

CONTRIBUTING TO SHIFT2RAIL'S NEXT GENERATION OF HIGH CAPABLE AND SAFE TCMS AND BRAKES.

D3.4 – Report on Safety Approval Concept

Due date of deliverable: 31/08/2018

Actual submission date: 21/09/2018

Leader/Responsible of this Deliverable: R. Mattes, SIEMENS

Reviewed: Y

Document status		
Revision	Date	Description
1	25/05/2018	Initial version
2	08/06/2018	Draft Version included chapter 1, 2.1, 2.2 and 2.2.1
2	09/07/2018	Version included chapter : <ul style="list-style-type: none"> - 3.5 “Definition of a safe Deployment Procedure for safety critical applications and its Parametrization” from “CTA-T3.4-T-BTD-002-02” - 2.3 “Separation of safety-relevant functions from non safety-relevant functions” from “CTA-T3.4-T-CAF-004-01”
3	12/07/2018	Contribution from CAF to ch. 3.1 added
4	22/08/2018	Updated Version : <ul style="list-style-type: none"> - Chapter 3.5 updated according to review-comments from CTA-T3.4-R-BTD-007-03 send via e-mail from T. Gallenkamp (BTG_rework_CTA-T3.4-D-SIE-003-03_-_Report_on_Safety_Approval_Concept - Kopie.docx) taken as the Base for this version 4 - integration of content from "CTA-T3.4-T-CAF-004-02" (Updated according the review document CTA-T3.4-R-BTD-007-003) to chapter 2.3 of D3.4 Version 4 - integration of content from "CTA-T3.4-T-CAF-005-02" (Updated according the review document CTA-T3.4-R-BTD-

		<p>007-003) to chapter 3.1 of D3.4 Version 4</p> <ul style="list-style-type: none"> - Report Contributors changed, ABBREVIATIONS AND ACRONYMS extended, chapter 1, 2, 2.1 and chapter 2.2 changed in accordance review comments from CTA-T3.4-R-BTD-007-003 - Chapter 3.4 included taken from: “CTA-T3.4-T-CAF-015-01” - Chapter 4.1 included taken from : “CTA-T3.4-T-BTG-016-01” - Chapter 4.2 included taken from : “CTA-T3.4-T-CAF-010-01” - Chapter 2.2.2 included taken from : “CTA-T3.4-T-BTD-013-01_-_Contribution_to_D3.4_chapter_2.2.2” - Chapter 3.2.2 included taken from : “CTA-T3.4-T-BTD-014-01_-_Contribution_to_D3.4_chapter_3.2.2.docx” - Annex B included taken from : “CTA-T3.4-T-BTD-017-02_-_Contribution_to_D3.4_Annex_B.docx” - Change the order of chapter 4.1 and 4.2 so now 4.1 is titled “door function” and 4.2 is titled “brake function” - “CTA-T3.4-T-SNF-012-01_-_Contribution_to_the_preparation_of_selected_safety_cases.docx” included in subchapter of 4.1 and 4.2.
5	29/08/2018	<p>Updated Version :</p> <ul style="list-style-type: none"> - wrong or missing references corrected/added - changes according review : CTA-T3.4-R-SIE-021-01 integrated - Chapter 3.3.2 : CTA-T3.4-T-BTD-020-01 included - Missing topics within chapter 2.2.1 added.
6	02/09/2018	<p>Updated Version :</p> <ul style="list-style-type: none"> - Included chapter 3.2.1, 3.2.3, 3.2.4, 3.3.1 and chapter 5
7	05/09/2018	<p>Updated Version :</p> <ul style="list-style-type: none"> - amended due to the review comments from the review meeting on September 4, 2018 and some additional comments from DB and BTG summarized in CTA-T3.4-R-SIE-021-02
8	06/09/2018	<p>Updated Version :</p> <ul style="list-style-type: none"> - editorial review with WP3 Partners - prepared for TMT Review
9	20/09/2018	<p>Updated Version :</p> <ul style="list-style-type: none"> - including changes from TMT Review and WP3 Review summarized in CTA-T3.4-R-SIE-026-01
10	20/09/2018	<p>Finale Version :</p> <ul style="list-style-type: none"> - converting fileformat “docx” to “pdf”

Project funded from the European Union's Horizon 2020 research and innovation programme		
Dissemination Level		
PU	Public	
CO	Confidential, restricted under conditions set out in Model Grant Agreement	X

Start date: 01/09/2016

Duration: 24 months

REPORT CONTRIBUTORS

Name	Company	Details of Contribution
Nerea Elorza Oscar Rozas Daniel Gutierrez	CAF	Sub-chapters: 2.3, 2.3.1, 2.3.2, 3.1, 3.4, 3.4.1, 3.4.2, 4.2, Annex B (together with Bombardier)
Rainer Mattes	SIEMENS	Sub-chapter: 1, 2, 2.1, 2.2.1, 3, 3.2.1, 3.2.3, 3.2.4, 3.3, 3.3.1, Annex A
Gernot Hans Thomas Gallenkamp Steffen Koller Benjamin Scherer	BTG	Sub-chapter: 2.2, 2.2.2, 3.2, 3.2.2, 3.3.2, 3.5, 3.6, 4, 4.1, 5, Annex B (together with CAF)
Philippe Laporte Clement Collet	SNCF-M	Sub-chapter: 4.1 and 4.2

EXECUTIVE SUMMARY

The safety approval concept which is subject of this document has the aim to provide:

1. A generic safety concept for a drive-by-data NG-TCMS by defining the generic safety architecture for the executions of safety functions up to SIL4 and more specifically by proposing a safety design for the two communication network related safety functions “safe train inauguration” and “safe data transmission”. An important aspect is to avoid or at least to minimize interference between function of different safety criticality.
2. Considerations how a generic certification process could look like, taking into account: the handling of faults, definition of safe states and determination of the safety function response time (SFRT). Another aspect is the definition of rules for standardized interfaces, as those interfaces are more resistant to changes and enforce a clear separation between different train functions, which helps especially in incremental certification. A further aspect is the safe deployment of safety related software, including parameterization of software for deployment in a safe manner.
3. A Demonstration exemplarily for two selected train functions, the door function and the brake function, how the generic certification process could be performed.

With the analysis and evaluation work performed in Task 3.4 and documented in this report, the objectives defined by Connecta for this task have been accomplished.

ABBREVIATIONS AND ACRONYMS

ATC	Automatic Train Control
BCU	Brake Control Unit
BLOB	Binary large object. Any non simple type data with any number of bytes, e.g. picture binary. Represented as byte array without specifying structure.
CCTV	Closed Circuit Television
CCU	Consist Control Unit (CCU is used synonymously to VCU)
COS	Customer Oriented Services
CRC	Cyclic Redundancy Check
CSM	Common Safety Methods
CSM-DT	Common Safety Method-Design Target
CSM RA	Common Safety Method for Risk evaluation and Assessment
CTA	Connecta
DCU	Door Control Unit
DHCP	Dynamic Host Configuration Protocol

DIP	Dual In-line Package
EEPROM	Electrically Erasable Programmable Read-Only Memory
E/E/PE	Electrical/Electronic/programmable electronic
E2E	End to End
ECN	Ethernet Consist Network
ECR	Ethernet Consist network Ring
ECU	Electronic Control Unit
ED	End Device
ED-S	End Device Safety relevant
EDV	Electronic Distribute Valve
EMC	Electromagnetic Compatibility
ETB	Ethernet Train Backbone
ETBN	ETB Node
EUC	Equipment Under Control
FBS	Functional Breakdown Structure
FDF	Functional Distribution Framework
FMECA	Failure mode, effects and criticality analysis
FOC	Functional Open Coupling
FS	Fail Safe
FSM	Functional Safety Management
FTA	Fault Tree Analysis
FW	Firmware
HACCP	Hazard Analysis And Critical Control Points
HAZOP	Hazard and Operability study
HMI	Human Machine Interface
HVAC	Heating Ventilation Air Conditioning
HW	Hardware
I/O or IO	Input/Output

IoT	Internet of Things
IP	Internet Protocol
IP-TCN	Internet Protocol Train Communication Network
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISO	International Standards Organization
IT	Information Technology
LAN	Local Area Network
LOPA	Layer Protection Analysis
MAC	Media Access Control
MCDA	Multi Criteria Decision Analysis
MIO	Modular Input/Output
MMU	Memory Management Unit
MRP	Media Redundancy Protocol
MVB	Multifunction Vehicle Bus
NG-TCMS	Next Generation TCMS
NG-TCN	Next Generation TCN
OFDT	One fault delay time
OMTS	On-board Multimedia and Telecommunication Services
OOS	Operator Oriented Services
OSHA	Operational Safety Hazards Analysis
OTD	Operational Train Directory
PAS	Passenger Alarm System
PDU	Protocol Data Unit
PFD _{avg}	Average probability of dangerous failure on demand
PFH	Probability of dangerous failure per hour
PHA	Preliminary Hazard Analysis
PROFINET	Process Field Network

PST	Process Safety Time
PTE	Portable Test Equipment. A laptop to be temporarily connected to the ECN for commissioning
QMS	Quality Management System
RAM	Reliability, Availability, Maintainability
RAMS	Reliability, Availability, Maintainability and Safety
RBD	Reliability Block Diagram
RRF	Risk Reduction Factor
RTOS	Real Time Operating System
S2R	Shift To Rail
SDSINK	Safe Data Sink
SDSRC	Safe Data Source
SDT	Safe Data Transmission
SDTv2	Safe Data Transmission version 2
SDTv4	Safe Data Transmission version 4
SFRT	Safety Function Response Time
SIL	Safety Integrity Level
SRAC	Safety-related application conditions
SRS	Safety Requirement Specification
SuC	System under Consideration
SW	Software
SWIFT	Structure <<What IF>>
TCMS	Train Control and Management System
TCN	Train Communication Network
TCU	Traction Control Unit
TD	Train Directory
TFFR	Tolerable Functional Failure Rate
THR	Tolerable Hazard Rate

TI	Train Inauguration
TND	Train Network Directory
TRDP	Train Realtime Data Protocol
TSN	Time Sensitive Networking
TTDB	Train Topology Data Base
TWCDT	Total Worst Case Delay Time
UDP	User Datagram Protocol
UIC	Union Internationale des Chemins de fer
VCU	Vehicle Control Unit (VCU is used synonymously to CCU)
VDP	Vital Data Paket
VLAN	Vitual Local Area Network
VTP	Validation Test Plan
V&V	Verification & Validation
WCDT	Worst Case Delay Time
WD	Watchdog
WDT	Watchdog Time
WP	Working Package
WSP	Wheel Slide Protection

TABLE OF CONTENTS

Report Contributors.....	3
Executive Summary	4
Abbreviations and Acronyms	4
Table of Contents.....	9
List of Figures	11
List of Tables.....	11
1. Introduction	13
2. Generic safety concept / safety case for drive-by-data architecture	14
2.1 General	14
2.2 Identification of safety functions on System Level	14
2.2.1 Component level / Subsystems ED-S	17
2.2.2 Network level	21
2.3 Separation of safety-relevant functions from non safety-relevant functions.....	29
2.3.1 Independence of safety-related functions	33
2.3.2 Techniques.....	34
2.3.3 Example for achieving non-interference	34
3. Considerations for generic certification process for drive-by-data enabled TCMS	36
3.1 Apportioning of a safety function from system level to component level “Top Down” principle	36
3.1.1 Apportionment with a FTA.....	40
3.2 Fault handling and safe state	42
3.2.1 Definition of the fault handling for the safety function.....	42
3.2.2 Definition of the safe state for the safety function	43
3.2.3 Calculation of the minimal Safety Function Response Time (SFRT)	46
3.2.4 Evaluation of the maximal Safety Function Response Time (SFRT)	49
3.3 Generic proof of no undetected interference between safety and non safety functions	49
3.3.1 Component level	49
3.3.2 Network level	51
3.4 Definition of standardized Interfaces on Train Level for different safety functions.....	52
3.4.1 Amount of Safety data.....	53
3.4.2 Timing requirements.....	55
3.5 Definition of a safe Deployment Procedure for safety critical applications and its Parametrization.....	57
3.5.1 Firmware Download	57
3.5.2 Software Items	58

3.5.3	Safe Software Deployment approach.....	58
3.5.4	SafeDeviceID	59
3.5.5	Per device initial configuration.....	59
3.5.6	Using parameters	59
3.5.7	Summary	61
4.	Preparation of selected safety cases for the selected functions for the demonstrator platform...	61
4.1	General Safety Case Methodology	62
4.1.1	Introduction.....	62
4.1.2	Quality management report.....	62
4.1.3	Safety Management report.....	64
4.1.4	Technical safety report	70
4.2	door function	78
4.2.1	Definition of the Subsystem.....	78
4.2.2	Functional breakdown	80
4.2.3	Doors safety goals.....	82
4.3	brake function	84
4.3.1	Definition of the subsystem	84
4.3.2	Functional breakdown	86
4.3.3	Brake safety goals.....	88
4.4	Safety measures	92
5.	Conclusion (statement about fulfilment of objectives).....	94
Annex A	Calculation of the minimum SFRT (Excel-Tool)	95
Annex B	Guideline for supporting certification procedure device	96
References	100

LIST OF FIGURES

Figure 1 Safety function with conventional train line	15
Figure 2 Safety function without conventional train line	16
Figure 3 HW-redundancy used for error detection	18
Figure 4 SW-redundancy used for error detection	19
Figure 5: SuC	22
Figure 6: Safe train inauguration function architecture	23
Figure 7: Train inauguration THR apportioning (example)	25
Figure 8: SuC Intra-consist communication	27
Figure 9: Architecture of intra-consist safe communication function	27
Figure 10: SuC Intra-consist communication	28
Figure 11: HW-Capsulation of Safe Data	35
Figure 12: Software encapsulation of data	35
Figure 13: Apportionment of functional safety requirements according EN50126-2 [18]	39
Figure 14: HW-Design of a Safety function using different ED-S and network	42
Figure 15: TTDB datasets	44
Figure 16: SDTv2 layer fault indication	46
Figure 17: SFRT calculation for intra-consist safety chain	47
Figure 18: SIL4 Organization chart	65
Figure 19: FTA example	69
Figure 20: Structure of technical safety report	71
Figure 21: Definition of the door system	79
Figure 22 Architecture with 2 consists	80
Figure 23: Overview of function brake	85
Figure 24: TCMS – System under Consideration	97

LIST OF TABLES

Table 1: TFFR and SIL of inauguration sub-functions	26
Table 2: Safety function examples (Table D1 of the EN50126-1[04])	31
Table 3: Tools used in Risk Assessment Process. Table A.1 of IEC/ISO 31010 [11]	32
Table 4: SIL versus TFFR	37
Table 5: SIL versus THR	37
Table 6: SIL versus PFD_{avg}	38
Table 7: SIL versus PFH	38
Table 8: Inauguration related to train operation use case	44
Table 9: Train inauguration failure consequences	45
Table 10: Quality management report. Procedures used.	64

Table 11: Design phase documentation (Table E.8 EN50129).....	64
Table 12: Safety organization (Table E.3 of EN50129)	65
Table 13: Safety planning and quality assurance activities (Table E.1 EN50129).....	66
Table 14: System requirements specification (Table E.2 of EN50129)	66
Table 15: Design and development of system/sub-system/equipment (Table E.7 of EN50129)	67
Table 16: Verification and validation of the system and product design (Table E.9 of EN50129) ..	68
Table 17: Application operation and maintenance (Table E.10 of EN50129)	70
Table 18: Safety management report. Techniques and procedures used	70
Table 19: Architecture of system/sub-system/equipment (Table E.4 of EN50129)	72
Table 20: Design features (Table E.5 of EN50129)	73
Table 21: Failure and hazards analysis methods (Table E.6 of EN50129).....	75
Table 22: Doors Sub-functions	82
Table 23: Doors Safety requirements from the TSI LOC&PAS (extracts)	84
Table 24: Brake Sub-functions.....	88
Table 25: Brake Safety requirements from the TSI LOC&PAS (extracts).....	92
Table 26: General Safety requirement from the TSI LOC&PAS (extract).....	92
Table 27: TCMS – System under Consideration	97
Table 28: TCMS – Precertification of components (preliminary)	98

1. INTRODUCTION

The Connecta project covers different TCMS research topics such as General TCMS Specification (WP1), Wireless TCMS and Train-to-Ground (WP2), Drive-by-Data (WP3), Functional Distribution Architecture (WP4), Brake Control (WP5) and transversal activities such as Virtual Placing on the Market (WP6).

In that context, WP3 work package's concrete goal is to make research on technologies and architectures for a new generation of a train communication system which allows to abstain from conventional train lines and which shall provide the sole communication platform for all type of applications spanning from safety critical functions up to SIL4 down to infotainment and CCTV applications.

The goal of this deliverable (D3.4 within WP3) is to provide a preparation of a generic safety concept / safety case for drive-by-data architectures defined in Task 3.5 (chapter 2), a definition of a generic certification process for drive-by-data enabled trains (chapter 3) and a preparation of selected safety cases for the selected functions/applications that are to be implemented for the demonstrator platform (chapter 4).

Results and defined principles from T3.3, e.g. "black-channel" approach and "failsafe-principle", are taken into account in order to ensure a largely safe communication as part of the overall safety function. The safety concept as well as the definition of a generic certification process will take place focused on the network side. This document takes as base the network architecture defined in CONNECTA D3.5 – Report on Drive-by-Data Architecture.

The concept is subdivided into three major parts.

Chapter 2 "preparation of a generic safety concept / safety case for drive-by-data architectures defined in Task 3.5" deals with identification of safety functions on System Level and the separation of safety relevant functions from non safety relevant functions each at network level and component level.

Chapter 3 "Considerations for generic certification process for drive-by-data enabled TCMS" basically describes a proposal that must be systematically considered in order to achieve certification according to the relevant safety standards for railway operations and how an extension or modification of an existing configuration and safety application can be incorporated without having to aim for recertification (iterative process). An essential objective of this chapter is to describe how the non-interference can be demonstrated or how it can be detected in the safety application if it could not be demonstrated.

Chapter 4 "Preparation of selected safety cases for the selected functions for the demonstrator platform" considers 2 safety functions, which exemplify how the safety concept from Chapter 2 and the certification process from Chapter 3 can be applied using the demonstrator platform. This chapter makes no claim to completeness of a complete safety function for the application examples shown. Simplifications are made at a more suitable point to improve understanding of a complex overall function (e.g. brake).

The document closes with a conclusion and 2 appendices. Annex A shows a tool-supported calculation of the minimum SFRT via Excel and Annex B describes a Guideline for supporting certification procedure.

2. GENERIC SAFETY CONCEPT / SAFETY CASE FOR DRIVE-BY-DATA ARCHITECTURE

2.1 GENERAL

The scope of this chapter focuses on the safety concept, so a Safety Plan or Functional Safety Management (FSM) Plan as a key document is expected as given. The FSM-Plan in general specifies how functional safety will be ensured throughout the entire development project and especially in train operation. The Safety Plan must identify roles and responsibilities as they apply to the development process and lists the techniques and measures that will be implemented as part of the development project to ensure that the targeted SIL can be achieved.

A Safety Requirements Specification (SRS) is also a central document when certification according to a functional basic standard (e.g. IEC61508) is required. This document lists all relevant safety requirements for a product or a system. It is a fundamental document for product or system design and it is used to clearly separate the safety requirements from the non-safety (functional / generic) requirements. For the last mentioned reason, this document is also a central part of this consideration, but not as an expected product SRS but as a system SRS. Nevertheless this should form the basis for design and verification and validation. At product level only suggestions can be made to achieve an easier certification (for example ED-S: Safe-Input or Safe-Output-Device). After completing the design and development, the Validation Test Plan (VTP) specifies how a product will be tested and is directly based on the SRS. This ensures that the final product or system requirements that were set forth at the beginning of the development of the product or the safety relevant system are met. In an IEC61508 compliant development process, the VTP should be created as soon as the SRS is complete. This will ensure that all requirements can be tested.

The main task of the safety concept (or generic safety concept) which is considered in this chapter besides parts of the SRS is to describe the safety-related HW and high level SW architecture and the safe communication channel. It decomposes the design of the safety functions and specifies the associated safety integrity functions and safety support functions such as operating and communication systems and justifies the partitioning.

This chapter describes a generic safety concept for an NG-TCN according to the common safety standards: IEC61508 and the railway specific standards: EN50126, EN50128, EN50657 and EN50129. In order to be able to provide simplified proof of safety, it is essential to separate the safety-relevant portions from the non-safety-relevant portions at system level within the SRS described above. In order to be able to carry out this separation consistently, it is important to correctly interpret the basic requirements of the safety functions. In addition, it is important to define a "safe-state" for the respective safety function because the concept follows in general the fail-safe approach.

2.2 IDENTIFICATION OF SAFETY FUNCTIONS ON SYSTEM LEVEL

The use of a modular system (system design) with respect to safety-relevant components or end-devices (ED-S) and a safe transmission channel allows the replacement of conventional train lines, if the required Safety Integrity Level (SIL) can be approved. In order to be able to perform the safety function with the required safety target, it is necessary to analyse whether the effectiveness

of the safety function is still given without the conventional train-line (elimination of the second independent safety path).

A Safety function with conventional train lines:

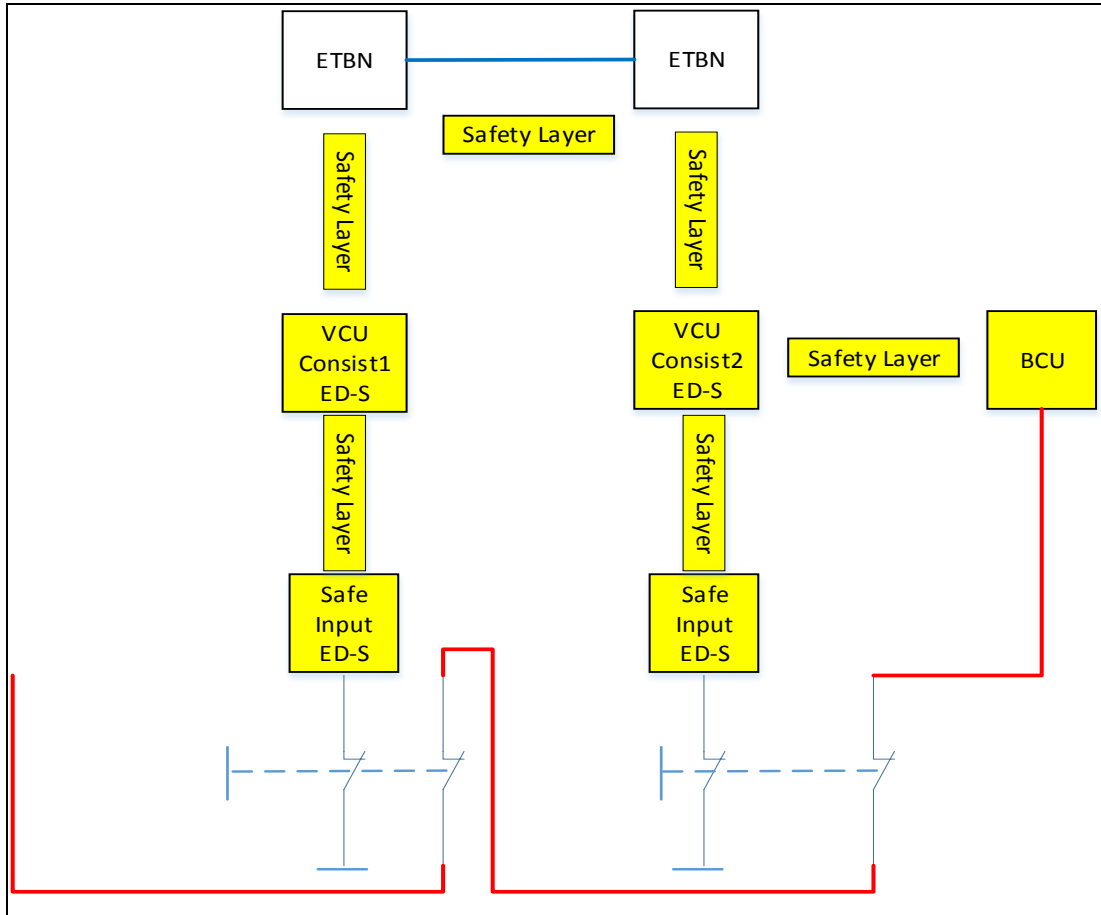


Figure 1 Safety function with conventional train line

The example figure 1 above shows in principle a safety function with an additional conventional train line (red marked) as an independent second operating path to achieve a high SIL (SIL3 or SIL4). This could represent for example a part of an emergency brake system without the claim to completeness of the overall safety functionality of an emergency brake system. In this safety case, the requirement to the remaining safety system (safe-Input-ED-S, Safety-Layer – VCU/CCU) is lower than for the whole safety function.

Future solution for NG-TCN without conventional train lines:

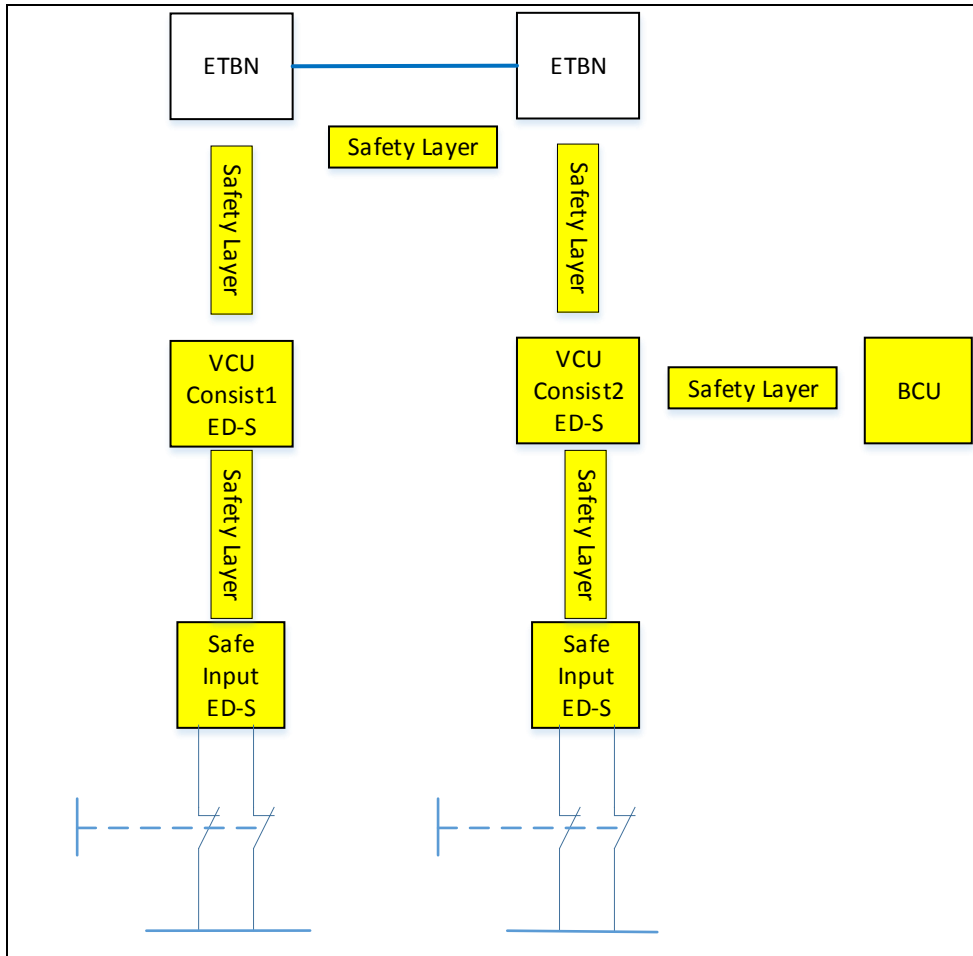


Figure 2 Safety function without conventional train line

The example figure 2 above shows in principle a safety function without an additional conventional train line. This could also represent like figure 1 for example an emergency brake system without the claim to completeness. In this safety case, the requirement to the remaining safety system (combinations of safe-Input-ED-S, Safety-Layer – VCU/CCU) is as high as for the whole safety function (safety loop). For safety related End-Devices and the safety protocol embedded in the safety loop the 1% rule of the THR should be generally striven for in order to achieve the SIL of the overall safety function.

