OCORA

Open CCS On-board Reference Architecture

Functional Vehicle Adapter

Design Guideline

Document ID: OCORA-TWS04-013

Version: 2.10

Date: 09.06.2022

Revision history

Version	Change Description	Initial	Date of change
1.00	Official version for OCORA Delta Release.	ED+JG	30.06.2021
2.00	Updated for the OCORA Release R1: ▪ Updated references. ▪ Modifications to be consistent with other R1 documents. Official version for OCORA Release R1.	ED+JG	26.11.2021
2.10	Updated to the new OCORA document template, document content is unchanged. Version first published in OCORA Release R2.	CG	09.06.2022

Table of contents

Table of figures

Table of tables

References

Reader's note: please be aware that the numbers in square brackets, e.g. [1], 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.

[1] OCORA-BWS01-010 – Release Notes

[2] OCORA-BWS01-020 – Glossary

[3] OCORA-BWS01-030 – Question and Answers

[4] OCORA-BWS01-040 – Feedback Form

[5] OCORA-BWS02-030 – Technical Slide Deck

[6] OCORA-BWS03-010 – Introduction to OCORA

[7] OCORA-BWS04-010 – Problem Statements

[8] OCORA-TWS01-030 – System Architecture

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

[10] OCORA-TWS04-012 – Functional Vehicle Adapter - Standard Communication Interface Specification

[11] 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 signaling' subsystems of the rail system in the European Union, amended by Commission Implementing Regulation (EU) 2019/776 of 16 May 2019 L 139I

1 Introduction

1.1 Purpose of the Document

The purpose of the document is to specify a design guideline for the Functional Vehicle Adapter with the aim to provide to the reader:

- The description of a proposed approach and methodology used to develop the functional vehicle adapter and its configuration in a specific project.
- The description of the necessary documentation from vehicle side, required with the purpose of being capable to configure the functional vehicle adapter when approaching the task as a third party.
- The design guideline of the functional vehicle adapter for different CCS on-board applications.

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 [4].

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

If you are an organization interested in developing on-board 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.

All technical consideration in this document have been based considering the most recent status of the released subsets at the date of the last revision. In case of specific release dependencies this is written explicitly in the context.

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 [1]. Before reading this document, it is recommended to read the Release Notes [1]. If you are interested in the context and the motivation that drives OCORA we recommend to read the Introduction to OCORA [6], and the Problem Statements [7]. The reader should also be aware of the Glossary [2] and the Question and Answer [3].

The design guideline defined in this document is based on the OCORA approach for integrating the CCS on-board with the vehicle by means of a Functional Vehicle Adapter. Therefore, it is suggested to previously read the Functional Vehicle Adapter introduction document [9] that illustrates the context of the Functional Vehicle Adapter itself.

2 Approach and methodology for the FVA development

This chapter describes the approach and methodology when developing the Functional Vehicle Adapter and its configuration in a specific project.

2.1 The Functional Vehicle Adapter (FVA)

The main purpose of the FVA today is to make on-board CCS systems fully portable: any on-board CCS system with a CCN interface (interface: SCI-FVA) can be plugged to any FVA- equipped vehicle.

The FVA allows to separate the interfaces of the on-board CCS systems (in this document, we limit the discussion to the ETCS on-board and 'ATO Vehicle' components because in the current TSI, the interfaces between other functions and the train are not yet defined) from the vehicle interface.

The FVA is hence also the means of choice to concentrate all vehicle specific decisions in one place for the integrated OCORA architecture of the future.

Therefore, for the above reason the FVA is a central element of the OCORA strategy.

This allows also the definition of a stable interface to the ETCS on-board and 'ATO Vehicle' systems.

The proposed CCN (interface: SCI-FVA) provides a way for the CCS systems to provide true plug & play functionality with any vehicle that is equipped with an FVA.

The CCN (interface: SCI-FVA) provides:

- An interface to tell the CCS on-board about the capabilities of the specific vehicle, so that the CCS on-board can provide the appropriate functionality or decide that the functionalities of the systems are not compatible.
- An interface for data from the CCS on-board to the train
- An interface for data from the train to the CCS on-board.

The FVA is modular and parametrizable.

- Modularity: additional functions and interfaces can be added in a well- defined way.
- Parametrizable: the actual configuration of the FVA is achieved by means of a parameter set.

The FVA provides the following main functionality:

- Routing: Data are routed from the CCN (interface: SCI-FVA) to the standard interfaces (in the case of 'ATO Vehicle' and ETCS on-board as defined in [SUBSET-139] and [SUBSET -119], respectively). In all projects where the vehicle does not support or not fully support [SUBSET -119] and [SUBSET -139], a Specific Vehicle Interface (SVI) is used. The routing functionality is bidirectional: this enables to integrate various vehicle bus systems and low- level digital interfaces with the FVA, leaving the CCS CCN (interface: SCI-FVA) unchanged.
- Standardization of "optional" configurations: Some interfaces allow alternative implementations in the SUBSETs (for example serial/ hardwired). With the FVA, this is done by adding FVA hardwire modules and / or parametrization of the FVA routing tables. The CCN (interface: SCI-FVA) remains stable across all installations.
- Closure of functional gaps: the FVA (for ATO) provides an API to add functionality that the vehicle is not providing, but that is expected by the CCS. Again, this allows leaving the CCS CCN (interface: SCI-FVA) unchanged.
- Definition of static values: the FVA allows to statically define some of the values for data that are usually transmitted by the vehicle and are expected by the CCS. This allows for plug & play installation of CCS on-board systems on a wider range of vehicles that have no way of providing this data.

2.2 Approach

Based on the requirements for function, safety, and configurability, a high- level architecture for the FVA is proposed.

This architecture is described in section 3 in a top-down approach.

Section 4 then discusses the interface

For each function and the related interfaces, the architectural design decisions are described in the context of the requirements.

The architecture has been derived from detailed bottom-up analysis of the functional requirements and the relevant specifications. (more specifically the SUBSETs -026, -034, -080, -088, -119, -120, -125, and -139).

3 Proposed FVA Architecture

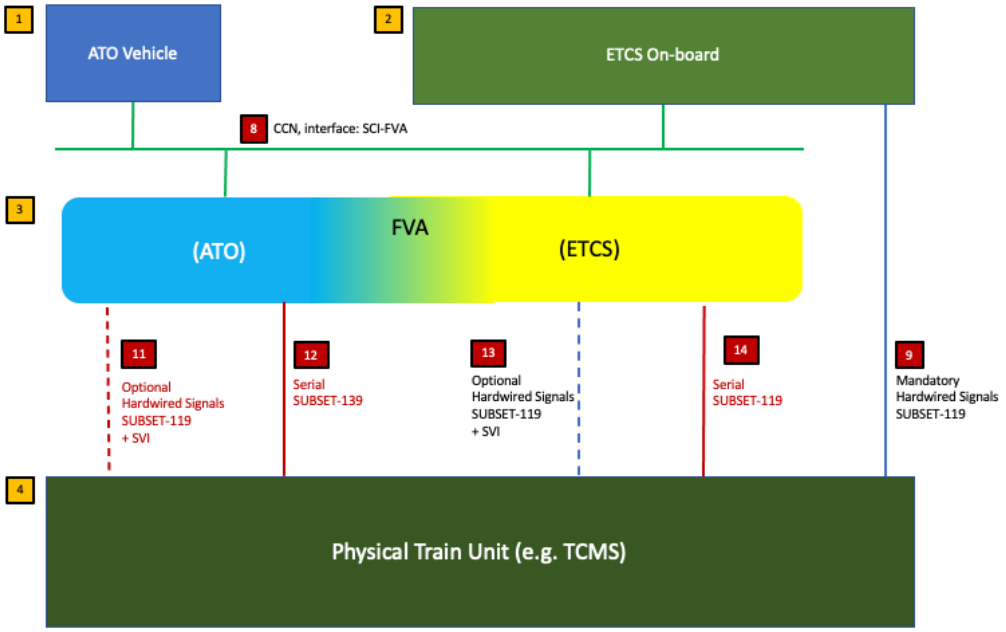

Figure 1: Proposed FVA architecture

3.1 Architecture description

3.1.1 Scope

While in future iterations of the OCORA architecture and platform the FVA scope might expand to other functional modules (for example vehicle location), we consider for this document release that essentially only the ETCS on-board component and the ‘ATO Vehicle’ component shall be connected with the TCMS using the standardized FVA approach.

Typically, the TCMS will have its own peripheral systems in order to access all required information and to issue all required commands.

Similarly, all ETCS peripheral systems will be connected to the ETCS on-board component only. The same applies to ‘ATO Vehicle’ peripheral systems.

3.1.2 Overview

The ‘ATO Vehicle’ and the ETCS on-board are connected to the TCMS through fully independent logical FVA channels.

The OCORA CCN (interface: SCI-FVA) provides independent logical channels that are separated from each other.

- The ‘ATO Vehicle’ component is connected to the ATO FVA with at least one NOT SAFETY CRITICAL channel on the CCN (interface: SCI-FVA).
- The ETCS on-board component is connected to the FVA (as far as ETCS functionality is concerned) with at least two independent SIL2 channels on the CCN (interface: SCI-FVA)
- The mandatory digital signals (Emergency Brake Release Command, Traction Cutoff Command, and Isolation) are directly hardwired from the ETCS on-board component to the TCMS and are hence out of scope of the ETCS FVA.

