OCORA

Open CCS On-board Reference Architecture

Functional Vehicle Adaptor (FVA)

High-Level Requirements

Revision History

Version	Change Description	Initials	Date of change
1.0	Official version for OCORA Delta Release	CG	17/06/2021
2.0	Official version for OCORA Release R1	CG	26/11/2021
3.0	Introduced modifications: • Formulation of the requirements has been updated based on the new guideline. • Added the "Acceptance Method" to each requirement. • OCORA-124: updated 'Rationale' and 'Remark' based on received feedback. • OCORA-134: updated 'Rationale' based on received feedback. • OCORA-605: updated 'Rationale' based on received feedback. • OCORA-606: updated 'Rationale' based on received feedback. • OCORA-609: updated 'Remark' based on received feedback.	CG	03/06/2022
4.0	Introduced modifications to be consistent with the architecture: • OCORA-120: updated interface designation. • OCORA-125: typo correction. • OCORA-136: updated interface designation. • OCORA-137: updated examples. • OCORA-138: updated interface designation. Version published the first time in OCORA Release R6.	CG	31/01/2025

Table of Contents

References

Reader's note: please be aware that the document ids in square brackets, e.g. [OCORA-BWS01-010], as per the list of referenced documents below, are used throughout this document to indicate the references to external documents. Wherever a reference to a TSI-CCS SUBSET is used, the SUBSET is referenced directly (e.g. SUBSET-026). OCORA always reference to the latest available official version of the SUBSET, unless indicated differently.

[OCORA-BWS01-010] – Release Notes

[OCORA-BWS01-020] – Glossary

[OCORA-BWS01-030] – Question and Answers

[OCORA-BWS01-040] – Feedback Form

[OCORA-BWS02-030] - Technical Slide Deck

[OCORA-BWS03-010] - Introduction to OCORA

[OCORA-BWS04-010] - Problem Statements

[OCORA-TWS01-030] – System Architecture

[OCORA-TWS04-010] - Functional Vehicle Adapter – Introduction

[OCORA-TWS04-013] – Functional Vehicle Adapter – Design Guideline

[OCORA-TWS05-010] – Requirements – Management Guideline

[EN 50126-1:2017-10] – Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process

[EN 50126-2:2017-10] – Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 2: Systems Approach to Safety

[EN 50128:2011-06] – Railway Applications – Communication, signalling and processing systems - Software for railway control and protection systems

[EN 50657:2017-08] - Railways Applications - Rolling stock applications - Software on Board Rolling Stock

[TSI CCS: 02016R0919] - EN - 16.06.2019 - 001.001 - 1: COMMISSION REGULATION (EU) 2016/919 of 27 May 2016 on the technical specification for interoperability relating to the 'control-command and signalling' subsystems of the rail system in the European Union

1 Introduction

1.1 Purpose of the document

The purpose of this document is to provide the collection of all D-level requirements for the component *Functional Vehicle Adaptor* (FVA) in a structured manner.

This document is addressed to experts in the CCS domain and to any other person, interested in the OCORA concepts for on-board CCS. The reader is invited to provide feedback to the OCORA collaboration and can, therefore, engage in shaping OCORA. Feedback to this document and to any other OCORA documentation can be given by using the feedback form [OCORA-BWS01-040] .

If you are a railway undertaking, you may find useful information to compile tenders for OCORA-inspired CCS building blocks, for tendering complete on-board CCS systems, or for on-board CCS replacements for functional upgrades or life-cycle considerations.

If you are an organization interested in developing CCS on-board building blocks according to the OCORA design principles, the information provided in this document can be used as input for your development.

1.2 Applicability of the document

The document is informative. Subsequent releases of this document will be developed based on a modular and iterative approach, evolving within the progress of the OCORA collaboration.

1.3 Context of the document

This document is published as part of an OCORA Release, together with the documents listed in the release notes [OCORA-BWS01-010] . Before reading this document, it is recommended to read the Release Notes [OCORA-BWS01-010]. If you are interested in the context and the motivation that drives OCORA we recommend to read the Introduction to OCORA [OCORA-BWS03-010], and the Problem Statements [OCORA-BWS04-010]. The reader should also be aware of the Glossary [OCORA-BWS01-020] and the Question and Answers [OCORA-BWS01-030].

