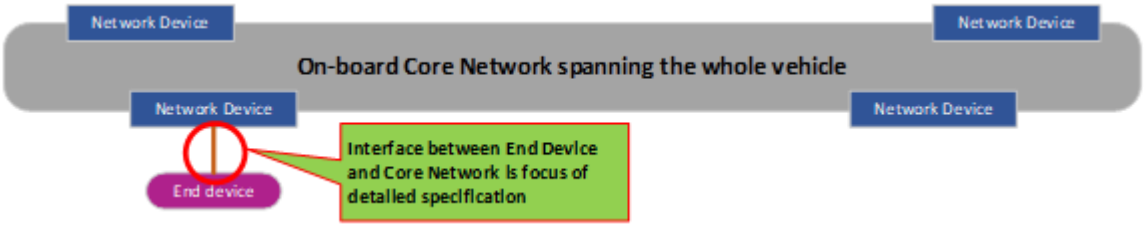

Figure 5: Separation of On-board Core Network and End Devices

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

[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.

[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 chapter8.3.2.3).

concepts/architectural patterns to offer redundancy within the network. For details, esp. on devices with multiple links, see 9.1.2. (I)

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 general 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 9.1.2
- 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 [22]. (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 [22] defines secured communication, as well as certificate management for ETCS, ATO and KMC. (R)

9 LOWER LAYERS (OSI LAYERS 1 AND 2)

TODO: WHOLE §9 REVIEW AND ADAPTIONS WRT NEW MIDDLE LAYERS CONTENT

9.1 BASE TECHNOLOGY

9.1.1.1 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)

9.1.1.2 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)

9.1.2 Network architecture

9.1.2.1 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)

9.1.2.2 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)

9.1.2.3 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)

9.1.2.4 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)

9.1.2.5 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.

[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

- 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.

9.1.3 On-board Core Network characteristics

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

9.1.3.2 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)

9.1.3.3 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)

9.1.4 End Device characteristics

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

9.2 OSI LAYER 1: PHYSICAL LAYER

9.2.1 Cabling

9.2.1.1 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)

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

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

9.2.1.4 For End Devices connected by M12 with coding D-Code (IEC 61076-2-101) operating at 100BASE-TX, CAT5e can be used. (R)

9.2.2 Connectors

9.2.2.1 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] In alignment with IEC61375-3-4 chapter 4.2.1

[9] Wireless technologies may be added to future revisions.

9.2.2.2 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)

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

9.2.3 Power supply over network cable

9.2.3.1 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, compliant to on-board railway european standards, may serve as external power supply. (R)

9.3 OSI LAYER 2: ASPECT OF SEPARATION / SEGMENTATION

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

9.3.1.1 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 [23] can be fulfilled. (R)

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

9.3.1.3 See also the chapter 9.5 on bandwidth limitation. (R)

9.3.2 Separation/segmentation of traffic towards End Devices

9.3.2.1 OSI layer 2 shall provide separation and segmentation based on VLANs as of IEEE802.1Q[10] [24], as the Ethernet CCS Consist Network targets to share one physical medium. (R)

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

9.3.2.3 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.

[10] Compliant with IEC61375-3-4

Any frames tagged differently shall be dropped at the On-board Core Network Port. (R)

9.3.2.4 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)

9.3.2.5 For links carrying traffic of multiple Logical Zones, tagged frames as described in IEEE802.1Q [24] shall be used. (R)

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

9.3.2.7 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)

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

9.3.3 Authentication / Authorization of End Devices

9.3.3.1 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)

9.3.3.2 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)

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

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

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

9.4 OSI LAYER 2: ASPECT OF QUALITY-OF-SERVICE

9.4.1 Quality-of-Service in general

9.4.1.1 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)

9.4.1.2 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 bandwidth[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

[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 bandwidth[13] [Mbit/s]	Typ. max delay[14] [ms]	Typ. usage example
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	20	Cab radio audio stream
5	5	Ordinary process data	100	5	IEC61375-3-4: “Process Data” CCS process data
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 2: Service Class overview

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

9.4.1.4 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)

9.4.1.5 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)

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

9.4.2.1 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)

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

9.4.3 Quality-of-Service towards End Devices

9.4.3.1 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)

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

9.4.3.3 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)

9.4.3.4 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)