The ATO FVA can be connected to the TCMS through a combination of configurable signals on the following interfaces:

- Messages and variables as defined in [Subset-139] via serial interface
- Custom messages, variables, and hardwired signals via the specific interface (SVI ATO)

The functionality of the ATO FVA can be extended through the addition of optional functions using a standardized API. That way, the ATO FVA can be engineered to function correctly with both old vehicles that lack the functionality required by the ‘ATO Vehicle’ (for example vehicles that do not support a SUBSET-139 Traction/Brake Command) and with modern existing vehicles that feature modern control functions (such as AFB automatic traction/ brake control).

The FVA (as far as ETCS on-board functionality is concerned) can be connected to the TCMS through a combination of configurable signals on the following interfaces:

- Messages and variables as defined in [Subset-119] via serial interface
- Hardwired signals as defined in [Subset-119].
- Custom hardwired signals via the specific interface (SVI ETCS)

3.2 Functions

Note 1: The numbers in {brackets} refer to the numbered labels in Figure 1: Proposed FVA architecture

Note 2: Some safety analyses consider safety hypothesis which must be validated from the RU/Driver point of view. Therefore, in order to achieve harmonized interface, it requires that the RU/Driver accept and take into account these "harmonized constraints".

3.2.1 ATO Vehicle {1}

3.2.1.1 General

The ‘ATO Vehicle’ functionality contains the logic as described in [Subset-125].

In addition, specific interfaces (e.g. [Subset-126] and [Subset-130]) are part of the ‘ATO Vehicle’ scope.

For the ‘ATO Vehicle’, we only consider requirements pertaining to levels GoA1 and GoA2.

In the future, additional requirements for GoA3 and GoA4 might be added.

3.2.1.2 Safety

Currently ‘ATO Vehicle’ (in the context of ATO over ETCS) is not considered safety critical. Typically, NOT SAFETY CRITICAL requirements are assumed.

In the future, additional safety requirements may result as constraints for some GoA3 and / or GoA4 functions and the related interfaces. These future requirements are out of scope of this document release.

3.2.1.3 Configuration/ Modularity

As far as the vehicle interface is concerned, the ‘ATO Vehicle’ shall be fully generic.

Typically, the ‘ATO Vehicle’ interface of the CCN (interface: SCI-FVA) {8} shall provide all information that the ‘ATO Vehicle’ needs in order to configure its functionality to work with a certain vehicle, and to determine compatibility (version number, scope of functionality)

3.2.1.4 Interfaces

The ‘ATO Vehicle’ is connected to the FVA ATO via CCN (interface: SCI-FVA).

All other ‘ATO Vehicle’ component interfaces are described in the relevant ERA specifications (e.g. [Subset-130], [Subset-126])

3.2.2 ETCS on-board {3}

3.2.2.1 General

The ETCS on-board functionality contains the logic as described in [Subset-026].

In addition, specific interfaces (e.g., JDR, BTM, STM, GSM-R….) are part of the ETCS on-board scope.

3.2.2.2 Safety

ETCS on-board is a safety- critical ATP system.

A detailed safety analysis is provided in [Subset-088].

Beyond the failure modes described in [Subset-088], [Subset-120] provides a detailed analysis of the safety constraints exported from the ETCS on-board to the ETCS-TCMS interface as described in [Subset-119].

These requirements are taken into consideration as basis for the detailed architecture of the ETCS on-board to FVA interface.

3.2.2.3 Configuration/ Modularity

As far as the vehicle interface is concerned, the ETCS onboard shall be fully generic.

Typically, the ETCS interface of the CCN (interface: SCI-FVA) {8} shall provide all information that the ETCS onboard needs in order to configure its functionality to work with a certain vehicle, and to determine compatibility (version number, scope of functionality)

3.2.2.4 Interfaces

The ETCS on-board is connected to the FVA (as far as ETCS on-board functionality is concerned) via CCN (interface: SCI-FVA).

The mandatory digital signals (Emergency Brake Command, Traction Cut-off Command, and Isolation) are directly hardwired from the ETCS on-board component to the TCMS.

All other ETCS on-board unit interfaces are described in the relevant ERA specifications (e.g. [Subset-058], [Subset-026], [Subset-127], and others).

3.2.3 FVA {3}

3.2.3.1 General

The FVA ATO provides, via the CCN (interface: SCI-FVA), an abstraction of the vehicle functions to the ‘ATO Vehicle’ and the ETCS on-board.

3.2.3.2 FVA functionality for ‘ATO Vehicle’

Its main functions are:

- Route the ‘ATO Vehicle’ → TCMS data
    - As far as available on the TCMS, the interface as defined in [Subset-139] is used.
    - For any functionality that is not implemented through [Subset-139] on the TCMS, the extensible specific interface SVI is used.
- Route the TCMS → ‘ATO Vehicle’ data
    - As far as available on the TCMS, the interface as defined in [Subset-139] is used.
    - For any functionality that is not implemented through [Subset-139] on the TCMS, the extensible specific interface SVI is used.
- Reformat and transcode the data as needed.
- Provide information concerning the available TCMS functionality as implemented and configured through the FVA ATO to the ‘ATO Vehicle’.
- Where the TCMS doesn’t provide the required functionality to support the ‘ATO Vehicle’ functions, the data may be routed through the Optional ATO Functions module.

Safety

Currently the FVA ATO (in the context of ATO over ETCS) is not considered safety critical. Typically, NOT SAFETY CRITICAL requirements are assumed.

In the future, additional safety requirements may result as constraints for some GoA3 and / or GoA4 functions and the related interfaces.

Configuration/ Modularity

The FVA ATO software shall be generic.

All routing and reformatting settings are configurable using parameters.

For the SVI, it shall be possible to add digital and analogue input and output hardware modules.

Interfaces

The FVA ATO is connected to the ‘ATO Vehicle’ via CCN (interface: SCI-FVA).

The interface to the optional ATO functions is only defined at functional level.

> It is up to the supplier to choose an implementation that fulfils the functional requirements and ensures the required performance.

The FVA may be connected to the TCMS via serial interface as defined in [Subset-139] (Messages and variables)

The specific interface SVI ATO may be used to exchange custom messages, variables, and hardwired signals with the TCMS.

3.2.3.3 Optional FVA ATO Functions module

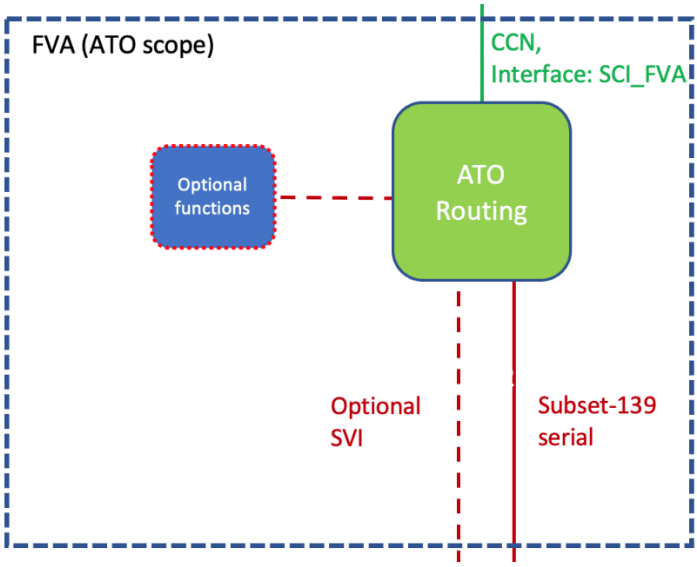

Figure 2: Optional FVA functions (ATO)

The Optional FVA ATO Functions module is an optional module of the FVA.

'ATO Vehicle' expects some minimal TCMS functionality. If the TCMS does not fulfil these requirements, then there is a gap. This gap can be closed by adding functions to the FVA via a defined API. This possibility removes the need to change 'ATO Vehicle' functionality or re-engineer the TCMS.

The FVA specification provides an API definition to integrate such additional functions.

Examples for optional FVA ATO functions include the implementation of low-level traction and brake control algorithms for vehicles that don't understand high- level commands like the traction/ brake message, but instead need a low-level direct control of power and/ or brake valves.

The implementation of this module is up to the supplier. It may be implemented as a software module on the ATO FVA or as one or more external hardware modules.

Safety

Currently the optional FVA ATO functions (in the context of ATO over ETCS) are not considered safety critical.

In the future, additional safety requirements may result as constraints for some GoA3 and / or GoA4 functions and the related interfaces. (GoA3/ GoA4 requirements are out of scope of this document release.)

Safety requirements may also result from functions implemented there. A safety analysis shall be carried out.

Configuration/ Modularity

The Optional ATO Functions module may be implemented either on one or more external controllers/ computers or be a software module on the FVA.

The functions themselves are not yet defined; they will typically be vehicle specific.

It could be considered to provide generic, parametrizable functions as a basis for vehicle- specific development.

Interfaces

The Optional ATO Functions interface to the FVA ATO is only defined on functional level. Data to and from the connected functions are routed through the FVA routing functionality, using the CCN (interface: SCI-FVA) on the 'ATO Vehicle' side and Subset-139 and / or the ATO SVI on the vehicle side. (Note: no hardwired signals are foreseen for the FVA- ATO)

It is up to the supplier to choose an implementation that fulfils the functional requirements and ensures the required performance.