An identification of safety functions on system level for the NG-TCN can be done by analysing the safety capability of ED-S (for example possibility to pre-configure “failsafe-value” for the defined safe state) and the capability of the network concerning the error detection mechanism for the required SIL (for example by the use of a pre-certified safety protocol).

2.2.1 Component level / Subsystems ED-S

Chapter 2.2.1 deals with the identification of safety functions at component level and how these can mainly be designed and implemented generically with the components in consideration (primarily ED-S). The following description contains examples and recommendations for implementation of safety functions.

Expectations on the functional safety capability of ED-S

- **Safe-Input-Device:**

- a) Redundancy of input-signals:

The majority of safety relevant signals in relation to their data type are binary signals. In this case, the signal quality of an operating action (push button/switch actuated) can already be checked within the digital input module by technological plausibility checking of the valence or antivalence of the two-channel read signals. Therefore the Safe-Input Device should be able to configure an associated second valent or antivalent channel together with an allowed discrepancy time.

The safe reading of analogue signals, standardized for example: 0..20mA or 4...20mA can be done via analogue sensors, at best to exclude common cause errors by different manufacturers and also be checked in a preconfigured discrepancy window (interval) with regard to tolerance.

- b) Internal error handling:

To best manage internal errors, the Safe-Input-Device should have a “dual-channel” hardware architecture (use of a second microprocessor), from which the input signals can be read separately and galvanically isolated. This dual channel design also has the advantage that the microprocessors can monitor each other for dormant errors in RTOS task monitoring, over- and undervoltage and overtemperature. Such errors must be propagated to the safety protocol interface. Alternative: Use of optocouplers and dc/dc converters for galvanic isolation and use of different ports in the same microcontroller to read inputs signals separately.

- c) Generating diagnostic messages in the non-safe-FW-part:

For every possible internal error within the module or a channel, there should at best be a complete asynchronous diagnostic option to the higher-level control unit (usually VCU/CCU). This diagnosis should be located in the non-safety-relevant software part of the device firmware and therefore should not have to lead to subsequent certification if changes are made in this part.

- d) Receiving and checking safety relevant configuration data:

The device firmware should be able to accept safety-relevant configuration data from the higher-level control device in the start-up phase before it switches to safety operation. It should be possible to check these safety-relevant project engineering data for transmission errors (e.g. by CRC check) and then save them protected against corruption or, in the event of a detected corruption, prevent safe operation of the device.

- e) Interface to a well-defined and safety-relevant safety protocol:

The device firmware must be able to pack the data read in as safe into a firmly defined safety protocol and execute the status machine defined for the generic safety protocol (e.g. SDTv2, or

manufacturer specific or in future SDTv4). In case of error detection (internal errors or channel errors), the error must be reported to the higher-level control application via safety protocol.

- **VCU/CCU:**

A VCU/CCU as a central control unit must be able to execute safety functions up to the required THR. To achieve higher safety requirements, there are basically 2 possible architecture variants:

The first one is a redundant HW-Structure with a single channel interface to the communication channel as shown in figure below:

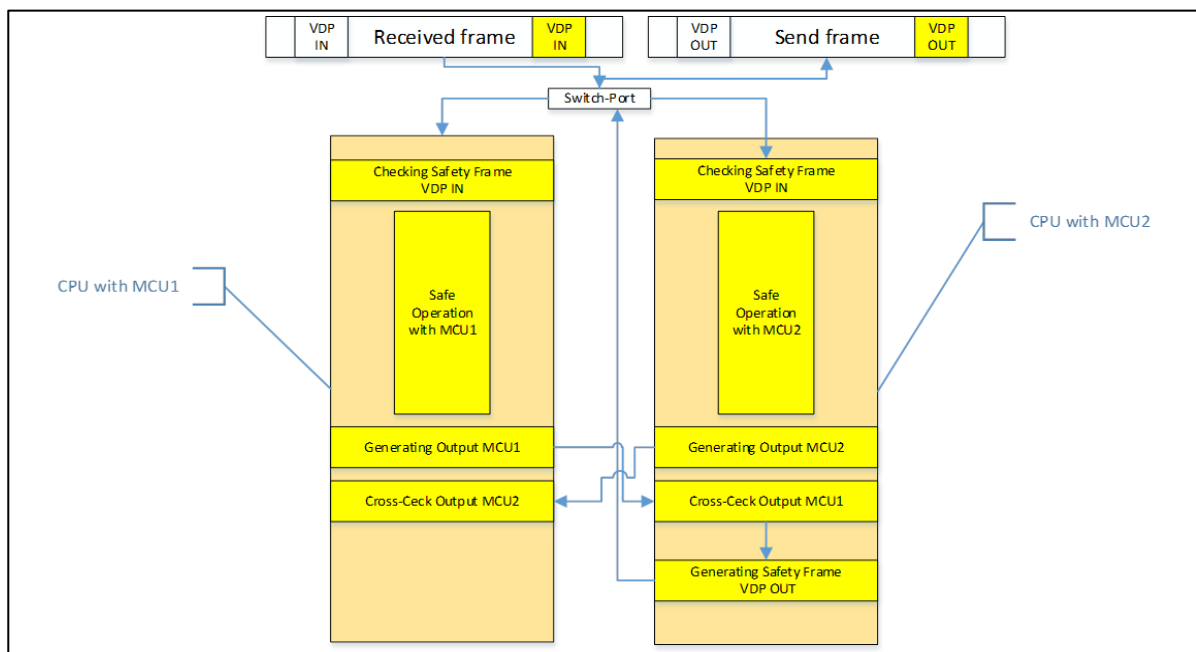


Figure 3 HW-redundancy used for error detection

The second one is a redundant SW-Structure with some HW-Extensions and a single channel interface to the communication channel as shown in figure below:

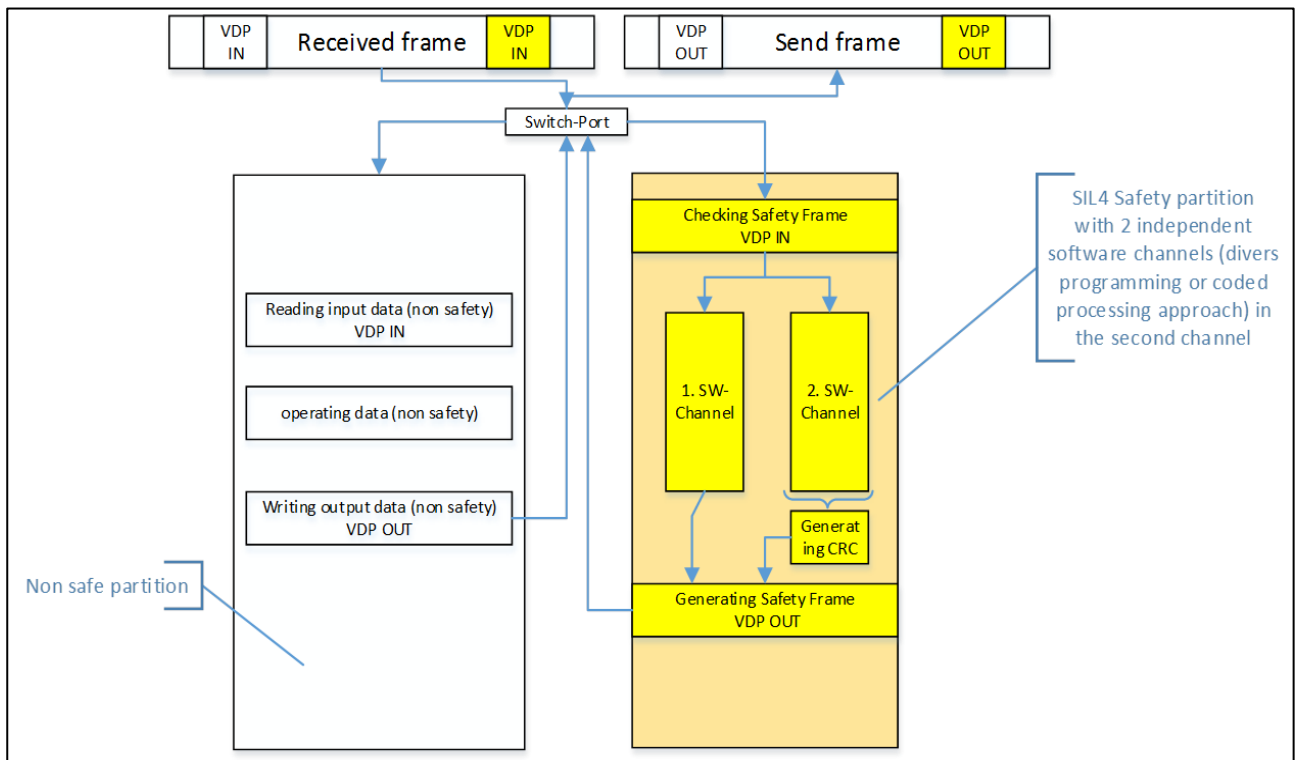


Figure 4 SW-redundancy used for error detection

- Safe-Output-Device:

a) Redundancy of output-signals:

As already described for the input signals the majority of safety relevant signals in relation to their data type are binary signals. This also applies to output signals. The methods of error detection for safe digital output are also largely dependent on the device architecture. For higher safety targets (SIL3 or SIL4), a dual-channel architecture of the output is highly recommended. This can be achieved for example by activating two transistors of two independent microprocessors in series for the output of one binary signal. This means that the output terminal only has voltage if both processors actuate their transistor independently. With an internal “dual-channel” hardware architecture it is also possible to switch the respective different potential for controlling an actuator, for example by one transistor switching +24V, the other switching the 0V. In the event of a fault, this means that only one transistor would switch and the actuator remains in the not actuated safe state. The module should also have cyclical self-test applications for detecting wire break, cross circuit and short circuit in order to detect sleeping channel errors.

- b) Internal error handling: (see description of the Safe-Input-Device)
- c) Generating diagnostic messages in the non-safe-FW-part: (see description of the Safe-Input-Device)
- d) Receiving and checking safety relevant configuration data: (see description of the Safe-Input-Device)

- e) Interface to a well-defined and safety-relevant safety protocol: (see description of the Safe-Input-Device)

Configuration and Deployment of safe application Software for ED-S

This chapter essentially describes the expectations for the safe-software components, which could change more frequently during the creation process of the train functions. Excluded from the consideration are, for example, FW components of safe input and output modules, which are usually only marginally changed after a general release and approval.

For the configuration of safe device parameters, the superimposed engineering tool should already be certified according to a common basic standard. Regardless of this, it is possible that an unintentional input error of a desired value may have occurred during input (for example, due to typing errors). For this, a common method is to print the configuration parameters and have them verified by an independent responsible person defined in the FSM plan using the dual control principle.

- Safe-Input-Device and Safe-Output-Device:

To configure safe input and output modules (devices), the engineering tool should provide the best possible support with regard to the possible adjustable value ranges. Possible plausibility checks should draw attention early to possible input errors during the engineering phase. For safe input and output modules or devices it should be possible to integrate a generic description file of each module or device within the engineering tool with a set of default values. These default values should be checked and changed if necessary.

Following listed set of parameter should be individually changed and checked. After the check of correctness was done, the parameter should be secured by CRC or Signature with same quality to check transmission errors to the device:

- Channel granular individual safe parameter:

For the reading of redundant signals (valent or antivalent), the desired value for the transmission of the unified signal after the discrepancy analysis by the module must be defined. Device or module individual safe parameter:

- Parameter of the supported safe data transmission channel for safe data transmission:

(Watchdog-Time, unique-address, functional address depending on the safe data transmission channel used for safe data transmission)

- VCU/CCU:

For configuration and deployment of safe application software for the VCU/CCU as a main controller it should be foreseen that safe parameters are secured via CRC or other signatures to proof, that changes only affect the safety-relevant part of the application. The CRC or signature can also be used to secure the download of the parameters against corruption. It is important to provide a single-channel interface for safe data transmission independent from the chosen architecture (HW-SW-Solution) of a VCU/CCU.

2.2.2 Network level

This sub-chapter considers the identification of safety functions at network level and how these can be generically designed and executed. NG-TCN defines two functions which are safety-related:

- Safe train inauguration
- Safe data transmission

Those two functions will be treated next.

Safe train inauguration as part of safe communication

Function

The function “safe train inauguration” is a safety-related function in accordance to EN50126-2 because its main task is to establish a train wide communication system which interconnects all “intelligent” equipment on-board trains.

The safe train inauguration is split in two phases: first the train backbone topology discovery (defined in IEC61375-2-5, IP-TCN specific extensions defined in [35]) and thereafter the discovery of the train composition (IEC61375-2-3, IP-TCN specific extensions defined in [35]). The first phase (“ETB inauguration”) aims to establish a train wide communication network allowing end devices of different consists to communicate, while the second phase (“operational train inauguration”) creates an application train view as a train composed of vehicles and consists. For the NG-TCN, this train view is presented with the TTDB, which is a repository containing all relevant information about the actual train composition, especially:

- Sequence of vehicles and consists
- Orientation of vehicles and consists
- Dynamic and static properties of vehicles and consists

Many train wide functions are relying on this information, like the side-selective door control or the brake control function.

System under Consideration (SuC)

The safety case requires a definition of the SuC. For the function of safe train inauguration the SuC (Figure 5) comprises the following network components as defined in [35]:

ETB:	The complete ETB with cables, connectors and repeaters, in topology variant D.
ETBN:	Device for connecting ECN and ETB, platform of safe train inauguration.
CCU	Platform for safe train inauguration validation and ETB control application

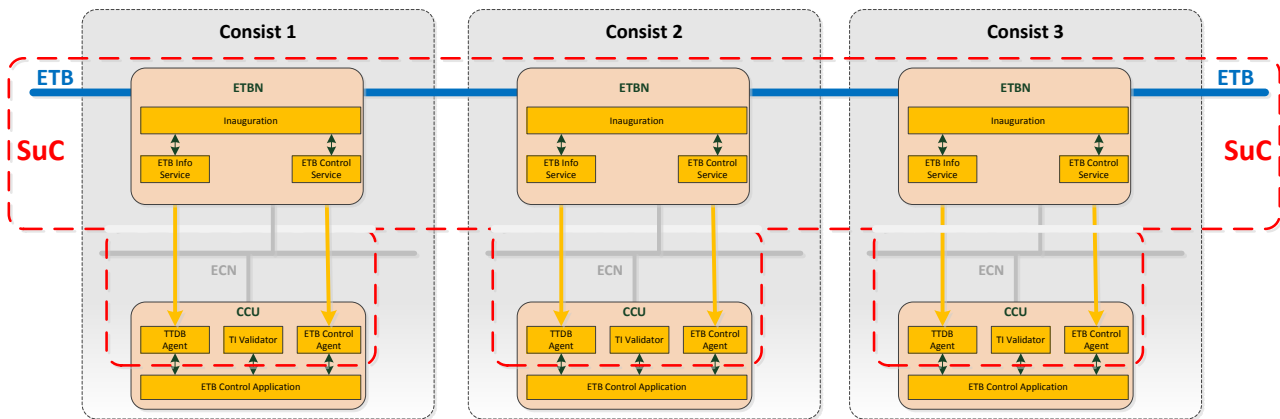


Figure 5: SuC

Not included are:

- ECN with cables, connectors, switches, routers
- CCU: ETB Control application itself and other applications
- End devices connected to ECN (except CCU)

The safe train inauguration function is the only safety-related function carried out by the SuC. Other, non-safety-related functions are for instance:

- IP routing between ECN and ETB
- Ethernet frame bridging along the ETB
- DNS service

Architecture for safe train inauguration function

Although the safe train inauguration function is a train wide function, it is not implemented as a central train function. Rather each consists provides a local implementation and all consist implementations are collaborating and so they are implementing the safe train inauguration decentralized.

The consist local architecture of train inauguration function as defined in [35] is shown in Figure 6. The complete train inauguration function is distributed to two devices, the ETBN and the CCU.

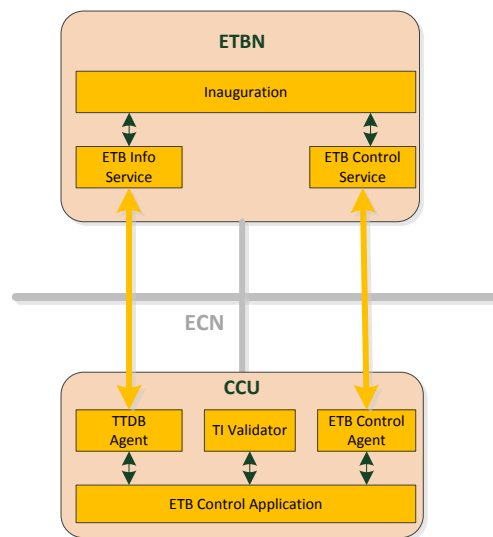


Figure 6: Safe train inauguration function architecture

ETBN and CCU comprise the following safe train inauguration elements as defined in [35]:

Inauguration:	Comprises ETB Inauguration and operational train inauguration functions. Produces the TTDB.
ETB Info Service:	Provides information about TTDB to CCU and other interested ED.
ETB Control Service:	Interface for ETB control and status, counterpart to ETB Control agent running on the CCU.
TTDB Agent:	Responsible to retrieve information from TTDB
TI Validator:	Train Inauguration Validator
ETB Control Agent:	Supports ETB control application in ETB control
ETB Control Application:	Application for project specific ETB control. Responsible to force safety reaction in case a dangerous failure occurs during inauguration

Safety-related Requirements

[30] defines the following three general requirements for the safe train inauguration:

ID_40016	The NG-TCN shall support the dynamic coupling or uncoupling of consists (train lengthening and train shortening) during service.
ID_40017	The NG-TCN shall continuously discover the actual train composition and shall maintain the discovery result in the Train topology database (TTDB) as defined in IEC61375-2-3.
ID_40018	The NG-TCN shall ensure that there is no more than one leading vehicle in the train during service.

These three general requirements can be broken down to functional safety requirements for the SuC implementing the safe train inauguration function:

- (1) Determine the number of rail cars in the train (train integrity)
- (2) Determine the sequence of rail cars in the train related to train reference directions defined in IEC61375-1
- (3) Identify the train end cars (train integrity)
- (4) Determine the orientation of rail cars in the train related to train reference directions defined in IEC61375-1

With the architectural choice to separate the safe train inauguration functions in the two parts TTDB computation and train inauguration validation (see [35]), it is useful to define additional functional safety requirements:

- (5) Provide independent¹ information about consist orientation and train end
- (6) Validate the TTDB with the aid of the independent information about consist orientation and train end

The train inauguration result shall be accessible by user applications, which leads to further functional safety requirement:

- (7) Provide safe access to the TTDB
- (8) Disseminate train inauguration validation result

And finally, a safety reaction is required (e.g. safe state) if a dangerous fault during train inauguration has been detected. Because the ETB control application is responsible for this which is outside the SuC, this is formulated as a contextual safety requirement²:

- (9) Enforce a safe state in case a dangerous fault is detected in the TTDB

In real implementations it has of course to be ensured that the result (TTDB) is safely generated (processed) and safely stored, which leads to additional technical safety requirements. This is not further considered herein.

Apportioning safety-related requirements

During safety analysis done in T3.3 (see [32]), THR values have been defined for the four functional safety requirements (hazards) of the inauguration function (1) until (4). According to EN50126-2, safety requirements have to be apportioned to the SuC components. In our case, this apportioning needs to be done between the functions running on the ETBN and the functions running on the CCU.

¹ Independent from train inauguration protocol

² For the definition of functional safety requirements, technical safety requirements and contextual safety requirements see EN50126-2.

Safe train inauguration is executed on the ETBN (TTDB computation) and independently validated by the CCU (TI validation), meaning that combination of both functions is used to counteract the hazard (“AND gate”).

In case of combination of multiple functions, the THR can be apportioned to sub-hazards and their TFFRs down to the level of the least independent function (EN50126-2 clause 10.2.2), which then receive a corresponding SIL.

For AND gate, the apportioning of the THR to sub-hazards follows the rule, that the THR is the product of the sub-hazard THR (or TFFRs) weighted with the SDT (safe down time)³. A possible apportioning of the safe train inauguration THR is shown in Figure 7.

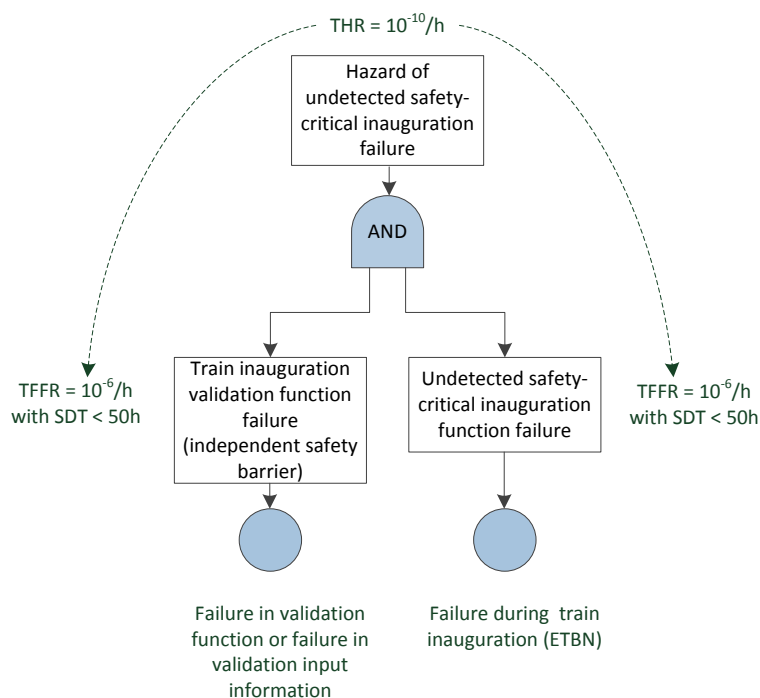


Figure 7: Train inauguration THR apportioning (example)

For the top level hazard the 1% rule is assumed, stating that the hazard of an undetected safety-critical inauguration failure contributes with about 1% to the train function which is using train inauguration information. This yield a value of $THR = 10^{-10}/h$ for this top-level hazard. The safe down time (SDT) implies that a safe train inauguration failure is detected and negated within a defined time. With the assumption of at least one train safe inauguration per service day, a failure will be detected within 24h.

Safe train inauguration functions as defined in [30] are analysed in [32] and safety targets are derived for the safe train inauguration functions. Table 1 lists the safe train inauguration functions together with the sub-functions and allocated TFFR and SIL values.

³ See EN50126-2 appendix D.3.2 and D.3.5.

Table 1: TFFR and SIL of inauguration sub-functions

Safe train inauguration function	Sub-Function	TFFR	Allocation to	SIL
Train inauguration (TTDB computation)	Determine the number of cars	$< 10^{-6}/h$	ETBN	2
	Determine the sequence of cars	$< 10^{-6}/h$	ETBN	2
	Identify the train end cars	$< 10^{-6}/h$	ETBN	2
	Determine the orientation of cars	$< 10^{-6}/h$	ETBN	2
TTDB validation (TI validation)	Provide independent information about consist orientation and train end	$< 10^{-6}/h$	CCU/IO	2
	Validate the computed TTDB with the aid of the independent information	$< 10^{-8}/h$	CCU	4
TTDB dissemination	Store train inauguration result in the TTDB and provide safe access to the TTDB	$< 10^{-6}/h$	ETBN	2
	Disseminate train inauguration validation result	$< 10^{-8}/h$	CCU	4
Safe state	Enforce a safety reaction in case a dangerous fault is detected in the TTDB	$< 10^{-8}/h$	CCU (ETB control application)	4

Intra-consist safe communication as part of a safety function

Function

As an architectural choice, NG-TCN provides safe communication between safe applications with the support of a safety protocol (SDTv4) using the transport capabilities of the network as a black channel. SDTv4 is defined in [35].

SDTv4 is an end-to-end protocol which can be based on any communication layer protocol underneath (TRDP, PROFINET IO, others). At sender side (safe data source SDSRC), SDTv4 adds protocol information needed for integrity checks (source identification, sequence counter, checksum), which is then used by the receiver(s) (safe data sink SDSINK) to check the integrity of the received telegrams.

System under Consideration (SuC)

EN50126 requires a definition of the SuC. For the function of safe data transmission, the SuC comprises the following network components for intra-consist communication as defined in [35]:

ED-S: SIL 4 capable device, e.g. CCU or IO devices connected to ECN.

ECN: ECN with cables, connectors, switches, routers.

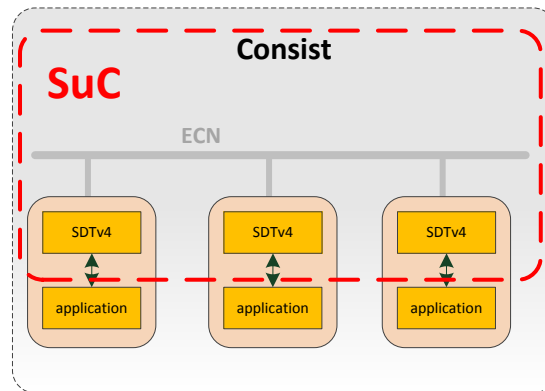


Figure 8: SuC Intra-consist communication

Not included are:

- ED-S: applications

Architecture for safe train communication function

The architecture of the intra-consist safe communication function is shown in Figure 9. The black communication channel between SDSRC and SDSINK is established with the communication layer protocol stacks (e.g. Ethernet, IP, UDP, TRDP, PROFINET IO) and the ECN network devices (passive and active). All application layer data are passing the SDTv4 protocol layer, where additional information for integrity checking is added (SDSRC) or removed (SDSINK). The SDTv4 protocol layer uses the lower level communication channel interface and the upper level SDTv4 application interface for interaction with application and black communication channel.