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

9.4.3.6 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)

9.5 OSI LAYER 2: ASPECT OF BANDWIDTH LIMITATION

9.5.1.1 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)

9.5.1.2 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)

9.5.1.3 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)

9.6 OSI LAYER 2: ASPECT OF AVAILABILITY / REDUNDANCY

9.6.1.1 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)

9.6.1.2 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)

9.6.2 Redundancy in the On-board Core Network

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

9.6.2.2 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)

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

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

9.6.3 Redundancy in connecting End Devices

9.6.3.1 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)

9.6.3.2 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)

9.6.3.3 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)

9.6.3.4 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)

9.7 OSI LAYER 2: ASPECT OF SECURITY

9.7.1.1 The security for the lower layers is focused on separating and segmenting network traffic to ensure non-interference between logical separate communications (see chapter 9.3). (I)

9.7.2 Confidentiality, Integrity and Authentication

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

9.7.2.2 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)

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

9.7.2.4 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)

9.8 OSI LAYER 2: ASPECT OF SAFETY

9.8.1.1 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)

10 NETWORK LAYER (OSI LAYER 3)

TODO: NEEDS TO BE REWRITTEN AND EXTENDED

10.1.1.1 The Ethernet CCS Consist Network shall support IPv4 according to IETF RFC 791. (R)

~~10.1.1.2 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)~~

~~10.1.1.3 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)~~

~~10.1.1.4 The OSI layers 3 to 6 are implicitly defined by the chosen communication technology. (I)~~

~~10.1.1.5 The system integrator shall choose one of the communication technologies, to which he wants to comply. (R)~~

11 MIDDLE LAYERS (OSI LAYERS 4 TO 6)

The middle layers specifications are divided into the following different communication types of the onboard communication:

- Process Data Communication
- Event based Communication
- Remote Procedure Calls (RPC) also called Request/Reply or Remote Method Invocations (RMI)
- Bulk Data Communication
- Audio & Video Streaming

The investigations on security have shown that there is no generic security solution for all communication types available on lower layers (OSI layer 2 or 3). Therefore, the topic of security is addressed for each communication type seperately on the middle layers (OSI layers 4 to 6).

The same is applicable for the aspect of safety. Also, safety is addressed for each communication type seperately as part of the middle layers (OSI layers 4 to 6).

In the following subchapters each communication type is introduced and the main requirements and open points are noted.

11.1 PROCESS DATA COMMUNICATION

11.1.1 Informative Introduction

Large portions of communication needs for on-train applications are the cyclic communication of so-called process data. Process data refer to the information generated during the operation of a system, process or application. It typically includes data related to the inputs, outputs, and operational parameters of a system, process or application.

Typically, safety requirements from applications are associated, where the discovery of unintended changes on the data needs to be reliably discovered.

For process data communication, the Train Real-Time Data Protocol (TRDP) will be used. It is a specialized communication standard tailored for the railway industry, focusing on the effective transmission of real-time data among various systems and devices within a train environment. Its primary goal is to enhance operational efficiency, safety, and interoperability across different railway applications. For safety-related data, the special protocols SDTv2 and SDTv4 are defined on top of TRDP.

A major gap that still needs closing, which is security for process data communication. Following the design decision, that security has to be handled within each of the communication functions, TRDP needs to provide a security layer. While all the other functions can rely on TLS, this is not applicable for TRDP being UDP based but not TCP based. Therefore, one of the major open topics is the development of a security layer for TRDP.

11.1.2 Requirements on Process Data Communication

TODO: MORE SPECIFIC REQUIREMENTS

11.1.2.1 For process data communication TRDP according to IEC 61375-2-3 [5] process data shall be used. (R)

11.1.2.2 For safety-related process data SDTv2 according to IEC 61375-2-3 [5] and SDTv4 according to Shift2Rail's CONNECTA Drive-by-Data Architecture Specification [2][15] shall be used on top of TRDP process data. (R)

11.1.3 Open Topics and Further Work for Process Data Communication

TODO: CLARIFICATION of OPEN TOPICS

Currently open topics include:

- Maximum frame size / fragmented frames in TRDP
- Security Layer of TRDP
- Aggregation of data for multiple receivers intro one datagram
- Weaknesses in specification of information model, e.g. bit-fields
- Alignment with evolution of IEC 61375-2-3
- Role of message data in contrast to event-based communication

11.2 EVENT BASED COMMUNICATION

11.2.1 Informative Introduction

In addition to cyclic process data, which represents a state, sporadic data messages or events are also present in vehicle communication. Common integration services must therefore provide a mechanism for event communication.

