

Rail to Digital automated up to autonomous train operation

D24.1 – Definitive and aligned requirements set for managing an Onboard Communication Network and concluded selection of suitable management functionality

Due date of deliverable: 30/06/2025

Actual submission date: 12/09/2025

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

Reviewed: Y

Document status		
Revision	Date	Description
01	12/09/2025	First issue of D24.1. Reviewed in WP and ready for TMT review.

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

Start date: 01/12/2022

Duration: 42 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
Moritz, Matthias	DB	Elaboration, second opinion, review
De Paola, Enrico	DB	Elaboration, second opinion, review
Abbati, Lorenzo	FSI	Review
Durante, Raffaele	FSI	Review
Ferri, Giulio	FSI	Review
Tarmati, Benedetta	FSI	Review
Dan, György	KTH	Review
Schuerch, Stefan	SBB	Elaboration, second opinion, review
Arndt, Igor	SMO	Elaboration, second opinion, review
Kirsche, Michael	SMO	Elaboration, second opinion, review
Knollmann, Volker	SMO	Elaboration, second opinion, review
Mattes, Rainer	SMO	Elaboration, second opinion, review
Rahn, Karsten	SMO	Elaboration, second opinion, review
Roelle, Harald	SMO	Elaboration, second opinion, review
Daniel, Christian	SNCF	Elaboration, second opinion, review
Roullier, Sylviane	SNCF	Elaboration, second opinion, review
Eriksson, Joachim	TRV	Review
Hallner, Pipsa	TRV	Review
Larsson, Henrik	TRV	Review

Disclaimer

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

EXECUTIVE SUMMARY

The present document constitutes the Deliverable D24.1 “Definitive and aligned requirements set for managing an Onboard Communication Network and concluded selection of suitable management functionality”. It is produced in the framework of Innovation Pillar Flagship Project R2DATO under Work Package 24 (WP24), Tasks T24.1 and T24.2.

This deliverable is part of a series contributing to a proposal for the upcoming TSI 202x, which will define the future common onboard communication network.

User stories, initially developed in R2DATO WP23, form the basis for the subsequent work in WP24. This approach ensures shared scoping and consistent specifications across communication functionality (WP23) and management functionality (WP24). These user stories are critical inputs, guaranteeing the inclusion of all necessary communication and management functionalities for their successful realization.

Within this deliverable, 25 user stories from all relevant stakeholders are selected and presented. From these user stories, corresponding functional and non-functional system requirements are derived. Based on these requirements and the required interface specification level for each user story, network management functionalities of various types (e.g., process definitions, functionality related to functional or technical interface specifications) are compiled.

ABBREVIATIONS AND ACRONYMS

CCS	Control Command and Signalling
DDOS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DOS	Denial of Service
ECN	Ethernet Consist Network
ERJU	Europe's Rail Joint Undertaking
FFFIS	Form Fit Function Interface Specification
FIS	Functional Interface Specification
HW	Hardware
ID	Identification number/token
IEEE	Institute of Electrical and Electronics Engineers
KPI	Key Performance Indicator
LAN	Local Area Network
MAC	Medium Access Control
NTP	Network Time Protocol
NTS	Network Time Security
OCN	Onboard Communication Network
OSI	Open Systems Interconnection
PoC	Proof of Concept
R2DATO	Rail to Digital automated up to Autonomous Train Operation
RAMS	Reliability, Availability, Maintainability and Safety
SW	Software
TCMS	Train Control and Management System
TLS	Transport Layer Security
TOC	Train Operating Company ¹
TRL	Technical Readiness Level
TSI	Technical Specification for Interoperability
VLAN	Virtual Local Area Network
WP	Work Package

¹ The term "TOC" was chosen intentionally. It is vital to clarify, that, in commercial setups where responsibility for the track and responsibility for the trains is held by different companies, the interests of the train-running company are addressed.

TABLE OF CONTENTS

Acknowledgements.....	2
Report Contributors.....	2
Executive Summary	3
Abbreviations and Acronyms	4
Table of Contents.....	5
1 Introduction	6
1.1 On the Change from Use Cases to User Stories.....	6
2 User Stories	8
2.1 Structure of User Stories	8
2.2 User Stories Selection Process	8
2.3 Universal Additive Explanatory Notes	8
2.4 User Stories in Detail.....	10
3 System Requirements	15
3.1 Structure of System Requirements	15
3.2 Universal Additive Explanatory Notes	15
3.3 Functional System Requirements in Detail	16
3.4 Non-Functional System Requirements in Detail.....	18
4 Elaboration of Management Functionality.....	22
4.1 Universal Additive Explanatory Notes	22
4.2 Management Functionality related to Process Descriptions	23
4.3 Management Functionality related to Interface Descriptions	24
4.3.1 Management Functionality related to Functional Interface Specifications.....	24
4.3.2 Management Functionality related to Technical Interface Specifications.....	25
4.4 Inherently Given Network Functionality.....	26
4.5 Additional Functionalities – Out-of-Scope of Subset-147	29
5 Conclusions	30
References	31

1 INTRODUCTION

The present document constitutes the Deliverable D24.1 *“Definitive and aligned requirements set for managing an Onboard Communication Network and concluded selection of suitable management functionality”* from ERJU’s R2DATO WP24 tasks T24.1 and T24.2.

The primary objective of R2DATO’s work packages WP23 and WP24 is to define the Onboard Communication Network (OCN) for realizing Control Command and Signaling (CCS) applications on top of it (in the sense of a layered communication architecture). The OCN serves as the primary communication system and the backbone within a train for those CCS applications. In contrast to a concrete application, the purpose of the OCN is to define common technologies suitable for all kinds of CCS applications.