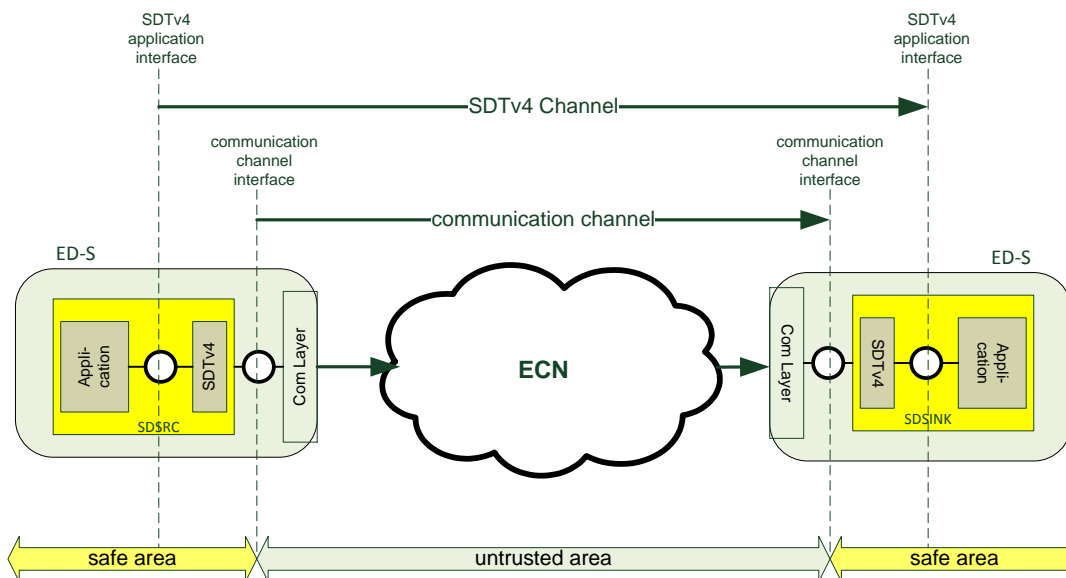


Figure 9: Architecture of intra-consist safe communication function

In intra-consist communication all communication relationships are static and can therefore be pre-configured.

Safety-related Requirements

[30] defines a bunch of requirements for the safe train communication, but the functionality is basically defined with the following 2 requirements:

ID_60005	ED-S connected to NG-TCN shall enter a defined safe state if the safe communication fails.
ID_60013	ED-S shall implement a safety layer in between the safe application(s) and the untrusted communication channel. The safety layer shall provide safety services as defined in EN50159 at least to detect following Message characteristics: Message authenticity Message integrity Message timeliness Message sequence

While ID_60005 defines a safety reaction of the safe application using SDTv4, ID_60013 defines the required functionality of the safe data transmission channel itself.

Inter-consist safe communication as part of a safety function

Function

Functions are identical to intra-consist communication, see above.

System under Consideration (SuC)

The SuC differs between intra-consist and inter-consist communication. For the function of safe data transmission the SuC comprises the following network components for inter-consist communication as defined in [35]:

ED-S: SIL 4 capable device, e.g. CCU or IO devices connected to ECN.
ECN: ECN with cables, connectors, switches, routers.
ETB: ETB with cables, connectors, switches, repeaters
ETBN: Interconnection between ECN and ETB

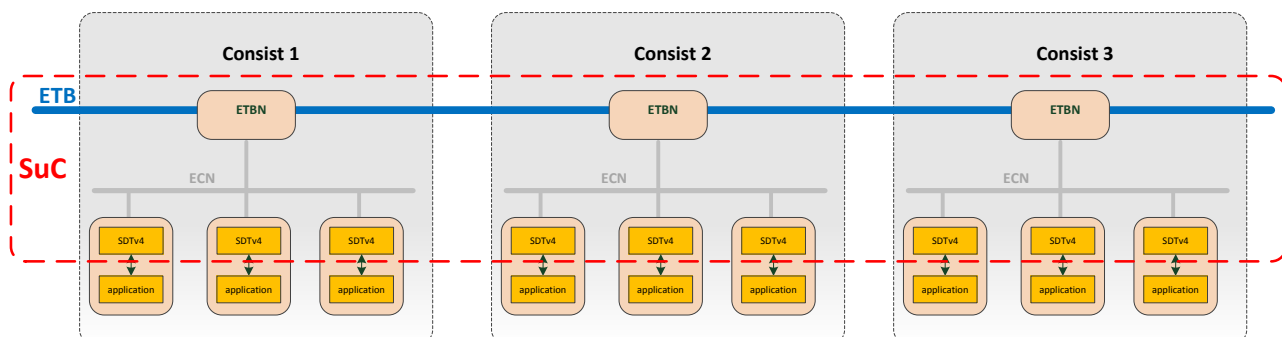


Figure 10: SuC Intra-consist communication

Not included are:

- ED-S: applications

Difference between intra-consist and inter-consist safe communication

The difference of the SuC between intra-consist and inter-consist communication has consequences for the usage and the configuration of the SDTv4 communication. Contrary to intra-consist communication where all communication relationships are static and can therefore be pre-configured, communication relationships are dynamic in inter-consist communication. Dependent on the actual train composition and the location of safety critical services (like leading car services), communication relationships may vary. This has consequences for the design of the safety layer (safe data transmission channel) but also on the design of the safe application (or the supporting middleware).

The safe train inauguration described before takes a key role here, as it provides the necessary information for the dynamic configuration of the communication relationships. SDTv4 is already prepared for this by using the safe topography counter (TTDB) within the SDSRC authentication process (SDSINK accepts only data from SDSRC if both share the same view on train composition).

For the application or the middleware handling the dynamic train composition, this is much more challenging. The following aspects need to be considered:

- 1) The potential maximal train composition. Application must be designed for this (availability of resources)
- 2) The actual sequence of consists. If there is a change in sequence, e.g. following a train lengthening or shortening, data flows might be rearranged.
- 3) Position of the leading consist. The leading consist position determines the operational train view (view from driver's perspective). If there is a change in leading position, data flows might be rearranged.
- 4) Role of leading consist. A consist in a leading role executes other functions than a guided consist. The leading role is dynamically assigned to a consist, so a consist must implement both the role of a leading consist and the role of a guided consist. In case of a change, data flows might be rearranged. Note that the safe inauguration protocol prevents a situation with two leading consists in a train.

2.3 SEPARATION OF SAFETY-RELEVANT FUNCTIONS FROM NON SAFETY-RELEVANT FUNCTIONS

Safety functions constitute an important element of the risk-reduction procedure described in the generic standard ENISO 12100 [03] and in the railway standard EN50126 [04]. The standards define the safety function as a “function of a machine whose failure can result in an immediate increase of the risk” and “function whose sole purpose is to ensure safety” respectively. Whether and to what extent the risk on a machine/train must be reduced is determined from the risk assessment. In this assessment, the risk presented by a train at the different stages of its life cycle is analysed and evaluated.

The architectural principles of NG-TCMS are described in D1.3 – Function Based Architecture [14] (Work Package 1). The list of these principles is the following one:

1. Function oriented.
2. Functional clustering.
3. Separation of the functions.
4. Minimise interfaces.

5. Security by design.
6. Scalability.
7. Support dependability.

Therefore, separation of the functions is one of the principles of the architectural model, which is described in Chapter 3.3 of D1.3 – Function Based Architecture [14]. In the same document, two domains are defined for functions of the NG-TCMS in the domain model. One is for services that are related to safety issues such as real train control and monitoring functions (TCMS). While the other one is for operator oriented services, such as on-board multimedia and telecommunication services (OMTS) that feature a direct value for the passenger

There are several types of breakdown structure, for example system breakdown structure or functional breakdown structure. For Safety purposes the focus is, as is described in D1.3 – Function Based Architecture [14], on a functional breakdown which groups the functions together in a way that they can be carried out by a subsystem. In this case the functions of the system under consideration should be identified and described when the phase of system definition is started. The norm EN50126-1[04] defines in the section 7 the “system definition” phase or phase 2 of the lifecycle.

Risk assessment process is based also on a system definition and an iterative method is applicable in different phases of the risk management lifecycle [08]. The system must be defined as functional breakdown approach considering the safety aspects.

Before any analysis relating to safety is undertaken, boundaries and functions of the system under consideration shall be established. Therefore, at least the following issues shall be outlined:

- The system objective (intended purpose) and its mission profile.
- The system boundary.
- The scope of operational requirements influencing the system.
- Existing safety measures and assumptions that determine the limits for the risk assessment.
- Identification of the system and related documents, including assumptions made about particular functions or subsystems that are different from an existing reference version, explicitly stating and justifying the deviation.

Major external factors of the system should be also considered, including: stakeholders and boundaries of the system, physical and functional interfaces and limits of risk assessment. System boundaries are defined in D1.2 – TCMS Use Cases [15] and an actor analysis of the NG-TCMS is done in chapter 5 of this document.

Functional breakdown examples in railway context are given in the following Table 2:

System	Functional breakdown group	Function	(Subsystem that carries out the function)
Fixed installations	Provide traction energy for trains	Convert, distribute and control electric energy	Substation & switching stations
		Transmit electric current to vehicle	Contact line systems
	Manage access to track	Open platform screen doors when train is present in station	Platform screen door system
	Control access to station	Allow full free passage in case of evacuation	Access gate system
Rolling stock	Control speed of train	Decelerate train	Brake system
		Hold train in standstill during stop	Brake system
	Control access to train	Hold all exits closed when vehicle is moving	Door control system
Control command and Signalling	Route control	Hold position of pointwork	Interlocking
		Indication signal aspect to driver	Interlocking
	Supervise speed of train	Ensure that train does not exceed maximum speed	Train control

Table 2: Safety function examples (Table D1 of the EN50126-1[04])

A preliminary list of functions and/or preliminary system requirements specification must be defined depending on the level of application and on the level of known details of the functions.

The identified functions should be grouped together on basis of:

- Contribution to the same function or higher level.
- Identified technical constraints (like subsystem to be reused).

Functions groups in railways application are listed in the norm EN15380-4[05] and Classification for system level is defined in the norm EN15380-5 [06]. As is done in D1.3 – Function Based Architecture [14], function breakdown analysis and function analysis are based on the breakdown structure of this norm. These analyses are done in chapter 5 and 6 of this document [14]

The risk management and independent assessment process from the CSM RA [08][07] specifies “system definition” and “hazards identification” as the first phases of the process. The strategy for the risk assessment is also detailed in the norm ENISO 12100[03] in a general way and the process is divided in 4 steps (determine the limits, identify hazards, estimate risk and evaluate the risk), where the second one is also the “identification the hazards and associated hazardous situations”.

The designer shall identify hazards taking into account:

- Human interaction during the whole lifecycle of the machine.
- Possible state of the machine.
- Unintended behaviour of the operator or reasonably foreseeable misuse of the machine.

The safety lifecycle begins with a Preliminary Hazard Analysis, which is performed using several methods and techniques. According to the norm 50126-2[09] techniques and methods for hazard identification (that are defined as useful) are HAZOP, PHA, FMECA and RBD (RBD as support of HAZOP).

The HAZOP technique has several limitations as detailed IEC61882:2016 [10] and therefore should be used in conjunction with other suitable approaches and other relevant studies should be coordinated within an effective, overall management system.

Other risk identification and analysis methods are detailed in IEC/ISO 31010 [11] and could be used in conjunction with the method previously explained. The following table shows a summary of the tools used for the risk assessment.⁴

Tools and techniques	Risk assessment process					See Annex
	Risk Identification	Risk analysis			Risk evaluation	
		Consequence	Probability	Level of risk		
Brainstorming	SA ¹⁾	NA ²⁾	NA	NA	NA	B 01
Structured or semi-structured interviews	SA	NA	NA	NA	NA	B 02
Delphi	SA	NA	NA	NA	NA	B 03
Check-lists	SA	NA	NA	NA	NA	B 04
Primary hazard analysis	SA	NA	NA	NA	NA	B 05
Hazard and operability studies (HAZOP)	SA	SA	A ³⁾	A	A	B 06
Hazard Analysis and Critical Control Points (HACCP)	SA	SA	NA	NA	SA	B 07
Environmental risk assessment	SA	SA	SA	SA	SA	B 08
Structure « What if? » (SWIFT)	SA	SA	SA	SA	SA	B 09
Scenario analysis	SA	SA	A	A	A	B 10
Business impact analysis	A	SA	A	A	A	B 11
Root cause analysis	NA	SA	SA	SA	SA	B 12
Failure mode effect analysis	SA	SA	SA	SA	SA	B 13
Fault tree analysis	A	NA	SA	A	A	B 14
Event tree analysis	A	SA	A	A	NA	B 15
Cause and consequence analysis	A	SA	SA	A	A	B 16
Cause-and-effect analysis	SA	SA	NA	NA	NA	B 17
Layer protection analysis (LOPA)	A	SA	A	A	NA	B 18
Decision tree	NA	SA	SA	A	A	B 19
Human reliability analysis	SA	SA	SA	SA	A	B 20
Bow tie analysis	NA	A	SA	SA	A	B 21
Reliability centred maintenance	SA	SA	SA	SA	SA	B 22
Sneak circuit analysis	A	NA	NA	NA	NA	B 23
Markov analysis	A	SA	NA	NA	NA	B 24
Monte Carlo simulation	NA	NA	NA	NA	SA	B 25
Bayesian statistics and Bayes Nets	NA	SA	NA	NA	SA	B 26
FN curves	A	SA	SA	A	SA	B 27
Risk indices	A	SA	SA	A	SA	B 28
Consequence/probability matrix	SA	SA	SA	SA	A	B 29
Cost/benefit analysis	A	SA	A	A	A	B 30
Multi-criteria decision analysis (MCDA)	A	SA	A	SA	A	B 31
¹⁾ Strongly applicable.						
²⁾ Not applicable.						
³⁾ Applicable.						

Table 3: Tools used in Risk Assessment Process. Table A.1 of IEC/ISO 31010 [11]

A general methodology to separate⁵ safety functions from non-safety functions is:

⁴ last column of the following table (see Annex) references the Annexes from Table A.1 of IEC/ISO 31010

⁵ “To separate” is not intended as independence between functions, but classification of the functions between safety related and non-safety related functions

1. Identification of the system functions.
2. Hazards identification.
3. Risk assessment in case of failure of the function.

As mentioned previously, the norm EN50126 [09] recommends the use of techniques as PHA, FMECA, HAZOP and RBD for the hazard identification. The risk evaluation of the function of the system shall be performed and depending on this evaluation, the function shall be considered as safety function or non-safety function.

After having an identification of the non-safety related function and safety related functions, justification and demonstration of non-interference between them is necessary for a certification.

2.3.1 Independence of safety-related functions

The norm IEC61508 [12] identifies qualitative requirements for independence of safety-related functions (IEC61508-2 [13] clause 7.4.2.3 and 7.4.2.5, IEC61508-3 [02] clauses 7.4.2.8 and 7.4.2.9):

- Where an E/E/PE safety-related system is to implement both safety and non-safety functions, then all hardware and software shall be treated as safety-related unless it can be shown that the implementation of safety and non-safety function is sufficiently independent (i.e. that the failure of any non-safety-related function does not cause a dangerous failure of the safety-related functions).

Note 1: Sufficient independence of implementation is established by showing that the probability of a dependent failure between the non-safety and safety-related parts is sufficiently low in comparison with the highest safety integrity level associated with the safety functions involved.

- When independence between safety functions is required then the following shall be documented during the design:
 - The method of achieving independence;
 - The justification of the method.

EXAMPLE: Addressing foreseeable failures modes, that may undermine independence, and their failure rates, use of FMECA or dependent failure analysis.

- Where the software is to implement both safety and non-safety functions, then all of the software shall be treated as safety-related, unless adequate design measures ensure that failures of non-safety functions cannot adversely affect safety functions.
- Where the software is to implement safety functions of different safety integrity levels, then all the software shall be treated as belonging to the highest safety integrity level, unless adequate independence between the safety functions of the different safety integrity level can be shown in the design. The justification of independence shall be documented.

As it is defined in D1.3 – Function Based Architecture [14], the architectural design must guarantee that any change made to a function will not affect other functions. This means, in NG-TCMS the independence between safety and non-safety related functions must be guaranteed and any

changes of hardware and software of the non-safety related functions shall not affect in the safety related functions.

2.3.2 Techniques

Techniques for achieving non-interference between functions are shown in Annex F of IEC61508-3 [02]. A causal factor analysis should be undertaken to identify all possible causes of execution interference between the notionally independent elements, therefore to demonstrate independence of execution. It must take into account that independence of execution should be achieved and demonstrated both in spatial and temporal domains.

Spatial independence: Used data of an element may not be changed by another element.

Temporal independence: An element may not influence the correct function of another element by:

- taking too high a share of the available processor execution time.
- blocking execution of the other element by locking a shared resource of some kind.

General techniques for achieving non-interference are shown in the annex F.4 (spatial interference) and F.5 (temporal independence) of the norm IEC61508-3 [02].

Techniques for achieving and demonstrating spatial independence include the following:

- Use of hardware memory protection between different elements.
- Use of an operating system which permits each element to execute in its own process with its own virtual memory space.
- In case where hardware memory protection is not available, use of rigorous design, source code and possibly object code analysis to demonstrate spatial independence.
- Software protection of data of higher integrity element from illegal modification by lower integrity element.

Techniques for ensuring temporal independence include:

- Deterministic scheduling methods.
- Strict priority based scheduling implemented by a real-time executive with means of avoiding priority inversion.
- Time fences which will terminate the execution of an element if it over-runs its allotted execution time or deadline.
- An operating system which guarantees that no process can be starved of processor time.

Definition of relevant terms of module coupling is given in Table F.1 of EN61508-3 [02] and aspects of module coupling can be distinguished in Table F.2 of the norm.

2.3.3 Example for achieving non-interference

One of the techniques is the encapsulation, defined in the norm IEC61508-3 [02] as “hiding of internal (private) data and subprograms from external access; term primarily used with object oriented programs”.

An example at components level is shown in Figure 11.

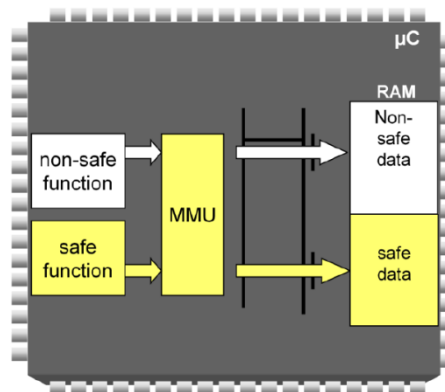


Figure 11: HW-Capsulation of Safe Data

In the previous example, non-safe functions may have only access to non-safe data. A memory management unit (MMU) is used in order to block access to safety data. The diagnosis of the MMU is carried out in this way: no safe function tries to access to safe data and the test is positive if the access is blocked by the MMU.

An example of encapsulation at system level is shown in Figure 12.

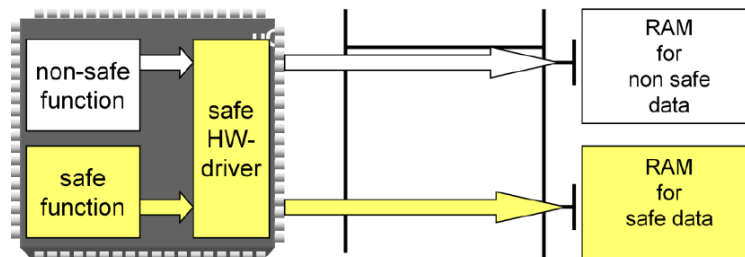


Figure 12: Software encapsulation of data

In the previous example safe and non-safe data share a common address/data bus. A safe hardware driver must ensure that non-safe function has not access to safety data.

3. CONSIDERATIONS FOR GENERIC CERTIFICATION PROCESS FOR DRIVE-BY-DATA ENABLED TCMS

3.1 APPORTIONING OF A SAFETY FUNCTION FROM SYSTEM LEVEL TO COMPONENT LEVEL “TOP DOWN” PRINCIPLE

The CSM regulation (402/2013/EU) [16] defines a harmonized and generic risk management process to be applied to new rail systems in agreement with the EN5012x [17][18][19][20] standards or to systems with a significant change that has an impact on safety. In this process SIL can specify safety requirements to safety-related functions given the conclusions of the risk analysis and evaluation. This process derives global safety objectives associated to hazards, some objectives being defined in terms of Tolerable Hazard Rate (THR).

Functions performed by a safety-related system to comply with SIL (or safety requirements in general) must be validated. Techniques and measures must also comply with the requirements of SIL. According to sectors, there are different methods to allocate SIL depending on standard in use, national practices and regulations, project's and operator's methods in use or available data (IEEE 1012 2012 [21], IEC62061 2005 [22], IEC61511 2003 [23]). Methods to allocate safety requirements mostly employed in railway domain are the risk matrix (EN50126 [17]) and the risk graph (IEC61508 [29]), even if they are mainly used to derive safety requirements in general.

Some safety parameters in the safety apportioning context are:

- PFD_{avg} : Average probability of dangerous failure on demand.
- PFH: Probability of dangerous failure per hour.
- THR: Tolerable Hazard Rate.
- TFFH: Tolerable Functional unsafe Failure Rate.
- RRF: Risk Reduction Factor.

According to the norm EN50129 [20], a methodology to determine safety integrity requirements for railways signalling equipment shall be systematically applied. Both the operational environment and the architectural design of the signalling system shall be taken into account. From a safety point of view, the interface between operational environment and the signalling system is defined by a list of hazards and associated THRs within the system. THR is a target measure with respect to both systematic and random failures.

The norm EN50126-2[18] replaces the term THR (used in the last version of the standard) to TFFR as a quantitative rate for safety-related functions. However THR is also defined in the norm as a quantitative rate for hazards. The quantitative safety target expressed as THR for a given hazard should relate to specific elementary functions without considering the number of instances⁶ of

⁶ In the context, instance is seen as subfunctions or part of a function.

those functions in the whole railway system (This will avoid that a given technical system fulfilling a defined THR and already accepted in a specific application, would no longer be considered accepted when used in a different application).

In railways context, as it said, the norm EN50126 [17] defines the risk acceptance criteria in terms of the Tolerable Hazard Rates and the TFFRs related to. THR is determined by the severity of the consequences resulting from the hazard. Quantitative measures according EN50126 [18] and EN50129 [20] are given in the following tables:

TFFR [h^{-1}]	SIL attribution	SIL qualitative measures
$10^{-9} \leq TFFR < 10^{-8}$	4	Defined in sector-specific standards
$10^{-8} \leq TFFR < 10^{-7}$	3	
$10^{-7} \leq TFFR < 10^{-6}$	2	
$10^{-6} \leq TFFR < 10^{-5}$	1	

Table 4: SIL versus TFFR

Tolerable Hazard Rate THR per hour and per function	Safety Integrity Level
$10^{-9} \leq THR < 10^{-8}$	4
$10^{-8} \leq THR < 10^{-7}$	3
$10^{-7} \leq THR < 10^{-6}$	2
$10^{-6} \leq THR < 10^{-5}$	1

Table 5: SIL versus THR

Alternatively, the generic norm IEC61508 [25] defines the allocation of the safety integrity level in terms of PFD and PFH. The first one is used for a low demand mode operation and the second one is used for both high demand mode operation and a continuous mode operation. The operation modes are defined in IEC61508-4 clause 3.5.16 as follows:

- *High demand mode*: where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is greater than one per year.
- *Continuous mode*: where the safety function retains the EUC in a safe state as part of normal operation.
- *Low demand mode*: where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is no greater than one per year.

Quantitative measures defined in the norm IEC61508 [25] are:

Safety integrity level (SIL)	Average probability of a dangerous failure on demand of the safety function (PFD _{avg})
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$

Table 6: SIL versus PFD_{avg}

Safety integrity level (SIL)	Average frequency of a dangerous failure of the safety function [h ⁻¹] (PFH)
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

Table 7: SIL versus PFH

In railways context (it could be also accepted in a generic context) and according the norm EN50126-2 [18], a hazard control process starts from risk analysis, which defines a list of hazards with their THR targets. For each hazard of the list, an apportionment is performed using a methodology or technique. After this methodology is performed: on the one hand, TFFR (Tolerable Functional Failure Rate) and SIL of each of the independent functions is determined, on the other hand, the independent function is distributed and apportioned to subsystems, therefore failure rate for subsystems and components is specified. The norm EN50126 defines the term “Hazard control” as the process of apportioning safety-related requirements to the components of the system under consideration. The apportionment of the functional safety requirements related to the hazard control is given in the Figure 13.

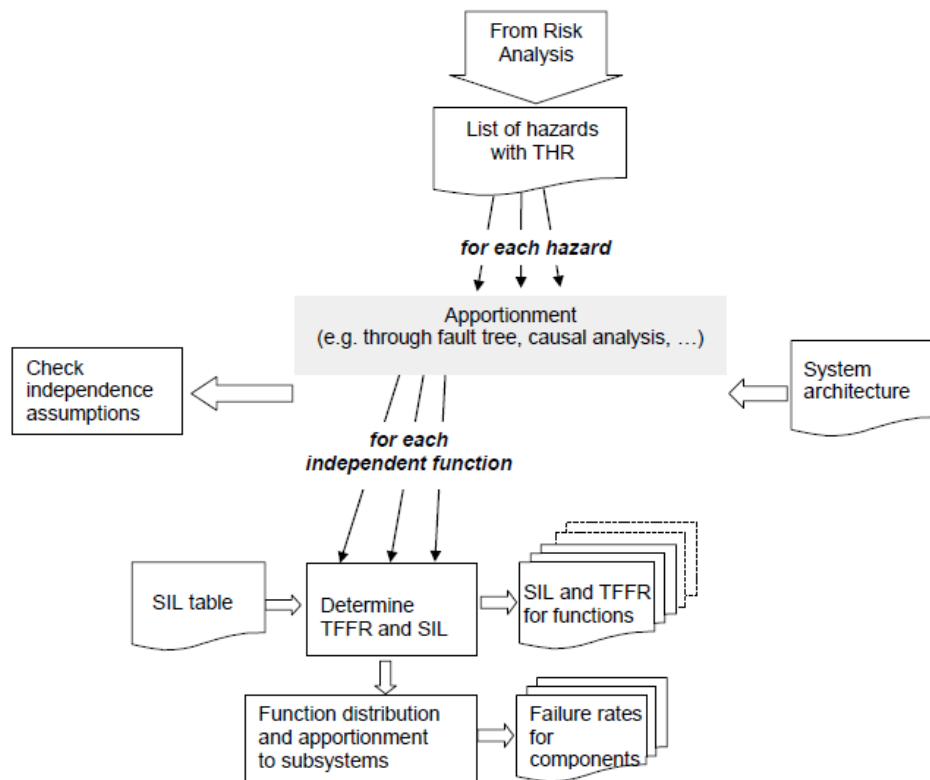


Figure 13: Apportionment of functional safety requirements according EN50126-2 [18]

The apportionment of the THR is done by causal analysis using various methods such as fault tree and taking into account the logic independences between the subsystems or functions.