3.2.3.4 FVA functions for ETCS

Its main functions are:

- Route the ETCS on-board → TCMS data
    - As far as available on the TCMS, the interface as defined in [Subset-119] is used.
    - For any functionality that is not implemented through [Subset-119] on the TCMS, the extensible SVI via freely configurable hardwired interfaces is used.
- Route the TCMS → ETCS on-board data
    - As far as available on the TCMS, the interface as defined in [Subset-119] is used.
    - For any functionality that is not implemented through [Subset-119] on the TCMS, the extensible SVI via freely configurable hardwired interfaces is used.
- Reformat and transcode the data as needed.
- Route the signals to and from optional hardwired interfaces as defined in [Subset-119] as needed
- Provide information concerning the available TCMS functionality as implemented and configured through the FVA ETCS to the ETCS onboard.

The primary hardwired signals for the ETCS on-board functions are not in the scope of the FVA.

Explanation: for variables that have a mandatory hardwired connection plus an optional one, we refer to the mandatory line as *primary*.

Direct hardwired connection shall be implemented for these signals (Emergency Brake Command, Traction Cut Off command and Isolation).

The secondary signals shall be handled by the FVA, which can be configured to route them either through serial connection or Subset-119-defined hardwired connection.

Safety

ETCS on-board is a safety- critical ATP system. In general, it is (as a whole) considered to be subject to SIL4 requirements. (this is a high-level view; it may be possible to identify functions with different safety requirements if implemented as modular system). A detailed analysis is provided in [Subset-088].

TCMS Systems are also subject to safety requirements: a detailed analysis is provided in [Subset-080].

[Subset-120] provides a safety argumentation for the [Subset-119] interface, which has been used as the basis for our FVA safety- related requirements.

No safety requirements for any signal/variable described in [Subset-120] exceed SIL2 requirements.

For the FVA this means that it will have to handle a mix of safe and unsafe signals and variables. A more detailed discussion, organised by functions, is provided below.

Configuration/ Modularity

The FVA ETCS software shall be generic.

All routing and reformatting shall be configurable using parameters.

For the SVI, it shall be possible to add digital input and output hardware modules.

Interfaces

The FVA (as far as ETCS functionality is concerned) is connected to the ETCS Onboard Unit via CCN (interface: SCI-FVA).

It can be connected to the TCMS through a combination of configurable signals on the following interfaces:

- Messages and variables as defined in [Subset-119] via serial interface
- Hardwired signals as defined in [Subset-119].
- Custom hardwired signals via the specific interface SVI ETCS

3.2.4 TCMS {4}

3.2.4.1 General

The TCMS is vehicle specific.

3.2.4.2 Safety

As the TCMS is vehicle specific, no general statement concerning safety requirements can be made in this document. [Subset-080] provides a detailed analysis of TCMS safety parameters.

3.2.4.3 For the FVA safety requirements, we use the TCMS related safety requirements as described in [Subset-120].

3.2.4.4 Configuration/ Modularity

Vehicle specific

3.2.4.5 Interfaces

For ETCS on-board functionality, the TCMS can be connected to the FVA through a combination of configurable signals on the following interfaces:

- Messages and variables as defined in [SUBSET-119] via serial interface
- Hardwired signals as defined in [SUBSET-119].
- Custom hardwired signals via the specific interface SVI ETCS

For ATP functionality, the TCMS can be connected to the FVA through a combination of configurable signals on the following interfaces:

- The FVA may be connected to the TCMS via serial interface as defined in [Subset-139] (Messages and variables)
- The specific interface SVI ATO may be used to exchange custom messages, variables, and hardwired signals with the TCMS.

4 FVA Interfaces

4.1 FVA ‘ATO Vehicle’

The FVA and the ‘ATO Vehicle’ are connected via the CCN (interface: SCI-FVA)

4.2 FVA ETCS on-board

The FVA and the ETCS on-board are connected via the CCN (interface: SCI-FVA)

4.2.1 General Safety considerations

A priori, the ETCS on-board and the TCMS are classified as safety critical systems.

[Subset-088] provides a detailed description of the fault tree analysis of the ETCS on-board.

[Subset-080] provides a detailed description of the fault tree analysis of the TCMS.

[Subset-120] describes safety considerations and -requirements for the interface between the ETCS on-board Unit and the TCMS. It distinguishes between:

- Data not concerned by safety requirements
- Data concerned by safety requirements, that may be communicated through serial interface alone with a defined max. tolerable failure rate (TFR) and a defined max. tolerable failure detection time (FDT).
- Data concerned by safety requirements, that shall be communicated through serial interface in combination with hardwired connection or by safe hardwired connection alone with a max. tolerable failure rate (TFR) and a defined max. tolerable failure detection time (FDT).
- Data concerned by safety requirements, that shall be communicated through serial interface in combination with hardwired connection or by safe hardwired connection alone with a max. tolerable failure rate (TFR) and a defined max. tolerable failure detection time (FDT), shall require two independent sources. For these data, the FVA shall provide the required independent signal paths.

4.2.2 Classification of functions and the related data according to Subset-120

Legend:

TR - Train

OBU - ETCS Onboard Unit

O - optional

M - mandatory

SIL - Safety Integrity Level

TFR - Tolerable Failure Rate

No	Functional I/O	Source	Hardwired	Serial*	Safety	SIL /TFR
1	Sleeping	TR	O	M	[Subset-120]: 3.2.1	SIL 1/2 TFR 1E-05 /h
2	Passive Shunting	TR	O	M	[Subset-120]: 3.2.2	SIL 1/2 TFR 1E-05 /h
3	Non- Leading	TR	O	M	[Subset-120]: 3.2.3	SIL 1/2 TFR 1E-05 /h
4	Isolation (of ETCS)	OBU	M	-	[Subset-120]: 3.2.4	Not safety-related
5	Service Brake Command	OBU	O	M	[Subset-120]: 3.3.1	Not safety-related
6	Brake Pressure	TR	-	M	[Subset-120]: 3.3.2	Not safety-related
7	Emergency Brake Command	OBU	M	M	[Subset-120]: 3.3.3	2x SIL2 independent 1E-07 /h
10	Regenerative Brake Inhibit	OBU	-	M	None	Not safety-related
11	Magnetic Shoe Brake Inhibit	OBU	-	M	None	Not safety-related
12	Eddy Current Brakes for Service Brake Inhibit	OBU	-	M	None	Not safety-related
13	Eddy Current Brakes for Emergency Brake Inhibit	OBU	-	M	None	Not safety-related
14	Special Brake Inhibit – STM Orders	OBU	O	M	None	Not safety-related
15	Special Brake Status	TR	O	M	[Subset-120]:3.3.6	Project-specific Potentially SIL4!
16	Additional Brake Status	TR	O	M	[Subset-120]:3.3.7	Not relevant for now

No	Functional I/O	Source	Hardwired	Serial*	Safety	SIL /TFR
17	Change of Traction System	OBU	-	M	None	Not safety-related
18	Powerless Section with Pantograph to be Lowered – Trackside Orders	OBU	-	M	None	Not safety-related
19	Pantograph – STM Orders	OBU	-	M	None	Not safety-related
20	Air Tightness – Trackside Orders	OBU	-	M	None	Not safety-related
21	Air Tightness – STM Orders	OBU	O	M	None	Not safety-related
22	Station Platform	OBU	-	M	[Subset-120]:3.4.4	Project-specific
23	Powerless Section with Main Power Switch to be Switched Off – Trackside Orders	OBU	-	M	None	Not safety-related
24	Main Power Switch – STM Orders	OBU	O	M	None	Not safety-related
25	Change of Allowed Current Consumption	OBU	-	M	None	Not safety-related
26	Traction Cut-Off	OBU	M	M	[Subset-120]: 3.4.8	SIL 1/2 1E-07 /h ≤ TFR < 1E-06 /h
27	Cab Status	TR	O	M	[Subset-120]: 3.5.1	SIL 1/2 TFR 1E-05 /h
28	Direction Controller	TR	O	M	[Subset-120]: 3.5.2	SIL 1/2 TFR 1E-05 /h
29	Train Integrity (to be harmonized)	TR	?	?	[Subset-120]: 3.5.3	Not implemented
30	Traction Status (only for STM)	TR	O	M	[Subset-120]: 3.5.4	Out of scope
31	Set Speed (for DMI indication)	TR	-	M	None	Not safety-related
32	Type of Train Data Entry	TR	O	M	None	Not safety-related
33	Train Data Information	TR	O (partial)	O	[Subset-120]:3.6.2	SIL 1/2 1E-7 /h - 1E-5 /h
34	National System Isolation	TR	O	M	[Subset-120]: 3.7	Out of scope

Table 1: Classification of Signals according to Subset- 120

4.2.3 Concepts

The basic concepts which are used for the design of the solution for each variable on the TCMS-ETCS interface of the FVA (as far as ETCS functionality is concerned) are listed in the following subsections:

4.2.3.1 FVA architecture

The FVA (as far as ETCS functionality is concerned) shall fulfil at least SIL2- requirements.

Note: The ETCS and TCMS remain responsible for the interpretation of the signals and variables.

4.2.3.2 Safety Integrity Level (SIL)

The safety integrity level is derived either directly from the hazard analysis or from Tolerable Failure Rate (TFR) data in [Subset-120].

The TFR ranges for the SIL levels, taken from best- practises from projects, have been provided from the related safety processes.