Applications for event data may include:

- Diagnostic messages (operational, maintenance, protocol)
- Data change events
- Process-oriented but sponanious / acyclic messages

The publish/subscribe pattern will be used here, in contrast to the request/response pattern, which is commonly employed in other services, for example the bulk data transfer. Communication patterns can be connected to one-to-one and one-to-many communication scenarios in general. Event-driven communication is often connected to one-to-many scenarios without explicit need for an acknowledgement. This is in contrast to other application fields (e.g., remote procedure call scenarios), where one might specifically require a direct feedback from a specific recipient of a request / datagram / message.

Another typical property of event communication is that the sender of an event is not interested in the actual receivers. Event revceivers may dynamically come and go without interfering with the

[15] The specification of SDTv4 will become an integral part of the IEC/EN 61375-2-3 Annex B in the subsequent version of the standard.

sender. The publish/subscribe pattern exactly serves this need. Using message brokers in between the sender and the receivers complete the decoupling of both sides.

The architectural pattern chosen here is the publish/subscribe pattern, the chosen technology is AMQP:

The Advanced Message Queuing Protocol (AMQP) is an open and standardised binary network protocol designed for the exchange of messages across distributed networks, supporting various broker architectures. It enables asynchronous communication and both point-to-point and publish-subscribe messaging patterns.

AMQP is implemented on a standard TCP/IP protocol stack. The core components of AMQP include the Message Broker, which routes messages between senders and receivers; the Queue, where messages wait for consumption; the Exchange, which directs messages to queues based on rules; and the Binding, which defines the routing relationship. These elements work together to enable flexible and interoperable messaging. AMQP supports message-oriented communication with message-delivery guarantees such as at-most-once, at-least-once and exactly once. Furthermore, it ensures the authentication and encryption of messages based on Transport Layer Security (TLS). Topic-based access control is also typically available in modern AMQP broker implementations in contrast to non-broker-based (e.g. HTTP-based) approaches.

While AMQP is the preferred solution for the future, there might exist scenarios (e.g. retrofit) where already existing TRDP Message Data (MD) use would be beneficial to be maintained. For those cases, and only those cases, TRDP MD could be continued to be used.

11.2.2 Requirements on Event based Communication

TODO: MORE SPECIFIC REQUIREMENTS

11.2.2.1 For event based communication, AMQP according to ISO/IEC 19464 [8] shall be used. (R)

11.2.2.2 For secured event based communication, AMQP with TLS shall be used. (R)

11.2.2.3 Configuration, concrete architecture / setup of an AMQP broker service are beyond this specification. (I)

11.2.2.4 For scenarios where existing End Devices which use TRDP MD for event communication will be integrated without modification, TRDP MD still may be used for event communication (R)

11.2.2.5 Being a legacy technology from the perspective of this specification, TRDP MD for event communication is deprecated and will be removed in a future version of the specification (I)

11.2.2.6 This specification intentionally does not specify a safety layer for AMQP. It is left for the user to decide if AMQP fulfils the safety needs of a specific application context. As an alternative, TRDP process data (with its safety layers) may be used (I)

11.2.3 Open Topics and Further Work for Event based Communication

TODO: CLARIFICATION of OPEN TOPICS

Currently open topics include:

- Information model.
- Message format/encoding of AMQP message content.
- Addressing: AMQP message hierarchy/structure, a.k.a. topic tree.
- Service discovery: “How do I find the broker“. By fixed DNS name, by bonjour/zeroconf, by ssd/upnp, by … ?

11.3 REMOTE PROCEDURE CALLS (RPC)

11.3.1 Informative Introduction

In addition to cyclic process data and acyclic event-based data exchange, Remote Procedure Calls (RPC) – also called Request/Reply or Remote Method Invocations (RMI) – represent a communication paradigm that is also present in vehicle communication. Consequently, it is necessary for common integration services to provide a mechanism for RPC/RMI communication.

