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

D4.1 – Requirement specification for each sub task

Due date of deliverable: 31/03/2017

Actual submission date: 10/04/2017

Leader/Responsible of this Deliverable: Karsten Koechlin, Bombardier Transportation

Reviewed: Y

Document status		
Revision	Date	Description
1	15/12/2016	First issue
2	06/01/2017	Added and updated chapter 2.1.
3	26/01/2017	Added and updated requirements after first review
4	06/02/2017	Added and updated requirements
5	27/02/2017	Added and updated requirements
6	09/03/2017	Added and updated requirements
7	14/03/2017	Added and updated requirements (review meeting)
8	07/04/2017	Updated after TMT review
9	10/04/2017	Final

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

Start date: 01/09/2016 Duration: 24 months

REPORT CONTRIBUTORS

Name	Company	Details of Contribution
Pascal Vivegnis Viencent Mayeux	Alstom (ALS)	Provided requirements. Review of T4.2, T4.3, T4.4 requirements.
Karsten Koechlin Armin-Hagen Weiss	Bombardier Transportation (BTG)	Provided requirements. Review of T4.2, T4.3, T4.4 requirements.
Xabier Artaetxebarria	Construcciones y Auxiliar de Ferrocarriles S.A. (CAF)	Provided requirements. Review of T4.2, T4.3, T4.4 requirements.
Thomas Waschulzik	Siemens (SIE)	Provided requirements. Review of T4.2, T4.3, T4.4 requirements.
Philippe Laporte	SNCF-M	Provided requirements. Review of T4.2, T4.3, T4.4 requirements.

EXECUTIVE SUMMARY

CONNECTA aims at contributing to the S2R's next generation of TCMS architectures and components with wireless capabilities as well as to the next generation of electronic braking systems. CONNECTA will conduct research into new technological concepts, standard specifications and architectures for train control and monitoring, with specific applications in train-to-ground communications and high safety electronic control of brakes.

This deliverable contains the requirements for the tasks

- T4.2 Functional Open Coupling,
- T4.3 Application Profile and
- T4.4 Functional Distribution Framework.

The objective of *function standardisation and open coupling* is to make possible the coupling of two or more consists supplied by any manufacturer and which could have different train functions. It would also allow the control-command and monitoring of a train made of different consists supplied by any manufacturers. In order to achieve this, it is intended to elaborate application profiles for each sub-system of the train and specify, design and develop a prototype of open coupling.

The *application profile* will define the standardised interfaces for each sub system of the train.

The *functional distribution* architecture aims to abstract applications from executing devices and communication technologies, it targets a new architectural concept based on a standardised framework and distributed computing to allow the execution of whichever functions on high performing end devices distributed along the vehicle, with different safety and integrity requirements. Functions will be plugged in the framework and run isolated from each other with the aim of avoiding complete TCMS re-commissioning after any application change.

ABBREVIATIONS AND ACRONYMS

Table 1: Abbreviations and Acronyms

COTS	commercial off-the-shelf
FDF	Functional distribution framework
FS/FOC	function standardisation and functional open coupling
static (statically)	Computing (of a process or variable) not able to be changed during a set period, for example while a program is running.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

The *context and background* of this document is the project CONNECTA::work package WP4::task T4.1.

CONNECTA answers the S2R-IP1-CFM-02-2016 call under the Shift2Rail umbrella and belongs to the so called Technical Demonstrator 1.2 (TD1.2) – Next Generation TCMS and Technical Demonstrator 1.5 (TD1.5) – Brakes. This means that the project

- Shall contribute to the overall goals of Shift2Rail, namely by:
- Cutting the life-cycle costs of railway transport by as much as 50%;
- Doubling railway capacity; and
- Increasing reliability and punctuality by as much as 50%.
- Is part of a larger work programme described by the Multi-Annual Action Plan (MAAP) which will continue until 2022.

CONNECTA aims at contributing to the S2R's next generation of TCMS architectures and components with wireless capabilities as well as to the next generation of electronic braking systems. CONNECTA will conduct research into new technological concepts, standard specifications and architectures for train control and monitoring, with specific applications in train-to-ground communications and high safety electronic control of brakes.

