

# OCORA

Open CCS On-board Reference Architecture

## Functional Vehicle Adaptor High-Level Requirements

This OCORA work is licensed under the dual licensing Terms EUPL 1.2 (Commission Implementing Decision (EU) 2017/863 of 18 May 2017) and the terms and condition of the Attributions- ShareAlike 3.0 Unported license or its national version (in particular CC-BY-SA 3.0 DE).



Document ID: OCORA-TWS04-011

Version: 1.0

Release: Delta

Date: 30.06.2021

## Revision History

Version	Change Description	Initials	Date of change
1.0	Official version for OCORA Delta Release	CG	17/06/2021
		-	

# Table of Contents

1	Introduction	5
1.1	Purpose of the document	5
1.2	Applicability of the document	5
1.3	Context of the document	5
1.4	Requirements Engineering Process	6
2	Requirements	7
2.1	Functional	7
2.2	Non-Functional	13

# References

Reader's note: please be aware that the document id's in square brackets, e.g. [OCORA-BWS01-010], as per the list of referenced documents below, is 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 compliant CCS building blocks, for tendering complete CCS system, or also for CCS replacements for functional upgrades or for life-cycle reasons.

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

## 1.2 Applicability of the document

The document is currently considered informative but may become a standard at a later stage for OCORA compliant on-board CCS solutions. 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 the OCORA Delta 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 [OCORA-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.

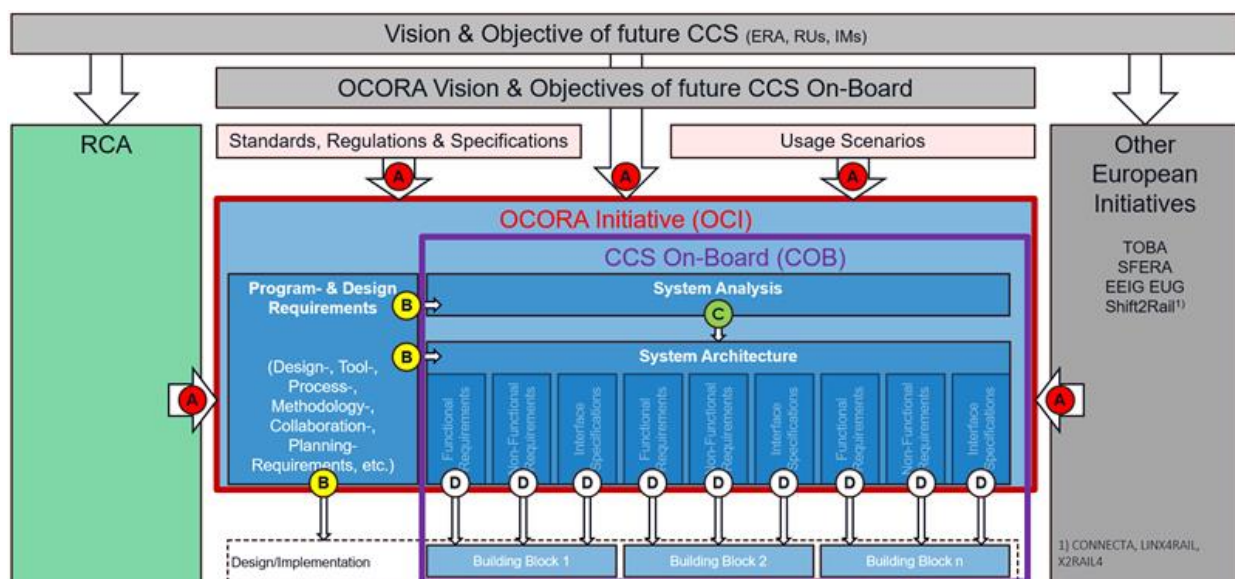


Figure 1 OCORA Requirements Engineering Process


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 implements the unified and standardized interface SCI-FVA to the CCS on-board applications.