The Tolerable Failure Rate is for the overall function. It is up to the supplier to ensure that the integrity and

reliability measures of the FVA (in case it is implemented as a separate system) are chosen in a way that this requirement is fulfilled. This may require a higher SIL rating for the FVA in some cases.

As EN 51028 knows the following SIL levels for software:

- Out of scope (no SIL)
- SIL 0
- SIL1/2
- SIL3/4

The bold number indicates the SIL that is derived from the TFR from [Subset-120].

4.2.3.3 Self- test

Failure Detection Rate:

The following requirements have been directly taken from the hazard analysis in [Subset-120].

As the FVA is an active hardware/ software system, its functionality is subject to the same Failure Detection Rate

4.2.4 Requirements for (1) Mode Control: Sleeping

4.2.4.1 Architecture

This functionality requires two independent paths in the FVA.

SIL1/2. (For software, the process and V&V for SIL1 and SIL2 are identical. We therefore mention SIL1/2 here. The requirement for the hardware is indicated in the bold number in the Safety Integrity column in the table below.

Serial connection.

Optional hardwired connection (defined in [Subset-119])

For evaluation of the redundant signals, the rules from [Subset-119] apply unchanged. The “coding” section of this document provides tables with valid combinations of signal levels.

Signal		Safety Integrity Level	Periodic Self- Test Rate
T_SL_E_N	Hardwired (optional)	SIL**1**/2	>= 1 per min
TR_OBU_TrainSleep	Serial	SIL**1**/2	>= 1 per min
T_SL_E_I	Hardwired (optional)	SIL**1**/2	>= 1 per min
TR_OBU_TrainSleep_Not	Serial	SIL**1**/2	>= 1 per min

4.2.4.2 Configurability

As the hardwired connection is optional, in order to be configurable, the hardwired connection should also be actively controlled by software.

A separate SVI interface is not required, as the optional hardwired connection already covers this possible need.

4.2.4.3 Safety

General Safety Requirements

As the FVA provides software- controlled functionality, it may introduce errors. For this reason, appropriate

mitigation measures shall be implemented, including a self- test functionality. The minimum self- test rate has been indicated.

In case of a failure (inappropriate reception of faulty antivalent Sleeping signal / loss of Sleeping signal) ERTMS/ETCS on-board equipment shall memorize the fault. [Subset-120 5.1.3.1.1.1]

ERTMS/ETCS on-board shall not be able to switch to SL (Sleeping) mode as long as a failure (inappropriate reception of faulty antivalent Sleeping signal / loss of Sleeping signal) is memorized. [Subset-120 5.1.3.1.1.2]

The alternative reaction is the transition to SF (System Failure) mode in case of the failure. [Subset-120 5.1.3.1.1.3]

Specific Requirements for the OBU ETCS on Board unit

The antivalent sleeping signals shall be read independently according to EN 50129.

Signal	Hazardous event	Failure Detection Time	Tolerable Failure Rate
T_SL_E_N	Erroneously takes the value 'Sleeping requested'	1 min	1E-05 /h
TR_OBU_TrainSleep	Erroneously takes the value 'Sleeping requested'	1 min	1E-05 /h
T_SL_E_I	Erroneously takes the value 'Sleeping requested'	1 min	1E-05 /h
TR_OBU_TrainSleep_Not	Erroneously takes the value 'Sleeping requested'	1 min	1E-05 /h

Specific Requirements for the vehicle

Exported constraint to the vehicle: The antivalent sleeping signals shall have two sources (common cause failures considered with 10%).

Exported constraint to the vehicle or operation: In the case of vehicle is at standstill and all desks connected to the ERTMS/ETCS on-board equipment are closed, an ERTMS/ETCS on-board equipment independent system is in charge to ensure the standstill (e.g. the driver applied brakes) or a desk connected to another ERTMS/ETCS on-board equipment is open.

Signal	Hazardous event	Failure Detection Time	Tolerable Failure Rate
T_SL_E_N	Erroneously takes the value 'Sleeping requested'	48h	1E-05 /h
TR_OBU_TrainSleep	Erroneously takes the value 'Sleeping requested'	48h	1E-05 /h
T_SL_E_I	Erroneously takes the value 'Sleeping requested'	48h	1E-05 /h
TR_OBU_TrainSleep_Not	Erroneously takes the value 'Sleeping requested'	48h	1E-05 /h

The FVA equipment shall ensure periodical self-tests at least at a rate of 1/min for the antivalent signals.

In case of a failure (inappropriate reception or output of faulty antivalent Sleeping signal / loss of Sleeping signal) FVA on-board equipment shall memorize the fault.

FVA on-board shall not be able to switch to Sleeping mode if a failure (inappropriate reception of faulty antivalent Sleeping signal / loss of Sleeping signal) is memorized.

This means that the FVA shall actively control each of the antivalent signals in independent channels (SIL1/2).

4.2.5 Requirements for (2) Mode Control: Passive Shunting

SIL1/2. (For software, the process and V&V for SIL1 and SIL2 are identical. We therefore mention SIL1/2 here. The requirement for the hardware is indicated in the bold number in the Safety Integrity column in the table below.

Serial connection.

Optional hardwired connection (defined in [Subset-119])

4.2.5.1 Architecture

Signal	Channel	Safety Integrity Level	Periodic Self- Test Rate
T_PS_E	Hardwired (optional)	SIL**1**/2	>= 1 per 48h
TR_OBU_PassiveShunting	Serial	SIL**1**/2	>= 1 per 48h

4.2.5.2 Safety

General Safety Requirements

As the FVA provides software- controlled functionality, it may introduce errors. For this reason, appropriate mitigation measures shall be implemented, including a self- test functionality. The minimum self- test rate has been indicated

Specific Requirements for the OBU

Signal	Hazardous event	Failure Detection Time	Tolerable Failure Rate
T_PS_E	erroneously takes the value 'Passive Shunting permitted'	48 h	1E-05 /h
TR_OBU_PassiveShunting	erroneously takes the value 'Passive Shunting permitted'	48 h	1E-05 /h

Specific Requirements for the vehicle

Exported constraint to the vehicle or operation: In the case of vehicle is at standstill and all desks connected to the ERTMS/ETCS on-board equipment are closed, an ERTMS/ETCS on-board equipment independent function is in charge to ensure the standstill.

Signal	Hazardous event	Failure Detection Time	Tolerable Failure Rate
T_PS_E	erroneously takes the value 'Passive Shunting permitted'	48 h	1E-05 /h
TR_OBU_PassiveShunting	erroneously takes the value 'Passive Shunting permitted'	48 h	1E-05 /h

4.2.5.3 Configurability

As the hardwired connection is optional, in order to be configurable, the hardwired connection should also be actively controlled by software. A separate SVI interface is not required, as the optional hardwired connection already covers this possible need.

4.2.6 Requirements for (3) Mode Control: Non leading

4.2.6.1 Architecture

SIL1/2 (For software, the process and V&V for SIL1 and SIL2 are identical. We therefore mention SIL1/2 here. The requirement for the hardware is indicated in the bold number in the Safety Integrity column in the table below.

Serial connection.

Optional hardwired connection (defined in [Subset-119])

Signal	Channel	Safety Integrity Level	Periodic Self- Test Rate
T_NL_E	Hardwired (optional)	SIL**1**/2	>= 1 per 48h
TR_OBU_NLEnabled	Serial	SIL**1**/2	>= 1 per 48h

4.2.6.2 Safety

General Safety Requirements

As the FVA provides software- controlled functionality, it may introduce errors. For this reason, appropriate mitigation measures shall be implemented, including a self- test functionality. The minimum self- test rate has been indicated

Specific Requirements for the OBU

Signal	Hazardous event	Failure Detection Time	Tolerable Failure Rate
T_NL_E	erroneously takes the value 'Non-Leading permitted'	48 h	1E-05 /h
TR_OBU_NLEnabled	erroneously takes the value 'Non-Leading permitted'	48 h	1E-05 /h

Specific Requirements for the vehicle

Signal	Hazardous event	Failure Detection Time	Tolerable Failure Rate
T_NL_E	erroneously takes the value 'Non-Leading permitted'	48 h	1E-05 /h
TR_OBU_NLEnabled	erroneously takes the value 'Non-Leading permitted'	48 h	1E-05 /h

4.2.6.3 Configurability

As the hardwired connection is optional, in order to be configurable, the hardwired connection should also be actively controlled by software. A separate SVI interface is not required, as the optional hardwired connection already covers this possible need.

4.2.7 Requirements for (4) Mode Control: Isolation

4.2.7.1 Architecture

Direct Hardwired connection between ETCS Onboard and TCMS. The FVA is not involved.

4.2.7.2 Safety

O_IS_S is not safety related.

This signal is not used for safety purposes e.g. it is not used to isolate the ERTMS/ETCS on-board from brakes.

4.2.7.3 Configurability

No requirements.

4.2.8 Requirements for (5) Service Brake Command

4.2.8.1 Architecture

SIL 0 (we consider SIL 0 also for not safety- related variables and signals. This is because their implementation is part of a safety- related system (the FVA)).

Serial connection.

Optional hardwired connection (defined in [Subset-119])

4.2.8.2 Safety

O_SB_C / OBU_TR_ServiceBrake is not safety-related if the ETCS On-board is not implemented to use Service Brake to protect the train against undesirable movements. If it is, a more detailed safety analysis is needed in order to show that a failure of this signal is recognized and the EB is applied as safeguarding.