This deliverable represents a continuation in a series that contributes to a proposal for the upcoming standardisation of the future common onboard communication network, subsequently defined in the Technical Specification for Interoperability (TSI) 202x.

User stories, initially proposed in R2DATO D23.1 [1], form the basis for the work done in WP24 tasks T24.1 and T24.2. Building on-top of the WP23 user stories will ensure shared scoping and consistent specifications across communication functionality (WP23) and management functionality (WP24). The user stories are essential inputs, ensuring the inclusion of all necessary communication and management functionalities for their successful realisation.

Within this deliverable, 25 user stories from all relevant stakeholders that are specifically related to network management are selected and presented in Chapter 2. From these user stories, corresponding system requirements are derived and elaborated in Chapter 3. In accordance with the specified requirements and the requisite interface specification level for each user story, network management functionalities of various types (e.g., process definitions, functionality related to functional or technical interface specifications) are compiled and presented in Chapter 4. The presented network management functionalities form the foundation for further specification work on network management processes and interfaces in subsequent R2DATO WP24 tasks and deliverables.

1.1 ON THE CHANGE FROM USE CASES TO USER STORIES

In “GRANT AGREEMENT Project 101102001 — FP2 - R2DATO”, the title of this deliverable is defined as “D24.1 – Definitive and aligned requirements set for managing an Onboard Communication Network and concluded selection of suitable management functionality” (defined as deliverable on page 138; the title also referred to on pages 12 and 105). Although the deliverable’s name and content description do not refer to use cases, the task description for T24.1 states that relevant use cases from T23.1 are to be compiled and defined for network management.

In contrast to the Grant Agreement, the authors of D23.1 [1] (task T23.1) jointly decided to switch from use cases to user stories. To build upon the work done for T23.1 and D23.1 [1], and to establish a solid basis for the network management requirements, the authors of this deliverable have jointly decided to deviate from the task description for T24.1 and continue with user stories. The reasons for favouring user stories over use cases are as follows.

First, it should be noted that use cases do not have a consistent, universal definition. As Martin Fowler² states, "There is no standard way to write the content of a use case, and different formats work well in different cases."³

According to Alistair Cockburn⁴, use cases typically define 13 properties⁵ in the most extensive way. Ideally, these properties can be described in such a way that one can directly derive an implementation from them.

The architecture and technology for the middle layers of the Onboard Communication Network were developed in the predecessor work package WP23. Many of the details required for extensive use cases were unavailable at the beginning of WP23, so user stories were used instead. Since the technology for managing the Onboard Communication Network builds upon the results of WP23, maintaining user stories within WP24 is a logical continuation of the work laid out in WP23. This deliverable aims to identify a set of requirements for managing the Onboard Communication Network. The user stories presented serve as input for identifying requirements to avoid blind spots in gathering requirements. Extensive use cases are neither required nor helpful for this purpose.

Fowler and Kent Beck⁶ use a stripped-down version of use cases. Fowler states: "It is all about how people use cases. I've seen many people use cases in a very formalized manner. Kent (Beck) does his User Stories in a much more approachable manner. I do use cases the way Kent does User Stories. I call them use cases to better communicate with other developers and to influence them to use a more lightweight approach."⁷

For the reasons outlined above, user stories are the most suitable tool for the purpose of this document and phase of the project without reducing the value for the effort and money spent. For clarity, the authors of this deliverable decided to use the term "user stories". Therefore, the decision was made to use "user stories" instead of "use cases".

With the switch to user stories, the deliverable goes beyond the usual user story. Each user story is enhanced by providing a motivation or driver, making it more comprehensible to the reader. The second addition is providing extra structuring and clustering from a technical perspective to support deriving and structuring requirements.

² Martin Fowler is a British software developer, author and international public speaker on software development, specialising in object-oriented analysis and design, UML, patterns, and agile software development methodologies, including extreme programming.

³ https://en.wikipedia.org/wiki/Use_case, Retrieved 08 September 2025.

⁴ Alistair Cockburn is an American computer scientist, known as one of the initiators of the agile movement in software development.

⁵ https://en.wikipedia.org/wiki/Use_case, Retrieved 08 September 2025.

⁶ Kent Beck is an American software engineer and the creator of extreme programming and was one of the 17 original signatories of the Agile Manifesto, the founding document for agile software development.

⁷ User Story and Use Case Comparison, <http://wiki.c2.com/?UserStoryAndUseCaseComparison>, Retrieved 08 September 2025.

2 USER STORIES

This chapter collects and introduces the user stories that serve as a basis for the work done in WP24. Structure of a user story, the selection process, and additional explanatory notes are described before the actual user stories are presented in detail.

2.1 STRUCTURE OF USER STORIES

The user stories presented in the following chapter follow an easy-to-comprehend structure:

1. ID: Identification number of the respective user story. Please note that some numbers are missing from the list. This is intentional and the result of selecting the collected user stories from WP23. Please refer to section 1.1 for further details.
2. Actor: The acting role of the user story, respectively the mainly interested role. One or more of the following stakeholders:
 - Train manufacturer,
 - Train operating company (TOC),
 - Train driver,
 - Maintainer,
 - 3rd party.
3. User Story: The user story itself, written in the form: "As a <role>, I want <goal/desire> so that <benefit>".
4. Driver 1 and Driver 2: One or two main motivations of the stakeholder for submitting the story. This is more from a business perspective than a technical one.
5. Technical Cluster: Unlike the business-oriented drivers, this category is a technical clustering of user stories that will help derive technical requirements for the next project phase. It is mostly orthogonal to the drivers, but not completely.
6. Specification Level: Defines the abstraction and specification level of user stories and related topics, e.g. interfaces, the work package members intend to specify during WP24. The specification level is either FIS or FFFIS.