Relationship between functions and hazards can be:

- One-to-one: The quantitative safety integrity requirement for each hazard expressed as THR shall be completely allocated to the function that protects against that hazard in terms of TFFR.
- Not one-to-one. A hazard can be caused by the unsafe failure of one or more functions. The quantitative safety integrity requirement for each hazard expressed as THR shall be apportioned in sub-hazards and the TFFR down to the *level of the last independent functions* (define as: A. Any of the functions is able to counteract the hazard at this level, regardless of the presence or absence of the other one, even though with different efficiency. B. No random common cause can jeopardize safety and no systematic common cause failures can jeopardize safety). In this level two or more functions control the same hazard.

The independence shall be demonstrated by a Common Cause Failure Analysis (3.3) and all assumptions⁷ made shall be properly documented and exported if needed. It shall be detailed how the overall THR is achieved including contributing factors from sub-functions (e.g. detection and negation requirements).

⁷ One assumption in the NG-TCMS is the one percent rule for the safe data transmission channel or Safety communication system described in CONNECTA D3.3 – Report on RAMS and Security Analysis [32] where the safe data transmission channel should reach a THR of 1%.

The result of the analysis is either the demonstration of independence or the understanding of existing (critical) common causes. As consequences of the analysis, the apportioning of the functions is carried out as follows:

If freedom from both systematic and random critical common cause failures is assured among two or more functions, TFFR may be further apportioned and the SIL may be allocated at the lowest level of these functions. (In SIL allocation, for function controlling the same hazard, apportioning in the lowest level of independence is applied and for function controlling multiple hazards, the most restrictive requirements is applied).

If freedom from only common random failures is assured then random integrity requirements (TFFR) may be further apportioned to the next lower architectural level of implementation but SIL remains unchanged.

The TFFR apportionment process may be performed by any method which allows a suitable representation of the combination logic, e.g. reliability block diagram, fault trees, binary decision diagrams, Markov model, Petri nets, etc. In any case, particular care is needed when independence in the sense of no critical common systematic and random failures of items is required. Assumptions made in this phase shall be checked and could lead to safety-related application conditions.

Only random failures can be quantified and it can be theoretically verified that the TFFR requirements are fulfilled. Systematic failures must be controlled by the adequate process and qualitative requirements stipulated by the SIL qualitative measures and therefore are not contributing to the calculation and quantitative fulfilment of the required safety integrity requirements. Qualitative measures are needed as protection against random and systematic failures. They are addressed as quality management conditions, safety management conditions and technical safety measures. They are correlated to a range of TFFR and defined in the annex A and annex E of the standards EN50128 [19] and EN50129 [20].

After SIL allocation, when the safety related function is apportioned in a number of sub-functions, the TFFR is further apportioned leading to the failure rates for the sub-functions/subsystem/elements. For a function controlling multiple hazards, if the derivation of the TFFR apportionment is performed separately for each hazard, then the most restrictive requirement shall be applied.

Apportionment of functional safety integrity may also be based on qualitative approaches.

3.1.1 Apportionment with a FTA

According to the norm IEC61025 [57] (which specifies a FTA procedure), Fault tree analysis is a deductive (top-down) method of analysis aimed at pinpointing the causes or combinations of causes that can lead to the defined top event. The analysis can be qualitative or quantitative, depending on the scope of the analyses.

THR should be specified (e.g. by the operator) and system designer must determine whether their system design is capable of meeting the target. In practice, the operator defines targets at the railway system level and may need to work together with the railway suppliers to define THR at the technical hazard level. The next step is to determine the SIL of the safety-related functions based

on safety targets allocated initially using THR, which are associated to each hazard (main criterion within SIL allocation in the railway domain).

FTA is used as method for the apportionment process of the figure 13.

This analysis allows to determinate the TFFR and SIL of each function/sub-function and failure rates of the subsystems/components

A general methodology includes the following phases:

- The allocations of the THR objective at the top of the fault tree. For hazards identified, a safety objective in terms of THR is set. Then these THR objectives are reported to the fault tree top event.
- Apportionment of the THR objective to safety related function using the procedure of the norm IEC61025 [57] using “OR” and “AND” gates. To justify the independence of the functions is needed to ensure the correctness of the apportionment process⁸.
- Modifications of THR according regulations, technical issues or commercial issues.
- Validation and verification of the apportionment. In the FTA, possible functions repeated in different branches or functions appearing in different hazards can involve more restrictive constraints⁹.
- SIL allocation based on apportioned and validated THR values is finally established according the norm EN50129 [20].

The system elements are considered from the functional point of view as several hardware/software architectures are possible. In the railway standards there is no explicit indication/rule or provided guidance on how to reduce or manage the SIL allocation considering dependable architectural solutions, as is done in the IEC61508 [29] generic standard. For a particular sub-function with a specific SIL, supplier architecture solutions may be different but equally satisfactory.

The verification can allow that functions and their associated sub functions have a constraint relaxation (consequence that other functions have more restrictive constraints). When the safety target THR is not achieved, the risk acceptability needs to be demonstrated (e.g. expert arguments).

⁸ Note that dependent functions get the same THR than the upper level function. The independence shall be demonstrated by a Common Cause Failure Analysis.

⁹ A Down-Top methodology is recommended for the verification

3.2 FAULT HANDLING AND SAFE STATE

3.2.1 Definition of the fault handling for the safety function

Depending on the various components that can be used to execute a safety function, a large number of possible errors may occur that must be reliably detected with the remaining residual error rate of the safety relevant component or safe End Device (ED-S). There are also many combinations regarding the reaction to detected errors, depending on the component that detected the error. The quality of the error detection measures of safety-relevant components determines whether the error handling is implicit or explicit or a combination of both. It is therefore important for the architecture and design of a safety function to determine how detected faults are handled or how the system reacts to detected faults.

The following example should provide an illustration:

A safety function is processed using a safety-relevant digital input device with a network connection via safety protocol to a safety-relevant processing central unit (VCU/CCU) and a network connection with safety protocol to a safety-relevant digital output device.

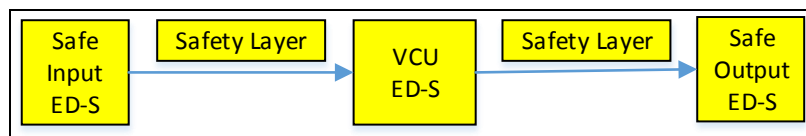


Figure 14: HW-Design of a Safety function using different ED-S and network

This simple safety function can therefore be divided into 5 subordinate functions:

1. Safe reading of digital redundant sensors via Safe-Input-Device (ED-S)
2. Safe data transmission via safety layer
3. Safe processing within the central unit VCU/CCU (ED-S)
4. Safe data transmission via safety layer
5. Safe output to the actuator via Safe-Output-Device (ED-S)

This leads to the question, how is a detected error in one of the 5 subordinate functions handled from the system view regarding the safety reaction? Finally, in this constellation, only the safe digital output (sub-function 5) can lead to a safe state. For this purpose, a detected error must be propagated to the safe digital output module.

Possibilities as examples of error propagation: (without claim to completeness)

1a) Overtemperature, over- or undervoltage, if detected by Safe-Input-Device => Error information added within sending data of the safety layer. The subsequent processing unit can decide how to react to this error.

1b) Overtemperature, over- or undervoltage, if not detected by Safe-Input-Device => In this case, it is assumed that the microprocessor(s) can no longer process the status machine for the safety protocol either. The subsequent processing unit is detecting the error by the safety layer and can decide how to react to this error as part of the safe application.

1c) Discrepancy error of the redundant signals detected by Safe-Input-Device => Error information added within the sending data of safety layer. The subsequent processing unit can decide how to react to this error as part of the safe application.

2a) Loss of data, Insertion of data, Data corruption,... => detected by the safety layer in VCU/CCU. The subsequent processing unit can decide how to react to this error as part of the safe application.

3a) Overtemperature, Over- or undervoltage, if detected by VCU/CCU => Error information added within sending data of the safety layer. The subsequent Safe-Output-Device outputs the safe substitution values instead of the process values.

3b) Overtemperature, Over- or undervoltage, if not detected by VCU/CCU => In this case, it is assumed that the microprocessor(s) can no longer process the status machine for the safety protocol either. The subsequent Safe-Output-Device is detecting the error by the safety layer and outputs the safe substitution values instead of the process values.

4a) Loss of data, Insertion of data, data corruption is detected by the safety layer in the Safe-Output-Device. The subsequent Safe-Output-Device is detecting the error by the safety layer and outputs the safe substitution values instead of the process values.

5a) Any error detected by the safe Safe-Output-Device itself leads to the safe state. (Output the safe substitution values instead of the process values)

Conclusion:

As the example shows, when dividing a safety function into sub-functions and sub-components, it is very important to consider the consequences of error detection and error inheritance up to the component that finally can force the safe state.

3.2.2 Definition of the safe state for the safety function

Function Safe Train Inauguration

The safe train inauguration concept as defined in [35] aims to discover the actual train composition, to compute the TTDB and provide a control&status interface for the controlling application (see sub-chapter 2.2.2 for a basic description of the safe train inauguration function). Safe train inauguration is executed in different phases, each phase leading to a specific dataset as it is defined in IEC61375-2-3:

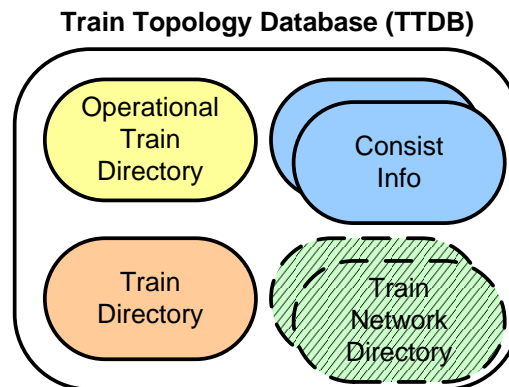


Figure 15: TTDB datasets

Consist Info:	Static description of the consist (number of rail-cars, supported functions, other properties)
Train Network Directory (TND):	ETB Topology, consist sequence
Train Directory (TD):	(Confirmed) composition of the train, ordered list of all consists which constitute the train. Changes only when train composition changes (train lengthening/shortening)
Operational Train Directory (OTD):	Operational train view as an ordered list of rail-cars according to operational train directions, indication of the leading cab. Changes each time the leading cab is changed.

In order to identify the safe state(s) another aspect is important. The amount of executed inauguration phases varies with the operational use case as it is shown in the subsequent table:

Table 8: Inauguration related to train operation use case

Train operation use case	Effect on inauguration function
Train power-up in Depot	All directories (TND, TD and OTD) will be re-computed.
Decoupling vehicles in the marshalling yard, in the station	All directories (TND, TD and OTD) will be re-computed.
Coupling vehicles in the marshalling yard, in the station	Until physical/virtual coupling occurs, the inauguration inhibition function prevents a re-computation of all the directories, in order to not influence the train operation during the coupling phase. After physical coupling, inauguration inhibition is removed resulting in a re-computation of all directories (TND, TD and OTD).
Decoupling (end) vehicles during run (unintended train separation)	The inauguration inhibition function prevents a re-computation of the TTDB, in order to not influence the train operation during running. The decoupling of vehicles is detected and signalled to the ETB control application.
Change of driver's cab (leading vehicle)	Only a new OTD is computed, other directories are not touched.

An important consequence is that new train inaugurations are only triggered when the train is in standstill.

Failures occurring during the individual inauguration phases may have different consequences as listed in the following table:

Table 9: Train inauguration failure consequences

Failure occurrence	Effect	Consequence	Safety reaction
Failure during TND computation	No train-wide communication over ETB possible. Consist local communication still possible.	Train-wide functions are not executable	Train has to enter/stay in safe state
Failure during TD computation	ETB communication possible, but train composition could not be determined. Consist local communication possible.	Train-wide functions are not or only in a degraded mode executable	Train has to enter/stay in safe state
Failure during OTD computation	Train composition known and valid, but operational train composition could not be determined.	Train-wide functions not relying on operational train view can be executed, like for instance HVAC control, passenger announcement etc. Train-wide functions relying on operational train view cannot be executed, e.g. all side-selective/location-selective or train moving direction related functions (e.g. door control, propulsion).	Train shall stay in standstill. Use of side-selective or location-selective functions prevented or restricted

As the safety reaction, and with this the definition of the safe state, is to some extent application specific, there cannot be a generic solution which is implemented in the inauguration function itself. Hence, the inauguration function itself reports only the occurrence of a failure, but the reaction to it belongs to the ETB control application and must be designed application specific.

Function Safe Data Transmission

The SDTv4 safety protocol defines the safe data exchange between a safe data source (SDSRC) and one or many safe data sinks (SDSINK). A characteristic use case is that safety critical data are sent from the leading consist to all guided consists, in which case SDSRC is in the CCU of the leading consist and the SDSINKs are located in the CCU of the guided consists.

The safe data transmission channel between SDSRC and SDSINKs is a black channel from a safety perspective. The main task of the SDTv4 protocol (and its implementation in the safe data transmission channel of SDSRC and SDSINK) is to detect any fault in the black communication channel which could lead to a loss of safety. Those faults might be:

- Loss of data
- Corruption of data

- Delay of data
- Re-sequencing of data

As long as frequencies of those failures are below defined thresholds, those failures are tolerable and shall not cause entering safe state. The definition of the tolerated thresholds is mostly application specific. Also, the reaction to exceeding the tolerance limit is application specific and cannot be generically defined by SDTv4. Consequently, it is up to the specific application to decide how to react in case the SDTv4 indicates a tolerance exceedance.

For example, the application may decide to ignore this when the train anyway is in an uncritical operational phase, e.g. at standstill in a railway station. Or the application may decide to bring the train in a safe state (e.g. standstill) by applying an emergency brake.

As a principle, if the SDTv4 detects a tolerance exceedance it shall indicate this event to the application, which then decides how to react. SDTv4 shall never by itself take an action.

There is another aspect to be considered. A fault might be temporary (e.g. a single time-out) or permanent. Especially for temporary faults the application must be informed when the SDTv4 considers the communication safe again. This leads to the state machine shown in Figure 16. Also here, it is up to the application to decide how to handle the situation when communication is considered safe again.

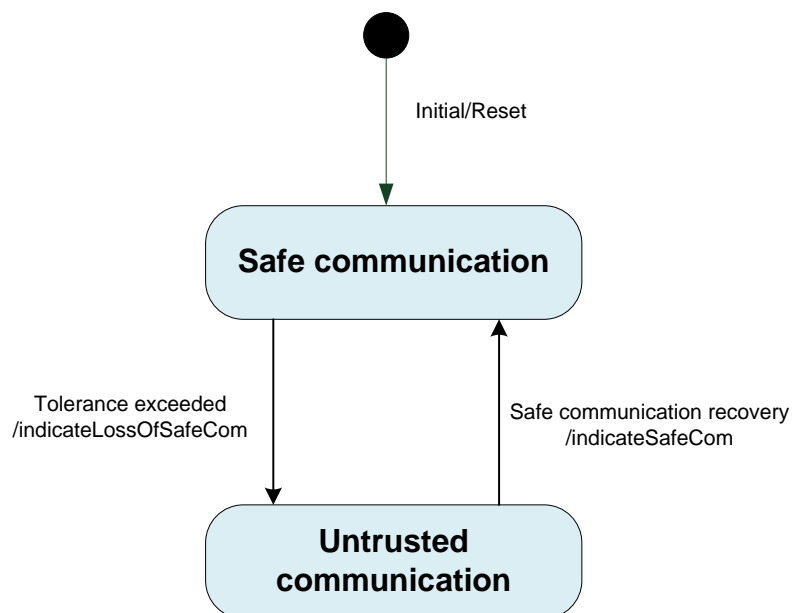


Figure 16: SDTv2 layer fault indication

3.2.3 Calculation of the minimal Safety Function Response Time (SFRT)

For a safety function, in addition to the definition of error handling (see chapter 3.2.1) and the definition of the safe state (see chapter 3.2.2), it is just as important to guarantee the time requirement for reaching the safe state upon request or after error detection.

To remain with the example from chapter 3.2.1 for an intra-consist safety function, the following SFRT would result under the assumed times when using SDTv4 as the safety protocol. The calculation follows the basic principle presented in [53], with the difference that the monitoring time of the bus system does not correspond to F_WD_Time , but to the sink time supervision used in SDTv4 (T_{rx_safe}). The calculation of sink time supervision is also presented in this chapter following the calculation of SFRT, as this is a summand for the calculation of SFRT.

The maximum time for a safety signal to pass through this chain taken from the introduced example is called “Total Worst Case Delay Time” = TWCDT

TWCDT is considering that all parts in the chain need their particular maximum cycle times. In case of safety the considerations go even further: The signal could be delayed even more if one of the parts just fails at that point in time. Thus, a delta time needs to be added for that particular part which represents the maximum difference between its watchdog time and its worst case delay time (there is no need to consider more than one failure at one time). Eventually, TWCDT plus this delta time comprise the SFRT. (see chapter 9.3 of [53])

Each and every ED-S shall provide information about its worst case delay time in order for the engineering tools to estimate the SFRTs.

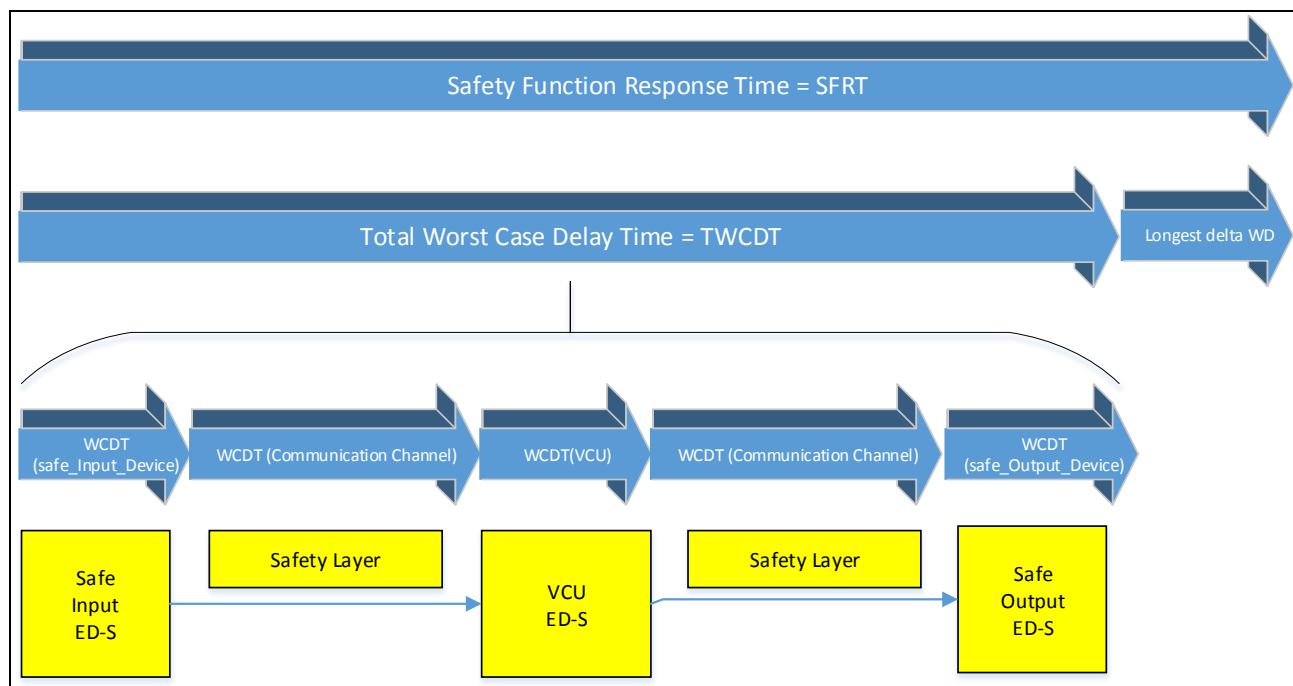


Figure 17: SFRT calculation for intra-consist safety chain

Any of these elements (Safe Input ED-S, VCU/CCU and Safe Output ED-S) have minimum (= processing) and maximum delay times (= processing + waiting). The actual delay may be any time (or time interval) in between these values. In this model the VCU/CCU is supposed to be a combined controller for standard and safety programs. The safety program is executed within a separate time triggered program level and may need a processing time for example of 50ms.

Trigger time in this case is for example each 100ms. This results in a processing delay of minimal 50ms and a maximum of 150ms.

The model for typical response times is used to define the safety function response time. Each of the cycles in the model can vary between a best case and a worst case delay time ($WCDT_i$). Every cycle has for safety reasons its superposed watchdog timer ($WDTIME_i$), which takes the necessary actions to activate the safe state whenever a failure or error occurs within that particular entity.

In order to calculate the safety function response time one error or failure¹⁰ shall be assumed in that entity (ED-S) or within the network of the signal path, which contributes the maximum difference time between its worst case delay time and its watchdog time ($WDTIME$). The corresponding equation taken from chapter 9.3 of [53] is shown below:

$$SFRT = \sum_{i=1}^n WCDT_i + \max_{i=1,2,\dots,n} (WDTIME_i - WCDT_i)$$

where:

SFRT	Safety function response time
TD	Transmission delay *
$WCDT_i$	Worst case delay time of entity i
$WDTIME_i$	The $WDTIME$ spans the time frame starting with the reception of a safety PDU with a new SSC and ending with the reaction on the expiration of the Sink Time Supervision. Following the particular expressions for the entities i:
– Safe-Input-Device:	$OFDT_{Input}$
– TD1:	T_{rx_safe1}
– VCU/CCU:	$OFDT_{VCU/CCU}$
– TD2:	T_{rx_safe2}
– Safe-Output-Device:	$OFDT_{Output}$
OFDT	One fault delay time of an entity, i.e. worst case delay time in case of a fault within the entity
$T_{cyVCU/CCU}$	VCU/CCU cycle time

¹⁰ An error or failure means that for detection the $WCDT$ may be exceeded by the superimposed monitoring function. The $WCDT$ with regard to data transmission assumes that telegram losses are taken into account. Example: The $WCDT$ should not be higher than 4ms, in this case the transmission rate must be set to 2ms, so that one telegram loss can be tolerated.

Example with assumed time values in ms:

		Input	data transmission	VCU/CCU	data transmission	Output	
WCDDT		10	2 ¹¹	100	2	10	124
WDTi		15	150	120	150	15	
delta		5	148	20	148	5	148
SFRT							272

The result shows that the maximum difference of the assumed values corresponds to the value 148 marked in red, which must be added once to the sum of all WCDDTs (TWCDT) to calculate the SFRT.

Calculation of the sink time supervision Trx_safe for the use of SDTv4:

For the calculation of the sink time supervision of SDTv4: $\text{Trx_safe} = \text{WCDDT (transmitter)} + \text{WCDDT (bus delay)} + \text{WCDDT (receiver)}$. For increased availability, a reserve of 30% of the value determined from this should be added here.

3.2.4 Evaluation of the maximal Safety Function Response Time (SFRT)

The maximum safety response time depends on the process or the safety function itself. For example, the brake must have stopped the train in a time of x (milli) seconds after the emergency stop has been actuated. Compared to the calculated minimum SFRT, there should be sufficient reserve so that the safety function is not required for reasons of availability.

What does this mean for the applicability of a safety function?

If the calculated minimum SFRT results in values greater than the maximum allowed SFRT, then the function cannot be extended over the subsystems as required, and additional adjustments of the communication parameters or time changes in the time system of the central control resulting in a lower minimum SFRT will be needed.

3.3 GENERIC PROOF OF NO UNDETECTED INTERFERENCE BETWEEN SAFETY AND NON SAFETY FUNCTIONS

The chapter has the aim to describe how the non interference can be proofed or how it could be detected in the safety application, when it could not be proofed.

3.3.1 Component level

In order to meet the objective that changes to non-safety-relevant functions have no influence on safety-relevant functions, it is mandatory to prove encapsulation of safety-relevant functions. Chapter 2.3.3 shows possible solutions how an encapsulation can look in this respect. For safety-

¹¹ 2ms is an assumed value for the data transmission time in the worst case

relevant TCMS software whose main part is loaded into a VCU/CCU and executed, it makes sense to secure the safety-relevant parts by CRC or signature, so that it is much easier to provide evidence to experts (notified bodies) that changes have only taken place in the non-safety-relevant part.

For the safety-relevant software components themselves, this is quite possible due to such encapsulation during creation. More problematic, however, is the proof of system behavior with regard to safety-relevant functions when changes are made in the non-safety-relevant part.

Examples would be here:

- memory allocation
- cycle time
- changes of non safety relevant communication parameter (for example: TSN)
- Increase network load (for example: by adding diagnostic services and non-safety-relevant but time-critical components.)

The proof of an unchanged system behaviour by modification or extension of non-safety relevant software or non-safety-relevant configuration data is clearly more difficult.

In order to exclude undetected interference from the non-safety-relevant components to the safety-relevant components, there are various error detection options to be shown on the examples mentioned.

- Memory allocation:
 - ⇒ Memory for the execution of safety-related software should be capable of demonstrably being protected against access from other memory areas. (The FDF has foreseen so called safe partitions)
 - ⇒ Depending on whether hardware or software redundancy is used as an error detection measure to achieve the required THR, unintentional overwriting of individual memory areas can also be reliably detected by this error detection measure if a common cause error can be excluded.
- Cycle time and cycle time interval:
 - ⇒ A changed real-time behaviour by downloading additional non-safety-relevant software should be detected within the error detection mechanisms of the central control unit VCU/CCU. This means that if safety-relevant and non-safety-relevant parts run within a task, only the call interval must be guaranteed in terms of safety, but not the actual processing time, since this can vary significantly due to the program structure.
 - ⇒ However, program processing errors caused by infinite loops or malfunctions of the real-time operating system, which are not detected by an internal monitoring unit, inevitably lead to error detection in the subsequent safety-relevant components by expiry of the sink time supervision of the safety protocol.
- Changes of non safety relevant communication parameter (for example: TSN):
 - ⇒ The sink time supervision of a safety relevant communication channel (SDT) should be set to provide reserve for future extensions. Changes in the time behaviour of the standard communication channel therefore only affect the

availability of the system. Independent of this, violations of the time limits are always reliably detected by the expiry of the sink time supervision and therefore do not present a problem with regard to this.

- Increase network load (for example: by adding diagnostic services and non-safety-relevant but time-critical components.):

⇒ In this case the same explanation as for: “changes of non safety relevant communication parameter” is valid.

3.3.2 Network level

Safety related functions are defined on network level:

- Safe train inauguration
- Safe data transmission

Hereafter, a contemplation about interference with non-safety related functions is given for these two functions.

Safe train inauguration

The safe train inauguration function, which is described in [35], is distributed across two devices: The ETBN and the CCU. Both device types host safety related as well as non-safety related modules. Therefore, the statements depicted in chapter 3.3.1 apply also for these devices. At least for the ETBN the proof can be easier, if the system is closed, meaning that no user applications can be installed on the ETBN.