Status	✓ Approved
Req. Class	Requirement
Rational	<ul style="list-style-type: none"> <li>• Reuse of the same CCS on-board applications, independently from the vehicle type, is key regarding life-cycle management and certification efforts.</li> <li>• CCS on-board applications using the FVA unified and standardized interface are easily integrated on all different vehicle types by means of the FVA.</li> <li>• 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.</li> </ul>
Remark	<p>The FVA of course can also have configuration parameters.</p> <p>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.</p>

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

The FVA implements the variable mapping / configuration between the two interfaces (refer to  OCORA-120 - [Interface to CCS on-board applications](#) and the vehicle interface  OCORA-125).

Status	✓ Approved
Req. Class	Requirement
Rational	<ul style="list-style-type: none"> <li>• This is to easily integrate CCS on-board applications into a vehicle by means of the FVA (specifics of the vehicle).</li> <li>• The variable mapping in the FVA allows to use the same CCS on-board applications in different vehicle types.</li> </ul>
Remark	<p>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.</p> <p>Design guidelines for the variable mapping will be provided in document <a href="#">[OCORA-TWS04-013]</a></p>



### OCORA-122, D-Level - Support several clients on CCS on-board side

The FVA supports more than one client simultaneously on the CCS on-board side

Status	✓ Approved
Req. Class	Requirement
Rational	<ul style="list-style-type: none"> <li>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.</li> </ul>
Remark	

### OCORA-123, D-Level - FIFO data processing

The data processing mechanism ensures that the data is processed in the sequence as the data exchange is triggered (FIFO) in the global queue.

Status	✓ Approved
Req. Class	Requirement
Rational	<ul style="list-style-type: none"> <li>This is to ensure that the data and commands are received by the receiving system in the same order as they have been forwarded by the sending system.</li> <li>FIFO concept: when multiple data packets from the same client are received, these data packets are processed in the same order as these data packets were sent.</li> <li>A global queue handles all data packets from the different clients. The data packets in the global queue are in the same order as they have been received.</li> </ul>
Remark	<p>Ensure no retroactive effects in the processing of safety relevant data, see  OCORA-137.</p> <p>Mitigation can be achieved by implementing the  OCORA-124 - <a href="#">Priority processing for safety relevant data</a> functionality.</p>



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

In case handling of safety relevant data (OCORA-137) cannot be ensured it is allowed to introduce a priority handling for safety relevant data in order to fulfil OCORA-137 - [Handling of safety relevant data](#).

Status	✓ Approved
Req. Class	Optional Requirement
Rational	<ul style="list-style-type: none"> <li>• Provide a priority channel for different clients or message types depending on the safety relevance of the transmitted data.</li> <li>• This to ensure a higher availability by reducing the number of incidents due to failsafe impact.</li> </ul>
Remark	Dependency to OCORA-123 - <a href="#">FIFO data processing</a> and OCORA-137 - <a href="#">Handling of safety relevant data</a> .

#### OCORA-125, D-Level - Interface to vehicle

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


Status	✓ Approved
Req. Class	Requirement
Rational	<ul style="list-style-type: none"> <li>• The (serial) interface to the TCMS is needed by the FVA exchange data with the vehicle.</li> <li>• The use of the 'I/O Ports' peripheral allows the FVA to interface with the vehicle by means of wired I/O connections.</li> </ul>
Remark	<p>It needs to be decided within the specific project which vehicle interface the FVA has to implement / use.</p> <p>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.</p>


### OCORA-126, D-Level - Support several clients on vehicle side

The FVA supports more than one client simultaneously on the vehicle side


Status	✓ Approved
Req. Class	Requirement
Rational	<ul style="list-style-type: none"> <li>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.</li> </ul>
Remark	


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

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 channels, then some delay between the channels can occur. This should not lead to a malfunctioning or reduced availability of the system.

Status	✓ Approved
Req. Class	Requirement
Rational	<ul style="list-style-type: none"> <li>Acquisition through different and independent channels might be needed. This does not have an impact on the performance of the whole system.</li> <li>Goal is to have a system that runs as smooth as possible</li> </ul>
Remark	Additional requirement in the context of  OCORA-125.

### OCORA-606, D-Level - Define and document how to handle persistent differences occurring in specific circumstances

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, then persistent differences between the channels can occur. For such cases the most stringent behaviour must be applied in order to ensure safe response.