2.2 USER STORIES SELECTION PROCESS

The user stories initially documented in R2DATO WP23's deliverable D23.1 [1] underwent a comprehensive analysis within R2DATO Task 24.1. This process involved a detailed review of each user story to assess its relevance and applicability to WP24's focus on managing the onboard communication network. Through this rigorous selection, the most critical and pertinent user stories were identified and chosen to serve as the foundational input for deriving system requirements and defining management functionalities within WP24.

2.3 UNIVERSAL ADDITIVE EXPLANATORY NOTES

For the user stories presented in section 2.4 please keep the following scoping and universal explanatory notes in mind:

1. In all the user stories, the term “network” refers to a train's Onboard Communication Network (ECN). It does NOT refer to the railroad network.
2. Ubiquitous non-functional properties are not explicitly mentioned. These include, but are not limited to, the following:
 - a. **Security:** All activities must maintain an adequate level of security. Therefore, the onboard communication technology must support this.
 - b. **Performance:** For any activity constrained by execution time or requiring specific performance properties, the onboard communication technology must support these needs.
 - c. **Safety:** For any activity constrained by a specific safety level, the onboard communication technology must support it.

Deliverable D24.1, section 3.4, will explicitly list the non-functional requirements resulting from the user stories presented here.

2.4 USER STORIES IN DETAIL

This section provides a detailed presentation of the user stories selected for R2DATO WP24. These user stories, stemming from the analysis of R2DATO WP23's deliverable D23.1 [1], are foundational for defining the requirements and management functionalities within this work package.

Table 1: User stories defined for the network management functionality

ID	Actor	User Story	Driver 1	Driver 2	Technical Cluster	Specification Level
10002	TOC	As a TOC, I want to assess the health status of the network so that can decide whether corrective actions on network devices are necessary.	Corrective Maintenance	Monitoring	Monitoring	FIS
10004	Train manufacturer / TOC	As a Train Manufacturer/TOC, I want to be able to add new end devices in the network without heavy/complex configuration tasks and without assistance (esp. from the manufacturer) so that PoC/new services deployment are made easy.	Extension	Interoperability	Network device changes	FFFIS
10005	TOC	As a TOC, I want to be able to add new end devices on the network without breaking the homologation status so that PoC/new services deployment are made easy.	Extension	Regulation	RAMS	FIS
10010	TOC	As a TOC, I want to be able to allow/forbid data exchanges between different services/end devices so that there are no irrelevant communications on the network.	Operations	Maintenance	Logical communication relations	FFFIS
10012	Maintainer / TOC	As a maintainer or TOC, I want to block devices intentionally so that they can neither use the network neither communicate with other devices.	Operations	Maintenance	Security	FFFIS

ID	Actor	User Story	Driver 1	Driver 2	Technical Cluster	Specification Level
10013	TOC	As a TOC, I want to be able to give priority to some flows over some others for a given end device/group of end devices so that the available bandwidth is properly used. For e.g., a safety traffic should be given priority over monitoring traffic (NB: a given end device may use both types of traffic).	Operations	Maintenance	Logical communication relations	FFFIS
10015	TOC	As a TOC, I want to be able to remotely upgrade/configure any end device so that there is no need to send someone on board to perform this task or restarting the network.	Maintenance	Cost reduction	Maintenance	FFFIS
10017	TOC	As a TOC, I want to be informed when any unusual traffic occurs so that corrective actions can be taken.	Maintenance	Monitoring	Monitoring	FIS
10022	Train manufacturer	As a train manufacturer, I want to put end devices into a "non-communicating state" without disrupting the overall network functionality. Rational: putting devices into an energy saving mode for example.	Operations		Network device configuration changes	FFFIS
10024	Train manufacturer	As a train manufacturer, I want to dynamically "wake up" devices from a non-communicating state so that these devices can resume their normal operation incl. communication with peer devices.	Operations		Network device configuration changes	FFFIS
10025	Train manufacturer / maintainer / TOC	As a train manufacturer/maintainer/TOC, I need to replace defective/obsolete network devices or end nodes without affecting the overall network functionality during the replacement process and without assistance from the	Maintenance		Maintenance	FIS

ID	Actor	User Story	Driver 1	Driver 2	Technical Cluster	Specification Level
		manufacturer. This user story implies that the new device uses a different hardware or different hardware version compared to the original part.				
10026	Train manufacturer / maintainer	As a train manufacturer or maintainer, I need to replace defective network devices or end nodes. These replacement parts must be able to communicate over the network immediately and without the need for significant configuration.	Maintenance		Maintenance	FIS
10029	Maintainer / TOC	As a maintainer or TOC, I want to receive alarms if failed IEEE 802.1X device authorization has been detected so that I can take appropriate security measures.	Monitoring	Operations	Security	FFFIS
10030	Train manufacturer / maintainer	As a train manufacturer or maintainer, I want to be able to permanently remove an end device from the network. Note: this user story is different from the "failed device" story because a "failed device" should be reported in the health monitoring while a "removed" device does not.	Maintenance		Network device changes	FFFIS
10031	Train manufacturer / maintainer	As a train manufacturer or maintainer, I need to be able to get a list of all configured network devices and end devices along with their identities and the data models and/or services they provide.	Maintenance	Configuration	Discovery (Services / Models)	FFFIS
10032	Train manufacturer / maintainer	As a train manufacturer or maintainer, I need to be able to get a list of all configured network devices and end devices along with their health state.	Monitoring	Maintenance	Discovery (Services / Models)	FFFIS