Typical IT and OT use cases for RPCs may include:

- Asynchronous command execution,
- Client-server communication,
- Communication between microservices,
- Inter-process communication,
- Remote administration.

A resemblance to or a combination with bulk data transfer solutions is often observed in RPC/RMI applications, such as the combination of an RPC-driven upload trigger with the subsequent data transfer. We therefore direct the reader to the separate chapter 11.4 on the evaluation of bulk data transfer technologies for further information on some of the technologies discussed in this paper.

A distinction can be made between the use cases of RPC and those of event-driven communication. This distinction is rooted in the underlying communication paradigm. Event-driven communication is often employed in scenarios involving one-to-many communication, whereas RPC use cases, at least in railway applications, rely on a one-to-one communication paradigm. This is because procedure calls are directed to a specific receiver, who is typically responsible for confirming the call’s receipt and execution. For further information regarding technologies that specifically tackle one-to-many communication use cases, please refer to chapter 11.2 on event event based communication.

RPC will be realised with HTTP/1.x or HTTP/2 plus TCP as the underlying transport protocol and RESTful designed APIs to employ standard HTTP methods (e.g., GET, POST, PUT, DELETE) to perform CRUD (i.e., Create, Read, Update, Delete) operations on resources, which are represented in formats such as JSON or XML. Specific HTTP requests are hence mapped to remote methods or procedures. Each API endpoint is associated with a method call, with the HTTP methods representing different operations on these calls. The Representational State Transfer (REST) design

principle describes that method information are not encoded in the Unified Resource Identifier (URI), as the URI specifies the location and name of the resource, but not the functionality that the (web) service offers for the resource.

While HTTP/1.x and HTTP/2 both rely on TCP as transport layer, HTTP/3 introduces QUIC as a new transport layer. As QUIC is not yet very commonly used today, and HTTP/1.x and HTTP/2 already fulfil our requirements quiet well, HTTP/3 is intentionally not part of the current specification. It might be added in a later version.

11.3.2 Requirements on Remote Procedure Calls (RPC)

TODO: MORE SPECIFIC REQUIREMENTS

11.3.2.1 For RPC communication HTTP over TCP according to according to IETF RFC 2616 or RFC 7540/7541 shall be used. (R)

11.3.2.2 The endpoints of RPC services shall be implemented in a RESTful designed API. (R)

11.3.2.3 For secured communication HTTP over TLS (HTTPS) according to IETF RFC 2818 shall be used. (R)

11.3.2.4 The minimum version a client or a server shall support is HTTP/1.1 according to IETF RFC 2616. (R)

11.3.2.5 Optionally HTTP/2 according to IETF RFC 7540/7541 can be supported and used on mutual handshake. (R)

11.3.3 Open Topics and Further Work for Remote Procedure Calls

TODO: CLARIFICATION of OPEN TOPICS

Currently open topics include:

- Upper layer, methodologies, or frameworks to specify and standardise the API interfaces, e.g. Web of Things (WoT).
- Addressing: URL format/scheme.
- Service discovery

11.4 BULK DATA COMMUNICATION

11.4.1 Informative Introduction

In addition to cyclic process data, acyclic event-based data exchange and RPC, bulk data communication is another fundamental communication paradigm for vehicle communication differentiated by its application specifics. Consequently, it is necessary for common integration services to provide a (transport) mechanism for bulk data transfer/communication.

Typical IT and OT use cases for bulk data communication may include:

- Data warehousing (i.e., loading large volumes of data into internal or external data storages),

- Backup and restore (e.g., of system images),
- Software updates (e.g., for firmware images or containers),
- Data replication and synchronization,
- Management and diagnosis (i.e., log file transfer).

A resemblance to or a combination with Remote Procedure Calls (RPC) solutions is often observed in bulk data applications, such as the triggering of a data upload process via a separate procedure call. We therefore direct the reader to the separate chapter 11.3 on the RPC technologies for further information.

The chosen technology here is the Hyper Text Transfer Protocol (HTTP) and the Representational State Transfer (REST) architectural concept.