The dissemination of the project's research activities and results are fundamental components of the CONNECTA project. The dissemination objectives of CONNECTA are:

- To ensure that the outputs of the project are delivered in a form which makes them immediately available for use by later phases (i.e. calls) and by on-going projects of Shift2Rail;
- To ensure that all important actors in the European railway sector are informed about CONNECTA;
- To facilitate acceptance of the project outcomes by the standardisation and regulatory bodies as well as by the main actors of the EU rail sector.
- To disseminate, engage and promote the project and its research activities to relevant audiences;

The *objectives of the deliverable* are:

- Requirements for Function Standardisation and Functional Open Coupling
- Requirements for Application Profile
- Requirements for Functional Distribution Framework

The objective of *function standardisation and open coupling* is to make possible the coupling of two or more consists supplied by any manufacturer and which could have different train functions. It would also allow the control-command and monitoring of a train made of different consists supplied by any manufacturers. In order to achieve this, it is intended to elaborate application profiles for each sub-system of the train and specify, design and develop a prototype of open coupling.

The *application profile* will define the standardised interfaces for each sub system of the train.

The *functional distribution* architecture aims to abstract applications from executing devices and communication technologies, it targets a new architectural concept based on a standardised framework and distributed computing to allow the execution of whichever functions on high performing end devices distributed along the vehicle, with different safety and integrity requirements. Functions will be plugged in the framework and run isolated from each other with the aim of avoiding complete TCMS re-commissioning after any application change.

The *inputs* for this document are:

- From work package 1 (WP1):
  - User stories and TCMS use cases (task T1.2 TCMS Use Cases)
  - High level requirements (task T1.5 Functional requirements (High Level Requirements))

2. OVERVIEW

This document specifies requirements for the following tasks:

- Task 4.2: Functional Standardisation and Functional Open Coupling (see chapter 3)

  Including general patterns, functions at train and consist level, properties of functions, function discovery and function interaction at train level
- Task 4.3: Application Profile (see chaper 0)
- Task 4.4: Functional Distribution Framework (see chapter 5)

Requirement Pattern

To simplify the reading and understanding of the requirements, the requirements are written whenever possible in the same style, that means the requirements are written in the same syntax (form and structure) by defined patterns.

The simplest pattern are:

The <system> <shall/should> <action>. Example: “The consist shall monitor the status of all external doors.”

Figure 1: Requirement Pattern for a simple action

The <system> <shall/should> provide <whom> with the ability to <action>. Example: “The train shall provide the driver with the ability to open the external doors on a train side.”

Figure 2: Requirement Pattern with “provide the ability”

Pattern with precondition and trigger:

GIVEN <precondition> WHEN <trigger>, THEN the <system> <shall/should> <action>. Example: GIVEN the train is standing still WHEN the driver requests to release the external doors on a selected train side, THEN the train shall release the external doors on the selected train side.

Figure 3: Requirement Pattern for action with precondition and trigger

- The keyword “GIVEN”, “WHEN” and “THEN” are written capitalized.
- Each keyword is written in a new line.
- If several preconditions have to be met, then each precondition (starting from the second) is written in a new line with the keyword “AND”.

3. TASK 4.2 FUNCTION STANDARDISATION AND FUNCTIONAL OPEN COUPLING

The subject in this chapter is the "*task 4.2 (function standardization and functional open coupling (FS/FOC))*".

The context is a train that is formed by two or more consists.

The scope is the consist interface, which provides the ability to couple consists and send commands to other consists and receive status from other consists.

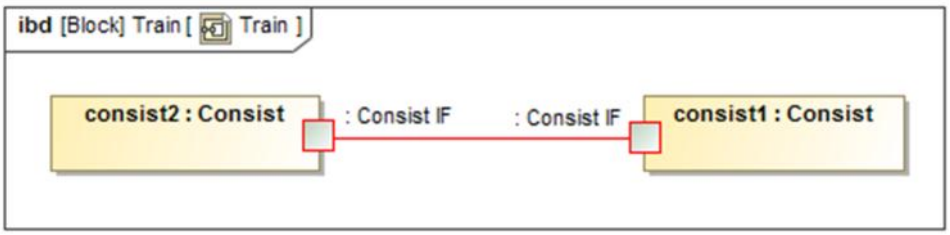


Figure 4: Scope of Task T4.2 Functional Standardisation and Functional Open Coupling

The border of Figure 4 represents a train. In this example the train is decomposed by two consists (consist1 and consist2). In the functional point of view, both consists are connected via a consist interface.

4. TASK 4.3 APPLICATION PROFILE

The subject in this chapter is the "*task 4.3 (application profile)*".