Status	✓ Approved
Req. Class	Requirement
Rational	<ul style="list-style-type: none"> <li>The FVA must provide a deterministic behaviour also in exceptional cases.</li> </ul>
Remark	Additional requirement in the context of  OCORA-605. Of course, the implemented behaviour needs to be documented.


### OCORA-127, D-Level - Diagnostic and monitoring

The FVA provides monitoring and diagnostics information to the DM according to the respective interface specification.

Status	✓ Approved
Req. Class	Requirement
Rational	<ul style="list-style-type: none"> <li>• In order to analyse the FVA behaviour and performance during development, test and operation, a diagnostic and monitoring interface is vital.</li> <li>• When commissioning or updating a vehicle, the diagnostic and monitoring information simplifies the test activities.</li> <li>• The diagnostic data includes the information that is needed to verify that the correct version of software, configuration, etc. is installed.</li> </ul>
Remark	<p>The DM information can be used on-board (on-board access point) or remotely (from off-board).</p> <p>The DM information includes the version of software, configuration, etc.</p>

### OCORA-128, D-Level - Publishing variable values

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

Status	✓ Approved
Req. Class	Optional Requirement
Rational	<ul style="list-style-type: none"> <li>• As part of the diagnostic and monitoring function (  OCORA-127) the FVA provides the status and the values of the different variables processed by the FVA.</li> <li>• When commissioning or updating a vehicle, the variable value information simplifies the test activities.</li> <li>• This information allows to be more efficient when verifying vehicle functions or analysing issues.</li> </ul>
Remark	The variable values information could be used on-board only (on-board access point).



### OCORA-129, D-Level - Static update process

The FVA provides a static update process (when vehicle is out of operation) to the DCM according to the respective interface specification. The update process involves the installation of at least one new file.

Status	✓ Approved
Req. Class	Requirement
Rational	<ul style="list-style-type: none"> <li>• The ability of updating the FVA is essential.</li> <li>• The FVA update process to only happen when the vehicle is out of operation.</li> </ul>
Remark	The update process via DCM can be used on-board (on-board access point) or remotely (from off-board).


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

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

Status	✓ Approved
Req. Class	Optional Requirement
Rational	<ul style="list-style-type: none"> <li>• When working on-board for commissioning or updating activities, the simulation function simplifies the test activities.</li> <li>• This function allows to be more efficient when verifying vehicle functions or analysing issues.</li> </ul>
Remark	Dependency to  OCORA-131 - <a href="#">Special state for simulation</a> and  OCORA-132 - <a href="#">Cancellation of induced values</a> .

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



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

Status	✓ Approved
Req. Class	Optional Requirement
Rational	<ul style="list-style-type: none"> <li>• To prevent malfunctioning of the vehicle due to simulation, this function is only available in a special state of the FVA.</li> </ul>
Remark	Compulsory to  OCORA-130 - <a href="#">On-board variable value simulation for test purposes</a> . 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.

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

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

The FVA stores the variable values when simulation starts. It then reuses the stored variable values when simulation is terminated and evaluates the variable values from the sources as configured.

Status	✓ Approved
Req. Class	Optional Requirement
Rational	<ul style="list-style-type: none"> <li>When simulation activity is terminated the FVA no longer processes the induced values but uses the values coming from the real systems.</li> <li>For data that is not updated periodically the original value is stored when simulation is started, so that it can be applied when simulation is terminated.</li> </ul>
Remark	Compulsory to  OCORA-130 - On-board variable value simulation for test purposes and  OCORA-131 - Special state for simulation.

## 2.2 Non-Functional

### OCORA-133, D-Level - FVA is a component acting at Application Layer level (OSI layer 7)

The FVA acts at Application Layer level (OSI layer 7) and is therefore supplied as a “software” component.

Status	✓ Approved
Req. Class	Optional Requirement
Rational	<ul style="list-style-type: none"> <li>The FVA runs on an existing processing unit where other functions are also executed. It should not run on a dedicated hardware.</li> </ul>
Remark	Intention is that the FVA is supplied as a “software” component, independent from the hardware.

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

The FVA consists of two parts: a non-safe part and a safe part.

The safe part to only be implemented when this is required in the specific project.