This pair represents a standardised and well-known approach in the contemporary Internet, facilitating the web-based transfer of data. HTTP versions 1 and 2 are deployed with the Transmission Control Protocol (TCP) as the underlying transport layer, whereas security is provided by using HTTP over TLS (HTTPS). The handshake to establish a secure connection is performed on top of the separate TCP handshake, which results in communication overhead for secured connections. In comparison with HTTP/1.x, HTTP/2 is the more complex and extensive protocol, leading to more extensive implementations and more load on client/server side. An upgrade path between different HTTP versions is available as common libraries and client/server implementations typically support both HTTP/1.x and HTTP/2 nowadays.

While HTTP/1.x and HTTP/2 both rely on TCP as transport layer, HTTP/3 introduces QUIC as a new transport layer. As QUIC is not yet very commonly used today, and HTTP/1.x and HTTP/2 already fulfil our requirements quiet well, HTTP/3 is intentionally not part of the current specification. It might be added in a later version.

For bulk data applications, standard HTTP methods (e.g., GET, POST, PUT, DELETE) are employed to perform operations on resources, which are identified by Uniform Resource Locators (URLs). RESTful Application Programming Interfaces (APIs) are stateless, meaning that each client request contains all the information necessary to process the request. This improves scalability since services can be offered and implemented in a distributed fashion. For bulk data transfers, a REST API can support endpoints that accept large payloads, typically in formats like JSON or XML, using POST or PUT methods to create or update multiple records at once. Furthermore, custom implementations of pagination, filtering, and batching mechanisms enable the efficient handling of large datasets, ensuring manageable request sizes and reducing server load. Additionally, the use of HTTP headers and status codes provides control over data transfer processes, allowing for reliable and standardised communication between clients and servers. Different HTTP versions can provide different features to simplify such implementations.

11.4.2 Requirements on Bulk Data Communication

TODO: MORE SPECIFIC REQUIREMENTS

11.4.2.1 For bulk data transfer, HTTP over TCP according to according to IETF RFC 2616 or RFC 7540/7541 shall be used. (R)

11.4.2.2 The endpoints of bulk data transfer services shall be implemented in a RESTful designed API. (R)

11.4.2.3 For secured communication HTTP over TLS (HTTPS) according to IETF RFC 2818 shall be used. (R)

11.4.2.4 The minimum version a client or a server shall support is HTTP/1.1 according to IETF RFC 2616. (R)

11.4.2.5 Optionally and only in addition to 11.4.2.1, HTTP/2 according to IETF RFC 7540/7541 can be supported and used on mutual handshake. (R)

11.4.2.6 Optionally and only in addition to 11.4.2.1, SFTPv3 can be used for bulk data transfer. Although not being formally specified by itself, the term SFTPv3 refers to the variant running over a ssh channel. Ssh itself is defined in IETF RFCs 4250-4256. (R)

11.4.2.7 SFTP must not be confused with FTPS (IETF RFC 4217). Either FTP (IETF RFC 959), or FTPS are not allowed for bulk data transfer. (I)

11.4.2.8 Being a legacy technology from the perspective of this specification, SFTP for bulk data communication is deprecated and will be removed in a future version of the specification. (I)

11.4.3 Open Topics and Further Work for Bulk Data Communication

TODO: CLARIFICATION of OPEN TOPICS

Currently open topics include:

- Upper layer, methodologies, or frameworks to specify and standardise the API interfaces, e.g. Web of Things (WoT).
- Addressing: URL format/scheme.
- Service discovery

11.5 AUDIO & VIDEO STREAMING

11.5.1 Informative Introduction

In contrast to bulk data communication also constant audio & video streaming data e.g. for loudspeaker announcements or video surveillance is present in vehicle communication. The media is encoded and transferred in a stream of data packets from a server to a client. The main parts of a streaming communication are the session control, the encoding of the data and the effective data transport. One of the most well-known protocol set used for audio/video streaming is:

- RTSP enables controlling the streaming session (opening/closing, forward/reward, pausing, etc.)

- RTP transports the effective video/audio streams from the server to the client
- SRTP is the secure version of RTP encrypting the data stream
- RTCP controls the quality of the stream and is able to switch the stream to a lower quality in case of network congestion/lower connection quality

These legacy protocols are the most widely supported and used protocols for the local audio and video streaming. Nevertheless, there are many other modern protocols nowadays such as HLS, MPEG DASH, HDS, MSS. All these protocols are optimized for certain use cases. Mostly, they are developed to be adaptive for the transmission over the internet. Another relatively new protocol is WebRTC, that allows streaming thanks to APIs specifically developed to run in a web browser and relying on encoding/decoding capabilities of this framework. This is probably not relevant for most of the use cases in a railway vehicle.