To better appreciate the D-level requirements provided in this document, it is suggested to previously read the Functional Vehicle Adapter introduction document [OCORA-TWS04-010] that illustrates the context of the Functional Vehicle Adapter itself.

1.4 Requirements Engineering Process

This OCORA requirement document is developed, using the Requirements Management Guideline [O CORA-TWS05-010]. The requirements are engineered in a top-down manner:

- As a starting point all **"Stakeholder Requirements"** towards the OCORA initiative **(A-Level requirements)** are captured and formalised.

- In a second step, the **"Program- and Design Requirements" (B-Level requirements)** are developed. These requirements define tools, processes, methodologies and design rules to be used within the program and to be considered during the system analysis and the system design/architecture work.

- As a next step, the A- and B-Level requirements are further developed in the MBSE analysis to become **"System Requirements" (C-Level requirements).**

- As part of the MBSE architecture work, building blocks are identified taking into account the MBSE analysis (C-Level requirements). All applicable requirements (A-Level, B-Level, and C-Level) are apportioned to the identified building blocks, resulting in **"Building Block Requirements" (D-Level requirements)**, forming the OCORA tender templates, together with the applicable program & design requirements.
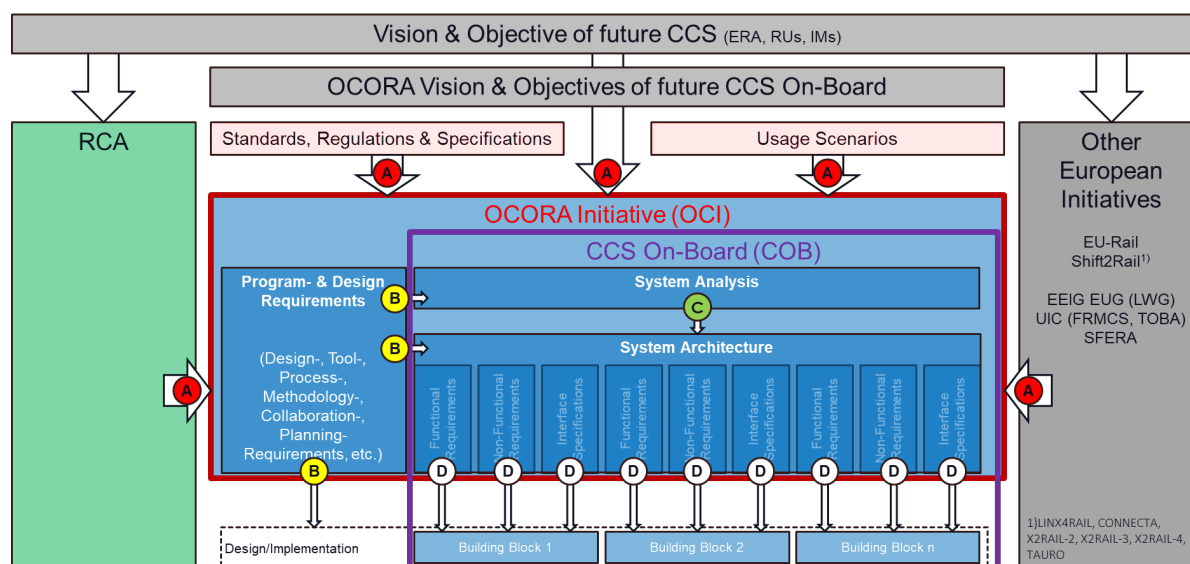

Figure 1 OCORA Requirements Engineering Process

Please note, that the A-Level requirements are applicable to the OCORA Initiative (OCI) while the B- and C-Level requirements are targeted towards the CCS On-Board System (COB) and its architecture. D-Level requirements are applicable to the respective building blocks.

2 Requirements

2.1 Functional

OCORA-120, D-Level - Interface to CCS on-board applications

The FVA shall implement the unified and standardized interface SCI-TCMS to the CCS on-board applications.