Status	✓ Approved
Req. Class	Requirement
Rational	<ul style="list-style-type: none"> <li>• The non-safe part of FVA handles most of the variables.</li> <li>• The non-safe part of FVA is a leaner and more flexible implementation, also in case modifications are needed.</li> <li>• 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).</li> </ul>
Remark	<p>The SIL allocation for the safe part has to be evaluated in the specific project based on the need for the specific vehicle.</p> <p>The objective is that the FVA does not provide functions higher than SIL2.</p>

#### OCORA-135, D-Level - Development process

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

Status	✓ Approved
Req. Class	Requirement
Rational	<ul style="list-style-type: none"> <li>• 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.</li> <li>• 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 <a href="#">[EN 50126-1:2017-10]</a>, <a href="#">[EN 50126-2:2017-10]</a>, <a href="#">[EN 50128:2011-06]</a> and <a href="#">[EN 50657:2017-08]</a>.</li> </ul>
Remark	

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

The FVA processing cycle time is as fast as the fastest bus cycle time to which it is connected. This data processing cycle time guarantees a maximum data processing latency between the different interfaces that in the worst case is 3 times the fastest bus cycle time (<sup>1</sup>see 'Remark' section for explanation).

Generally, the maximum allowed cycle time is 100 ms.

Time period measured from the moment the data is received on one interface (e.g. SCI-FVA) until it is processed and sent on the other interface (e.g. CI-TCMS).

Status	✓ Approved
Req. Class	Requirement
Rational	<ul style="list-style-type: none"> <li>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 takes, may vary, but the system must be able to react in case data is not exchanged within a known maximum exchange time.</li> <li>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.</li> </ul>
Remark	<p>SUBSET-041 for ETCS on-board requires: &lt; 1 sec. delay between receiving of a balise message and applying the emergency brake.</p> <p>In SS-119 the maximum cycle time for the fastest signals is defined with 100 ms (for ECN).</p> <p>From a CCS on-board application perspective there is a need to rely on a maximum reaction time.</p> <p><sup>1</sup>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.</p>

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

It is ensured that safety relevant data (e.g. Emergency Brake and Traction Cut-Off) is processed without retroactive effects.

Status	✓ Approved
Req. Class	Requirement
Rational	<ul style="list-style-type: none"> <li>Safety relevant data is processed without being affected by the treatment of not safety relevant or less time sensitive data.</li> <li>It is avoided that safety relevant data is delayed what causes a failsafe impact (typically activation of Emergency Brake and Traction Cut-Off).</li> </ul>
Remark	

### OCORA-138, D-Level - Compliance with CCN

In case the computation unit, on which the FVA runs, is connected to the CCN then the interface complies with the specifications of the CCN (interface 300).

Status	✓ Approved
Req. Class	Requirement
Rational	<ul style="list-style-type: none"> <li>The FVA and its environment comply with the OCORA architecture.</li> </ul>
Remark	

### OCORA-139, D-Level - Adapt to the cycle times of the different connected domains

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

Status	✓ Approved
Req. Class	Requirement
Rational	<ul style="list-style-type: none"> <li>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 connection to these domains adapts to the different cycle times of the busses / networks so that it can properly communicate with the different domains.</li> </ul>
Remark	



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

The computation unit, on which the FVA runs, complies 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
Req. Class	Requirement
Rational	<ul style="list-style-type: none"> <li>• 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.</li> <li>• A failure of the FVA hardware could lead to a reduced service with the consequence of a reduced performance.</li> <li>• 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.</li> </ul>
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).

### OCORA-608, D-Level - Cyber security

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

Status	✓ Approved
Req. Class	Requirement
Rational	<ul style="list-style-type: none"> <li>• 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.</li> </ul>
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.

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

The design of the FVA allows 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 is not affected.

Costs for the extension are 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.

Status	✓ Approved
Req. Class	Requirement
Rational	<ul style="list-style-type: none"> <li>• To handle the lifecycle of a whole train it is essential that extensions / modifications can be introduced with reasonable effort impact.</li> <li>• To deploy innovation, it is essential that extension / modifications can be introduced with reasonable effort impact.</li> </ul>
Remark	