Safety related information will be exchanged (between ETBN and CCU, but also between CCU devices of different consists) using a safe data transmission protocol as described in next section.

The safety analysis done in [32] can also be considered for proving non-interference.

Safe data transmission

SDTv4 as defined in [35] has been chosen for safe data transmission in NG-TCN. This protocol is by design robust against interference: The combination of safety measures Safety Code, Safe Sequence Counter and Source Identifier ensures – with a very low remaining risk of non-detection – that wrongly received data from a non-safety function is not accepted by safety function. In case of receiving such data, the safe data transmission channel will discard these.

In contrast to communication on ETB, where SDTv4 is the only agreed safe data transmission channel, proprietary protocols could be used on ECN for safe data transmission. In this case the proof of non-interference must be given by the vendor of the system.

In addition to the safe data transmission channel, which only can detect interferences but not prevent them, a further technology has been selected for NG-TCN: Scheduled traffic with TSN. This mechanism provides defined time slots for safety critical data exchange and therefore averts, that non-safety critical data is forwarded over the network during these slots. More details about TSN can be found in [35]. Please keep in mind, that TSN is a non-safety related function. For

vehicle engineering it should be considered to reserve enough bandwidth for future TSN data. This can be necessary, if new safety functions need to be added later in a vehicle project.

3.4 DEFINITION OF STANDARDIZED INTERFACES ON TRAIN LEVEL FOR DIFFERENT SAFETY FUNCTIONS

In the railways context safety application must be in accordance with the norm EN50128 [19] or EN50657 [36]. The first one is related to signalling software and the second one to software on Board Rolling Stock. Therefore, most safety critical applications in CONNECTA shall fulfil the norm EN50657 [36], except signalling applications.

According the norm some interfaces requirements that the software architecture and software design must fulfil are:

- Interfaces with other part of the software shall be clearly identified and documented, that is a restriction for the use of pre-existing software(7.3.4.7)
- A software interface Specification for all Interfaces between the components of the software and the boundary of the overall software shall be written, under responsibility of the Designer, on the basis of the Software Requirements Specification and the Software Architecture Specification (7.3.4.18).

For the basic integrity software, the software interface specification is only required for the boundary of the overall software.

- The description of the interfaces shall address: (7.3.4.19)
 - a) Pre/post conditions,
 - b) Definition and description of all boundary values for all specified data,
 - c) Behaviour when the boundary value is exceed,
 - d) Behaviour when the value is at the boundary,
 - e) For time-critical input and output data:
 - 1) Time constraints and requirements for correct operations,
 - 2) Managements of exceptions,
 - f) Allocated memory for the interfaces buffers and mechanism to detect that the memory cannot be allocated or all buffers are full, where applicable,
 - g) Existence of synchronization between functions, see e)
 - h) Definition and description of all equivalence classes for all specified data and each software function using them,
 - i) Definition of unused or forbidden equivalence classes.
- Interfaces between the software components shall be addressed by the Software Design Specification.(7.3.4.23)

- The Software Integration Test Specification shall address that it shall be shown that each software component provides the specified interfaces for the other components by executing the components together (7.3.4.29).

Interface requirements in components design:

- The software component design specification shall address their detailed interfaces with the environment and other components with detailed inputs and outputs. (7.4.4.3).

Interface requirements in integration:

- The integration of software components shall be the process of progressively combining individual and previously tested components into a composite whole in order that components interfaces and the assembled software may be adequately proven prior to system integration and system test (7.6.4.1).

Interface requirements in development of Software configured by application data:

- During the design of the software the detailed interfaces between the software and the application data shall be specified, unless this has already been specified at an earlier phase of the lifecycle, for example as result of a requirement to use an existing application-specific language (7.8.2.3).

Techniques and measures for high safety integrity levels in software lifecycle shall be “fully defined interfaces”, which is mandatory according Table A.3 and Table A.20 of the norm EN50657 [36]. This technique is described in D.38 of this standard. “Interface testing” is highly recommended in Table A.5 of the standard for high safety integrity level. This technique is described in D.34 of the standard.

In the deliverable CONNECTA D3.1 – Requirement Specification [30] of WP3, requirement specifications including those related to the interfaces are defined. In the mentioned deliverable, in Annex B performance values in terms of data size, data rate, cycle time and latency are specified and Annex C of the deliverable provides also the interface between NG-TCMS with ERTMS/ETCS subsystem.

The NG-TCN is delimited by two operational interfaces

1. Interface between NG-TCN and ED.
2. Interface between consists, which is important for train interoperability when this train is connected to another train during operation

Standardized interfaces facilitate the development of SIL4 functions in train level. These functions or applications must be developed following the standards EN50126, EN50129 and EN50128 / EN50657. In addition of independence of safety relevant functions with non-safety relevant functions, it is needed a high safety integrity level of the Functional Distribution Framework (FDF) in which run the safety applications.

3.4.1 Amount of Safety data

For the safety assessment, a standardization of amount of data has the following benefits:

- Standardized the amount of data can simplify the code of the application for new recertification of the software, allow to reused part of the software and the development cost is reduced in successive projects.
- The standardization of amount of data can reduce the number of test for new software changes, which is needed due error or bugs found in later stages of the whole lifecycle of the product or in new version for improving functionalities.
- Another advantage of the standardization is in the changes in the development phase. The standardization facilitates the impact analysis of these changes and can also reduce the number of repeated tests. Norms EN50126, EN50128/EN50657 and EN50129 will have to be followed, which state the need of an impact analysis and, eventually, the update of a number of documents and the repetition of all or part of the application validation tests.

An example of the importance of standardization of amount of data is in the SDTv4 analysis and justification. In the application layer is very important to know the amount of data in safety relevant function. One of the proposals in CONNECTA D3.5 – Report on Drive-by-Data Architecture [35] is to reduce to 8 bytes the amount of data in application layer. In this way, safety applications would have 8 bytes as standardized amount of data and with this standardization it is assumed that the protocol SDTv4 fulfil the requirements of SIL4.

Example of amount of data in brake function (input from WP5)

WSP status transmission

This sub-function has the main goal to share data information between EDV units implementing a WSP function on the given axle controlled.

- Each EDV unit controls the WSP of 1 axle.
- Each EDV unit send to the network the WSP information listed in the following table.
- Each EDV unit has access to the WSP data shared by all the other units.

Data content	Dimension
Angular speed axle 1	4 bytes
Estimated train speed	4 bytes
Braking Force axle 1	2 bytes
Load axle 1	2 bytes
WSP application data	10 bytes

Total: 22 bytes.

ED brake request transmission

This sub-function has the main goal to represent the link between ED brake request and ED brake application. Data shared between EDV brake unit and Traction Control Unit is shown in the following table (This list is intended for one motor).

Brake&WSP → TCU	
Data content	Dimension
ED-Brake Effort Request	2 bytes
ED-Brake Status	2 bytes

Total: 4 bytes.

TCU → Brake&WSP	
Data content	Dimension
ED-Brake Effort Applied	2 bytes
Traction Effort	2 bytes
Traction Status	2 bytes

Total: 6 bytes.

Brake status transmission

This sub-function has the main goal to share data information between EDV units implementing the brake function on the given axle controlled.

- Each EDV unit controls the brake of 1 axle.
- Each EDV unit send to the network the brake information listed in the following table.
- Each EDV unit has access to the brake data shared by all the other units.

Data content	Dimension
EDV Brake Data	48 bytes

Total: 48 bytes.

3.4.2 Timing requirements

Standardization of timing in application is very helpful in the certification process. New applications that are added to the system need their timing requirements. A simple solution in the TCMS is to previously reserve time in the partition schedule in the FDF¹², so that new partitions can be inserted in the previously unused slots. An alternative solution, which implies the rescheduling of previously existing partitions, shall be avoided because this would require the re-certification of all the functions affected by the scheduling change. Therefore, adding a new application that does not modify the scheduling of the other partitions shall not require the re-certification of the other applications.

Calculation of the PST / SFRT can be easy to recalculate or justify in the certification process if the timing requirement is standardized. The norm 61784-3-3 [37] in section 9 defines the SFRT and explains how to calculate and optimize it.

In general, it can be said that a correctly specified and implemented standardization would have a positive contribution to the process in terms of increased safety, reduced assessment effort and cost.

¹² It is assumed that the application run on the top of a certified FDF.

Example of Timing requirement for brake functions (input from WP5)

Brake request transmission

- TrainBrReq&EBReq message shall be transmitted to all train ED-S by NG-TCN with a max communication delay: < 20ms
- TrainBrReq&EBReq message shall have a periodicity: 50ms
- TrainBrReq&EBReq message shall be a broadcast message, transmitted at Train level
- TrainBrReq&EBReq message shall be transmitted with communication constraints able to guarantee SIL4 integrity

WSP status transmission

- WSPstatus message shall have a periodicity: 5ms
- WSPstatus message shall be a broadcast message between EDV nodes, transmitted at Consist level
- WSPstatus message shall be transmitted with communication constraints able to guarantee SIL4 integrity

ED brake request transmission

- EDbrakeReq message shall have a periodicity: 20ms
- EdbrakeReq message shall be a point-to-point message between EDV node and TCU node, transmitted at Consist level
- EdbrakeReq message shall be transmitted with communication constraints able to guarantee SIL2 integrity
- EdbrakeStatus message shall have a periodicity: 20ms
- EdbrakeStatus message shall be a point-to-point message between EDV node and TCU node, transmitted at Consist level
- EdbrakeStatus message shall be transmitted with communication constraints able to guarantee SIL2 integrity

Brake status transmission

- BrakeStatus message shall have a periodicity: 50ms
- BrakeStatus message shall be a broadcast message between EDV nodes, transmitted at Consist level
- BrakeStatus message shall be transmitted with communication constraints able to guarantee SIL4 integrity

Train Integrity Subfunction- PROPOSAL

EDV shall check the train integrity condition, according to the reception of the TrainBrReq&EBReq message

Train Integrity timeout : 5 consecutive TrainBrReq&EBReq messages loss at application (safety) level – $[5 * 50\text{ms}] = 250\text{ms}$.

- EDV (local) reactions of loss of train integrity: EDV Fail Safe (FS) condition has to be applied: EDV emergency brake application.

NG-TCN shall check the train integrity condition, verifying the capability to communicate between the train lead and tail.

- NG-TCN reactions of loss of train integrity: an emergency brake request has to be transmitted to all the EDV units still connected on the network: TrainBrReq&EBReq message shall be transmitted, requesting emergency brake.

3.5 DEFINITION OF A SAFE DEPLOYMENT PROCEDURE FOR SAFETY CRITICAL APPLICATIONS AND ITS PARAMETRIZATION

Here the term “deployment” is used as an umbrella term for the tasks required to put existing train application software into operation on an actual train. It mainly includes the firmware download to devices. It also includes the slight tailoring possible by just “calibrating” parameters to adapt existing software without the need for recompilation and without the associated high effort for reassessment of safe software.

3.5.1 Firmware Download

Part of the deployment of the application software is the process to load (commonly called “flash”) a device firmware and/or parameter set to the non-volatile memory of and end device installed on the train. That applies to field programmable devices, these are devices whose firmware is intended to be changed on the train (as opposed to factory configured devices, which would require a physical exchange of the device to change the functionality). The download of software is part of the commissioning of a train. Two basic use cases can be distinguished:

Firstly, the initial commissioning phase is the phase, where factory new installed devices are set up for the first time. As it is shown the initial commissioning requires some extra steps in the context of safe devices (especially setting up a “SafeDeviceID”, see below). Since those extra steps need to be carried out only once per device installation some overhead is deemed acceptable.

Secondly, subsequent update phase. Updating of firmware and/or parameters occurs more often (especially during the commissioning phase). To reduce the commissioning effort the process should be optimized for time without sacrificing safety.

Basically, the download of safety and non-safety-related software is similar. For practical reasons the process and tooling for the download of safety-related software shall support as a superset the download of non-safety-related software also.

It is assumed that the download process is restricted to a complete consist (not covering a complete train consisting of multiple inaugurated consists). It is also assumed that the process involves no wireless technology, i.e. the devices are accessed over the wired ECN.

3.5.2 Software Items

“Software items” are the smallest units handled during the deployment of software. Each (programmable) device may be loaded with one or more software items. A software item has the following properties:

- Binary “payload” (e.g. code, data, parameters)
- Version information
- Integrity. Use Checksums to check correctness.
- “Magic number” to allow checks whether the software item fits to the device
- Security. Keys to verify its authenticity (ensure that the software item is generated by trusted source).

Examples for software items include

- Application constituting a functionality, e.g. vehicle control
- Data items, e.g. time-table information, station lists, etc.
- Parameter sets to adapt a “generic” application, e.g. number of cars in consist
- Parameter sets to establish uniqueness of a consist, e.g. UIC ID

Configuration management needs to be applied to all software items. A baseline needs to be drawn over software items which are dependent.

3.5.3 Safe Software Deployment approach

Safe functionality is implemented using one or multiple devices which each are in turn programmed with several software items. It is crucial that the devices are programmed with the intended software items in its entirety. This means that it is of crucial importance to have the expected software on every device related to a common baseline. The devices are typically not self-contained, but a function can be distributed upon multiple devices. Therefore, it is equally critical that the software items put on different devices belong to the same software baseline in a consist application configuration management context. To achieve that goal (make sure to have the correct and fitting software items distributed across the consist) a highly automated and robust mechanism is deemed mandatory.

That implies a tool support for the deployment and the accessibility of all devices through a network connection. The tool will automate the download and verification process. The vehicle TCMS engineering process will create and maintain a project file or file structure, which contains all the software items together with the information on which device to load which software item. This project file will be used by the deployment tool to basically carry one of two functions: Firstly, execute the download. Secondly allow a verification to check that all software items are correctly loaded.

As said it is assumed that all the devices are accessible over the network (ECN). That implies that especially for the safety related parts it is critical to address the correct devices during deployment. The automated mechanism can check whether an addressed device is of the correct type (e.g. door control or break control) but not if the correct device instance (if multiple devices of one type are present) is addressed. To cope with that special attention need to be paid to make sure that the correct devices are addressed. This leads to the introduction of a “SafeDeviceID” as discussed in the following chapter

3.5.4 SafeDeviceID

Existing unique identifications like MVB-Address, IP-Address or MAC-Address are not well suited to identify a device. Instead a SafeDeviceID is introduced as a unique identification of safety related devices to support the software deployment process.

The SafeDeviceID is a geographical address and shall have the following properties:

- Unique per device across consist
- Identical from consist to consist for the same device at the same position
- Serves as a geographic address
- Alphanumeric (optional for better readability)
- Integrity checked (checksum). e.g. that excludes the use simple DIP switches
- Temper proof. To some degree, e.g. accidental change shall not be possible.

As a consequence, assigning or changing a SafeDeviceID involves physical access to the corresponding device. Note that ideally the SafeDeviceID assignment only happens initially, once per device during commissioning. Subsequent accesses to the device can be done over the network based on its SafeDeviceID.

3.5.5 Per device initial configuration

In addition to the SafeDeviceID further settings can and should be done during the initial configuration to allow the subsequent remote access via the network. Examples for these parameters include physical network property settings (like speed and duplex mode), VLAN settings and interface IP address (if not using a layer2 discovery protocol or DHCP).

The initial configuration together with the SafeDeviceID can be stored either in a memory key (e.g. using a serial EEPROM) or be programmed into the device by temporarily connecting a PTE with a tool to update an internal non-volatile memory.

The initial configuration sets the correct SafeDeviceID and allows to complete the commissioning consist wide via the network (ECN). Since only a very few settings are part of the initial commissioning any further system update (other than repair action on a device) will not require physical access to the devices.

3.5.6 Using parameters

From an application point of view parameters are variables (of a certain type, like integer, float, string or array, but also "BLOB"s like bitmaps) which get initialized to a user configurable value and stay constant during the execution of the program. From a user point of view the parameter is identified by a keyword and assigned a constant value which is taken as the initial value during the initialization of the program code. Parameters allow to change the behaviour of an implemented function after the function has been already compiled to binary code. That is the behaviour can be changed without recompiling the corresponding program.

Parameters shall be strongly checked for correct type, size and range limits (where applicable) by the tooling, but also by the application as far as reasonable. Tooling support can also be used to do plausibility checks on sets of parameters containing more complex dependencies.

Using a smart parameterization scheme, that is choosing the right set of parameters, can significantly reduce the effort for the reassessments in safety critical applications. The approach is to have a generic application for a dedicated functionality that is tailored by setting parameters.

Doing so there are several benefits in that approach:

- If the parameter has just a few options, all options can be proven during safety assessment of the functionality and no further actions for certification are needed. All given options are directly usable because the overall functionality was covered by the verification of the application already.
- With a given design of an application it can be proven that a parameter to configure a certain safe function is independent from other parameters. This supports an easy and efficient regression test and value change of one single parameter without the need to redo a full certification cycle.
- Parameters allow to adapt/react to environmental influences that are not predefined or well known. Due to that, parameters are seen as part of the commissioning and not as part of the engineering.

It is obvious that the design of the application and its parameterization has impact on:

- Certification of the application itself
- Certification of the effects of parameter changes
- Testing (Verification/Validation)
- Roles, responsibilities and Software Configuration Procedure

The challenge is to find an optimum balance between what is statically implemented by the application and what is dynamically adjustable through parameters. To simplify the application assessment effort by shifting the assessment effort to the parameterization would not be an optimal approach.

Parameters as software items

Parameters are typically grouped together as a parameter set if they are functionally dependent. A change of the parameterization of a certain function would just require the change of the one dedicated parameter set. Such a parameter set will then be maintained as a software item. The software item handling then features versioning, verification, integrity check, configuration management, authentication as discussed in 3.5.2.

Situations to use parameters

Base for the parameterization is the certified application. The dedicated values of the parameters are not always readily known but may depend on situations in the field. Due to that the tooling to handle the parameters must be seen not as an engineering tool, but as a commissioning tool.

Some typical cases for parameterization:

1. Assigning a type or subtype for a functionality. This is the case when the application is generic and allows to choose one of several operational modes. The options are somehow predefined. If the functionality can be fully tested and qualified for all existing options, then no validations need to be done.
Such a parameter is mostly not to be changed later again because it must fit to the hardware environment and the system requirements.
2. Tuning the setup. Changing certain parameters or parameters sets having a large range of possible values. In that case the application cannot be certified for all possible settings

beforehand. The resulting functionality need to be verified and assessed. Any modification requires reassessment. Due to that effort, this case should be avoided. However still having a common and certified application can have a benefit. It is clear, that the approach should be to not modify that system later again.

3. Parameters that need an adaption or modification during the life time of the system. Obviously those shall not require a recertification of the application.

Requirements for parameters

Especially considering functional safety a given parameterization shall fulfil the following requirements:

Independent: A parameter shall be either functionally independent or if dependent shall be grouped in a parameter set with the dependent parameters.

Stringent: A parameter shall be as strictly limited as possible. A predefined choice is preferred against a free parameter and a free parameter like a wheel diameter should have plausible limitations.

Understandable: Content and impact should be clear and obvious.

Manageable: Keep complexity of parameterization reasonably low.

3.5.7 Summary

Deployment is independent of the content of the software items. This means the process is the same for applications and parameters.

It is based upon a reliable device identification that must be done in advance but typically only once.

Dealing with parameters is a wide field. The overall process involves the selection of parameters for the application, the grouping of parameters and plausibility checks.

Deployment means to provide the correct software items to a device. That requires a verification process that must demonstrate that the software item reaches the intended device.

A careful and proper design of the application, its parameterization, but also the procedure will finally save a lot of effort by avoiding tests and reassessments during the maintenance of a system.

4. PREPARATION OF SELECTED SAFETY CASES FOR THE SELECTED FUNCTIONS FOR THE DEMONSTRATOR PLATFORM

This chapter aims to give input for the creation of safety cases for selected functions: door function and brake function. Therefore, this deliverable does not claim to provide a complete safety case for these two functions.

For the functions considered in this chapter, the basis of the work is given by the standard EN15380-4 Railway applications - Classification system for railway vehicles - Part 4: Function groups [05]. This standard proposes train functions and sub-functions FBS commonly agreed among the railways industry through Europe. It has also been already used as a basic document

for CONNECTA's work, e.g. the deliverable of the Task 1.3 **Fehler! Verweisquelle konnte nicht gefunden werden..**

4.1 GENERAL SAFETY CASE METHODOLOGY

4.1.1 Introduction

The norm EN50129 [20] specifies a defined structure for the safety cases, which is detailed in this section. The safety case is structured in 6 parts according to the norm:

Definition of the subsystem

⇒ For door function see chapter 4.2.1 and for brake function see chapter 4.3.1

Quality management report

⇒ See chapter 4.1.2

Safety management report

⇒ See chapter 4.1.3

Technical safety report

⇒ See chapter 4.1.4

Related Safety Cases

Conclusion

4.1.2 Quality management report

In order to achieve the acceptance of the safety requirement, the system quality must be controlled for an effective management system during the life cycle. In this way systematic fault risks are reduced because humans' errors are also minimized. Evidence must be showed to ensure the effectiveness of quality management system (QMS).

QMS usually complies the ISO: 9001[40] norm and quality process could be followed according to 50126/8/9 [17][18][19][20].

Procedures used

Techniques and procedures must be specified for the next activities as described in the norm EN50129 [20] section 5.2.

Quality activities (part 5.2 EN50129)	Used techniques and procedures
Organizational structure	Flowchart based on personnel competence for: Design, SW design, RAMS, quality, V&V, etc. Explained in document Project Global Plan.
Quality planning and procedures	Quality plan is based on the Life Cycle (ENISO 9001 and EN50126). Quality Plan and Configuration Management Plan of the project define the applied procedures. Techniques and measures of quality assurance activities are defined in table 13.

Quality activities (part 5.2 EN50129)	Used techniques and procedures
Specification of requirements	Requirement specification so as to be: accurate, concise, unambiguous, understandable for people who have not defined them, defining correctly the objective, accessible and maintainable. This way system and subsystems requirements are defined.
Design control	The entire system electronic design composed of the different subsystems hardware, software and programmable logic is performed as specified in the different design procedures. The modular and structured design, RAMS analysis and environmental analysis, coding techniques and rigorous design documentation are some of the techniques required.
Design verification and reviews	All design documentation is reviewed according to the "process of generation and review of documents" specified in the Configuration Management Plan. Additionally, all items are checked with the criteria specified in the verification plan for the application. In both cases they are used predefined checklists and the results and corrective actions are defined. The configuration management tool allows identifying if an item has been checked and verified.
Application engineering	Design architecture is established according to the RAMS analysis, which define the objectives and topologies more suitable in order to fulfil the RAM and safety requirements
Procurement and manufacturing	System manufacturing is performed in accordance with the Manufacturing Process, which defines the procedures, defining the scope of supply, storage of raw material and traceability of products and raw material, manufacturing, inspections, labelling and packaging. Moreover, to guarantee that Safety Integrity Level is not compromised, a subset of V&V Test will be carried out for each manufactured Item, so this way, safety requirements will be check under operational conditions.
Product identification and traceability	Traceability requirements identified in Process Manufacturing are resolved by following the instructions in the General Specification Manufacturing Process, Specification of Raw material Traceability and the Specification of the Final Product Traceability. Every product has a unique identifier that permits to identify it from the moment that starts its manufacturing, in order to identify possible problems even in the manufacturing process.
Handling and Storage	The general specification of manufacturing process together with the specification of the final product packaging to be handled, define how shall be handled and stored raw materials and final product. Environmental conditions and the dates of entry / exit of the raw material are controlled. The final product packaging protects against bumps or electrostatic discharges.
Inspection and testing	The general specification of the manufacturing procedure defines inspections to make to the final product: <ul style="list-style-type: none"> • Visual inspection at certain points in the process • Automatic Optical Inspection in electronic boards • Specific serial tests for each article
Non-conformance and corrective actions	In the specification of disconformities a processing method is defined: <ul style="list-style-type: none"> • Open a disagreement • Decide the corrective actions • Shipment of nonconforming material • The closure of the disagreement • Impact analysis of disagreement
Packing and delivery	In the packing specification the measures taken to protect the product from shocks and electrostatic discharges during transport are defined.
Installation and commissioning	The System Installation Manual specifies: <ul style="list-style-type: none"> • How to perform the mechanical installation of the system • How to perform the electrical installation of the system • Inspections to be carried out before commissioning
Operation and maintenance	It must be documented how to perform predictive and corrective maintenance. This documentation must be used by the maintenance staff in order to ensure the proper functionality of the application. Operation documentation is related to how to use properly this function by the driver.
Quality monitoring and feedback	Periodic internal audits of the project are realized with execution control of corrective actions.

Quality activities (part 5.2 EN50129)	Used techniques and procedures
Documentation and records	The review and verification of activities are documented in Review Records or Verification Records. Internal Quality Audits are documented in the Quality Audit Reports.
Configuration management / change control	All items (documents / hardware / software) are uniquely identified and mapped versions must be generated. A change management procedure (request, impact analysis, modifications, testing, validation, creation of the new version) must be also documented.
Personnel competency and training	Staff selection must be done by identifying in advance the required profiles. The profiles of all participants are documented and several training tasks shall be developed according to the risk areas identified in the project.
Quality audits and follow-up	External quality audit shall be carried out within the Independent Safety Assessment.
Decommissioning and disposal	The Decommissioning Manual of the System defines how the decommissioning and disposal shall be performed and the treatment to be given to each of the elements of the system.

Table 10: Quality management report. Procedures used.

Techniques¹³ used in order to achieve a high SIL are summarized in the following and in Table 14:

Techniques / Measures	REQUIREMENT			
	SIL 1	SIL 2	SIL 3	SIL 4
1. Graphical description of sub-systems	HR	HR	HR	HR
2. Description of interfaces	HR	HR	HR	HR
3. Environment (EMC, vibrations) studies	R	R	HR	HR
4. Modification procedure	HR	HR	HR	HR
5. Maintenance manual	HR	HR	HR	HR
6. Manufacturing documentation	HR	HR	HR	HR
7. Application documentation	HR	HR	HR	HR

Table 11: Design phase documentation (Table E.8 EN50129)

Lifecycle

Lifecycle of the development of the application must be briefly explained. Function or application lifecycle shall be developed according to EN50126 [17].

4.1.3 Safety Management report

The effectiveness of a safety management system is ensured with the RAMS process management described in the norm EN50126 [17]. Residual risks from systematic fault are minimized and the impact of human errors decreases.

¹³ In order to achieve the safety requirements, techniques and methods of the norm EN50129 must be fulfilled and justified with the proper documentations. In addition all techniques mentioned in the safety case must be referenced with the documents that justify them.