The context is a consist that contains several subsystems, e.g. TCMS, door systems, HVAC systems.

The scope is the interface between the TCMS and the other subsystems.

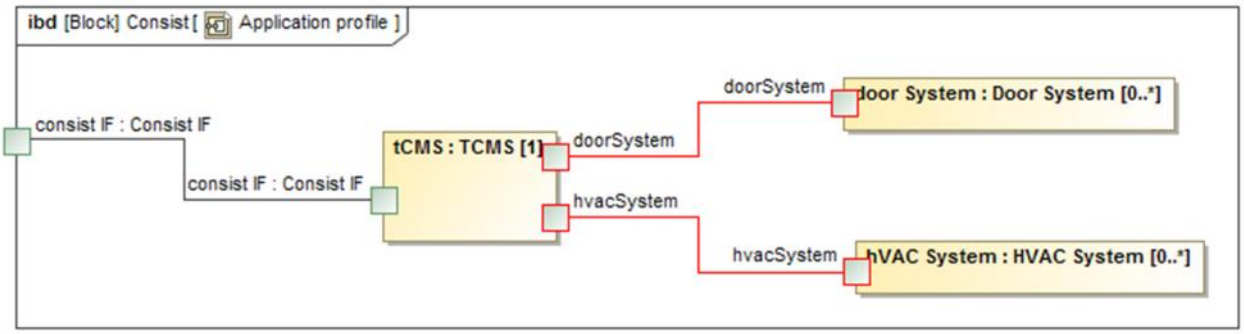


Figure 5: Scope of Task T4.3 Application Profile

5. TASK 4.4 FUNCTIONAL DISTRIBUTION FRAMEWORK

The subject in this chapter is the "*task 4.4 (functional distribution framework)*".

The context is the consist with its subsystems.

The scope is the distribution of behaviour (e.g. software parts).

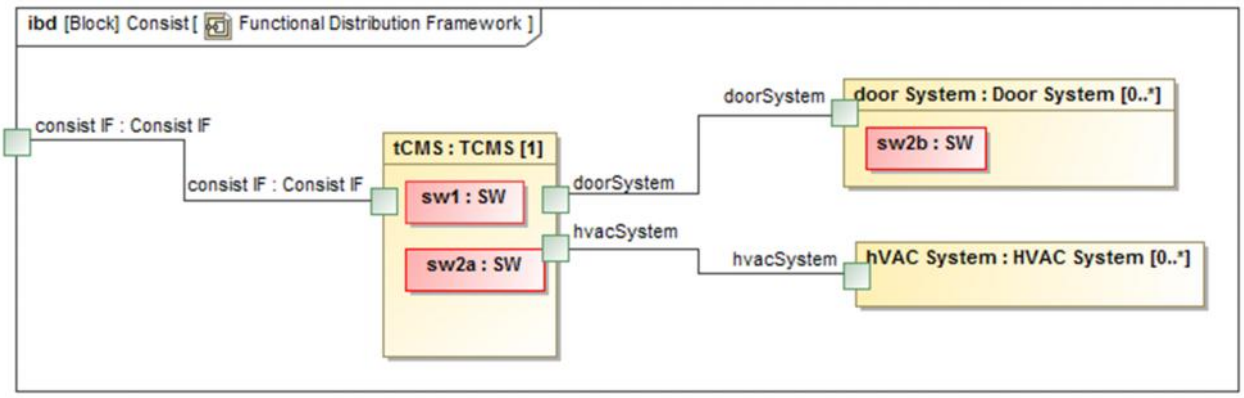


Figure 6: Scope of Task T4.4 Functional Distribution Framework

6. REQUIREMENTS

This chapter contains the requirements for task T4.2, task T4.3 and task T.4.4 in [Table 2].