Status	✔ Approved
Classification	Requirement
Rationale	- Reuse of the same CCS on-board applications, independently from the vehicle type, is key regarding life-cycle management and certification efforts. - CCS on-board applications using the FVA unified and standardized interface are easily integrated on all different vehicle types by means of the FVA. - The same CCS on-board applications are reused on different vehicle types without software modification of the CCS on-board applications, only by adapting the provided configuration parameters of the CCS on-board applications.
Remark	The FVA of course can also have configuration parameters. FVA also implements the interfaces to the vehicle CI-TCMS, CI-WIOC (typically TCMS and / or wired connections), see separate requirement 📋OCORA-125 for the vehicle side.
Acceptance Method	Test

OCORA-121, D-Level - Variable mapping / configuration

The FVA shall implement the variable mapping / configuration between the two interfaces (refer to O CORA-120 - Interface to CCS on-board applications and the vehicle interface OCORA-125).

Status	✔ Approved
Classification	Requirement
Rationale	• This is to easily integrate CCS on-board applications into a vehicle by means of the FVA (specifics of the vehicle). • The variable mapping in the FVA allows to use the same CCS on-board applications in different vehicle types.
Remark	FVA is implemented according to the specific mapping / configuration needs, depending on the vehicle and its TCMS capabilities. Likewise, the FVA can be used to integrate into the vehicle through wired connections, see OCORA-125. Design guidelines for the variable mapping will be provided in document [OCORA-TWS04-013]
Acceptance Method	Test

OCORA-122, D-Level - CCS on-board side client support

The FVA shall support more than one client simultaneously on the CCS on-board side.

Status	✔ Approved
Classification	Requirement
Rationale	• There might be more than one CCS on-board application interacting with the vehicle through the FVA (e.g. ETCS on-board, 'ATO vehicle', etc.). All applications are supported that need interaction with the vehicle.
Remark	
Acceptance Method	Test

OCORA-123, D-Level - FIFO data processing

The FVA shall use a data processing mechanism which ensures data computation in the order as the data is received (first in first out - FIFO). The data shall be processed based on the sequence order in the global queue of incoming data (first in first out - FIFO).

Status	✔ Approved
Classification	Requirement
Rationale	• This is to ensure that the data and commands are received by the external sink system in the same order as they have been forwarded by the external sending system. Basically the order is not changed within the FVA. • FIFO concept: when multiple data packets from the same client are received, these data packets are processed in the same sequence order as these data packets were sent. • A global queue handles all data packets from the different clients. The data packets in the global queue are in the same sequence order as they have been received.
Remark	Ensure no retroactive effects in the processing of safety relevant data, see OCORA-137. Mitigation can be achieved by implementing the OCORA-124 - Priority processing for safety relevant data functionality.
Acceptance Method	Test

OCORA-124, D-Level - Priority processing for safety relevant data

The FVA shall support a priority handling mechanism for safety relevant data in order to fulfil ⬛OCOR A-137.

Status	✔ Approved
Classification	Optional Requirement
Rationale	• Function is needed in case the FVA has to manage safety relevant data (⬛ OCORA-137). • Provide a priority channel for different clients or message types depending on the safety relevance of the transmitted data. • This to ensure a higher availability by reducing the number of incidents due to failsafe impact.
Remark	• Dependency to ⬛OCORA-123 - FIFO data processing and ⬛OCORA-137 - Handling of safety relevant data. • Compulsory to ⬛OCORA-137 - Handling of safety relevant data. If the FVA manages safety relevant data, priority handling for safety relevant data shall be introduced. This independently from the FVA transforming the variables involved in a safety relevant function, or the FVA just acting as a gateway between the TCMS and the ETCS on-board for data enriched with a safety layer.
Acceptance Method	Test

OCORA-125, D-Level - Interface to vehicle

The FVA shall implement the (serial) interface CI-TCMS to the TCMS, or the interface CI-WIOC to the 'Wired I/O Control' peripheral, or both.

Status	✔ Approved
Classification	Requirement
Rationale	• The (serial) interface to the TCMS is needed by the FVA to exchange data with the vehicle. • The use of the 'I/O Ports' peripheral allows the FVA to interface with the vehicle by means of wired I/O connections.
Remark	It needs to be decided within the specific project which vehicle interface the FVA has to implement / use. Interface CI-TCMS is to a certain extent defined by SUBBSET-119 and -139. However, from the FVA concept it is not required that TCMS provides a SUBSET-119 and -139 compliant interface.
Acceptance Method	Test

OCORA-126, D-Level - Vehicle side client support

The FVA shall support more than one client simultaneously on the vehicle side.