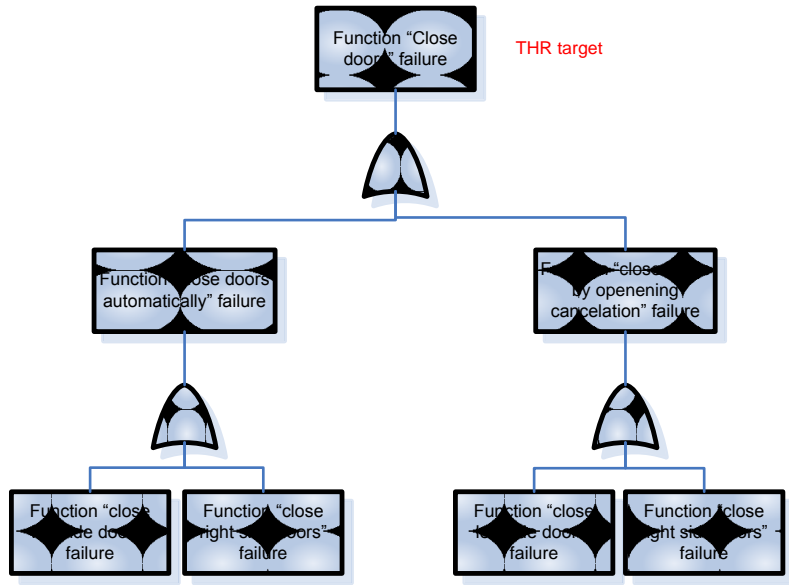
The evidences of safety management must be provided in this section.

Safety Activities (part 5.3 EN50129)	Techniques and procedures used																								
Introduction (5.3.1 EN50129)	In this section safety process in the lifecycle must be briefly defined and safety plan must be linked.																								
Safety Life Cycle (5.3.2 EN50129)	The safety lifecycle of the application can be integrated inside the system lifecycle of the application. It can be defined in the project plan. and shall be based on the lifecycle of EN50126[17]																								
Safety Organisation (5.3.3 EN50129)	Depending on the SIL target of the specific application the independence level between departments/roles in the project must be appropriated according the norm EN50129 [20]. For example to achieve SIL4 the independence between roles/organization must be:																								
	<div><div><div><div>PM</div><div>DI</div></div><div><div>VER, VAL</div></div></div><div><div>ASSR</div></div></div> <div>OR</div> <div><div><div><div>PM</div><div>DI</div></div><div><div>VER</div></div><div><div>VAL</div></div></div><div><div>ASSR</div></div></div> <div>Figure 18: SIL4 Organization chart</div>																								
	Techniques and measures for the safety organization are showed in the following table:																								
	<table><tr><th rowspan="2">Techniques / Measures</th><th colspan="4">REQUIREMENT</th></tr><tr><th>SIL 1</th><th>SIL 2</th><th>SIL 3</th><th>SIL 4</th></tr><tr><td>1. Training of staff in safety organization</td><td>HR</td><td>HR</td><td>HR</td><td>HR</td></tr><tr><td>2. Independence of roles</td><td></td><td></td><td></td><td></td></tr><tr><td>3. Qualification of staff in safety organization (see note)</td><td>HR</td><td>HR</td><td>HR</td><td>HR</td></tr></table> <div>NOTE: Staff involved in safety activities shall be competent to perform those activities (see 5.3.3 of EN50129).</div>	Techniques / Measures	REQUIREMENT				SIL 1	SIL 2	SIL 3	SIL 4	1. Training of staff in safety organization	HR	HR	HR	HR	2. Independence of roles					3. Qualification of staff in safety organization (see note)	HR	HR	HR	HR
Techniques / Measures	REQUIREMENT																								
	SIL 1	SIL 2	SIL 3	SIL 4																					
1. Training of staff in safety organization	HR	HR	HR	HR																					
2. Independence of roles																									
3. Qualification of staff in safety organization (see note)	HR	HR	HR	HR																					
	Table 12: Safety organization (Table E.3 of EN50129)																								

Safety Activities (part 5.3 EN50129)	Techniques and procedures used																																																	
Safety Plan (5.3.4 EN50129)	<p>The safety plan is elaborated in the first phase “Concept and planning” of the project in which all safety activities are defined. The following table shows the techniques and measures for the safety plan and quality assurances activities. These activities refer also the section 4.1.2</p> <table><tr><th rowspan="2">Techniques / Measures</th><th colspan="4">REQUIREMENT</th></tr><tr><th>SIL 1</th><th>SIL 2</th><th>SIL 3</th><th>SIL 4</th></tr><tr><td>1. Checklists</td><td>R</td><td>R</td><td>R</td><td>R</td></tr><tr><td>2. Audit of tasks</td><td>R</td><td>R</td><td>HR</td><td>HR</td></tr><tr><td>3. Inspection of issues of documentation</td><td>HR</td><td>HR</td><td>HR</td><td>HR</td></tr><tr><td>4. Review after change in safety plan</td><td>HR</td><td>HR</td><td>HR</td><td>HR</td></tr><tr><td>5. Review of the safety plan after each safety life-cycle phase</td><td>HR</td><td>HR</td><td>HR</td><td>HR</td></tr></table> <p>Table 13: Safety planning and quality assurance activities (Table E.1 EN50129)</p>	Techniques / Measures	REQUIREMENT				SIL 1	SIL 2	SIL 3	SIL 4	1. Checklists	R	R	R	R	2. Audit of tasks	R	R	HR	HR	3. Inspection of issues of documentation	HR	HR	HR	HR	4. Review after change in safety plan	HR	HR	HR	HR	5. Review of the safety plan after each safety life-cycle phase	HR	HR	HR	HR															
Techniques / Measures	REQUIREMENT																																																	
	SIL 1	SIL 2	SIL 3	SIL 4																																														
1. Checklists	R	R	R	R																																														
2. Audit of tasks	R	R	HR	HR																																														
3. Inspection of issues of documentation	HR	HR	HR	HR																																														
4. Review after change in safety plan	HR	HR	HR	HR																																														
5. Review of the safety plan after each safety life-cycle phase	HR	HR	HR	HR																																														
Hazard log (5.3.5 EN50129)	<p>This document is elaborated in the phase “System requirements and risk analysis” in which all hazards identified in the safety lifecycle are mapped. It must be updated through the whole life cycle.</p>																																																	
Safety Requirements Specification (5.3.6 EN50129)	<p>The requirements specified in the different phases of the life cycle have been carried out according to the Procedure of Requirement Management and ensuring traceability. Safety requirements specifications can be integrated in the project requirement specification. The results of the phases 1 to 4 described in EN50126 [17] shall be documented in the System Requirements Specification, which shall take account of the techniques and measures of the following table.</p> <table><tr><th rowspan="2">Techniques / Measures</th><th colspan="4">REQUIREMENT</th></tr><tr><th>SIL 1</th><th>SIL 2</th><th>SIL 3</th><th>SIL 4</th></tr><tr><td>Separation of Safety-Related Systems from Non Safety-Related Systems</td><td>R</td><td>R</td><td>HR</td><td>HR</td></tr><tr><td>Graphical description including for example block diagrams</td><td>HR</td><td>HR</td><td>HR</td><td>HR</td></tr><tr><td>Structured Specification</td><td>HR</td><td>HR</td><td>HR</td><td>HR</td></tr><tr><td>Formal or semiformal methods</td><td>-</td><td>-</td><td>R</td><td>R</td></tr><tr><td>Computer aided specification tools</td><td>-</td><td>R</td><td>R</td><td>R</td></tr><tr><td>Checklists</td><td>R</td><td>R</td><td>R</td><td>R</td></tr><tr><td>Hazard Log</td><td>HR</td><td>HR</td><td>HR</td><td>HR</td></tr><tr><td>Inspection of the specification</td><td>R</td><td>R</td><td>HR</td><td>HR</td></tr></table> <p>NOTE: Checklists or computer aided specification tools shall be used with another method since they usually state what to do (in order not to forget something), but cannot guarantee the quality of what is actually achieved.</p> <p>Table 14: System requirements specification (Table E.2 of EN50129)</p>	Techniques / Measures	REQUIREMENT				SIL 1	SIL 2	SIL 3	SIL 4	Separation of Safety-Related Systems from Non Safety-Related Systems	R	R	HR	HR	Graphical description including for example block diagrams	HR	HR	HR	HR	Structured Specification	HR	HR	HR	HR	Formal or semiformal methods	-	-	R	R	Computer aided specification tools	-	R	R	R	Checklists	R	R	R	R	Hazard Log	HR	HR	HR	HR	Inspection of the specification	R	R	HR	HR
Techniques / Measures	REQUIREMENT																																																	
	SIL 1	SIL 2	SIL 3	SIL 4																																														
Separation of Safety-Related Systems from Non Safety-Related Systems	R	R	HR	HR																																														
Graphical description including for example block diagrams	HR	HR	HR	HR																																														
Structured Specification	HR	HR	HR	HR																																														
Formal or semiformal methods	-	-	R	R																																														
Computer aided specification tools	-	R	R	R																																														
Checklists	R	R	R	R																																														
Hazard Log	HR	HR	HR	HR																																														
Inspection of the specification	R	R	HR	HR																																														

Safety Activities (part 5.3 EN50129)	Techniques and procedures used																																		
System / subsystem / equipment design (5.3.7 EN50129)	<p>A Safety Analysis must be realized and a system design must be obtained according to the safety procedure to fulfil the operational and safety requirements. System design Validation and Verification is demonstrated by System Validation and System Verification Reports. Techniques and measures for the design method are given in the following table.</p> <table><tr><th rowspan="2">Techniques / Measures</th><th colspan="4">REQUIREMENT</th></tr><tr><th>SIL 1</th><th>SIL 2</th><th>SIL 3</th><th>SIL 4</th></tr><tr><td>1. Structured design</td><td>HR</td><td>HR</td><td>HR</td><td>HR</td></tr><tr><td>2. Modularisation</td><td>R</td><td>HR</td><td>HR</td><td>HR</td></tr><tr><td>3. Formal or semiformal methods</td><td>-</td><td>-</td><td>R</td><td>R</td></tr><tr><td>4. Computer-aided design tools</td><td>-</td><td>R</td><td>R</td><td>R</td></tr><tr><td>5. Environmental studies (EMC, vibration, etc.)</td><td>R</td><td>R</td><td>HR</td><td>HR</td></tr></table> <p>Table 15: Design and development of system/sub-system/equipment (Table E.7 of EN50129)</p>	Techniques / Measures	REQUIREMENT				SIL 1	SIL 2	SIL 3	SIL 4	1. Structured design	HR	HR	HR	HR	2. Modularisation	R	HR	HR	HR	3. Formal or semiformal methods	-	-	R	R	4. Computer-aided design tools	-	R	R	R	5. Environmental studies (EMC, vibration, etc.)	R	R	HR	HR
Techniques / Measures	REQUIREMENT																																		
	SIL 1	SIL 2	SIL 3	SIL 4																															
1. Structured design	HR	HR	HR	HR																															
2. Modularisation	R	HR	HR	HR																															
3. Formal or semiformal methods	-	-	R	R																															
4. Computer-aided design tools	-	R	R	R																															
5. Environmental studies (EMC, vibration, etc.)	R	R	HR	HR																															
Safety Reviews (5.3.8 EN50129)	Safety reviews must be specified in the safety plan, where safety team shall review each phase of the lifecycle. Specific application function is subject to review when there is any alteration to the function.																																		

Safety Activities (part 5.3 EN50129)	Techniques and procedures used																																																																
Safety Verification and Validation (5.3.9 EN50129)	Safety Validation and Verification are demonstrated by function Validation and System Verification Reports. They are performed according to documents Verification Plan and Validation Plan. Test and analysis of verification and validation must be included and techniques and measures used are shown in the next table. Note that verification and validation could be use different techniques and measures.																																																																
	<table><tr><th rowspan="2">Techniques / Measures</th><th colspan="4">REQUIREMENT</th></tr><tr><th>SIL1</th><th>SIL2</th><th>SIL3</th><th>SIL4</th></tr><tr><td>1. Checklists</td><td>R</td><td>R</td><td>R</td><td>R</td></tr><tr><td>2. Simulation</td><td>-</td><td>R</td><td>R</td><td>R</td></tr><tr><td>3. Functional testing of the system</td><td>HR</td><td>HR</td><td>HR</td><td>HR</td></tr><tr><td>4. Functional testing under environmental conditions</td><td>HR</td><td>HR</td><td>HR</td><td>HR</td></tr><tr><td>5. Surge immunity testing</td><td>HR</td><td>HR</td><td>HR</td><td>HR</td></tr><tr><td>6. Inspection of the documentation</td><td>HR</td><td>HR</td><td>HR</td><td>HR</td></tr><tr><td>7. Ensure design assumptions are not compromised by manufacturing process.</td><td>-</td><td>-</td><td>HR</td><td>HR</td></tr><tr><td>8. Test facilities</td><td>R</td><td>R</td><td>HR</td><td>HR</td></tr><tr><td>9. Design Review</td><td>HR</td><td>HR</td><td>HR</td><td>HR</td></tr><tr><td>10. Ensure design assumptions are not compromised by installation and maintenance processes</td><td>HR</td><td>HR</td><td>HR</td><td>HR</td></tr><tr><td>11. High confidence demonstrated by use (optional where some previous evidence is not available)</td><td>R</td><td>R</td><td>R</td><td>R</td></tr></table>	Techniques / Measures	REQUIREMENT				SIL1	SIL2	SIL3	SIL4	1. Checklists	R	R	R	R	2. Simulation	-	R	R	R	3. Functional testing of the system	HR	HR	HR	HR	4. Functional testing under environmental conditions	HR	HR	HR	HR	5. Surge immunity testing	HR	HR	HR	HR	6. Inspection of the documentation	HR	HR	HR	HR	7. Ensure design assumptions are not compromised by manufacturing process.	-	-	HR	HR	8. Test facilities	R	R	HR	HR	9. Design Review	HR	HR	HR	HR	10. Ensure design assumptions are not compromised by installation and maintenance processes	HR	HR	HR	HR	11. High confidence demonstrated by use (optional where some previous evidence is not available)	R	R	R	R
	Techniques / Measures		REQUIREMENT																																																														
		SIL1	SIL2	SIL3	SIL4																																																												
	1. Checklists	R	R	R	R																																																												
	2. Simulation	-	R	R	R																																																												
	3. Functional testing of the system	HR	HR	HR	HR																																																												
	4. Functional testing under environmental conditions	HR	HR	HR	HR																																																												
	5. Surge immunity testing	HR	HR	HR	HR																																																												
	6. Inspection of the documentation	HR	HR	HR	HR																																																												
	7. Ensure design assumptions are not compromised by manufacturing process.	-	-	HR	HR																																																												
	8. Test facilities	R	R	HR	HR																																																												
	9. Design Review	HR	HR	HR	HR																																																												
10. Ensure design assumptions are not compromised by installation and maintenance processes	HR	HR	HR	HR																																																													
11. High confidence demonstrated by use (optional where some previous evidence is not available)	R	R	R	R																																																													
	NOTE Checklists, computer aided specification tools and inspection of the specification can be used in the verification activity of a phase.																																																																
	Table 16: Verification and validation of the system and product design (Table E.9 of EN50129)																																																																

Safety Activities (part 5.3 EN50129)	Techniques and procedures used
<p>Safety justification (5.3.10 EN50129)</p>	<p>For safety argumentation is done with the Safety Case that shall be developed according to the standard EN50129[20]. Safety analysis is proposed by the technique FTA in order to do a THR/TFFR distribution of system function. A basic example of a door function is shown in the following Figure.</p>  <p style="text-align: center;">Figure 19: FTA example</p>
<p>System / subsystem / equipment handover (5.3.11 EN50129)</p>	<p>It must reach the Product Acceptance. In this phase Safety Plan and Test Plan are applied. Product Acceptance will be reached with the execution of planned system validation tests and the independent safety assessment of the system.</p>

Safety Activities (part 5.3 EN50129)	Techniques and procedures used																																														
Operation and maintenance (5.3.12 EN50129)	<p>Evidences that prove that procedures are carried out according to the Maintenance Manual and Operation Manual must be provided and evidences that demonstrate that each request for modification have been assessed to ensure that modifications made do not reduce the level of safety unacceptably.</p> <p>Any modification request after the commissioning of the system should be evaluated from the safety standpoint, to make sure that the modification does not decrease unacceptably the safety integrity level. In case that the modification requests are for the software developed, the Software Maintenance Plan shall specifies how to carry them out properly. Application, operation and maintenance procedures shall be documented taking into account the techniques and measures given in the following table.</p> <table><tr><th colspan="2" rowspan="2">Techniques / Measures</th><th colspan="4">REQUIREMENTS</th></tr><tr><th>SIL 1</th><th>SIL 2</th><th>SIL 3</th><th>SIL 4</th></tr><tr><td>1.</td><td>Production of applications operational and maintenance instructions</td><td>R</td><td>R</td><td>HR</td><td>HR</td></tr><tr><td>2.</td><td>Training in the execution of operational and maintenance instructions</td><td>HR</td><td>HR</td><td>HR</td><td>HR</td></tr><tr><td>3.</td><td>Operator friendliness</td><td>HR</td><td>HR</td><td>HR</td><td>HR</td></tr><tr><td>4.</td><td>Maintenance friendliness</td><td>HR</td><td>HR</td><td>HR</td><td>HR</td></tr><tr><td>5.</td><td>Protection against operation errors</td><td>R</td><td>R</td><td>HR</td><td>HR</td></tr><tr><td>6.</td><td>Protection against sabotage</td><td></td><td></td><td>R</td><td>R</td></tr></table> <p>Table 17: Application operation and maintenance (Table E.10 of EN50129)</p>	Techniques / Measures		REQUIREMENTS				SIL 1	SIL 2	SIL 3	SIL 4	1.	Production of applications operational and maintenance instructions	R	R	HR	HR	2.	Training in the execution of operational and maintenance instructions	HR	HR	HR	HR	3.	Operator friendliness	HR	HR	HR	HR	4.	Maintenance friendliness	HR	HR	HR	HR	5.	Protection against operation errors	R	R	HR	HR	6.	Protection against sabotage			R	R
Techniques / Measures				REQUIREMENTS																																											
		SIL 1	SIL 2	SIL 3	SIL 4																																										
1.	Production of applications operational and maintenance instructions	R	R	HR	HR																																										
2.	Training in the execution of operational and maintenance instructions	HR	HR	HR	HR																																										
3.	Operator friendliness	HR	HR	HR	HR																																										
4.	Maintenance friendliness	HR	HR	HR	HR																																										
5.	Protection against operation errors	R	R	HR	HR																																										
6.	Protection against sabotage			R	R																																										
Decommissioning and disposal (5.3.13 EN50129)	It must be provided evidences that prove the decommissioning according to the measurements defined in the decommissioning manual has been made.																																														

Table 18: Safety management report. Techniques and procedures used

4.1.4 Technical safety report

Technical evidence that ensures the safety of the design is the third condition to accept the system as safe. According to the norm EN50129[20], the technical safety report must be structured as follows:

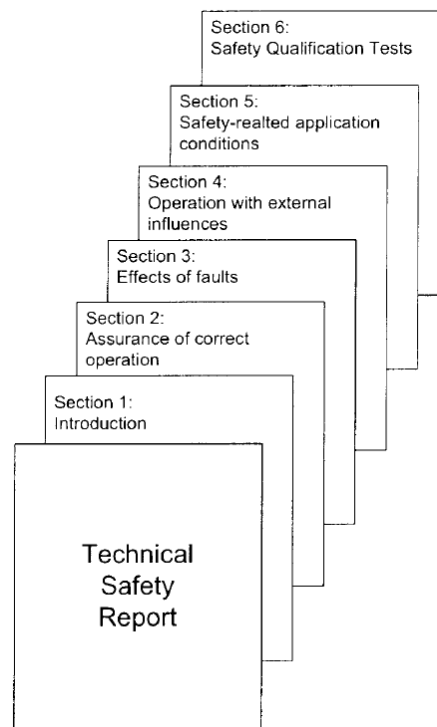


Figure 20: Structure of technical safety report

Introduction

The following section summarizes the approach and results of the safety analyses performed for the door system offered and integrated by a generic door system supplier. This section aims to demonstrate that the safety requirements defined in the system requirements are met by the design of the system.

Assurance of correct functional operation

This section must contain all the evidences necessary to demonstrate the correct operation of the door system under normal conditions, without failures according to safety and functional requirements specified.

Hazards of the system must be identified using PHA and OSHA techniques.

In the PHA hazard modes are identified and those shall be mitigated if the risk category is not considered as “Negligible”. After considering the mitigating conditions, the probability of occurrence of many hazards could be de-rated based upon the redundancies in the door system capability and assumptions made on maintenance practices and system diagnostic capability.

The results of the PHA identify the areas where potential hazards may exist due to events or conditions within the door system.

After considering the mitigating conditions, the described hazards shall have a very low probability of occurrence.

In the OSHA analysis, considering the mitigation conditions for the hazards identified, those must have a very low probability of occurrence based upon the redundancies in the door system capability and assumptions made on maintenance practices and system diagnostic capability.

Probability of equipment failures shall be reduced by the identification and correction of equipment failures and by the proper training of maintenance personnel.

Passenger related hazards can be nearly eliminated by safety rules provided by driver and staff to the passengers. Staff related hazards can be nearly eliminated mainly by good training and supervision of maintenances and operation personnel.

System architecture description

During the lifecycle phase design and implementation, phase 6 according EN50126, the system architecture description shall be documented according the techniques and measures with consideration to the Table 19.

Techniques / Measures		REQUIREMENT			
		SIL 1	SIL 2	SIL 3	SIL 4
1.	Separation of safety-related systems from non-safety-related systems	R	R	HR	HR
2.	Single electronic structure with self-tests and supervision	R	R	-	-
3.	Dual electronic structure	R	R	-	-
4.	Dual electronic structure based on composite fail-safety with fail-safe comparison	R	R	HR	HR
5.	Single electronic structure based on inherent fail-safety	R	R	HR	HR
6.	Single electronic structure based on reactive fail-safety	R	R	HR	HR
7.	Diverse electronic structure with fail-safe comparison	R	R	HR	HR
8.	Justification of the architecture by a quantitative reliability analysis of the hardware	HR	HR	HR	HR
Note: All techniques of the grey shaded group are alternatives, i.e. R means that at least one of these techniques is recommended					

Table 19: Architecture of system/sub-system/equipment (Table E.4 of EN50129)

Definition of interfaces

System Interfaces, for example, between Door application and FDF must be defined. These shall be defined in, deliverable D4.3 of WP4 of the Shift2Rail Grant Agreement [01]. Man-machine interfaces, operator, configuration (for example software parameterization) and maintenance, shall be also properly defined.

Techniques and measures for design features for avoidance and control of fault are given in Table 20.

Techniques / Measures		REQUIREMENT			
		SIL 1	SIL 2	SIL 3	SIL 4
1.	Protection against operating errors	R	R	HR	HR
2.	Protection against sabotage	-	-	HR	HR
3.	Protection against single fault for discrete components	R	R	HR	HR
4.	Protection against single fault for reintegrated circuits for digital electronic technology	R	R	HR	HR
5.	Physical independence within the safety-related architecture	R	R	HR	HR
6.	Detection of single faults	R	R	HR	HR
7.	Retention of safe state	R	R	HR	HR
8.	Multiple faults	R	R	HR	HR
9.	Dynamic fault detection	R	HR	HR	HR
10.	Program sequence monitoring	RR	HR	HR	HR
11.	Measures against voltage breakdown, voltage variations, overvoltage, low voltage	HR	HR	HR	HR
12.	Measures against temperature increase	HR	HR	HR	HR
13.	Software architecture	See EN50128 [19]			

Table 20: Design features (Table E.5 of EN5019)

Fulfilment of System Requirement specification

This shall be demonstrated how the operational functional requirements specified in the application requirements specification are fulfilled by the design. All relevant evidence shall be included or referenced (for example validation tests)

Fulfilment of Safety Requirement specification

The door system must fulfil quantitative safety requirements, SIL requirements and optionally qualitative safety requirements.

The SIL requirements of the door application shall be defined according to EN50128 [19].

Quantitative safety requirements are THR of the hazards identified in door system and TFFR required for the safety-related door functions.

Assurance of correct Hardware functionality

This shall describe the hardware architecture. Causal analyses must be performed, which can include FMECA and FTA and all failure modes must be allocated to an acceptable risk level of the risk assessment matrix.

This, on the one hand, arises from the use of low failure rates of single components (using high quality components), and on the other hand from the use of proven design with redundancy, diversity and adequate diagnostic capability.

Assurance of correct software functionality

Software of the door system must be developed according to a development process respecting the requirements defined in EN50128 [19] in order to ensure the adequate safety of SW controlled system function and to satisfy the normative requirements stated in EN50126/8/9 [17][18][19][20].

The software residing in the VCU/CCU must be developed according to the SIL required in SRS and the software development process must be defined in the Software Development Plan and developed and performed with an independent external assessor. The independent external assessor must verify the software development process, which must be approved by a certificate.

Interaction between hardware and software must be explained. Some topics that should receive attention are:

- Dependence between hardware and software
- Sequence of interaction
- Response times
- Self-test routines
- Health monitoring
- Data acquisition techniques
- Graceful degradation
- Negation methods

Effects of faults

This section must show the ability of the door system to fulfil the safety requirements in case that random fault in Hardware occurs and systematic faults in Software and Hardware.

Methods to identify and evaluate the effects of faults are given in the following table.

Techniques / Measures	REQUIREMENT			
	SIL1	SIL2	SIL3	SIL4
1. Preliminary hazard analysis *	HR	HR	HR	HR
2. Fault tree analysis	R	R	HR	HR
3. Markov diagrams	R	R	HR	HR
4. FMECA	R	R	HR	HR
5. HAZOP	R	R	HR	HR
6. Cause-consequence diagrams	R	R	HR	HR
7. Event tree	R	R	R	R
8. Reliability block diagram	R	R	R	R
9. Zonal analysis	R	R	R	R
10. Interface Hazard Analysis	R	R	HR	HR
11. Common cause failure analysis	R	R	HR	HR
12. Historical event analysis	R	R	R	R
* PHA should only be considered at the early stages of the development. When precise technical information is available, during the design, the other methods should be preferred.				

Table 21: Failure and hazards analysis methods (Table E.6 of EN50129)

Effects of single faults

It is necessary to ensure that the system remain safe in the event of any kind of single random hardware fault. Whichever technique or combination of techniques is used, assurance that no single random hardware component failure mode is hazardous shall be demonstrated using appropriate structured analysis methods. The procedures to identify components failure modes are defined in Annex C of the EN50129. In addition, techniques to achieve fail-safety principle are described in B.3.1 of this standard.

Independence of Items

Independence between items is a mandatory precondition for safety concerning single faults. Appropriate rules or guidelines shall be fulfilled to ensure this independence. The measures taken shall be effective for the whole life-cycle of the system. The door application design shall be arranged to minimize potentially hazardous consequences of loss-of-independence by, for example, a systematic design fault.

Independence could be lost by several types of influences: physical and functional internal influences and physical and functional external influences.