Table 2: Requirements

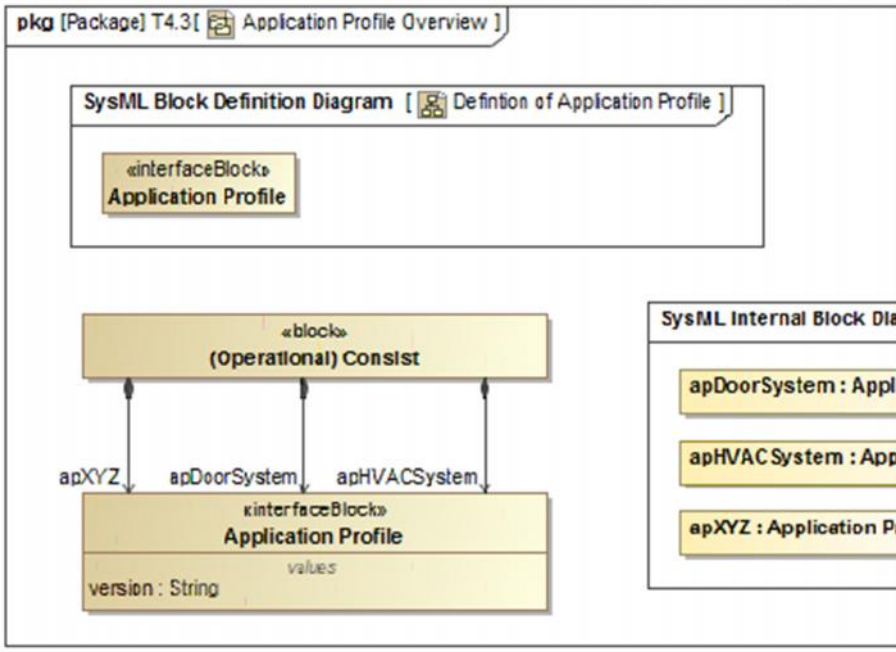
ID	ObjectType	Object Short Text	D4.1 Requirements	Status
CTA-D4.1-1	heading		1 CONNECTA	approved
CTA-D4.1-22	info		This module contains the requirements of task T4.1 of the CONNECTA work package WP4.	approved
CTA-D4.1-56	heading		1.1 Definitions	approved
CTA-D4.1-58	info	Train	Train shall be defined as operational formation consisting of one or more consists.	approved
CTA-D4.1-57	info	Consist	Consist shall be defined as single vehicle or a group of vehicles which are not separated during normal operation.	approved
CTA-D4.1-302	info	System of interest	System of interest shall be defined as the subject under development.	approved
CTA-D4.1-305	info	Monitoring	Monitoring shall be defined as function type which is responsible for the behaviour/process of observing and checking the progress or quality of something over a period of time.	approved
CTA-D4.1-306	info	Diagnostic	Diagnostic shall be defined as function type which is responsible for the detection of defect line-replaceable-units (LRU).	approved
CTA-D4.1-2	heading		2 Requirements for Task T4.2	approved
CTA-D4.1-15	info	Chapter introduction	This chapter contains the requirements for the task T4.2 "Function Standardisation and Functional Open Coupling" (FS/FOC).	approved
CTA-D4.1-43	heading		2.1 Scope	approved
CTA-D4.1-34	info	Interoperable interface	The objective of the task T4.2 is to provide an interface that allows the coupling and operation of (operational) consists - (operational) consists of different versions (same type) - (operational) consists of different types - (operational) consists of different suppliers.	approved

CTA-D4.1-24	requirement	Inter-(operational) consist interface	The task T4.2 (FS/FOC) shall provide a concept for a functional inter-(operational) consist interface.	approved
CTA-D4.1-46	requirement	Couple (operational) consists of different software versions	IF couplers are mechanically (including pneumatically) and electrically compatible, THEN the task T4.2 shall provide the operator with the ability to couple and operate (operational) consists of the same type but with different software versions without additional homologation overhead.	approved
CTA-D4.1-45	requirement	Couple (operational) consist of different (operational) consist types	IF couplers are mechanically (including pneumatically) and electrically compatible, THEN the task T4.2 shall provide the operator with the ability to couple and operate (operational) consists of different types without additional homologation overhead.	approved
CTA-D4.1-44	requirement	Couple (operational) consists of different manufacturers	IF couplers are mechanically (including pneumatically) and electrically compatible, THEN the task T4.2 shall provide the operator with the ability to couple and operate (operational) consists of different manufacturers without additional homologation overhead.	approved
CTA-D4.1-304	info		A (operational) consist can support a list of functions. Each function can fulfil a safety integrity level (SIL). If two (2) (operational) consists are coupled, then it is possible that these two (operational) consists provide the "same" function but the safety integrity level (SIL) of the function is different. In this case the FOC detects the same function and the different SIL and provides this information, so that the vehicle can indicate this for example to the driver. If such an incompatibility is detected, the train shall stay in a safe state unless explicitly released by an authorised instance, for example the driver.	approved
CTA-D4.1-303	requirement	Check safety integrity level of functions	IF two (2) (operational) consists are coupled, that provide a function which is from the point of behaviour equal but the safety integrity level is different, THEN the FOC shall detect these different implementations which have different SIL and provide an information which can be indicated for example to the driver.	approved
CTA-D4.1-272	requirement	Design life	The task T4.2 shall provide the operator with the ability to maintain the FS/FOC during the whole TCMS life time (at least 30 years).	approved