4.2.8.3 Configurability

As the hardwired connection is optional, in order to be configurable, the hardwired connection should also be actively controlled by software. A separate SVI interface is not required, as the optional hardwired connection already covers this possible need.

4.2.9 Requirements for (6) Brake Pressure

4.2.9.1 Architecture

SIL 0 (we consider SIL 0 also for not safety- related variables and signals. This is because their implementation is part of a safety- related system (the FVA)).

Serial connection.

Optional hardwired connection (defined in [SVI specification])

4.2.9.2 Safety

TR_OBU_BrakePressure is not safety related.

If the ETCS On-board is implemented using Service Brake to protect the train against undesirable movements and the Brake Pressure signal is used as Service Brake feedback, then a project specific safety analysis is needed.

4.2.9.3 Configurability

A separate SVI interface (hardwired) may be used instead of the serial connection.

4.2.10 Requirements for (7) Emergency Brake Command

4.2.10.1 Architecture

Two variants are possible:

Emergency Brake Command out of FVA scope (hardwired only)

For the Solution 1 and Solution 2 described in [Subset-119], it shall be possible to configure the FVA ETCS in such a way that the Emergency Brake Command is not processed.

In this case, the Emergency Brake Command is under the responsibility of the ETCS Onboard Unit and the TCMS only.

This requires that both ETCS OBU and TCMS each support either Solution 1 or Solution 2.

Emergency Brake Command through the FVA (with serial connection through a safe bus; Subset-119 Solution 3)

The serial information is communicated through the CCN (interface: SCI-FVA, on the ETCS on-board side) and through the Subset-119 (on the TCMS side).

The primary hardwired interface remains a direct connection outside the FVA scope.

It is the task of the FVA to transcode the CCN (interface: SCI-FVA) information to Subset-119 format.

4.2.10.2 Safety

General Safety Requirements

EB lines are redundant for safety reasons. The contacts of the ERTMS/ETCS on-board in each line shall be controlled separately in order to be able to test each line independently.

[Subset-119] specifies three different concepts that are valid for implementing the emergency brake command.

Architecture Solution 1: Four NO contacts for two EB lines

Out of FVA scope

Architecture Solution 2: Two NO contacts (and two NC contacts for the EB feedback signal) for two EB lines

Out of FVA scope

Architecture Solution 3: One NO contact for one EB line and serial interface

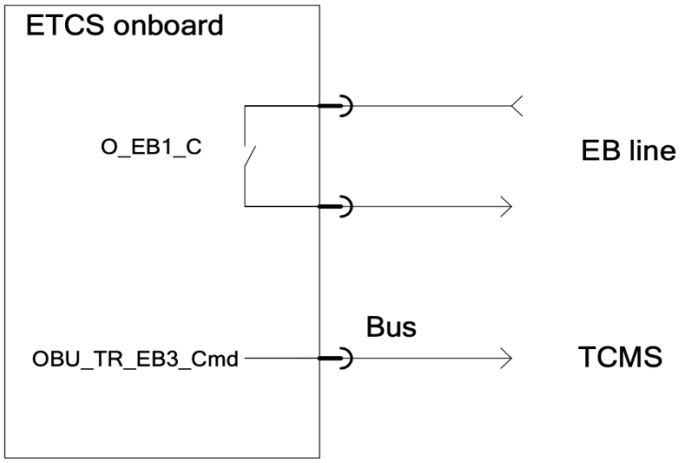

Figure 3: [Subset-119]: Figure 5-6 EB function, Solution 3: 1 EB line, serial interface

Specific Requirements for the OBU

Note: `O_EB1_C` is out of scope of the FVA (this is the hardwired signal)

Signal	Hazardous event	Failure Detection Time	Tolerable Failure Rate
`OBU_TR_EB3_Cmd`	erroneously take the value 'EB not commanded'	48 h	1E-07 /h ≤ TFR < 1E-06 /h

Note: Above Tolerable Failure Rate is for the overall function. It is up to the supplier to ensure that the integrity and reliability measures of the FVA (in case it is implemented as a separate system) are chosen in a way that this requirement is fulfilled. This may require a higher SIL rating for the FVA in some cases.

Exported constraint to the operator: FDT = 48 h.

Exported constraint to the vehicle: The emergency brake signals O_EB1_C and OBU_TR_EB3_Cmd shall be processed in the vehicle with independence as required by TSI LOC & PAS, section 4.2.4.4.1.

4.2.10.3 Configurability

It shall be possible to configure the FVA for

- Inactive
- Active (Solution 3)

4.2.11 Requirements for Special Brake Inhibition Area – Trackside Orders

4.2.11.1 Architecture

SIL 0 (we consider SIL 0 also for not safety- related variables and signals. This is because their implementation is part of a safety- related system (the FVA)).

Serial connection.

Optional hardwired connection (SVI).

4.2.11.2 Safety

From [Subset-120]

OBU_TR_RBI_D_Entry, OBU_TR_RBI_D_Exit, OBU_TR_MGI_D_Entry, OBU_TR_MGI_D_Exit, OBU_TR_ECS_D_Entry, OBU_TR_ECS_D_Exit, OBU_TR_ECS_D_Entry and OBU_TR_ECS_D_Exit are not safety related.

Exported constraint to the OBU:

It is assumed that EB curve is calculated in such a way that EB distance is not extended by a faulty special brake inhibition signal. This can be achieved if the degree of reliability of OBU_TR_RBI_D_Entry, OBU_TR_RBI_D_Exit, OBU_TR_MGI_D_Entry, OBU_TR_MGI_D_Exit, OBU_TR_ECS_D_Entry, OBU_TR_ECS_D_Exit, OBU_TR_ECS_D_Entry, OBU_TR_ECS_D_Exit, and is considered adequately in the Kdry_rst (V, EBCL, set) values.

As a consequence, the FVA specification is only valid for ETCS OBU that fulfils above exported constraint.

4.2.11.3 Configurability

It shall be possible to configure a digital output per trackside order for each Special Brake Inhibition area via the SVI.

4.2.12 Requirements for Special Brake Inhibit – STM Orders

4.2.12.1 Architecture

Special brake inhibit – STM orders is out of scope of this document.

4.2.12.2 Safety

Analysis is national system specific. Special brake inhibit – STM orders is out of scope of this analysis.

4.2.12.3 Configurability

Special brake inhibit – STM orders is out of scope of this document.

4.2.13 Requirements for Special Brake Status

4.2.13.1 Architecture

SIL 0 (we consider SIL 0 also for not safety- related variables and signals. This is because their implementation is part of a safety- related system (the FVA)).

Serial connection.

Optional hardwired connection (SVI as defined in [detailed FVA spec])

4.2.13.2 Safety

General Safety Requirements

From [Subset-120]

“If the vehicle is equipped with special brakes the special brake status can be relevant to calculate the brake model.

It is assumed that EB curve is calculated in such a way that EB distance is not extended by a faulty special brake status signal. This can be achieved if the degree of reliability of OBU_TR_RBI_D_Entry, OBU_TR_RBI_D_Exit, OBU_TR_MGI_D_Entry, OBU_TR_MGI_D_Exit, OBU_TR_ECS_D_Entry, OBU_TR_ECS_D_Exit, OBU_TR_ECS_D_Entry, and OBU_TR_ECS_D_Exit is considered adequately in the Kdry_rst (V, EBCL, set) values.

Application Constraint (see Subset-080): If using Special Brake as available and affecting the Emergency Brake curve, the failure of the input ‘Special Brake status’ could have catastrophic safety severity. A project specific safety analysis is required.

Specific Requirements for the OBU

Exported constraint: The EB curve shall be calculated in such a way that EB distance is not extended by a faulty special brake status signal. This can be achieved if the degree of reliability of OBU_TR_RBI_D_Entry, OBU_TR_RBI_D_Exit, OBU_TR_MGI_D_Entry, OBU_TR_MGI_D_Exit, OBU_TR_ECS_D_Entry, OBU_TR_ECS_D_Exit, OBU_TR_ECS_D_Entry, and OBU_TR_ECS_D_Exit is considered adequately in the Kdry_rst (V, EBCL, set) values. "

If the special brake status signals are taken into account for the calculation of the EB braking curve of the ETCS onboard, they become safety relevant. We therefore require that the ETCS onboard calculates the EB braking curve without considering any special brakes (exported constraint).

4.2.13.3 Configurability

It shall be possible to configure a digital input per status signal for each Special Brake Inhibition area via the SVI.

4.2.14 Requirements for Additional Brake Status

4.2.14.1 Architecture

Not implemented.

4.2.14.2 Safety

Specific Requirements per signal

Currently no Additional Brakes, in addition to the special brakes, are known. Additional brakes should be handled identically as the special brakes are.

4.2.14.3 Configurability

Not implemented.

4.2.15 Powerless Section with Pantograph to be Lowered – Trackside Orders

4.2.15.1 Architecture

SIL 0 (we consider SIL 0 also for not safety- related variables and signals. This is because their implementation is part of a safety- related system (the FVA)).

Serial connection.

Optional hardwired connection (defined in [detailed FVA spec])

4.2.15.2 Safety

Main power switch information is not safety related.

4.2.15.3 Configurability

It shall be possible to configure a digital output via the SVI.