For the function “Release doors” it could be possible to demonstrate the independence of the following sub functions:

- Generation of door enable signal
- Generation of zero speed signal
- Door opening only if enable signal is active
- Traction inhibition signal when a door is enabled

Detection of single faults

Single faults must be detected to fulfil the required SIL level and the safety requirements specifications. To achieve that, mitigation measurements and SRACs (e.g. for driver, operator, etc.) must be defined. THR and PST targets must be met by a THR distribution and PST distribution. Techniques as FMEA and FTA could be used for the quantification. In addition for the control of random failure techniques and measures defined in IEC61508-2 [13] must be followed.

Action following detection (including retention of safe state)

In a safety system is not enough with the detection of the error: a protection (safe state) and retention of this protection is necessary too. The actuation of different detection mechanisms in case of an error must be defined and justify. The safe state shall be reached in a time sufficiently short that the combined detection-plus-negation time fulfils the specified safety target (normally in terms of SDT).

Effects of multiple faults

There are some second and third order cut-sets, that is, combination of two or three failures that lead to the failure of the function. The failure rate of the combination of two failures depends on the failure rates of the single elements and the detection plus negation time¹⁴ of individual failures. In some particular cases, it is necessary to monitor single failures in order to reduce this detection plus negation time and achieve the required failure rate for the second order cut-set. Therefore, it is essential to make sure that this detection plus negation times are fulfilled. A suitable method (for example FTA) shall be used to demonstrate the effects of multiple faults

Defence against systematic faults

Defence against systematic faults in the door system must be detailed in this subsection. It is usually justify with the system life-cycle according EN50126 [17][18], annex E of EN50129 [20] and annex A of EN50128 [19]

Operation with external influences

This section must demonstrate that functional and safety requirements are still fulfilled when the door system is subject to the specified external influences.

The justification of the methods used to endure the following external influence must be provided and the appropriate values for them are listed in EN50125-1 [43] and EN50125-3 [45].

- Climatic conditions
- Mechanical conditions
- Altitude

¹⁴ According to EN50129[20], negation time is defined as time span which begins when the existence of a fault is detected and ends when safe state is enforced

- Electrical conditions
- Protection against unauthorized access (definition of access level, protection, external devices, encapsulation)

For electrical conditions the values of EN50121-1 [41], EN50124-1 [42] and EN50155 [44] should be used as a basis.

Safety-related application conditions

This section should specify (or reference) the rules, conditions and restrictions that should be observed in the door system application.

It must be taken into account:

- Configuration of the programmable systems.
- Cautions in the manufacture, installation, testing and commissioning.
- Rules and methods for maintenance and faults.
- Instructions for the operation of the door system.
- Safety notification and cautions.
- Precautions with electromagnetic compatibility.
- Information concerning the modifications and the eventual decommissioning of service.
- Justification of the safety of the equipment and of the support tools, such as equipment for testing, equipment for maintenance and configuration tools.

Safety qualification test

This section should provide evidence to demonstrate the successful completion of the validation tests associated with the safety requirements. This section must refer to safety test cases report developed according the Safety Plan

Conclusions

Evidences described in previous sections must ensure that Doors System is safe enough according to the safety requirements specifications. Qualitative and quantitative targets of the EN50128 [19] and EN50129 [20] standards shall be achieved according to specified SIL for systematic and random failures.

4.2 DOOR FUNCTION

4.2.1 Definition of the Subsystem

The purpose of the function “Releasing (selective) doors” is to allow or forbid passengers to get on-board the train or to leave the train. Leaving the train is not permitted where there is no platform or when the train is in movement.

The subsystem under analysis is a generic door system integrated in the NG-TCMS. To be executed in a safe way according to the requirements, this function needs the high level functions analyzed in CONNECTA D3.3 – Report on RAMS and Security Analysis [32] and CONNECTA D3.5 – Report on Drive-by-Data Architecture [35]:

- Safe data communication provided by the safe data transmission channel.
- Data calculation by the Safe Train Inauguration.

As defined in the analysis of safe data transmission channel in CONNECTA D3.3 – Report on RAMS and Security Analysis [32], to achieve the SIL4 requirement for a given Safety Function (safety loop), it is mandatory that the THR is less or equal than $1 \cdot 10^{-8}$ 1/h. Therefore the communication should reach a THR of 1%, so that a whole safety function can be realized with a maximum of 100 safety relevant sections (ED-S, Safe data transmission channel, sensors and actors).

The Safe data transmission channel is based on the on the “black-channel” approach and the failsafe-principle. Safe data transmission channel should reach a $THR < 10^{-10}$ 1/h in order to achieve the safety requirement of SIL4. The SDTv2-Protocol described in Annex B of IEC61375-2-3 [38] must be extended and improved concerning the weaknesses identified in CONNECTA D3.3 – Report on RAMS and Security Analysis [32] to provide safe data transmission, resulting the SDTv4-Protocol described in CONNECTA D3.5 – Report on Drive-by-Data Architecture [35].

Safe train inauguration defines the train backbone topology discovery, called “ETB inauguration”, and the train composition discovery, called “operational train inauguration”. The function aims to provide the train composition information with a high safety integrity level (SIL4) which the existing TCN standards (IEC61375-2-5 [39] and IEC61375-2-3 [38] cannot provide.

According to the table 24 of CONNECTA D3.3 – Report on RAMS and Security Analysis [32], the THR target for the functions “Releasing doors” and “Releasing selective doors” must be 10^{-8} and 10^{-6} respectively. In order to achieve these targets, DCU needs to know several inauguration parameters, which must be safely stored in the TTDB. Some parameters that the DCU needs to know are leader vehicle, train orientation, consist orientation and orientation of vehicles. In addition, for the function “releasing selective doors”, parameters as number of consist, number of vehicle, sequence of consists and sequence of vehicles are also needed for the safe operation of the function.

Therefore, this train application needs information about the train composition itself, which is provided by the safe inauguration function in two different views: the train directory (TrainDirectory) in combination with the consist information (ConsistInfoList). It provides the information about the train length, sequence and orientation of consists and vehicles. It will only change if the train composition is changed (adding/removing consists).

The apportionment of the SIL requirement must be done in the higher level functions of the door applications. These functions are, in addition of the functions previously mentioned, the function door control. To achieve the THR target, these functions (communication, inauguration and door control) must fulfill the TFFR according this apportionment.

A high level architecture of the door function within the NG-TCN architecture in a consist is given in the next Figure 21

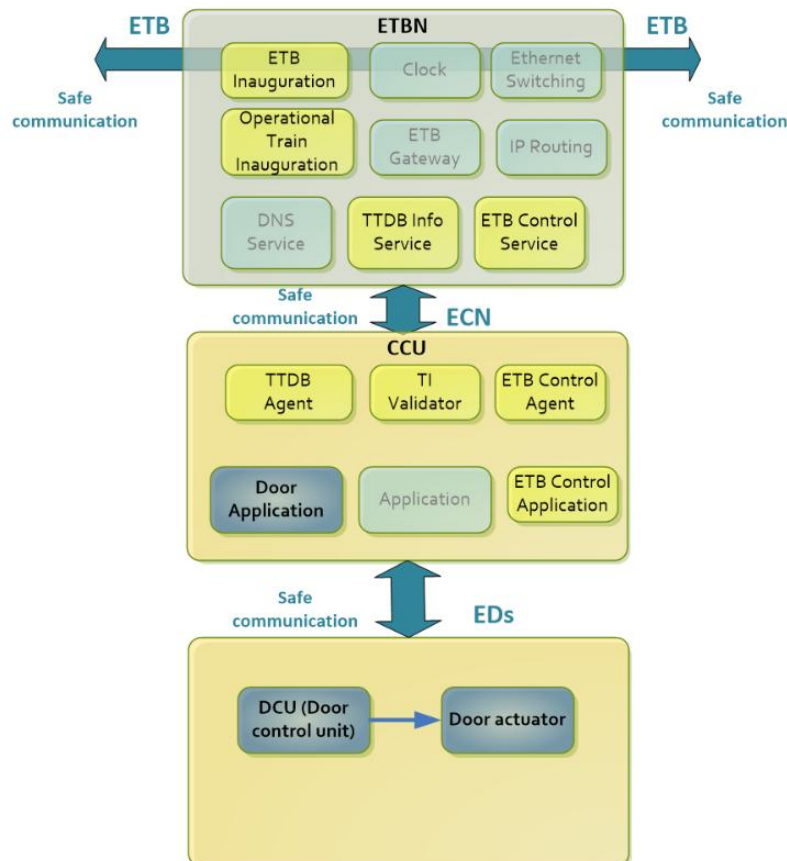


Figure 21: Definition of the door system¹⁵

Door application is integrated in the CCU, which communicates with the DCU using the safe data transmission channel. As mentioned previously, SDTv4 is needed to ensure the safe communication. On the other hand, this application needs also to have safe access to some inauguration data, stored safely in the TTDB.

Each train door is equipped with an actuator (e.g. electric motor). The actuator is commanded by a local door command system which receives valid information for the whole train (e.g. train speed, opening authorization from the driver or from a train controller). Depending on the train, the door opening may occur automatically or only if a passenger issues an opening request (e.g. by pushing a button on the train door).

¹⁵ It is shown only one system door in the consist to simplify

In case of more than one consist, it must be taken into account the definition and standardization of the interfaces between them, ensuring the interoperability between consists. In this case the safe data transmission channel ensures a safe communication allowing the interchange of information point-to-point between the CCUs of each consists.

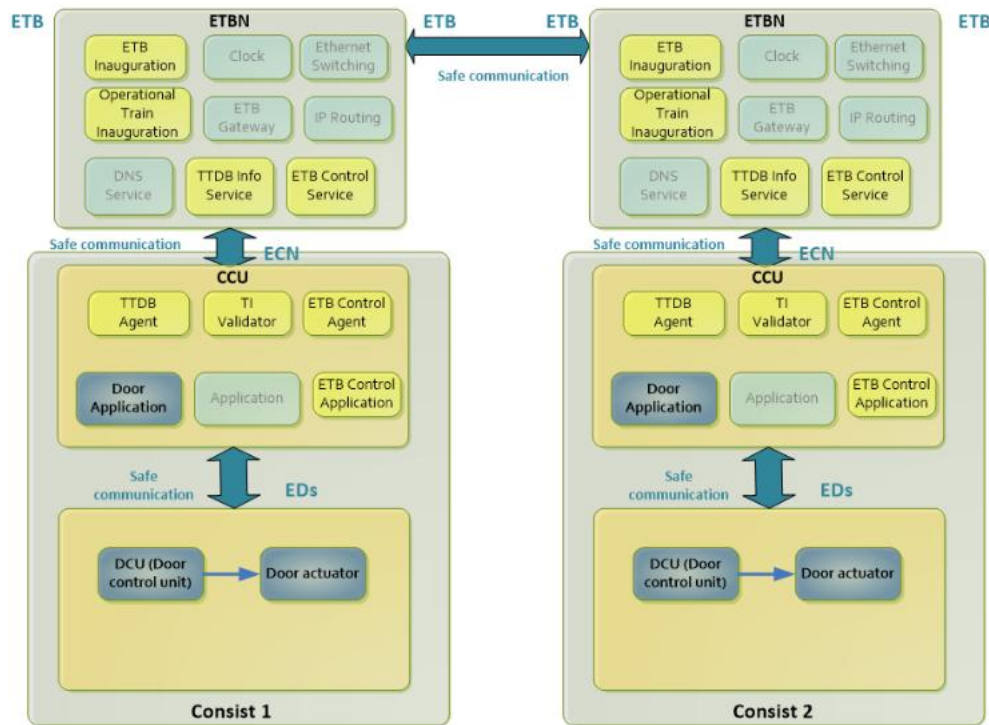


Figure 22 Architecture with 2 consists

An identification service of the components within the system (hardware and software) is needed. Moreover it is also necessary to specify the current versions of the components for the safety case.

4.2.2 Functional breakdown

NOTE: The sub-functions regarding the steps, the ramps, and the interior doors are not in the scope of this study.

Levels			Function (level 3)
1	2	3	
D	B	B	Release external doors
D	B	B	Release external door by driver
D	B	B	Release external doors by beacon/ATC
D	B	B	Enable release external doors
D	B	B	Cancel release external
D	B	B	Indicate external doors released
D	B	C	Open external doors
D	B	C	Open external doors by local control (mechanical handle or push button)

Levels			Function (level 3)
1	2	3	
D	B	C	Open external doors following driver or crew activation
D	B	C	Open external doors automatically
D	B	C	Open external doors by actuating ramp
D	B	C	Open external doors by actuating lift
D	B	C	Enable selective external door opening
D	B	D	Close external doors
D	B	D	Close external doors automatically
D	B	D	Close the external doors upon exceeding a speed threshold
D	B	D	Enable selective external door closing
D	B	D	Close external doors by driver or the staff command
D	B	D	Close external doors by passenger request
D	B	E	Manage door system upon obstacle
D	B	E	Detect obstacle
D	B	E	Manage the door according to obstacle detection
D	B	F	Lock external doors
D	B	F	Lock external doors mechanically
D	B	F	Lock external doors mechanically automatically
D	B	F	Lock external doors mechanically manually
D	B	F	Lock external doors electrically
D	B	F	Lock external doors electrically automatically
D	B	F	Lock external doors electrically manually
D	B	G	Unlock external doors
D	B	H	Enable selective external door opening
D	B	H	Enable individual door opening
D	B	H	Enable side selective door opening
D	B	H	Enable section selective door opening
D	B	H	Allow a local door to remain open under crew control
D	B	K	Isolate external doors
D	B	L	Signal all external door closed and locked state
D	B	M	Signal external door status change/open/close
D	B	M	Signal external door status change internal and or external to the vehicle
D	B	M	Signal external door status to the crew
D	B	N	Enable external door opening in emergency

Levels			Function (level 3)
1	2	3	
D	B	N	Enable external door opening in emergency while driving
D	B	N	Enable external door opening in emergency while standing
H	E	F	Manage access and loading
H	E	F	Manage exterior door system

Table 22: Doors Sub-functions

Contrary to the Table 25 of the section 4.3.3 of this document, no assumption is made about the ability of the NG-TCMS to manage the Doors sub-functions.

4.2.3 Doors safety goals

Following the same principle as in the section concerning the Brake safety goals (section 4.3.3), the Table 23 above gives the safety requirements included in the TSI LOC&PAS [47] for the Door function. Similarly, some functional requirements strongly linked to the safety and to the scope of the Task 3.4 have been kept.

TSI reference	Title	Safety Requirement (extract)
4.2.5.5.3	Door closing and locking	<p>(1) The door control device shall allow the train crew to close and lock all the doors before the train departs.</p> <p>(3) When the centralised door closing and locking is activated from a local control, adjacent to a door, it is permissible for this door to remain open when the other doors close and lock. The door control system shall allow the staff to close and lock this door subsequently before departure.</p> <p>(4) The doors shall be kept closed and locked until they are released in accordance with clause 4.2.5.5.6 'Door opening' [of document [47]]. In the event of loss of power to the door controls, the doors shall be kept locked by the locking mechanism.</p>
4.2.5.5.5	Information available to the train crew	<p>(1) An appropriate 'doors-closed proving system' shall allow the train crew to check at any moment whether or not all the doors are closed and locked.</p> <p>(2) If one or more doors are not locked, this shall be continuously indicated to the train crew.</p> <p>(3) An Indication shall be provided to the train crew of any fault of a door closing and/or locking operation.</p> <p>(4) Audible and visual alarm signal shall indicate to the train crew an emergency opening of one or more doors.</p>
4.2.5.5.6	Door opening	<p>(1) A train shall be provided with door release controls, which allow the train crew or an automatic device associated with the stop at a platform, to control the release of doors separately on each side, allowing them to be opened by passengers or, if available, by a central opening command when the train is at</p>

TSI reference	Title	Safety Requirement (extract)
		<p>a standstill.</p> <p>(3) At each door, local opening controls or opening devices shall be accessible for passengers from both the outside and the inside of the vehicle.</p>
4.2.5.5.7	Door-traction interlock	<p>(1) Traction power shall be applied only when all doors are closed and locked. This shall be ensured through an automatic door-traction interlock system. The door-traction interlock system shall prevent traction power being applied when not all of the doors are closed and locked.</p>
4.2.5.5.8	Safety requirements for clauses 4.2.5.5.2 to 4.2.5.5.7 [of document [47]]	<p>(1) For the scenario one door is unlocked (with train crew not correctly informed of this door status) or released or opened in inappropriate areas (e.g. wrong side of train) or situations (e.g. train running), it shall be demonstrated that the risk is controlled to an acceptable level, considering that the functional failure has typical credible potential to lead directly to:</p> <ul style="list-style-type: none"> — ‘single fatality and/or severe injury’ for units in which passengers are not supposed to stay in standing position in the door area (long distance), or to — ‘single fatality and/or severe injury’ for units in which some passengers stay in standing position in the door area in normal operation. <p>(2) For the scenario several doors are unlocked (with train crew not correctly informed of this door status) or released or opened in inappropriate areas (e.g. wrong side of the train) or situations (e.g. train running), it shall be demonstrated that the risk is controlled to an acceptable level, considering that the functional failure has typical credible direct potential to lead to:</p> <ul style="list-style-type: none"> — ‘fatality and/or severe injury’ for units in which passengers are not supposed to stay in standing position in the door area (long distance), or to — ‘fatalities and/or severe injuries’ for units in which some passengers stay in standing position in the door area in normal operation. <p>(3) The demonstration of conformity (conformity assessment procedure) is described in clause 6.2.3.5 of this TSI [document [47]].</p>
4.2.5.5.9	Door emergency opening	<p>Internal emergency opening:</p> <p>(1) Each door shall be provided with an individual internal emergency-opening device accessible to passengers, that shall allow the door to open; this device shall be active when the speed is below 10 km/h.</p> <p>(2) It is allowed to have this device active at any speed (independent of any speed signal); in such a case, this device shall be operated after a succession of at least two actions.</p>

TSI reference	Title	Safety Requirement (extract)
		<p>Safety requirement:</p> <p>(4) For the scenario ‘failure in the internal emergency opening system of two adjacent doors along a through route (as defined in clause 4.2.10.5 of this TSI [document [47]]), the emergency opening system of other doors remaining available’, it shall be demonstrated that the risk is controlled to an acceptable level, considering that the functional failure has typical credible potential to lead directly to ‘single fatality and/or severe injury’. The demonstration of compliance (conformity assessment procedure) is described in clause 6.2.3.5 of this TSI [document [47]].</p>

Table 23: Doors Safety requirements from the TSI LOC&PAS (extracts)

As for the Brake function, the document [49] is applicable. In the case of the Doors function and in the context of our study, it refers to the following "TSI references" of the Table 23:

Complementary to the requirements above extracted from the TSI LOC&PAS, the Doors function shall fulfil the section 4.8 of the standard EN14752 [50].

4.3 BRAKE FUNCTION

This chapter outlines only the different aspects of the function itself since the generic approach is already described in chapter 4.1.

4.3.1 Definition of the subsystem

The brake function must have the two main capabilities:

- Reduce the speed, maintain the speed on slope, stopping the train by applying a retarding force during running;
- Immobilize the train in standstill for an unlimited period of time.

The function is distributed over several electrical as well as mechanical components and spans over the complete train. It consists generally of input devices (sensors), computing devices and brakes (actors). Furthermore, the communication path is also part of the function.

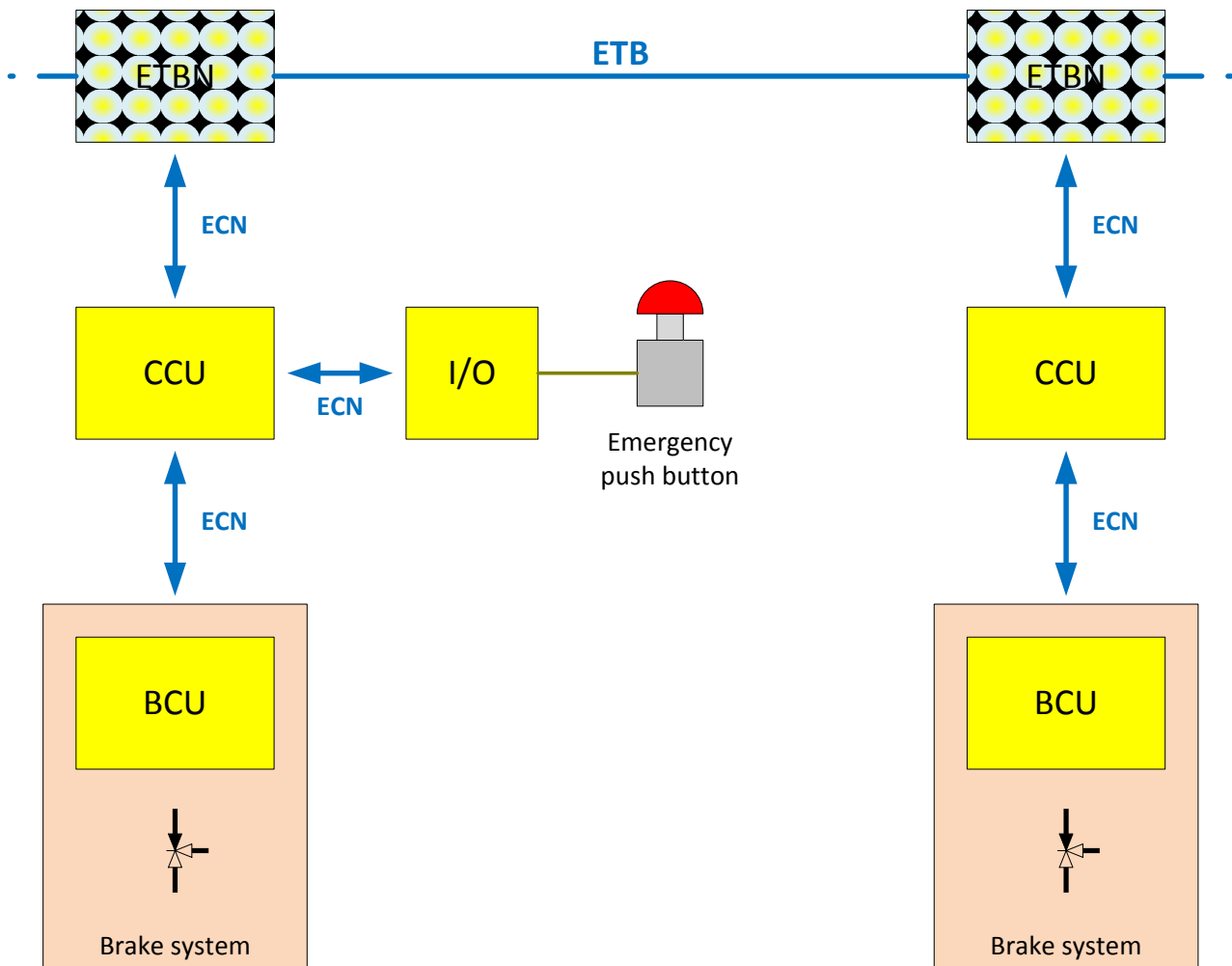


Figure 23: Overview of function brake

Figure 23 depicts an example architecture for an emergency brake. This type of brake has been chosen for further treatment since the emergency brake has the highest requirements regarding safety and reliability. Thus, the following scenario is conceivable: The driver pushes a button for emergency breaking, which is read by an I/O unit. The signal is transmitted to the local CCU and this device distributes an emergency brake command (directly or over all control units) to BCU devices in the whole train. Each BCU in turn induces the brake to apply a predefined brake force to stop the train with a defined level of brake performance.

The complete chain must be designed to not only have a high integrity but also to respond in a very short time. For example, if the emergency brake command is delayed by just 1 second at a train speed of 200 km/h, the train moves 55 meters further before starting to brake.

4.3.2 Functional breakdown

At its 3rd level and most detailed level, the standard [05] splits the brake functions in the Table 25 above.

Levels			Function (level 3)	Comment
1	2	3		
E	B	F	Provide reaction on uncoupling	
G	B	C	Acquire demand for dynamic brake force from brake control	
G	C	B	Configure brake system	
G	C	B	Configure brake system according to train configuration	
G	C	B	Configure brake system according to activated cabin	
G	C	B	Configure brake system according to operational restrictions and degraded mode conditions	
G	C	B	Get status of brake systems	
G	C	B	Get status of automatic brake system	
G	C	B	Get status of direct brake system	
G	C	B	Get status of electrodynamic brake system	
G	C	B	Get status of hydrodynamic brake system	
G	C	B	Get status of eddy current brake system	
G	C	B	Get status of magnetic track brake system	
G	C	B	Isolate brake systems / devices	
G	C	B	Isolate brake systems at train level	
G	C	B	Isolate brake systems / devices at consist level	
G	C	B	Isolate brake systems / devices at car level	
G	C	B	Isolate brake systems / devices at bogie level	a
G	C	B	Isolate brake systems / devices at axle level	a
G	C	C	Acquire brake demand	
G	C	C	Acquire brake demand from the driver	
G	C	C	Acquire brake demand from the driver's automatic brake controller	
G	C	C	Acquire brake demand from the traction brake controller	
G	C	C	Acquire brake demand from direct brake controller	
G	C	C	Acquire brake demand from emergency devices	
G	C	C	Acquire brake demand from the train protection functions	
G	C	C	Acquire brake demand from the driver activity control	
G	C	C	Acquire brake demand from ATP	
G	C	C	Acquire brake demand from brake signal transmission	

Levels			Function (level 3)	Comment
1	2	3		
G	C	C	Acquire brake demand from internal speed control	
G	C	C	Acquire brake demand from passengers and crew	b
G	C	D	Prioritise brake demand and select braking mode	a
G	C	D	Set up service brake mode	
G	C	D	Set up emergency brake mode	
G	C	D	Set up holding brake mode	
G	C	D	Set up holding brake mode automatically	
G	C	D	Set up holding brake mode manually	
G	C	D	Set up parking brake mode	
G	C	E	Allocate braking effort	a
G	C	E	Calculate needed braking effort	a
G	C	E	Calculate needed brake effort at train level	a
G	C	E	Calculate needed brake effort at consist level	a
G	C	E	Calculate needed brake effort at vehicle level	a
G	C	E	Calculate needed brake effort at bogie level	a
G	C	E	Prioritise executing braking systems	a
G	C	E	Acquire available braking effort	
G	C	F	Handle braking due to train configuration, brake mode and brake demand	
G	C	F	Handle braking at higher levels	
G	C	F	Handle braking at train level	
G	C	F	Handle braking at consist level	
G	C	F	Handle braking at vehicle level	
G	C	F	Handle braking at bogie level	a
G	C	F	Determine set points and control depending on brake mode at local level	
G	C	F	Provide Brake Command for parking Braking	
G	C	F	Provide Brake Command for Holding Braking	
G	C	F	Provide Brake Command for Service Braking	
G	C	F	Provide Brake Command for Emergency Braking	
G	C	F	Manage brake blending at local level	a
G	C	F	Request traction cut-off	
G	C	F	Acquire realised braking effort	
G	C	G	Apply and release braking forces	a
G	C	G	Generate and reduce braking forces	a

Levels			Function (level 3)	Comment
1	2	3		
G	C	G	Generate braking forces by friction brake	a
G	C	G	Generate braking forces by eddy-current brake	a
G	C	G	Generate braking forces by magnetic track brake	a
G	C	G	Command electrodynamic brake	a
G	C	G	Release braking forces (manually and emergency release)	
G	C	G	Dissipate heat	a
G	C	G	Provide storage of energy for braking (at train level)	a
G	C	G	Provide intermediate storage of energy for braking	a
G	C	G	Control storage level and energy flow	a
G	C	G	Protect stored energy for braking	a
G	C	G	Detect non-release of braking forces	
G	C	H	Provide Wheel Slide Protection	a
G	C	H	Detect sliding	a
G	C	H	Control sliding	a
G	C	H	Manage brake release	

Table 24: Brake Sub-functions

Key to Table 24:

a: A sub-function not managed by the NG-TCMS

b: This sub-function is included in the PAS. It shall be studied with the PAS which is not a part of the Brake system.