CTA-D4.1-271	requirement	Ability for future technology	The task T4.2 shall provide the operators with the ability to adapt the FS/FOC principles to future consists.	approved
CTA-D4.1-55	requirement	Discovery mechanism	The task T4.2 shall provide a discovery mechanism to detect the functional properties of the other consists.	approved
CTA-D4.1-307	requirement	Safety Integrity Level (SIL)	The FOC shall provide the ability to implement functions with a safety integrity level up to SIL 4.	approved
CTA-D4.1-48	heading		2.1.1 Scope of Example	approved
CTA-D4.1-25	requirement	Scope for example: external doors functions	The task T4.2 (FS/FOC) shall provide an example in the scope of external doors functions.	approved
CTA-D4.1-47	requirement	Scope for example: HVAC functions	The task T4.2 (FS/FOC) shall provide an example in the scope of HVAC functions.	approved
CTA-D4.1-18	heading		2.2 State of a function	approved
CTA-D4.1-5	requirement	General pattern for states of a function	The task T4.2 (FS/FOC) shall use a general pattern for states of a function.	approved
CTA-D4.1-10	requirement	State of a function: Not existing	While a function is statically not present (in the system of interest), the task T4.2 (FS/FOC) shall describe the state of the function as "not existing".	approved
CTA-D4.1-11	requirement	State of a function: Existing	While a function is statically present (in a system of interest), the task T4.2 (FS/FOC) shall describe the state of this function as "existing".	approved
CTA-D4.1-12	requirement	State of a function: Isolated	While a function is statically present (in a system of interest) AND due to a failure this function is not available, the task T4.2 (FS/FOC) shall describe the state of this function as "isolated".	approved
CTA-D4.1-13	requirement	State of a function: Available	While a function is statically present (in a system of interest) AND this function is not isolated, the task T4.2 (FS/FOC) shall describe the state of this function as "available".	approved
CTA-D4.1-9	requirement	State of a function: Disabled	While a function is statically present (in a system of interest) AND this function is not isolated AND there is no opportunity to activate a function (constraint due to operational conditions), the task T4.2 (FS/FOC) shall describe the state of this function as "disabled".	approved
CTA-D4.1-8	requirement	State of a function: Enabled	While a function is statically present (in a system of interest) AND this function is not isolated AND there is the opportunity to activate this function, the task T4.2 (FS/FOC) shall describe the state of this function as "enabled".	approved

CTA-D4.1-7	requirement	State of a function: Inactive	While a function is statically present (in a system of interest) AND this function is not isolated AND there is the opportunity to activate this function AND this function is not executed, the task T4.2 (FS/FOC) shall describe the state of this function as "inactive".	approved
CTA-D4.1-6	requirement	State of a function: Active	While a function is executed, the task T4.2 (FS/FOC) shall describe the state of this function as "active".	approved
CTA-D4.1-19	requirement		2.3 System Hierarchy Level	approved
CTA-D4.1-20	requirement	Predefined system hierarchy levels	The task T4.2 (FS/FOC) shall use the predefined system hierarchy level: - railway system - train - consist - vehicle - element (for example door, current collector).	approved
CTA-D4.1-21	info		Each function of the task T4.2 (FS/FOC) should be related to a defined system of interest. The system of interest can be either the "railway system", the "train" or the "consist", "vehicle", "element". That means the function "Open the external doors of the train" and the function "Open the external doors of the consist" are two different function, because the system of interest is not the same.	approved
CTA-D4.1-52	heading		2.4 Properties	approved
CTA-D4.1-308	requirement	TCN standard	The task T4.2 shall use the IEC61375-2-5 and IEC61375-2-3.	approved
CTA-D4.1-53	info	Maximum number of consists in a train composition	Maximum number of consists in a train composition shall be [63].	approved
CTA-D4.1-289			2.4.1 Additional requirements	approved
CTA-D4.1-290	info	Physical preconditions for FOC	The following physical interface criteria's are out of scope of the task T4.3 (FS/FOC): - coupler - brake pipe - battery voltage - low-voltage logic - network technology. That means if these preconditions are not fulfilled, then the FOC doesn't need to ensure compatibility between two consists.	approved