ID	Actor	User Story	Driver 1	Driver 2	Technical Cluster	Specification Level
10033	TOC / train manufacturer / maintainer	As a TOC or train manufacturer or maintainer, I need to be able to retrieve key performance indicators (e.g., bandwidth) of the network and its devices so that I can identify bottlenecks or other critical issues.	Monitoring	Maintenance	Monitoring	FIS
10038	Maintainer / TOC	As a maintainer, I want to have a procedure to add or update a safe functionality, ensuring that all affected devices are updated, and that the functionality is still safe after the update. That shall be proven and visible remotely. User story remark: Please refer to deliverable D23.6 [2] for further information on how this user story is satisfied.	Upgrades	Maintenance	RAMS	FFFIS
10039	Maintainer / TOC / 3rd party	As TOC, train manufacturer or 3rd party, I want to be able to integrate a new network-device or new end device solely based on independently acquired certificates. These certificates are based on lab tests and the vehicle specifications.	Extension	Maintenance	Network device changes	FIS
10041	TOC	As a TOC, I want to limit protocols to already standardised ones so that we do not end up with exotic protocols.	extension	Cost reduction	Logical communication relations	FIS
10042	Train manufacturer	As a train manufacturer, I want to have a sense of time, so that the network components have the common base for sharing information reliably.	Operations	Maintenance	Logical communication relations	FIS

ID	Actor	User Story	Driver 1	Driver 2	Technical Cluster	Specification Level
10045	Train manufacturer	As a train manufacturer, I want to have access to DNS/DHCP services, so that the onboard network components can be identified.	Operations	Security	Logical communication relations	FIS
10050	Maintainer / TOC	As a TOC/Maintainer I want to have a fault tolerant update mechanism for the firmware/software/configuration of the network.	Upgrades	Maintenance	Maintenance	FFFIS
10051	TOC	As a TOC, I want to prohibit unauthorized routing activities so that different network segments and security zones can't be accidentally connected.	Security	Integration	Security	FIS
10053	TOC	As a TOC, I want to prohibit unauthorized access to monitoring and management functions of the network.	Security	Integration	Security	FIS

3 SYSTEM REQUIREMENTS

Building upon the user stories detailed in the preceding chapter, this chapter outlines the comprehensive set of functional and non-functional system requirements derived from them. These requirements are fundamental for guiding the design and implementation of the onboard communication network's management functionalities presented in the subsequent chapter.

3.1 STRUCTURE OF SYSTEM REQUIREMENTS

The system requirements presented in the following sections follow an easy to comprehend structure. First of all, the list of requirements is split into separate sections for functional requirements (section 3.3) and non-functional requirements (section 3.4). Then each of these sections contain a table of the requirements as such with the following attributes for each entry:

1. ID: Identification number of the respective requirement.
2. Category: a high-level scope criterion such as “Communication Patterns”, “Security”, etc.
3. The requirement text itself
4. Rationale / comment: background for the requirement and/or guidance how the requirement should be interpreted or applied.
5. Covered by TSI 2023: whether the requirement has already been considered by the TSI 2023.

3.2 UNIVERSAL ADDITIVE EXPLANATORY NOTES

For the following system requirements please keep the following scoping and universal explanatory notes in mind:

1. In all requirements, the term “network” refers to a train’s Onboard Communication Network. It does NOT refer to the railroad network.
2. The present list heavily builds up on the list of requirements developed in course of work package WP23. Thus, a solid base for continuity from WP23 is ensured.

3.3 FUNCTIONAL SYSTEM REQUIREMENTS IN DETAIL

D23.2 [3] defines a selection of functional system requirements in its chapter 2.3. WP24's functional system requirements shall be based on the work done in WP23. All previously defined functional requirements which are suitable for communication network management functionalities shall continue to be observed and upheld. Functional requirements that are not suitable for network management functionalities, and which only concern communication technologies (e.g. safety requirements that are met by using a separate safety protocol, latency or jitter requirements that are inherently met through the use of Subset-147 network features) will be omitted.

Table 2: Functional system requirements defined for the network management functionality

ID	Category	Requirement: "The Communication Infrastructure Technology Stack shall..."	Rationale / Comment	Covered by TS12023
ComStackReq-Mngt-Func-01	Service Functions	... provide health status of network devices.	–	–
ComStackReq-Mngt-Func-02	Service Functions	... provide configuration support to add new network devices.	–	–
ComStackReq-Mngt-Func-03	Service Functions	... provide data transport services with differentiated priorities.	–	–
ComStackReq-Mngt-Func-04	Service Functions	... provide service to remotely upgrade/configure network devices.	–	–
ComStackReq-Mngt-Func-05	Service Functions	... be able to replace defective network devices so that communication is continued and without major configuration efforts.	Improve defect handling and maintenance. In maintenance scenarios, an exchange of a faulty asset should be as easy as possible.	–
ComStackReq-Mngt-Func-06	Service Functions	... be able to add new end devices with support up to a pre-defined class-of-service, which determines e.g. bandwidth priority for the new end device.	The network will only guarantee performance characteristics and functionality up to the pre-defined class-of-service.	–

ID	Category	Requirement: “The Communication Infrastructure Technology Stack shall...”	Rationale / Comment	Covered by TSI2023
ComStackReq-Mngt-Func-07	Service Functions	... provide a service to list all configured network and end devices along with their identities and data models and/or services they provide.	–	–
ComStackReq-Mngt-Func-08	Service Functions	... provide a service that measures and offers the network's and its devices' key performance indicators (KPIs), such as bandwidth, to enable the identification of bottlenecks or other critical issues.	–	–
ComStackReq-Mngt-Func-09	Service Functions	... provide communication mechanisms for remote software updates of end devices and network devices.	–	–
ComStackReq-Mngt-Func-10	Service Functions	... provide communication mechanisms for remote parameter setting.	–	–
ComStackReq-Mngt-Func-11	Service Functions	... provide communication status of end devices.	–	–
ComStackReq-Mngt-Func-12	Service Functions	... provide configuration support to add/remove end devices.	–	–
ComStackReq-Mngt-Func-13	Service Functions	... provide a service that detects and reports unusual network activity.	–	–
ComStackReq-Mngt-Func-14	Service Functions	... provide a unique clock to synchronise all network and end devices.	–	–
ComStackReq-Mngt-Func-15	Service Functions	... provide identification/authentication procedures to prohibit unauthorized access to monitoring and management functions of the network.	–	–