Status	✔ Approved
Classification	Requirement
Rationale	• There is more than one client system interacting with the FVA on the vehicle side: e.g. one non-SIL TCMS, one SIL2 TCMS, interface CI-WIOC, passenger information system. All systems are supported that need interaction with the CCS on-board applications.
Remark	
Acceptance Method	Test

OCORA-606, D-Level - Definition, implementation and documentation of the handling of persistent differences occurring under specific circumstances

The FVA implementer shall define, implement and document how persistent differences occurring under specific circumstances are handled. For such cases the most stringent behaviour shall be applied in order to ensure safe response.

Status	✔ Approved
Classification	Requirement
Rationale	- As indicated in ⬛OCORA-125 the FVA can implement different independent interfaces to the vehicle for data acquisition. If the same information is acquired through different hardwired channels, or different serial channels, or a combination of hardwired and serial, then persistent differences between the channels can occur. - The FVA shall provide a deterministic behaviour also in exceptional cases.
Remark	Additional requirement in the context of ⬛OCORA-605. Of course, the implemented behaviour needs to be documented.
Acceptance Method	Analysis

OCORA-127, D-Level - Diagnostic and monitoring

The FVA shall provide monitoring and diagnostics information to a diagnostic and monitoring on-board component according to the respective interface specification.

Status	✔ Approved
Classification	Requirement
Rationale	• In order to analyse the FVA behaviour and performance during development, test and operation, a diagnostic and monitoring interface is vital. • When commissioning or updating a vehicle, the diagnostic and monitoring information simplifies the test activities. • The diagnostic data includes the information that is needed to verify that the correct version of software, configuration, etc. is installed.
Remark	The diagnostic and monitoring information can be used on-board (on-board access point) or remotely (from off-board). The diagnostic and monitoring information includes the version of software, configuration, etc.
Acceptance Method	Test

OCORA-128, D-Level - Publishing variable values

The FVA shall publish the status and the values of the different variables processed by the FVA.

As part of the diagnostic and monitoring function (📋OCORA-127) the FVA shall provide the status and the values of the different variables processed by the FVA.

Status	✔ Approved
Classification	Optional Requirement
Rationale	- When commissioning or updating a vehicle, the variable value information simplifies the test activities. - This information allows to be more efficient when verifying vehicle functions or analysing issues.
Remark	The variable values information could be used on-board only (on-board access point).
Acceptance Method	Test

OCORA-129, D-Level - Static update process

The FVA shall provide a static update process (when vehicle is out of operation) to a configuration and maintenance on-board component according to the respective interface specification. The update process involves the installation of at least one new file.

Status	✔ Approved
Classification	Requirement
Rationale	- The ability of updating the FVA is essential for an efficient life cycle management. - The FVA update process to only occur when the vehicle is out of operation to prevent malfunctioning of the vehicle.
Remark	The update process via a configuration and maintenance on-board component can be used on-board (on-board access point) or remotely (from off-board).
Acceptance Method	Test

OCORA-130, D-Level - On-board variable value simulation for test purposes

For the system engineer the FVA shall support the simulation function (induce a specific variable value). The function shall be available on-board, when the system engineer is connected to the FVA on-board the vehicle.

Status	✔ Approved
Classification	Optional Requirement
Rationale	• When working on-board for commissioning or updating activities, the simulation function simplifies the test activities. • This function allows to be more efficient when verifying vehicle functions or analysing issues.
Remark	Dependency to ⬚OCORA-131 - Special state for simulation and ⬚OCORA-132 - Cancellation of induced values.
Acceptance Method	Test

OCORA-131, D-Level - Special state for simulation

The simulation function shall only be available in a special state of the FVA.

Status	✔ Approved
Classification	Optional Requirement
Rationale	• To prevent malfunctioning of the vehicle due to simulation, this function is only available in a special state of the FVA.
Remark	Compulsory to ⬚OCORA-130 - On-board variable value simulation for test purposes. To be evaluated how the FVA can assess if simulation (special state) is permitted. For instance, it could be activated through a special switch on-board.
Acceptance Method	Test

OCORA-132, D-Level - Cancellation of induced values

When the simulation activity is terminated (system engineer is disconnected) the induced values shall be cancelled.

The FVA shall store the variable values when simulation starts. It then shall reuse the stored variable values, when simulation is terminated, and shall evaluate the variable values from the sources as configured.