4.2.16 Powerless Section with Pantograph to be Lowered – STM Orders

4.2.16.1 Architecture

Out of scope of this document

4.2.16.2 Safety

Out of scope of this document

4.2.16.3 Configurability

Out of scope of this document

4.2.17 Requirements for (22) Train Functions: Station Platform

4.2.17.1 Architecture

SIL1/2 . (For software, the process and V&V for SIL1 and SIL2 are identical. We therefore mention SIL1/2 here. The requirement for the hardware is indicated in the bold number in the Safety Integrity column in the table below.

Serial connection.

Optional hardwired connection (defined in [detailed FVA spec])

Signal	Channel	Safety Integrity Level	Periodic Self- Test Rate
OBU_TR_SP_D_Entry(K)	Serial	SIL1/**2**	>= 1 per 48h
OBU_TR_SP_D_Exit(K)	Serial	SIL1/**2**	>= 1 per 48h
OBU_TR_SP_Height(K)	Serial	SIL1/**2**	>= 1 per 48h
OBU_TR_SP_Right(K)	Serial	SIL1/**2**	>= 1 per 48h
OBU_TR_SP_Left(K)	Serial	SIL1/**2**	>= 1 per 48h

4.2.17.2 Safety

The related hazard (vehicle allows opening of passenger doors untimely or at the wrong location, compare FMEA) is not part of the ETCS Core Hazard.

Therefore, the safety target and the hazard analysis are project specific.
The serial communication between ERTMS/ETCS on-board equipment and TCMS or a door control system must fulfil the safety target.

Exported constraint to the vehicle and operation: A function on vehicle side or an operational regulation is necessary to handle this information in a safe way.

4.2.17.3 Configurability

It shall be possible to configure a digital output per status signal for the next station platform via the SVI.

4.2.18 Requirements for (23) Train Functions: Powerless Section with Main Power Switch to Be Switched Off – Trackside Orders

4.2.18.1 Architecture

SIL 0 (we consider SIL 0 also for not safety- related variables and signals. This is because their implementation is part of a safety- related system (the FVA)).

Serial connection.

Optional hardwired connection (defined in [detailed FVA spec])

4.2.18.2 Safety

Main power switch information is not safety related.

4.2.18.3 Configurability

It shall be possible to configure a digital output via the SVI.

4.2.19 Requirements for (24) Train Functions: Main Power Switch – STM Orders

4.2.19.1 Architecture

Out of scope

4.2.19.2 Safety

Main power switch information is not safety related.

4.2.19.3 Configurability

Out of scope

4.2.20 Requirements for (25) Train Functions: Change of Allowed Current Consumption

4.2.20.1 Architecture

SIL 0 (we consider SIL 0 also for not safety- related variables and signals. This is because their implementation is part of a safety- related system (the FVA)).

Serial connection.

Optional hardwired connection (SVI)

4.2.20.2 Safety

Change of Allowed Current Consumption is not safety-related

4.2.20.3 Configurability

It shall be possible to configure a digital output per status signal for the next station platform via the SVI.

4.2.21 Requirements for (26) Train Functions: Traction Cut-Off

4.2.21.1 Architecture

SIL1/2 . (For software, the process and V&V for SIL1 and SIL2 are identical. We therefore mention SIL1/2 here. The requirement for the hardware is indicated in the bold number in the Safety Integrity column in the table below.

The primary signal is the mandatory direct ETCS – TCMS hardwired connection (defined in [Subset-119])

Serial connection through the FVA.

Optional hardwired connection through the FVA (as defined in [Subset-119]).

Signal	**Channel**	**Safety Integrity Level**	**Periodic Self- Test Rate**
O_TC1_C	Hardwired (optional)	SIL**1**/2	>= 1 per 48h
OBU_TR_TCO_Cmd	Serial	SIL1/**2**	>= 1 per 1h

4.2.21.2 Safety

General Safety Requirements

TCO with hard-wired output O_TC1_C and serial output OBU_TR_TCO_Cmd allowing a safe TCO affecting the braking curves.

Specific Requirements for the OBU

Signal	Hazardous event	Failure Detection Time	Tolerable Failure Rate
O_TC1_C	erroneously take the value 'Do not cut off traction'	48 h	1E-5 /h
OBU_TR_TCO_Cmd	erroneously take the value 'Do not cut off traction'	1 h	1E-07 /h ≤ TFR < 1E-06 /h

Specific Requirements for the vehicle

Signal	Hazardous event	Failure Detection Time	Tolerable Failure Rate
O_TC1_C	erroneously take the value 'Do not cut off traction'	48 h	1E-5 /h
OBU_TR_TCO_Cmd	erroneously take the value 'Do not cut off traction'	1 h	1E-07 /h ≤ TFR < 1E-06 /h

SIL for TCMS (incl. brake control or other electronic devices): SIL 2, i.e. 1E-07 /h ≤ THR < 1E-06 /h.

Exported constraint to the operator: FDT of O_TC1_C hard-wired = 48 h.

Exported constraint to the vehicle: The TCO signals O_TC1_C and OBU_TR_TCO_Cmd shall be processed in the vehicle with independence as required by TSI Loc&Pas, section 4.2.4.4.1.

Note: Above Tolerable Failure Rate is for the overall function. It is up to the supplier to ensure that the integrity and reliability measures of the FVA (in case it is implemented as a separate system) are chosen in a way that this requirement is fulfilled. This may require a higher SIL rating for the FVA in some cases.

4.2.21.3 Configurability

It shall be possible to configure a digital output via the SVI.

4.2.22 Requirements for (27) Train Functions Status Information: Cab Status

4.2.22.1 Architecture

SIL1/2 . (For software, the process and V&V for SIL1 and SIL2 are identical. We therefore mention SIL1/2 here. The requirement for the hardware is indicated in the bold number in the Safety Integrity column in the table below.

Serial connection through the FVA.

Optional hardwired connection through the FVA (as defined in [Subset-119]).

Signal	Channel	Safety Integrity Level	Periodic Self- Test Rate
T_FW_S	Hardwired (optional)	SIL**1**/2	>= 1 per 48h
TR_OBU_DirectionFW	Serial	SIL**1**/2	>= 1 per 48h
T_BW_S	Hardwired (optional)	SIL**1**/2	>= 1 per 48h
TR_OBU_DirectionBW	Serial	SIL**1**/2	>= 1 per 48h

4.2.22.2 Safety

Specific Requirements for the OBU

Signal	Hazardous event	Failure Detection Time	Tolerable Failure Rate
T_CS_A	erroneously takes the value of the opposite boolean value	48 h	1E-5 /h
TR_OBU_CabStatusA	erroneously takes the value of the opposite boolean value	48 h	1E-5 /h
T_CS_B	erroneously takes the value of the opposite boolean value	48 h	1E-5 /h
TR_OBU_CabStatusB	erroneously takes the value of the opposite boolean value	48 h	1E-5 /h

Exported constraints to the ERTMS/ETCS on-board equipment: The cab status signals T_CS_A / TR_OBU_CabStatusA and T_CS_B / TR_OBU_CabStatusB shall be read independently according to EN50129.

Specific Requirements for the vehicle

Signal	Hazardous event	Failure Detection Time	Tolerable Failure Rate
T_CS_A	erroneously takes the value of the opposite boolean value	48 h	1E-5 /h
TR_OBU_CabStatusA	erroneously takes the value of the opposite boolean value	48 h	1E-5 /h
T_CS_B	erroneously takes the value of the opposite boolean value	48 h	1E-5 /h
TR_OBU_CabStatusB	erroneously takes the value of the opposite boolean value	48 h	1E-5 /h

Exported constraint to the vehicle: The cab status signals T_CS_A / TR_OBU_CabStatusA and T_CS_B / TR_OBU_CabStatusB shall have two independent sources (common cause failures considered with 10%).

4.2.22.3 Configurability

It shall be possible to configure a digital input via the hardwired Subset-119- Interface.

4.2.23 Requirements for (28) Train Functions Status Information: Direction Controller

4.2.23.1 Architecture

SIL1/2 . (For software, the process and V&V for SIL1 and SIL2 are identical. We therefore mention SIL1/2 here. The requirement for the hardware is indicated in the bold number in the Safety Integrity column in the table below.

Serial connection through the FVA.

Optional hardwired connection through the FVA (as defined in [Subset-119]).

Signal	Channel	Safety Integrity Level	Periodic Self- Test Rate
T_FW_S	Hardwired (optional)	SIL**1**/2	>= 1 per 48h
TR_OBU_DirectionFW	Serial	SIL**1**/2	>= 1 per 48h
T_BW_S	Hardwired (optional)	SIL**1**/2	>= 1 per 48h
TR_OBU_DirectionBW	Serial	SIL**1**/2	>= 1 per 48h

4.2.23.2 Safety

Specific Requirements for the OBU

Signal	Hazardous event	Failure Detection Time	Tolerable Failure Rate
T_FW_S	erroneously takes the value 'Forward'	48 h	1E-5 /h
TR_OBU_DirectionFW	erroneously takes the value 'Forward'	48 h	1E-5 /h
T_BW_S	erroneously takes the value 'Backward'	48 h	1E-5 /h
TR_OBU_DirectionBW	erroneously takes the value 'Backward'	48 h	1E-5 /h

Specific Requirements for the vehicle

Signal	Hazardous event	Failure Detection Time	Tolerable Failure Rate
T_FW_S	erroneously takes the value 'Forward'	48 h	1E-5 /h
TR_OBU_DirectionFW	erroneously takes the value 'Forward'	48 h	1E-5 /h
T_BW_S	erroneously takes the value 'Backward'	48 h	1E-5 /h
TR_OBU_DirectionBW	erroneously takes the value 'Backward'	48 h	1E-5 /h

Exported constraint to the vehicle or operation: In case of vehicle is at standstill an ERTMS/ETCS on-board equipment independent system is in charge to ensure the roll away protection.