3.4 NON-FUNCTIONAL SYSTEM REQUIREMENTS IN DETAIL

D23.2 [3] sets out a selection of non-functional system requirements in its chapter 2.4. The non-functional system requirements of WP24 shall be based on the work carried out in R2DATO's WP23. All previously defined non-functional requirements that are relevant to communication network management functionalities shall continue to be observed and upheld. In a manner consistent with the functional requirements, all non-suitable non-functional requirements that do not concern the network management functionalities shall be omitted.

Table 3: Non-functional system requirements for the network management

ID	Category	Requirement: "The Communication Infrastructure Technology Stack shall..."	Rationale / Comment	Covered by TSI2023
ComStackReq-Mngt-nonFunc-01	Interoperability	... come with compliance testing and certification processes in a lightweight way.	Foster interchangeability of end devices and second source approach. Lightweight means, 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.	–
ComStackReq-Mngt-nonFunc-02	Interoperability	...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.	–
ComStackReq-Mngt-nonFunc-03	Interoperability	... 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.	–

ID	Category	Requirement: “The Communication Infrastructure Technology Stack shall...”	Rationale / Comment	Covered by TSI2023
ComStackReq-Mngt-nonFunc-04	Compatibility	... provide mechanisms to enable / support backward compatibility management for any given set of functionalities.	Allow for future extension of protocol stacks or even hardware upgrades. Example: protocol version negotiation during a TLS handshake. Preserve compatibility while enabling innovation.	–
ComStackReq-Mngt-nonFunc-05	Portability	... be platform-independent (HW from SW). There shall be no dependency to a specific CPU model or platform or specific hardware.	Decoupling and flexibility in hard- and software.	–
ComStackReq-Mngt-nonFunc-06	Portability	... be physical transport medium independent (i.e., support communication links over fibre and over copper).	Decoupling from physical connection and openness for future technologies.	X
ComStackReq-Mngt-nonFunc-07	Portability	... support different physical topologies such as star, ring, ladder and hybrid combinations of these.	Support all possible topologies for different vehicle architectures.	X
ComStackReq-Mngt-nonFunc-08	Adaptability	... not imply the use of a specific programming language/environment.	Leave the flexibility to realize cost effective solutions and enable innovation.	–
ComStackReq-Mngt-nonFunc-09	Adaptability	... not enforce a specific operating system.	Leave the flexibility to realize cost effective solutions and enable innovation.	–
ComStackReq-Mngt-nonFunc-10	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-Mngt-nonFunc-11	Adaptability	... be deployable and usable on a variety of (component) device classes.	Leave the flexibility to realize cost effective solutions and enable innovation.	–
ComStackReq-Mngt-nonFunc-12	Security	... support authentication of communication entities.	Authentication is a prerequisite to make any authorization decision.	–
ComStackReq-Mngt-nonFunc-13	Security	... support the auditing of communication and management activities.	Enabling activity tracing in combination with (possibly external) trace infrastructure.	–

ID	Category	Requirement: “The Communication Infrastructure Technology Stack shall...”	Rationale / Comment	Covered by TSI2023
ComStackReq-Mngt-nonFunc-14	Security	... provide optional encryption functionality to allow for management data confidentiality. The necessary encryption functionality shall be available for all communication patterns and functions.	–	–
ComStackReq-Mngt-nonFunc-15	Security	... provide the possibility to enable the 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.	–
ComStackReq-Mngt-nonFunc-16	Security	... support integrated authorization of communication and management 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.	–
ComStackReq-Mngt-nonFunc-17	Security	... be resilient to (D)DoS attacks.	Base for consolidation	–
ComStackReq-Mngt-nonFunc-18	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 management applications that only need lower security levels.	–
ComStackReq-Mngt-nonFunc-19	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.	–
ComStackReq-Mngt-nonFunc-20	Cost	... avoid any unnecessary cost (e.g., royalties for standards).	Enable cost efficient solutions.	–

ID	Category	Requirement: "The Communication Infrastructure Technology Stack shall..."	Rationale / Comment	Covered by TSI2023
ComStackReq-Mngt-nonFunc-21	Adaptability	... able to provide different stages of management features to enable cost effective, "fit-to-the problem" solutions.	Enable cost efficient solutions and/or application-specific feature profiles.	–
ComStackReq-Mngt-nonFunc-22	Scalability	... have no restrictions for the scalability of management services and functions other than execution time and necessary memory (i.e., support an arbitrary number of managed nodes).	TCMS and CCS number of entities are defined in other standards and WP23 requirement definitions.	–
ComStackReq-Mngt-nonFunc-23	Maturity	... make use of functionality that is available on the market.	Avoid getting trapped by vapourware or delayed realization of standards.	–
ComStackReq-Mngt-nonFunc-24	Maturity	... make use of solutions that are available from multiple vendors.	No vendor lock in. Attractive price points.	–
ComStackReq-Mngt-nonFunc-25	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.	–
ComStackReq-Mngt-nonFunc-26	Maturity	... be supported by a community approach.	Quality-in-use rises with support options being available.	–
ComStackReq-Mngt-nonFunc-27	Maturity	... be supported by commercial consulting services.	Quality-in-use rises with support options being available.	–

4 ELABORATION OF MANAGEMENT FUNCTIONALITY

This chapter builds upon the system requirements defined in the previous chapter, elaborating on the necessary management functionalities for the onboard communication network. As a preliminary measure, the network management functions are identified and catalogued. This process involves the exploration of the aspects and, consequently, the functionalities that are within the scope of management. This ensures a clear and focused approach to the exploration of the solution space. The results of the exploration of these management functionalities are presented in a structured approach according to the specific level given by the underlying user stories.