Status	✔ Approved
Classification	Optional Requirement
Rationale	- When simulation activity is terminated the FVA no longer processes the induced values but uses the values coming from the real systems. - For data that is not updated periodically the original value is stored when simulation is started, so that is can be applied when simulation is terminated.
Remark	Compulsory to 📦OCORA-130 - On-board variable value simulation for test purposes and 📦OCORA-131 - Special state for simulation.
Acceptance Method	Test

2.2 Non-Functional

OCORA-133, D-Level - Component acting at Application Layer level (OSI layer 7)

The FVA shall be a component acting at Application Layer level (OSI layer 7) and is therefore supplied as a "software" component that has no wired in- or output interfaces.

Status	✔ Approved
Classification	Optional Requirement
Rationale	The FVA runs on an existing processing unit where other functions are also executed. If possible it should not run on a dedicated hardware to minimize the costs.
Remark	Intention is that the FVA is supplied as a "software" component, independent from the hardware.
Acceptance Method	Design Review

OCORA-134, D-Level - Supported safety integrity level (SIL)

The FVA shall consist of two independent parts: a non-safe part and a safe part.

Status	✔ Approved
Classification	Requirement
Rationale	- The safe part shall only be implemented when this is required in the specific project. - The non-safe part of FVA is a leaner and more flexible implementation. This means that it is easier to introduce modifications in case these are needed. - The independency allows introducing modifications in the non-safe part without affecting the safe part and its accreditation / documentation. - The safe part of FVA handles the variables that are involved in safety relevant functions. This in case there is no safety layer between CCS on-board and TCMS side, or the variables involved in a safety relevant function need to be transformed within the FVA, or the TCMS does not provide the functions in an adequate SIL (i.e. FVA needs to provide it by means of wired I/O connections).
Remark	The SIL allocation for the safe part has to be evaluated in the specific project based on the need for the specific vehicle. The objective is that the FVA does not provide functions higher than SIL2.
Acceptance Method	Design Review

OCORA-135, D-Level - Development process

The FVA shall be implemented according to the development process defined in EN 50126, EN 50128 and EN 50657.

Status	✔ Approved
Classification	Requirement
Rationale	• The FVA is deployed on-board railway vehicles. It is ensured that functional completeness and prevention of systematic failures are achieved by the development process to the required level. • It is a requirement that the software components installed in a CCS on-board system is implemented according to the development process defined in the CENELEC standards [EN 50126-1:2017-10], [EN 50126-2:2017-10], [EN 50128:2011-06] and [EN 50657:2017-08].
Remark	
Acceptance Method	Process Review

OCORA-136, D-Level - Performance / execution, processing latency

The FVA data processing cycle time shall be as fast as the fastest bus cycle time to which it is connected.

Generally, the maximum allowed transfer delay time in the FVA (including the time for computation logic) shall be 100 ms. Time period measured from the moment the data is received on one interface (e.g. SCI-TCMS) until it is processed and sent on the other interface (e.g. CI-TCMS).

Status	✔ Approved
Classification	Requirement
Rationale	- The data processing cycle time guarantees a maximum data processing delay between the different interfaces that in the worst case is 3 times the fastest bus cycle time ([1]see 'Remark' section for explanation). - The different vehicle functions need to rely on a maximum data exchange time between the CCS on-board and the vehicle (typically the TCMS). The actual time a data exchange needs, may vary, but the system must be able to react in case data is not exchanged within a known maximum exchange time. - Deterministic computing time is key for the FVA implementation. This is used when it is imperative that an event be reacted to within a strict deadline.
Remark	SUBSET-041 for ETCS on-board requires: < 1 sec. delay between receiving of a balise message and applying the emergency brake. In SS-119 the maximum cycle time for the fastest signals is defined with 100 ms (for ECN). Furthermore, in 4.2.3.6 the additional transfer delay introduced due the implementation of a gateway shall be below 200ms (worst case). From a CCS on-board application perspective there is a need to rely on a maximum reaction time. [1]First cycle elapses if FVA finishes reading just before clients writes. Second cycle elapses for the data processing. Third cycle elapses if FVA writes just after client finishes reading.
Acceptance Method	Test

OCORA-137, D-Level - Handling of safety relevant data

The FVA implementation shall ensure processing of safety relevant data (e.g. Sleeping Mode or Train Integrity) without retroactive effects.