As it can be seen in the Table 24 not all the brake sub-functions have to be considered for the safety case of the brake function of the train, as far as the TCMS is concerned. Many sub-functions are nowadays supported by the TCMS, as well as they will be supported by the NG-TCMS, but also many brake sub-functions are – and will keep on being – controlled at local level.

As a result 54 sub-functions are listed in the Table 24, including 25 not directly managed by the NG-TCMS. The 19 remaining sub-functions are the purpose of the safety case.

4.3.3 Brake safety goals

The safety goals are globally determined through Europe by the TSI LOC&PAS [47] for the scope of CONNECTA (i.e. not considering the freight wagons). Nevertheless, it shall not be forgotten that all the safety regulations are not completely harmonized and many national regulations still exist, especially for the brake functions. This is because among other things braking a train is dependent of the infrastructure where the train is operated (e.g. through the maximum speed limit), as well as some operational rules (e.g. for degraded modes operations like coupling consists when a train requests for assistance, etc.).

Anyway, the TSI LOC&PAS gives the basis for the search for brake safety goals: its chapter 4.2.4 *Brakes* gives some functional requirements upon the brake system together with some system safety requirements, which are summarized in the following Table 25 (extracted from the document [47]).

Even though the Table 25 should list only the safety requirements, some functional requirements have been included. The reason for keeping those functional requirements is their impact on the global safety of the brake function of the train.

In addition, it shall be noticed that some of the requirements listed in the Table 25 might be completed by the comments listed in the document: Guide for the application of TSI LOC&PAS [49].

In the context of our study, this concerns the "TS references": 4.2.4.1, 4.2.4.4.1, 4.2.4.4.2, 4.2.4.4.5.

TSI reference	Title	Safety Requirement (extract)
4.2.4.2.1.	Functional requirements	<p>The main brake function of a train shall be:</p> <p>(3) continuous: the brake application signal is transmitted from a central command to the whole train by a control line.</p> <p>(4) automatic: an inadvertent disruption (loss of integrity, line de-energised, etc.) of the control line leads to brake activation on all vehicles of the train.</p> <p>(8) The braking performance shall be consistent with safety requirements expressed in clause 4.2.4.2.2 <i>[of document [47]]</i> in case of inadvertent disruption of the brake control line, and in the event of the braking energy supply being disrupted, the power supply failing or other energy source failure.</p> <p>(11) In case of unintentional train separation, the two parts of the train shall be brought to a standstill; the braking performances on the two parts of the train are not required to be identical to the braking performance in normal mode.</p>
4.2.4.2.2	Safety requirements	Application of the Table 3 "Braking system — safety requirements" <i>[of document [47]]</i> .
4.2.4.4.1	Emergency braking command	<p>(2) The sequential activation of these two devices may be considered in the demonstration of compliance to the safety requirement No 1 of Table 3 of clause 4.2.4.2.2 <i>[of document [47]]</i>.</p> <p>(3) The activation of the emergency brake shall also be possible by the Control-Command and signalling on-board system, as defined in the TSI CCS [48].</p> <p>(4) Unless the command is cancelled, the emergency brake activation shall lead permanently, automatically to the following actions:</p> <p>— transmission of an emergency brake command along the train by the brake control line,</p> <p>— cut-off of all tractive effort in less than 2 seconds; this cut-off shall not be</p>

TSI reference	Title	Safety Requirement (extract)
		able to be reset until the traction command is cancelled by the driver, — an inhibition of all ‘release brake’ commands or actions.
4.2.4.4.2	Service braking command	(4) When the speed of the train is higher than 15 km/h, the service brake activation by the driver shall lead automatically to the cut-off of all tractive effort; this cut-off shall not be reset until the traction command is cancelled by the driver.
4.2.4.4.4	Dynamic braking command	If a unit is equipped with a dynamic brake system: (1) It shall be possible to prevent the use of regenerative braking on electric units so that there is no return of energy to the overhead contact line when driving on a line which does not allow that.
4.2.4.4.5	Parking braking command	(2) The parking braking command shall lead to the application of a defined brake force for an unlimited period of time, during which a lack of any energy on board may occur. (4) For units assessed in fixed or predefined formations, and for locomotives assessed for general operation, the parking brake command shall be activated automatically when the unit is switched off. For other units, the parking brake command shall be either activated manually, or activated automatically when the unit is switched off.
4.2.4.7.	Dynamic brake - Braking system linked to traction system	Where the braking performance of the dynamic brake or of braking system linked to the traction system is included in the performance of the emergency braking in normal mode defined in clause 4.2.4.5.2 <i>[of document [47]]</i> , the dynamic brake or the braking system linked to traction: (1) Shall be commanded by the main brake system control line (see clause 4.2.4.2.1 <i>[of document [47]]</i>). (2) Shall be subject to a safety analysis covering the hazard ‘after activation of an emergency command, complete loss of the dynamic brake force’. This safety analysis shall be considered in the safety analysis required by the safety requirement N° 3 set out in clause 4.2.4.2.2 <i>[of document [47]]</i> for the emergency brake function. For electric units, in case the presence on-board the unit of the voltage delivered by the external power supply is a condition for the dynamic brake application, the safety analysis shall cover failures leading to absence on-board the unit of that voltage.
4.2.4.9.	Brake state and fault indication	(1) Information available to train staff shall allow the identification of degraded conditions concerning the rolling stock (brake performance lower than the performance required), for which specific operating rules apply. To that end, it shall be possible at certain phases during operation for the train staff to identify the status (applied or released or isolated) of the main (emergency and service) and parking brake systems, and the status of each part (including one or several actuators) of these systems that can be controlled and/or isolated

TSI reference	Title	Safety Requirement (extract)
		<p>independently.</p> <p>(3) The phases that shall be considered during operation are standstill and running.</p> <p>(4) When at a standstill, train staff shall be able to check from inside and/or outside of the train:</p> <ul style="list-style-type: none"> — The continuity of the train brake control command line, — The availability of the braking energy supply along the train, — The status of the main brake and parking brake systems and the status of each part (including one or several actuators) of these systems that can be controlled and/or isolated separately (as described above in the first paragraph of this clause), excepted for dynamic brake and braking system linked to traction systems. <p>(5) When running, the driver shall be able to check from the driving position in the cab:</p> <ul style="list-style-type: none"> — The status of the train brake control command line, — The status of the train brake energy supply, — The status of the dynamic brake and braking system linked to traction system where they are included in the performance of the emergency braking in normal mode, — The status applied or released of at least one part (actuator) of the main brake system which is controlled independently (e.g. a part which is installed on the vehicle fitted with an active cab). <p>(6) The function providing the information described above to the train staff is a function essential to safety, as it is used for the train staff to evaluate the braking performance of the train. [...] Where a centralised control system allowing the train staff to perform all checks from one location (i.e. inside the drivers cab) is provided, it shall be subject to a reliability study, considering the failure mode of components, redundancies, periodic checks and other provisions; [...]</p> <p>(7) Applicability to units intended for general operation:</p> <p>Only functionalities that are relevant to the design characteristics of the unit (e.g. presence of a cab, ...) shall be considered.</p> <p>The signals transmission required (if any) between the unit and the other coupled unit(s) in a train for the information regarding the brake system to be available at train level shall be documented, taking into account functional aspects.</p>
4.2.4.10.	Brake requirements	(2) For units intended to be operated on other track gauge systems than 1 520 mm system, it shall be possible, following a failure during operation, to rescue

TSI reference	Title	Safety Requirement (extract)
	for rescue purposes	<p>a train with no energy available on board by a recovery power unit equipped with a pneumatic brake system compatible with the UIC brake system (brake pipe as braking control command line).</p> <p>(3) During the rescue, it shall be possible to have a part of the brake system of the rescued train controlled by means of an interface device; in order to meet this requirement, it is allowed to rely on low voltage provided by a battery to supply control circuits on the rescued train.</p>

Table 25: Brake Safety requirements from the TSI LOC&PAS (extracts)

For the purpose of the Task 3.4, these safety requirements directly linked with the Brake function shall be completed by the following requirement from document [47]:

TSI reference	Title	Safety Requirement (extract)
4.2.1.3	Safety aspects	(4) Electronic devices and software, which are used to fulfil functions essential to safety shall be developed and assessed according to a methodology adequate for safety related electronic devices and software.

Table 26: General Safety requirement from the TSI LOC&PAS (extract)

4.4 SAFETY MEASURES

The brake function needs the same safe functions as the door function so that it can be executed in safe way:

- Safe data communication provided by the safe data transmission channel.
- Data calculation by the safe train inauguration.

Besides these two measures the communication path must be based on TSN as described in T3.5 [35] since for the brake function it is essential to have a guaranteed minimal response time. But TSN is not classified as safety measure, because a development of TSN with safety requirements would be too expensive. However, the safe data transmission channel shall supervise the correct operation of TSN and trigger safe state in case of failure.

The emergency brake function can be valued with $THR < 10^{-8}/h$ according CONNECTA D3.3 – Report on RAMS and Security Analysis [32]. This corresponds to safety requirements of SIL4, which needs to be considered for safety measures.

Safe data transmission channel

Like for safety function, the SDTv4 protocol as described in CONNECTA D3.5 – Report on Drive-by-Data Architecture [35] shall be used for safe data communication, because this protocol is capable of SIL4.

Safe train inauguration

Brake and door function relies on several parameters from train inauguration. According to CONNECTA D3.3 – Report on RAMS and Security Analysis [32] these parameters are relevant: Leader vehicle, number of consists and number of vehicles. For the service brake function, the parameters train orientation, consist orientation and vehicle orientation are further necessary.

The safe train inauguration described in CONNECTA D3.5 – Report on Drive-by-Data Architecture [35] is designed for high safety integrity level (SIL4) and therefore also suitable for brake function.

5. CONCLUSION (STATEMENT ABOUT FULFILMENT OF OBJECTIVES)

The safety approval concept which is subject of this document has been analysed and defined from different perspectives. First, a generic safety concept for a drive-by-data centric NG-TCMS has been developed in chapter 2 by defining the generic safety architecture for the executions of safety functions up to SIL4 and more specifically by proposing a safety design for the two communication network related safety functions “safe train inauguration” and “safe data transmission”. An important aspect is to avoid or at least to minimize interference between function of different safety criticality. Here some principles for a suitable safety architecture design have been described and have been more specifically applied later on to NG-TCMS related components and network safety functions (sub-chapter 3.2).

Next, in chapter 3, considerations for a generic certification process have been made. One aspect for certification is the handling of faults, definition of safe states and determination of the safety function response time (SFRT). Another aspect is the definition of rules for standardized interfaces, as those interfaces are more resistant to changes and enforce a clear separation between different train functions, which helps especially in incremental certification. A further aspect is the safe deployment of safety related software, including parameterization of software for deployment in a safe manner.

Finally, the process for safety cases has been demonstrated exemplarily for two selected train functions, the door function and the brake function.

With the analysis and evaluation work performed in Task 3.4 and documented in this report, the objectives defined by Connecta for this task should be addressed. The Technical Annex of CONNECTA ([01]) has defined three objectives for the Task 3.4:

- *how the safety requirement will be accomplished*
- *how the safety case should be conducted*
- *how the authorisation process (homologation) for a drive-by-data capable TCMS should be shaped*

All these objectives are covered, whereat these objectives have partly been treated in a more generic way and partly very specific, especially in relation to the network safety functions and the selected safety cases. It should also be mentioned that the work in this task, but also the work in other tasks of CONNECTA WP3, was accompanied by Safe4Rail as complementary action. Safe4Rail provided expertise with respect to safety certification, namely through the support of TÜV SÜD as a member of Safe4Rail. With this support, the expectation of an independent assessment of the safety approach could be satisfied sufficiently.

Annex A Calculation of the minimum SFRT (Excel-Tool)

The Excel tool for the calculation of the minimum SFRT is provided in [55].

Annex B Guideline for supporting certification procedure device

General

During the homologation process of train vehicles and the related approval procedure¹⁶, the conformance to functional requirements and conformance to safety must be proven. Safety requirements are resulting from a risk management process (CSM, see [34]) which must be executed for each significant change of the railway system.

The verification (certification) of functional and safety requirements is carried out through technical specifications, test reports, assessment reports, safety cases and safety analysis reports as it is ruled in the related standards, like EN50129 for hardware and EN50128/EN50657 for software.

Compared to legacy TCMS, a Drive-by-Data enabled TCMS brings some new challenges for the safety design, although the certification procedure remains identical:

1. Mixed critically applications from the TCMS, OOS and COS functional domains share a common physical computer platform (FDF). This aspect is discussed in [51].
2. Mixed critically applications from the TCMS, OOS and COS functional domains share a common physical communication network (NG-TCN). From a safety perspective, this challenge is handled by defining the physical communication channel as a black channel (no safety requirements at all) and using a safe data transmission channel on top of it to ensure the safe data transmission. However, as cyber security is affected, this item plays a role in the certification procedure.
3. Absence of train lines requires higher safety integrity for related functions. E.g., the absence of the 'orientation' train line in NG-TCN required a change of ETB topology and the introduction of "BEACON" telegrams, see [35].
4. Higher integration of formerly mostly independent sub-systems like the brake system (CTA WP5) and signaling (S2R project X2Rail). This motivated the definition of a SIL4 safe data transmission protocol (SDTv4).
5. Increasing software share in safety-critical functions accompanied with a reduced hardware part, for the sake of cost reduction (example: Electronic Distributed Valve in CTA WP5). This implies also an increase in software SIL.

Especially the fact that more software is involved in safety and that functions of different safety criticality share resources, bears the risk that the effort for safety certification will increase. To counteract on this risk, a set of measures, like the measures already defined for the FDF (see [51]), have been defined (see below) which shall help to support the overall certification process.

System under Consideration

In a first step, the SuC shall be defined (Figure 24, with explanations given in Table 27). Dependent on the scope of safety assessment, the whole TCMS (including OOS and COS functions) can be broken down to a set of SuCs.

¹⁶ A comprehensive description of the railway approval process is presented in [51] chapter 5.

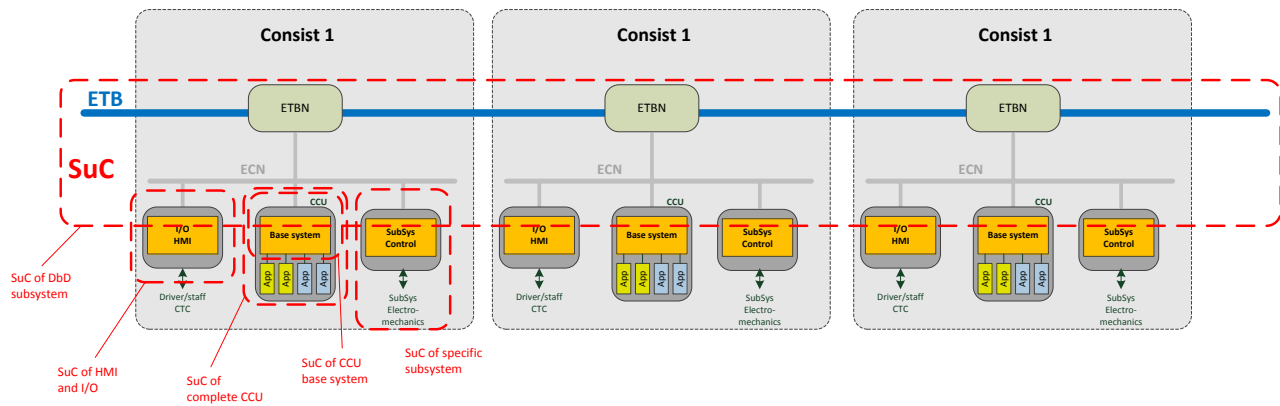


Figure 24: TCMS – System under Consideration

Table 27: TCMS – System under Consideration

SuC	Description	Basic safety requirements
NG-TCN	Train communication network with ETB and ECN	<ul style="list-style-type: none"> Safe train inauguration SDTv4 protocol
HMI	Input/Output of regular and safety-related information to/from train staff.	<ul style="list-style-type: none"> Safe display of information Safe input of information Separation between regular and safe display information SDTv4 for communication with CCU
I/O	Input/Output of regular and safety-related signals provided by the conventional train control subsystem (electro-mechanical parts).	<ul style="list-style-type: none"> Safe input/output Separation between regular and safe I/O SDTv4 for communication with CCU
CCU – Base System	The generic part of the CCU, including: <ul style="list-style-type: none"> Hardware boot loader operating system communication protocol stacks (incl. SDTv4) middleware (FDF) generic applications (e.g. ETB Control) 	<ul style="list-style-type: none"> Safe processing hardware platform (e.g. 1oo2) Safe execution of applications <ul style="list-style-type: none"> Spatial and time separation Execution supervision Voting Safe middleware (incl. SDTv4 protocol)
CCU complete	CCU with project specific application software and configuration	<ul style="list-style-type: none"> Safe applications Safe configuration of the CCU and the communication relationships (SDTv4).
Specific subsystem (brake, door etc.)	Subsystem responsible for the execution of specific subsystem functions under the control of the CCU (application).	<ul style="list-style-type: none"> Safe function execution Safe operation of electro-mechanical parts SDTv4 for communication with CCU

Pre-certification of generic components

All generic components or subsystems should be pre-certified in order to avoid project specific certification activities for those parts. This is obvious for hardware because project specific adaptations of hardware should be avoided. Also generic software parts, like operating systems, the FDF or other generic components, can be pre-certified. The Development of hardware shall follow the requirements set in EN50129. Software can be developed generically in a way that adaptations to specific vehicle applications are only done by specific configuration. For that case, the development of the generic software shall respect the requirements defined in clause 7.8 of EN50657. The project specific configuration of the generic software components shall obey the requirements set in clause 8 of EN50657.

Table 28 lists those NG-TCN components and items for which a pre-certification could be done.

Table 28: TCMS – Precertification of components (preliminary)

Item/Component	Description	Scope of assessment ¹⁷
ETBN	Ethernet Train Backbone Node in accordance to [35]	Safety case of ETBN as generic product in accordance to EN50126, including: EN50129 (hardware) EN50657 (software)
Safe Train Inauguration	Safe train inauguration concept as defined in [35] with its parts on ETBN and CCU	Concept approval in accordance to EN50126
SDTv4	Protocol for safe data transmission for data up to SIL4	Concept approval in accordance to EN50159
NG-TCN	Complete network with all network and security functions	Compliance of NG-TCN to EN50159 closed transmission system ¹⁸ requirements. The compliance statement should be driven by an IEC62443 based security analysis.
CCU base system (hardware)	CCU hardware platform	Fulfillment of EN50129
CCU base system (middleware)	Middleware as defined in CTA WP4 (FDF)	Fulfillment of EN50657 clause 7.8 Fulfillment of EN50128 for signalling related applications.

Safety change management

To facilitate the certification process, it is useful to have clear separations of the different components, especially between HW and SW and also between different SW parts, and well-defined interfaces in between.

For each change on a component, independent whether the change affects a safety related function or a regular (non-safety related) function, it must be demonstrated with an impact analysis that this change has no or only a defined impact on other components and safety functions (see EN50657). If there is a potential impact on a safety related component (function), the impact analysis has to assess the criticality of the impact and has to define countermeasures for the case that the impact is not acceptable.

¹⁷ The more generic standard IEC61508 could also be the scope of assessment

¹⁸ More precisely, a category 1 or category 2 transmission system in accordance to EN50159.

Safety and (cyber) security

Although there is a separation between safety and security in the railway safety standardization, it cannot be ignored that there is some relationship in between. This relationship is for example expressed, without details, in EN50657 as it is cited underneath:

“This European Standard does not specify the requirements for the development, implementation, maintenance and/or operation of security policies or security services needed to meet security requirements that may be needed by the safety-related system. IT security can affect not only the operation but also the functional safety of a system. For IT security, appropriate IT security standards should be applied.”

Although the standard says “may” and “should”, it can be concluded that those requirements become mandatory for most future railway applications, and therefore must be also considered during the certification process¹⁹. Security can be seen as a precondition for safety, in the sense of “no safety without security”. This of course may have some consequences for the change management, as not only changes on TCMS, but also changes in other functional domains like OOS and COS require an impact analysis which investigates the potential impact on TCMS (safety) functions²⁰.

¹⁹ In fact, during the railway approval process conformance to functional requirements and conformance to safety must be demonstrated, and a functional degradation due to insufficient security may put the homologation at risk although safety might not be affected!

²⁰ For example, firewall rules need to be re-checked after a configuration change in OOS or COS functional domains.

REFERENCES

- [01] Shift2Rail Grant Agreement; Number 730539; 2016.
- [02] IEC61508-3 *Functional safety of electrical/electronic/programmable electronic safety-related system-Part 3: Software requirements.*
- [03] ISO 12100: Safety of machinery- General principles for design- Risk assessment and risk reduction.
- [04] EN50126-1:2017 Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 1: Generic RAMS Process.
- [05] EN15380-4:2014 Railway application – Classification system for railways vehicles- Part 4: Functions groups.
- [06] EN15380-5:2014 Railway application – Classification system for railways vehicles- Part 5: System Breakdown Structure (SBS).
- [07] Guideline for the application of harmonised design targets (CSM-DT) for technical systems as defined in (EU) Regulation 2015/1136 within the risk assessment process of Regulation 402/2013
- [08] Common Safety method for risk evaluation and assessment- Guidance on the application of Commission regulation (EU) 402/2013.
- [09] EN50126-2:2017 Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 2: Systems Approach to Safety.
- [10] IEC61882:2016-03 Hazard and operability studies (HAZOP studies)- Application guide.
- [11] IEC/ISO 31010_2009-11: Risk management –Risk assessment techniques.
- [12] IEC61508 Functional safety of electrical/electronic/programmable electronic safety-related system.
- [13] IEC61508-2 Functional safety of electrical/electronic/programmable electronic safety-related system-Part 2: Requirements for electrical/electronic/programmable electronic safety related system.
- [14] D1.3 – Function Based Architecture
- [15] D1.2 – TCMS Use Cases
- [16] Regulation 402/2013 on the CSM for risk assessment and repealing Regulation 352/2009
- [17] EN50126-1:2017 Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 1: Generic RAMS Process
- [18] EN50126-2:2017 Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 2: Systems Approach to Safety
- [19] EN50128:2011 Railway applications – Communications signalling and processing systems – Software for railway control and protection systems.
- [20] EN50129:2003 Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling.
- [21] IEEE Std 1012-2012: IEEE Standard for System and Software Verification and Validation
- [22] IEC62061:2005 Functional safety of safety-related electrical, electronic and programmable electronic control systems
- [23] IEC61511:2003 Functional safety – Safety instrumented systems for the process industry sector
- [24] Safety integrity level allocation shared or divergent practices in the railway domain, Kiswendsida Abel Ouedraogo, Julie Beugin, El-Miloudi El-Koursi
- [25] IEC61508-1:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems – Part1: General requirements
- [26] IEC61508-2:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems – Part2: requirements for electrical/electronic/programmable electronic safety-related systems

- [27] IEC61508-3:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems – Part4: Software requirements
- [28] IEC61508-4:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems – Part4: Definition and abbreviation
- [29] IEC61508-5:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems – Part5: Examples of methods for the determination of safety integrity levels
- [30] CONNECTA D3.1 – Requirement Specification; CTA-T3.1-D-ANS-023-08
- [31] CONNECTA D3.2 – Technology Evaluation Report; CTA-T3.2-D-BTD-003-07
- [32] CONNECTA D3.3 – Report on RAMS and Security Analysis; CTA-T3.3-D-CAF-006-14
- [33] CONNECTA D3.4 – Report on Safety Approval Concept; CTA-T3.4-D-SIE-003-08
- [34] Common Safety Method (CSM) on risk evaluation and assessment; Leaflet ERA
- [35] CONNECTA D3.5 – Report on Drive-by-Data Architecture; CTA-T3.5-D-BTD-002-09
- [36] EN50657:2017 Railways Applications – Rolling stock applications – Software on Board Rolling Stock
- [37] IEC61784-3-3 Industrial communication networks – Profiles- Part 3-3 Functional safety fieldbuses – Additional specifications for CPF3
- [38] IEC 61375-2-3 – Train Communication Network – Communication Profile; 2015
- [39] IEC 61375-2-5 – Train Communication Network – Ethernet Train Backbone; 2014
- [40] ISO 9001:2015
- [41] EN50121-1:2017 Railway applications – Electromagnetic compatibility
- [42] EN50124-1:2017 Railway applications – Insulation coordination
- [43] EN50125-1:2014 Railway applications – Environmental conditions for equipment – part 1
- [44] EN50155:2017 Railway applications – Rolling stock – Electronic equipment
- [45] EN50125-3:2014 Railway applications – Environmental conditions for equipment - part 3
- [46] EN15380-4 Railway applications — Classification system for railway vehicles — Part 4: Function groups
- [47] Commission Regulation (EU) No 1302/2014 of 18 November 2014 concerning a technical specification for interoperability relating to the 'rolling stock — locomotives and passenger rolling stock' subsystem of the rail system in the European Union
- [48] 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
- [49] Guide for the application of TSI LOC&PAS - ERA/GUI/07-2011/INT – Version 2.00 – 01 January 2015.
- [50] EN14752:2015 Railway applications — Body side entrance systems for rolling stock
- [51] CONNECTA D4.4 – Report on technology evaluation for application distribution
- [52] PROFIsafe System Description – Safety Technology and Application Version November 2010 Order Number 4.342
- [53] PROFIsafe – Profile for Safety Technology on PROFIBUS and PROFINET Profile part, related to
- [54] IEC61784-3-3 Technical Specification Version 2.6 MU1 – Date: April 2018 Order No.: 3.192
- [55] CONNECTA D3.4 – CTA-T3.4-T-SIE-024-01 ANNEX A OF CTA-T3.4-D-SIE-003-08
- [56] IEC61375-1: Edition 3.0 2012-06 Electronic railway equipment – Train communication network (TCN) –Part 1: General architecture
- [57] IEC61025 Second Edition 2006-12 Fault tree analysis (FTA)