4.1 UNIVERSAL ADDITIVE EXPLANATORY NOTES

In preparation for the subsequent listings, we present definitions and terminology that apply to the descriptions in the following subsections on management functions.

Regarding technical constraints, Subset-147 asserts that the network is regarded as a black box, signifying that its internal mechanisms and functionalities are obscured and not subject to direct management or specification. Consequently, the network management functionality is scoped to focus exclusively on the end devices and their interfaces, ensuring compliance with the Subset-147 standard while enabling effective control and monitoring at the system boundaries.

The specification level (FIS versus FFFIS) of each user story is determined based on its functional relevance and integration depth. User stories that describe system-level interactions and behaviours are assigned to the Functional Interface Specification (FIS) group, whereas those that detail internal functional flows and implementation-specific aspects are assigned to the Form, Fit, and Function Interface Specification (FFFIS) group. This distinction ensures clarity in traceability of requirements and subsequent system design. The allocation of a user story to the FIS group signifies an expanded system-level responsibility and the potential for cross-system ramifications. Conversely, FFFIS assignments generally reflect localised functionality with restricted external dependencies. The overall grouping of user stories in these two categories is given in Table 4.

Table 4: Designation which user stories are associated with FIS and FFFIS specification level

User Story Specification level	User Stories selected for network management
FIS Functional Interface Specification	10002 , 10005 , 10017 , 10025 , 10026 , 10033 , 10039 , 10041 , 10042 , 10045 , 10051 , 10053
FFFIS Form, Fit, and Function Interface Specification	10004 , 10010 , 10012 , 10013 , 10015 , 10022 , 10024 , 10029 , 10030 , 10031 , 10032 , 10038 , 10050

The identified management functionalities are subsequently presented in tables, each of which is identified by the name of the network functionality under consideration and links to the corresponding user stories that define their purpose and scope. The descriptions in the tables delineate the fundamental technical constraints that govern the operation of each functionality, including limitations imposed by standards such as Subset-147.

4.2 MANAGEMENT FUNCTIONALITY RELATED TO PROCESS DESCRIPTIONS

This subsection outlines the abstract process descriptions that govern the management of the onboard communication network, providing a high-level conceptual framework for its operation. These descriptions define the sequences and interactions required to achieve the desired management outcomes, linking directly to the user stories.

Table 5 lists the network management functionality as a process description to add a new device to the network.

Table 5: Management functionality to add a new end device to the network

Network Management Functionality	Linked User Stories
<i>Add new or differing end devices to the network</i>	10005 , 10025 , 10026 , 10039
<ul style="list-style-type: none"> ▪ The train manufacturer will provide an abstract process description containing the content that will be provided. The specification of the process description will be provided by the train manufacturer based on the abstract process description. The process description will also detail device obsolescence and maintenance as well as conformity of devices (e.g. proven via certifiable lab and/or conformance tests). ▪ The process description shall be valid both for (1) adding completely new devices to the network and (2) replacing faulty/defective devices with different hardware or the same hardware but different software/firmware versions. ▪ Current homologation status of the network is immune to new devices being added. ▪ The network will only guarantee performance characteristics and functionality up to the pre-defined class-of-service (e.g. if a best-effort device is added, it will not be given any performance guarantee). ▪ Cross-interferences of the homologation statuses on the application level are out-of-scope. 	

Table 6 lists the network management functionality as a process description to allow/forbid data exchanges.

Table 6: Management functionality to allow/forbid data exchanges

Network Management Functionality	Linked User Stories
<i>Allow / forbid data exchanges</i>	10010
<ul style="list-style-type: none"> ▪ Inherently provided by the network and its underlying network functions (i.e. VLANs) ▪ We do not use MAC address filtering on Layer-2 ▪ VLANs are assigned during registration of a network device <ul style="list-style-type: none"> ○ VLANs need to be added and configured 	

4.3 MANAGEMENT FUNCTIONALITY RELATED TO INTERFACE DESCRIPTIONS

Moving from the conceptual processes and the outcomes of the requirement analysis process, this subsection lists the management functionality that is related to the various interfaces required for network management. The description is divided into management functionality that is related to functional interface specifications and technical interface specifications.

4.3.1 Management Functionality related to Functional Interface Specifications

The following descriptions specify the capabilities and services to support the defined (FIS-related) management functionalities.

Table 7 lists the network management functionality to get the health status of network devices.

Table 7: Management functionality to get network device health status

Network Management Functionality	Linked User Stories
<i>Health Status</i>	10002 , 10025 , 10026
<ul style="list-style-type: none"> ▪ Shall include the minimal viable example of a device health status and the granularity of status information ▪ For granularity level “network device”: <ul style="list-style-type: none"> ○ Result of Boolean intersection of individual device health indicators 	

Table 8 lists the network management functionality for event notifications to support various functions (e.g. add, remove, enable and disable devices).

Table 8: Management functionality covered by event notifications

Network Management Functionality	Linked User Stories
<i>Event Notification</i>	10004 , 10017 , 10029
<ul style="list-style-type: none"> ▪ List of suggested event notifications to cover functionality derived from the user stories: <ul style="list-style-type: none"> ○ Device added (US: 10004, 10025, 10026) ○ Device removed (US: 10004, 10030) ○ Device enabled (US: 10004) ○ Device disabled (US: 10004) ○ Unusual traffic detected (US: 10017) ○ Failed IEEE 802.1X authorization (US: 10029) 	

Table 9 lists the network management functionality for polling network KPIs.