4.2.23.3 Configurability

It shall be possible to configure a digital input via the SVI.

4.2.24 Requirements for (29) Train Functions Status Information: Train Integrity

4.2.24.1 Architecture

Not implemented.

4.2.24.2 Safety

Out of scope of this document release.

4.2.24.3 Configurability

Not implemented.

4.2.25 Requirements for (30) Train Functions Status Information: Traction Status (only for STM)

4.2.25.1 Architecture

Out of scope of this document.

4.2.25.2 Safety

Out of scope of this document.

4.2.25.3 Configurability

Out of scope of this document.

4.2.26 Requirements for (31) Train Functions Status Information: Set Speed (for DMI indication)

4.2.26.1 Architecture

SIL 0 (we consider SIL 0 also for not safety- related variables and signals. This is because their implementation is part of a safety- related system (the FVA)).

Serial connection.

Optional hardwired connection (SVI)

4.2.26.2 Safety

Set speed is not safety related.

4.2.26.3 Configurability

It shall be possible to configure a set of digital inputs via the SVI.

4.2.27 Requirements for (32) Train Functions Status Information: Type of Train Data Entry

4.2.27.1 Architecture

SIL 0 (we consider SIL 0 also for not safety- related variables and signals. This is because their implementation is part of a safety- related system (the FVA)).

Serial connection.

Optional hardwired connection (defined in [detailed FVA spec])

4.2.27.2 Safety

General Safety Requirements

Type of train data entry is not safety related.

Exported constraint to the operation (see Subset-080): Driver shall be informed on the type of train when Train Data entry is selected.

4.2.27.3 Configurability

It shall be possible to configure a set of digital inputs via the SVI.

4.2.28 Requirements for Train Functions Status Information: Train Data Information: Train category / Cant deficiency

4.2.28.1 Architecture

SIL1/2. (For software, the process and V&V for SIL1 and SIL2 are identical. We therefore mention SIL1/2 here. The requirement for the hardware is indicated in the bold number in the Safety Integrity column in the table below.

Serial connection.

Optional hardwired connection (defined in [detailed FVA spec])

Optional hardwired connection (defined in [Subset-119]) for the variables `T_TH_S_N` and `T_TH_S_I`.

Signal	Channel	Safety Integrity Level	Periodic Self- Test Rate
`TR_OBU_TiltingHealthStatus`	Serial	SIL**1**/2	>= 1 per 48h
`TR_OBU_TiltingHealthStatus_Not`	Serial	SIL**1**/2	>= 1 per 48h
`T_TH_S_N`	Hardwired (optional)	SIL**1**/2	>= 1 per 48h
`T_TH_S_I`	Hardwired (optional)	SIL**1**/2	>= 1 per 48h
`TR_OBU_TrainCatCantDef`	Serial	SIL**1**/2	>= 1 per 48h
`TR_OBU_TrainComposition`	Serial	SIL**1**/2	>= 1 per 48h

4.2.28.2 Safety

General Safety Requirements

Note: The train interface allows the ETCS on-board to determine the cant deficiency value based on the

value of the cant deficiency which is transferred via train interface or train type input or train composition input and tilting health status input.

Specific Requirements for the OBU

Signal	Hazardous event	Failure Detection Time	Tolerable Failure Rate
`TR_OBU_TiltingHealthStatus`	inappropriately received or lost	48 h	1E-5 /h
`TR_OBU_TiltingHealthStatus_Not`	inappropriately received or lost	48 h	1E-5 /h
`T_TH_S_N`	inappropriately received or lost	48 h	1E-5 /h
`T_TH_S_I`	inappropriately received or lost	48 h	1E-5 /h
`TR_OBU_TrainCatCantDef`	inappropriately received or lost		
`TR_OBU_TrainComposition`	inappropriately received or lost		

SIL 2 is needed for the serial transmission of the cant deficiency value, train type input, train composition input, and tilting health status input.

Specific Requirements for the vehicle

Signal	Hazardous event	Failure Detection Time	Tolerable Failure Rate
TR_OBU_TiltingHealthStatus	inappropriately output or lost	48 h	1E-5 /h
TR_OBU_TiltingHealthStatus_Not	inappropriately output or lost	48 h	1E-5 /h
T_TH_S_N	inappropriately output or lost	48 h	1E-5 /h
T_TH_S_I	inappropriately output or lost	48 h	1E-5 /h
TR_OBU_TrainCatCantDef	inappropriately output or lost		
TR_OBU_TrainComposition	inappropriately output or lost		

The on-board configuration shall require driver validation for changes in Cant Deficiency Train Data information (see Subset-026, 3.18.3.3 and 5.17.2.2).

Exported constraint to the vehicle: The ATP system assumes that the train manufacturer has checked the safety of the whole function cant deficiency considering the transmission between OBU and vehicle. Therefore, a specific project can regard the failure mode of this input as having a 'RAM Issue' only if adequate safety margin against derailment can be demonstrated for the vehicle exceeding maximum authorized speed for its train category. This shall be done specific for the respective vehicle.

4.2.28.3 Configurability

It shall be possible to configure a set of digital inputs via the SVI for the variables for which [Subset-119] does not foresee any optional hardwired interface. For the optional hardwired connections (according to [Subset-119]) T_TH_S_N, T_TH_S_I it shall be possible to configure the routing accordingly.

4.2.29 Requirements for Train Functions Status Information: Train length

4.2.29.1 Architecture

SIL1/2 . (For software, the process and V&V for SIL1 and SIL2 are identical. We therefore mention SIL1/2 here. The requirement for the hardware is indicated in the bold number in the Safety Integrity column in the table below.

Serial connection.

Signal	Channel	Safety Integrity Level	Periodic Self- Test Rate
TR_OBU_TrainLength	Serial	SIL1/**2**	>= 1 per 48h

4.2.29.2 Safety

General safety requirements

Note: The train interface allows the ETCS on-board to determine the train length value based on the

• value of the train length which is transferred via train interface or

• train type input or

• train composition input.

Note: The brake build-up time using the conversion models can be based on 'brake position' and 'train length'.

Requirements for ERTMS/ETCS on-board equipment and vehicle:

SIL 2 is needed for the serial transmission of the train length value, train type input and train composition input.

4.2.29.3 Configurability

It shall be possible to configure static info.

4.2.30 Requirements for Train Functions Status Information: Traction model

4.2.30.1 Architecture

SIL1/2. (For software, the process and V&V for SIL1 and SIL2 are identical. We therefore mention SIL1/2 here. The requirement for the hardware is indicated in the bold number in the Safety Integrity column in the table below.

Serial connection.

Optional hardwired connection (SVI)

Signal	Channel	Safety Integrity Level	Periodic Self- Test Rate
`TR_OBU_TrainType`	Serial	SIL1/**2**	>= 1 per 48h
`TR_OBU_TrainComposition`	Serial	SIL1/**2**	>= 1 per 48h

4.2.30.2 Safety

The traction parameters consist of the time for traction cut-off (`T_traction_cut_off`) (traction model).

The train interface allows the ETCS on-board to determine the traction model value (value of time delay T_traction_cut_off as follows:

• By selecting the train data set including the adequate traction model value based on the “train type” input.

• By selecting/calculating the adequate traction model value in a project specific way based on the “train composition” input.

Note: the traction model value can depend on the train length value and the selection of the adequate traction model value can therefore be based on the train composition input.

Specific Requirements for the OBU and for the vehicle

SIL 2 is needed for the serial transmission of train type input and train composition input.

4.2.30.3 Configurability

It shall be possible to configure a set of digital inputs via the SVI.

4.2.31 Requirements for Train Functions Status Information: Brake build up time model and speed dependent deceleration model

4.2.31.1 Architecture

SIL1/2 . (For software, the process and V&V for SIL1 and SIL2 are identical. We therefore mention SIL1/2 here. The requirement for the hardware is indicated in the bold number in the Safety Integrity column in the table below.

Serial connection.

Optional hardwired connection (defined in [detailed FVA spec])

Signal	Channel	Safety Integrity Level	Periodic Self- Test Rate
T_EP_S_N	Hardwired (optional)	SIL1/**2**	>= 1 per 48h
T_EP_S_I	Hardwired (optional)	SIL1/**2**	>= 1 per 48h
T_EC_S_N	Hardwired (optional)	SIL1/**2**	>= 1 per 48h
T_EP_S_I	Hardwired (optional)	SIL1/**2**	>= 1 per 48h
T_RB_S_N	Hardwired (optional)	SIL1/**2**	>= 1 per 48h
T_RB_S_I	Hardwired (optional)	SIL1/**2**	>= 1 per 48h
T_MG_S_N	Hardwired (optional)	SIL1/**2**	>= 1 per 48h
T_MG_S_I	Hardwired (optional)	SIL1/**2**	>= 1 per 48h
EP_S	Serial	SIL1/**2**	>= 1 per 48h
EP_S_Not	Serial	SIL1/**2**	>= 1 per 48h
EC_S	Serial	SIL1/**2**	>= 1 per 48h
EC_S_Not	Serial	SIL1/**2**	>= 1 per 48h
RB_S	Serial	SIL1/**2**	>= 1 per 48h
RB_S_Not	Serial	SIL1/**2**	>= 1 per 48h
MG_S	Serial	SIL1/**2**	>= 1 per 48h
MG_S_Not	Serial	SIL1/**2**	>= 1 per 48h

4.2.31.2 Safety

Note

The train interface allows the ETCS on-board to determine the brake build up time model and speed dependent deceleration model based on the train type input plus the status of special brakes.