As the market of streaming protocols is rapidly evolving and IT solutions are implemented more and more in the railway sector, some of the modern protocols may become beneficial compared to the legacy protocols.

Therefore, no standardised solution for audio/video streaming will be required as mandatory.

11.5.2 Requirements on Audio & Video Streaming

For the transfer of streaming data (audio/video), appropriate streaming data protocols may be used, as for instance (list not exhaustive): (I)

- RTSP Real Time Streaming Protocol according to IETF RFC 2326
- RTP Real Time Transport Protocol according to IETF RFC 3550
- SRTP Secure Real Time Transport Protocol according to IETF RFC 3261
- RTCP Real Time Control Protocol according to IETF RFC 3605

12 APPLICATION SPECIFIC TECHNOLOGIES

12.1.1.1 In addition to the already referenced technologies, there exist number of specific protocols/technologies for specific purposes. While the given technologies of §9-§11 are mandatory, there are cases where it makes no sense to rebuild functionalities of specialized protocols with the protocols of SUBSET-147. (I)

12.1.1.2 This chapter lists those pre-defined, specialized protocols/technologies which shall be used in addition to §11. (I)

12.1.1.3 For end devices in scope, any application in scope shall not introduce other technologies/protocols than the ones referenced in §9-§12. (R)

12.2 LOCAL TIME SYNCHRONIZATION

TODO: DESCRIBE USE OF NTP/NTS.

ALIGN WITH SYSTEM PILLAR SECURITY WORKGROUP.

ALIGN WITH:

1. Secure Component Specification, Baseline “V0.90, Draft 03/2024”

2. Secure Communication Specification, Baseline “V0.90, Draft 03/2024”

3. Shared Security Services Specification, Baseline “V0.90, Draft 03/2024”

4. Security Program Requirements, Baseline “V0.90, Draft 03/2024”

May be shortened or replaced by a reference to System Pillar document

12.3 AUTOMATIC IPV4 ADDRESS CONFIGURATION

TODO: DESCRIBE USE OF DHCP.

12.4 HOST NAME RESOLUTION

TODO: DESCRIBE USE OF DNS / DNSsec.

ALIGN WITH SYSTEM PILLAR SECURITY WORKGROUP.

ALIGN WITH:

1. Secure Component Specification, Baseline “V0.90, Draft 03/2024”

2. Secure Communication Specification, Baseline “V0.90, Draft 03/2024”

3. Shared Security Services Specification, Baseline “V0.90, Draft 03/2024”

4. Security Program Requirements, Baseline “V0.90, Draft 03/2024”

May be shortened or replaced by a reference to System Pillar document

12.5 CERTIFICATE DISTRIBUTION

TODO: DESCRIBE USE OF CMP.

ALIGN WITH SYSTEM PILLAR SECURITY WORKGROUP.

ALIGN WITH:

1. Secure Component Specification, Baseline “V0.90, Draft 03/2024”

2. Secure Communication Specification, Baseline “V0.90, Draft 03/2024”

3. Shared Security Services Specification, Baseline “V0.90, Draft 03/2024”

4. Security Program Requirements, Baseline “V0.90, Draft 03/2024”

May be shortened or replaced by a reference to System Pillar document

12.6 DEPLOYMENT OF FRMCS

TODO: DESCRIBE RELATION TO FRMCS.

12.7 OTHER TOPICS

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

12.7.2 Network configuration and management

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

12.7.3 Authentication data provider

12.7.3.1 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)

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

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

~~13 TRAINTIME AND LOCATION SERVICE~~

<removed>

The Train Time and Location Service is an application layer service and should either be integrated in an appropriate application layer subset or should be moved in a new subset on its own.

14 ITEMS FOR FURTHER STUDIES

TODO: NEEDS TO BE ADAPTED ACCORDINGLY TO NEW CONTENT

~~14.1.1.1 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)~~

14.1.1.2 Strategy on conformance tests. (I)

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

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

~~14.1.1.5 Higher layer protocol suits, their relation between communication models and protocols, information models and their technical representation. (I)~~

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