Table 9: Network functionality for polling network KPIs

Network Management Functionality	Linked User Stories
<i>Network Key Performance Indicators</i>	10033
<ul style="list-style-type: none"> ▪ List of suggested KPI categories: 	

- Traffic and bandwidth KPIs (e.g. throughput in bits per second, queue lengths)
- Error and quality KPIs (e.g. dropped packets and CRC errors)
- Performance usage KPIs (e.g. RAM and CPU utilization)
- Availability KPIs (e.g. link status, up- or downtime)
- Security related KPIs (e.g. unauthorized access attempts)

4.3.2 Management Functionality related to Technical Interface Specifications

Building on the requirements and functional definitions, this subsection provides the network management functionality that is related to the technical specifications for the FFFIS-related management interfaces. In terms of security, all subsequently described interfaces shall be authenticated and authorised.

Table 10 lists the network management functionality for adding new devices.

Table 10: Management functionality to add a new device

Network Management Functionality	Linked User Stories
Add Device	10004 , 10025 , 10026
<ul style="list-style-type: none"> ▪ Device shall be usable on a specific network switch port ▪ Inform other subsequent services via publishing an event to inform recipients: <ul style="list-style-type: none"> ○ Authentication, Authorization, DNS, DHCP, Audit ▪ Device will be added to the “inventory” (our assumption that such an inventory exists) 	

Table 11 lists the network management functionality for removing devices.

Table 11: Management functionality to remove a device

Network Management Functionality	Linked User Stories
Remove Device	10004 , 10025 , 10026 , 10030
<ul style="list-style-type: none"> ▪ Device shall be removed from a specific network switch port ▪ Inform other subsequent services via publishing an event to inform recipients: <ul style="list-style-type: none"> ○ Authentication, Authorization, DNS, DHCP, Audit ▪ Device will be removed from the “inventory” 	

Table 12 lists the network management functionality for blocking a port.

Table 12: Management functionality to block a port

Network Management Functionality	Linked User Stories
Block Port	10012 , 10030
<ul style="list-style-type: none"> ▪ Network switch port shall be “deactivated” ▪ Default state for unused ports 	

- Used to “disable” a port via a management call

Table 13 lists the network management functionality for unblocking a port.

Table 13: Management functionality to unblock a port

Network Management Functionality	Linked User Stories
<i>Unblock Port</i>	10012 , 10025 , 10026
<ul style="list-style-type: none"> ▪ Network switch port shall be “activated” (open for devices to connect and use IEEE 802.1X to authenticate/authorize themselves) ▪ Used to “enable” a port via a management call ▪ Note: does not omit the need for subsequent IEEE 802.1X processes 	

Table 14 lists the network management functionality for updating firmware, software and configurations.

Table 14: Management functionality to update firmware, software or configuration

Network Management Functionality	Linked User Stories
<i>Firmware/Software/Config Update</i>	10015 , 10025 , 10026 , 10050
<ul style="list-style-type: none"> ▪ List of (software) updates for corresponding end device(s) that will be exchanged <ul style="list-style-type: none"> ○ Shall include release notes for the software package ▪ The fault tolerant (e.g., via an A/B, respectively old/new approach) update mechanism must be aligned in accordance with Secure Component Specification when specification is available. 	

Table 15 lists the network management functionality for querying the network inventory.

Table 15: Management functionality to get the new network inventory

Network Management Functionality	Linked User Stories
<i>Get Inventory</i>	10031 , 10032
<ul style="list-style-type: none"> ▪ Request information from the central network inventory <ul style="list-style-type: none"> ○ Request shall include filter possibilities ▪ Response shall include: <ul style="list-style-type: none"> ○ Device identities, data models, provided services, device health state, network health state 	

4.4 INHERENTLY GIVEN NETWORK FUNCTIONALITY

Beyond the newly defined management functionalities, this subsection identifies and describes those network functionalities that are inherently present or pre-existing within the onboard communication

network as defined in Subset-147. While not requiring new management specification, their presence is acknowledged for a complete understanding of the system's capabilities within the solution space.

Table 16 lists the inherently given network functionality for blocking network access.

Table 16: Network functionality to block network access

Network Management Functionality	Linked User Stories
Network access blockade	10012
<ul style="list-style-type: none"> ▪ Network access blocked for unauthorised network end devices <ul style="list-style-type: none"> ○ Due to IEEE 802.1X (e.g. EAP-TLS, MAC address, ...) 	

Table 17 lists the inherently given network functionality for using traffic flow priorities.

Table 17: Network functionality to use traffic flow priorities

Network Management Functionality	Linked User Stories
<i>Traffic flow priorities</i>	10013
<ul style="list-style-type: none"> ▪ Traffic flow priorities support <ul style="list-style-type: none"> ○ Due to IEEE 802.1P (PCP value) and Class-of-Service 	

Table 18 lists the inherently given network functionality for using traffic flow profiles.

Table 18: Network functionality to use traffic flow profiles

Network Management Functionality	Linked User Stories
<i>Traffic flow profiles</i>	10013
<ul style="list-style-type: none"> ▪ Previously reserved traffic flows (due to added applications) added to the network <ul style="list-style-type: none"> ○ End devices are expected to use Class-of-Service (which are subsequently used to derive IEEE 802.1Q PCP values). ○ TOC provides traffic profiles (e.g., number of ports, input-/output bandwidth capacities, traffic priorities) so that proper sizing of the network is feasible for future use. 	