Status	✔ Approved
Classification	Requirement
Rationale	- Safety relevant data shall be processed without being affected by the treatment of not safety relevant or less time sensitive data. - It shall be avoided that safety relevant data is delayed what causes a failsafe impact (typically activation of Emergency Brake and Traction Cut-Off).
Remark	
Acceptance Method	Certification

OCORA-605, D-Level - Proper handling of different channels on the interface to the vehicle

The design of the FVA shall not lead to a malfunctioning or reduced availability of the whole system due to a temporary information inconsistency during data acquisition. Basically, the design of the FVA shall consider the temporary information inconsistency due to the delay between independent channels.

Status	✔ Approved
Classification	Requirement
Rationale	- As indicated in OCORA-125 the FVA implements different independent interfaces to the vehicle for data acquisition. If the same or related information is acquired through different channels, then it may occur that there are some timing differences between the independent channels (more latency on one channel compared to the other, timing shifts are not constantly the same but can dynamically change). As a consequence there is a delay between the information acquired through the independent channels. - Acquisition through different and independent channels might be needed. Such an implementation shall not have an impact on the performance of the whole system. - Goal is to have a system that runs as smooth as possible
Remark	Additional requirement in the context of OCORA-125.
Acceptance Method	Test

OCORA-138, D-Level - Compliance with Ethernet CCS Consist Network (CCN)

In case the computation unit, on which the FVA runs, is connected to the Ethernet CCS Consist Network (CCN) then the interface shall comply with the correspondent specification for the Ethernet CCS Consist Network (CCN).

Status	✔ Approved
Classification	Requirement
Rationale	• The FVA and its environment comply with the OCORA architecture and the TSI CCS.
Remark	This is the new SUBSET-147.
Acceptance Method	Test

OCORA-139, D-Level - Adaptation to cycle times of the connected domains

The computation unit, on which the FVA runs, shall adapt to the different bus/network cycle times to which it is connected. These buses / networks are in CCS on-board and TCMS domains.

Status	✔ Approved
Classification	Requirement
Rationale	• The computation unit, on which the FVA runs, is connected to the different domains CCS on-board and TCMS that potentially have different bus cycle times. The different connections to these domains adapt to the different cycle times of the busses / networks so that FVA can properly communicate with the different domains.
Remark	
Acceptance Method	Test

OCORA-607, D-Level - Reliability of the FVA

The computation unit, on which the FVA runs, shall comply with the following reliability:

- Minor failure: MTBF < 8'000 hours.

- Reduced service failure: MTBF < 300'000 hours.

- Immobility failure: MTBF < 2'700'000 hours.

The mission profile for these values is defined in document 02S126 version 6 (ERA informative specification).

Status	✔ Approved
Classification	Requirement
Rationale	- A minor failure of the FVA hardware could lead to a warning information requiring service intervention within a failure specific period to prevent reduced performance. - A failure of the FVA hardware could lead to a reduced service with the consequence of a reduced performance. - A failure of the FVA hardware could lead to immobility, for instance in case of a transition of the ETCS on-board into the system failure (SF) mode.
Remark	The FVA hardware reliability to be coherent with the reliability of the CCS on-board functions (e.g. ETCS on-board). Values taken from document 02S126 version 6 (ERA informative specification).
Acceptance Method	Design Review

OCORA-608, D-Level - Cyber security

The FVA shall be included in the cyber security considerations made at CCS on-board and / or vehicle level.

Status	✔ Approved
Classification	Requirement
Rationale	The data handled in the FVA can be sensitive regarding the vehicle behaviour. It has therefore to be prevented that it can be deliberately manipulated by not appropriate people.
Remark	For the different activities that involve the FVA, cyber security issues at CCS on-board and / or vehicle level need to be considered and prevented.

Acceptance Method	Design Review

OCORA-609, D-Level - Expandability to support future extensions / modifications

The design of the FVA shall allow implementing modifications or further functions in the FVA non-safe part with reasonable effort (impact on costs).

This means that certification of the FVA safe part shall not be affected.

Status	✔ Approved
Classification	Requirement
Rationale	- To handle the lifecycle of a whole train it is essential that extensions / modifications can be introduced with reasonable effort impact. - To deploy innovation, it is essential that extension / modifications can be introduced with reasonable effort impact.
Remark	Costs for the extension shall be in about the same proportion to the original overall costs as the number of modified or added functions relative to the total number of implemented functions.
Acceptance Method	Demonstration