Calculation of the brake build up time using the conversion models based on ‘brake position’ and ‘train length’ and calculation of the speed dependent deceleration models by applying the conversion model to the brake percentage value.

Specific Requirements for Transmission

SIL 2 is needed for the serial transmission of train type input and special brake status.

Specific Requirements for the OBU

Signal	Hazardous event	Failure Detection Time	Tolerable Failure Rate
T_EP_S_N	inappropriately received or lost	48 h	1E-7 /h
T_EP_S_I	inappropriately received or lost	48 h	1E-7 /h
T_EC_S_N	inappropriately received or lost	48 h	1E-7 /h
T_EP_S_I	inappropriately received or lost	48h	1E-7 /h

Specific Requirements for the vehicle

Signal	Hazardous event	Failure Detection Time	Tolerable Failure Rate
T_EP_S_N	inappropriately output or lost	48 h	1E-7 /h
T_EP_S_I	inappropriately output or lost	48 h	1E-7 /h
T_EC_S_N	inappropriately output or lost	48 h	1E-7 /h
T_EP_S_I	inappropriately output or lost	48h	1E-7 /h

4.2.31.3 Configurability

It shall be possible to configure a set of digital inputs via the interface as defined in [Subset-119].

4.2.32 Requirements for Train Functions Status Information: Brake percentage

4.2.32.1 Architecture

SIL1/2 . (For software, the process and V&V for SIL1 and SIL2 are identical. We therefore mention SIL1/2 here. The requirement for the hardware is indicated in the bold number in the Safety Integrity column in the table below.

Serial connection.

Optional hardwired connection (SVI)

Signal	Channel	Safety Integrity Level	Periodic Self- Test Rate
TR_OBU_BrakePercentage	Serial	SIL1/**2**	>= 1 per 48h
TR_OBU_TrainType	Serial	SIL1/**2**	>= 1 per 48h
TR_OBU_TrainComposition	Serial	SIL1/**2**	>= 1 per 48h

4.2.32.2 Safety

Note

The train interface allows the ETCS on-board to determine the brake percentage (TR_OBU_BrakePercentage) based on the

• value of brake percentage is transferred via train interface,

• train type input or

• train composition input.

Specific Requirements for Transmission

SIL 2 is needed for the serial transmission of the brake percentage value, train type input and train composition input.

4.2.32.3 Configurability

It shall be possible to configure a set of digital inputs via the SVI.

4.2.33 Requirements for Train Functions Status Information: Brake position

4.2.33.1 Architecture

SIL1/2 . (For software, the process and V&V for SIL1 and SIL2 are identical. We therefore mention SIL1/2 here. The requirement for the hardware is indicated in the bold number in the Safety Integrity column in the table below.

Serial connection.

Optional hardwired connection (defined in [Subset-119])

Signal	Channel	Safety Integrity Level	Periodic Self- Test Rate
T_BP_S1_N	Hardwired (optional)	SIL1/**2**	>= 1 per 48h
T_BP_S1_I	Hardwired (optional)	SIL1/**2**	>= 1 per 48h
T_BP_S2_N	Hardwired (optional)	SIL1/**2**	>= 1 per 48h
T_BP_S2_I	Hardwired (optional)	SIL1/**2**	>= 1 per 48h
TR_OBU_BrakePosition1	Serial	SIL1/**2**	>= 1 per 48h
TR_OBU_BrakePosition1_Not	Serial	SIL1/**2**	>= 1 per 48h
TR_OBU_BrakePosition2	Serial	SIL1/**2**	>= 1 per 48h
TR_OBU_BrakePosition2_Not	Serial	SIL1/**2**	>= 1 per 48h

4.2.33.2 Safety

Note: The train interface allows the ETCS on-board to determine the brake position (TR_OBU_BrakePosition1 and TR_OBU_BrakePosition2) based on the

- value of brake position is transferred via train interface or
- train type input or
- train composition input.

Specific Requirements for Transmission

SIL 2 is needed for the serial transmission of the brake position value, train type input and train composition input.

Specific Requirements for the OBU

Signal	Hazardous event	FDT	TFR
T_BP_S1_N	inappropriately received or lost	48 h	1E-7 /h
T_BP_S1_I	inappropriately received or lost	48 h	1E-7 /h

Specific Requirements for the vehicle

Signal	Hazardous event	FDT	TFR
T_BP_S1_N	inappropriately output or lost	48 h	1E-7 /h
T_BP_S1_I	inappropriately output or lost	48 h	1E-7 /h

4.2.33.3 Configurability

It shall be possible to configure a set of digital inputs via the hardwired interface as defined in [Subset-119].

4.2.34 Requirements for Train Functions Status Information: Nominal rotating mass

4.2.34.1 Architecture

SIL 0 (we consider SIL 0 also for not safety- related variables and signals. This is because their implementation is part of a safety- related system (the FVA)).

Serial connection.

4.2.34.2 Safety

Nominal rotating mass Train Data information is not safety related.

4.2.34.3 Configurability

None.

4.2.35 Requirements for Train Functions Status Information: Maximum train speed

4.2.35.1 Architecture

SIL1/2 . (For software, the process and V&V for SIL1 and SIL2 are identical. We therefore mention SIL1/2 here.

Serial connection.

4.2.35.2 Safety

Specific Requirements for Transmission

SIL 2 is needed for the serial transmission of train type input, train composition input and tilting health status.

4.2.35.3 Configurability

None.

4.2.36 Requirements for Train Functions Status Information: Loading gauge

4.2.36.1 Architecture

SIL1/2 . (For software, the process and V&V for SIL1 and SIL2 are identical. We therefore mention SIL1/2 here)

Serial connection.

4.2.36.2 Safety

Loading gauge is safety related.

Under assumption that Traffic planning, lineside signs and driver´s route knowledge shall prevent any hazardous situation a specific project can regard the failure mode of this input as having a ‘RAM Issue’.

Inappropriate value of loading gauge is not part of the ETCS Core Hazard. In case of a project specific safety target a specific analysis is necessary.

4.2.36.3 Configurability

None.

4.2.37 Requirements for Train Functions Status Information: Axle load category

4.2.37.1 Architecture

SIL1/2. (For software, the process and V&V for SIL1 and SIL2 are identical. We therefore mention SIL1/2 here. The requirement for the hardware is indicated in the bold number in the Safety Integrity column in the table below.

Serial connection.

Optional hardwired connection (defined in [detailed SVI- Spec])

Signal	Channel	Safety Integrity Level	Periodic Self- Test Rate
TR_OBU_AxleLoadCat	Serial	SIL1/**2**	>= 1 per 48h

4.2.37.2 Safety

Note: The train interface allows the ETCS on-board to determine the axle load category value based on the

- value of axle load category is transferred via train interface or
- train type input or
- train composition input.

Specific Requirements for Transmission

SIL 2 is needed for the serial transmission of axle load category value, train type input, and train composition input.

4.2.37.3 Configurability

It shall be possible to configure a set of digital inputs via the hardwired interface as defined in [SVI].

4.2.38 Requirements for Train Functions Status Information: Traction system(s) accepted by the engine

4.2.38.1 Architecture

SIL 0 (we consider SIL 0 also for not safety- related variables and signals. This is because their implementation is part of a safety- related system (the FVA)).

Serial connection.

4.2.38.2 Safety

Traction system(s) accepted by the engine is not safety related

4.2.38.3 Configurability

None.

4.2.39 Requirements for Train Functions Status Information: Train fitted with airtight system

4.2.39.1 Architecture

SIL1/2. (For software, the process and V&V for SIL1 and SIL2 are identical. We therefore mention SIL1/2 here.

Serial connection.

Optional hardwired connection (SVI)

4.2.39.2 Safety

The information whether the train fitted with airtight system is marginal for safety.

(we consider SIL 1/2 requirements nevertheless, as the cost is also marginal)

4.2.39.3 Configurability

It shall be possible to configure a digital input via the hardwired interface as defined in [SVI].

4.2.40 Requirements for Train Functions Status Information: National System Isolation

4.2.40.1 Architecture

Not relevant.

4.2.40.2 Safety

This is level NTC only which is seen as out of scope of this safety analysis focusing on level 1 and level 2 aspects.

4.2.40.3 Configurability

None

4.3 Configuration and parametrization

A key concept of the FVA is that it is implemented through generic software and that its behaviour is fully parametrizable. In addition, depending on the CCS on-board, additional functions can be added using an API.

A first example of FVA specification for Subsets -119 and -139 has been defined by OCORA in 2020 with a proposal for a complete definition of all parameters, routing functions, default value settings and coding information for all variables, accompanied by detailed formal models.

Since the FVA discussion has developed since then, a new revision of this detailed specification and models will be provided with the next release.