Table 19 lists the inherently given network functionality for limiting the protocol usage.

Table 19: Network functionality to limit protocol usage

Network Management Functionality	Linked User Stories
<i>Used protocol limitations</i>	10041
<ul style="list-style-type: none"> ▪ Only standards that are defined by future Subset-147 revisions shall be allowed. 	

Table 20 lists the inherently given network functionality for synchronizing time.

Table 20: Network functionality to synchronize time

Network Management Functionality	Linked User Stories
<i>Time synchronization</i>	10042
<ul style="list-style-type: none"> Secure Components Specification will provide a means to synchronize time in the network based on standardized and proven time synchronization protocols (e.g. NTS, NTP). 	

Table 21 lists the inherently given network functionality for identifying network components.

Table 21: Network functionality to identify network components

Network Management Functionality	Linked User Stories
<i>Network component identification via DNS/DHCP</i>	10045
<ul style="list-style-type: none"> Network component identification via DNS and DHCP are covered by future Subset-147 revisions and will be aligned with the Secure Component Specification. 	

Table 22 lists the inherently given network functionality for prohibiting unauthorized routing.

Table 22: Network functionality to prohibit unauthorized routing

Network Management Functionality	Linked User Stories
<i>Prohibit unauthorized routing activities between network segments</i>	10051
<ul style="list-style-type: none"> Subset-147 does only define an OSI Layer-2 network structure which interfaces between devices and switches, where switches make forwarding (not routing!) decisions for network traffic; routing between network segments or different security zones relies on additional components (i.e. security gateways) and are not covered by Subset-147. 	

Table 23 lists the inherently given network functionality to add a new safe function to the network.

Table 23: Network functionality to add new or update safe functionality to the network

Network Management Functionality	Linked User Stories
Add new or update safe functionality to the network	10038
<ul style="list-style-type: none"> The train manufacturer will provide a process description containing the initial requirements and the steps needed to add or update a safe functionality. The process description will be split into a configuration management (i.e. the precondition) and the runtime management part (the actual process to add/update the safe function). 	

4.5 ADDITIONAL FUNCTIONALITIES – OUT-OF-SCOPE OF SUBSET-147

This section briefly highlights additional potential management functionalities that, while relevant to the overall system, fall outside the defined scope of Subset-147 and thus outside the scope of this deliverable. Their inclusion here serves to provide a comprehensive overview of the solution space.

Table 24 lists the out-of-scope network functionality for supporting end device sleep power state.

Table 24: Network functionality to support end device sleep power state

Network Management Functionality	Linked User Stories
<i>End device sleep power state support</i>	10022
<ul style="list-style-type: none"> End devices shall not support bridge ports or switching functionality and thus have no need to inform additional devices (e.g. daisy-chained devices) about their sleep power state, putting end devices into sleep is out-of-scope. 	

Table 25 lists the out-of-scope network functionality for supporting end device wake-up power state.

Table 25: Network functionality to support end device wake-up power state

Network Management Functionality	Linked User Stories
<i>End device wake-up power state support</i>	10024
<ul style="list-style-type: none"> End devices shall not support bridge ports or switching functionality and thus have no need to inform additional devices (e.g. daisy-chained devices) about their wake-up power state, support for Wake-on-LAN is out-of-scope. 	

Table 26 lists the out-of-scope network functionality for supporting train network segment routing.

Table 26: Network functionality to support train network segment routing

Network Management Functionality	Linked User Stories
<i>Train network segment routing</i>	10051
<ul style="list-style-type: none"> Support for routing between different train network segments relies on (secure) gateways, whose management is not covered / out-of-scope for Subset-147. 	

5 CONCLUSIONS

The present document constitutes the Deliverable D24.1 *“Definitive and aligned requirements set for managing an Onboard Communication Network and concluded selection of suitable management functionality”*.

This deliverable builds on the previous work completed in R2DATO's WP23, leveraging the D23.1 [1] user stories to establish a shared foundation for defining the functional and non-functional requirements of the system. These requirements pertain to management functionalities for network devices within the common onboard network.

Out of all the user stories introduced in D23.1 [1], 25 were selected for further consideration within Task 24.1 because of their significance for network management. Following the selection of user stories, requirements were established and grouped into functional and non-functional system requirements in Sections 3.3 and section 3.4 respectively. A total of 15 functional requirements and 27 non-functional requirements were defined in D24.1. Based on these requirements and the required interface specification level for each user story, network management functions were identified, selected and catalogued in Chapter 4. The selection also included an exploration of all involved aspects of network management to identify the relevant communication functionality and determine boundary conditions.

In the next step, R2DATO's task T24.3 will define the technical management processes for the various stakeholders and define the actual technical interfaces that are going to be used for the network management. These specifications will form the basis for a laboratory demonstrator that will serve as a verification setup in task T24.4.

REFERENCES

- [1] Z. Ahmed, C. Daniel, E. De Paola, V. Knollmann, M. Moritz, K. Rahn, H. Roelle, S. Roullier, P. Rozijn and S. Schuerch, "D23.1 – List of user stories for the Onboard Communication Network," ERJU Innovation Pillar R2DATO, 2024.
- [2] R. Mattes, H. Roelle and S. Roullier, "D23.6 – Homologation concept for Onboard Communication Network (aka One Common Bus)," ERJU Innovation Pillar R2DATO, 2025.
- [3] Z. Ahmed, C. Daniel, E. De Paola, V. Knollmann, M. Moritz, K. Rahn, H. Roelle, S. Roullier, P. Rozijn and S. Schuerch, "D23.2 – Definitive and aligned requirements set for Onboard Communication Network and Basic Services," ERJU Innovation Pillar R2DATO, 2024.