CTA-D4.1-291	requirement	Compatibility	IF two (2) (operational) consists are coupled, THEN the FOC shall check the compatibility between these two (2) consists, which means that a compare between the provided functions of both (operational) consists is executed (including mandatory and optional functions; function version, function SIL), and shall provide a result ("compatible"; "not compatible").	approved
CTA-D4.1-334	info	Conformance test	The risk of incompatibility of consists could be avoided, when a conformance test is mandatory for the usage of the FOC. This means a consist has to pass a conformance test for a specific version of FOC, that contains a list of mandatory functions.	draft
CTA-D4.1-292	requirement	Evolution	The FOC shall be backward compatible, that means a new version of the FOC can implement new functions that are not present in a previous version, but existing functions shall not be removed.	approved
CTA-D4.1-294	requirement	Monitoring: Provide status	The FOC shall provide a guided (operational) consist of the train with the ability to provide (send) status data (including failure messages and remedy texts necessary for operation) to the leading (operational) consists of the train.	approved
CTA-D4.1-293	requirement	Monitoring: Receive status	The FOC shall provide the leading (operational) consist of the train with the ability to receive status data (including failure messages and remedy texts necessary for operation) from other (guided) (operational) consists of this train.	approved
CTA-D4.1-295	requirement	Diagnostics: Provide	The FOC shall provide a guided (operational) consist of the train with the ability to provide (send) diagnostic information to the leading (operational) consist of the train.	approved
CTA-D4.1-296	requirement	Diagnostics: Receive	The FOC shall provide the leading (operational) consist of the train with the ability to receive diagnostic information from other (guided) (operational) consists of this train.	approved
CTA-D4.1-298	info	Sustainability	FOC shall be possible for the next 30 years, thus material definition, if any, shall be available and maintainable during this period (obsolescence management).	approved
CTA-D4.1-299	info	Availability	FOC shall be available during train operation. The loss of a (operational) consist in the train shall be detected and the train put in safe condition.	approved
CTA-D4.1-300	info	Performance	Coupling between 2 (operational) consists shall not lead to a local inauguration (consist internal).	approved
CTA-D4.1-301	requirement	Inauguration performance	The FOC shall provide the ability to inaugurate two (2) (operational) consists as a train in less than or equal to 1 minute.	approved
CTA-D4.1-3	heading		3 Requirements for Task T4.3	approved

CTA-D4.1-16	info	Chapter introduction	This chapter contains the requirements for the task T4.3 "Application Profile".	approved
CTA-D4.1-23	requirement		The task T4.3 (application profile) shall develop the mechanism for application profiles, which are a definition of interface between the subsystem TCMS and another subsystem.	approved
CTA-D4.1-51	info			
CTA-D4.1-35	heading		3.1 Scope	approved
CTA-D4.1-36	requirement	Generic (type)	The task T4.3 shall describe an application profile (generic interface) to a subsystem.	approved
CTA-D4.1-37	requirement	Instances	The task T4.3 shall ensure that an application profile can be instantiated several times.	approved
CTA-D4.1-39	requirement	Version	The task T4.3 shall provide a mechanism for version management of application profiles.	approved
CTA-D4.1-38	requirement	Backward compatibility	The task T4.3 shall provide a concept for backward compatible version of application profiles.	approved

CTA-D4.1-287	requirement	Generic (type)	The application profile definition shall be so detailed, that a formal validation of an implementation against the profile is possible.	approved
CTA-D4.1-284			3.1.1 Command/Request	approved
CTA-D4.1-41	requirement	Command/Request data(subsystem to TCMS)	The application profile definition shall provide the ability to transfer request data from the TCMS to a subsystem.	approved
CTA-D4.1-282	requirement	Command/Request data (TCMS to subsystem)	The application profile definition shall provide the ability to transfer request data from a subsystem to the TCMS.	approved
CTA-D4.1-285			3.1.2 Monitoring	approved
CTA-D4.1-42	requirement	Monitoring data (subsystem to TCMS)	The application profile definition shall provide the ability to transfer monitoring data from a subsystem to the TCMS.	approved
CTA-D4.1-283	requirement	Monitoring data (TCMS to subsystem)	The application profile definition shall provide the ability to transfer monitoring data from the TCMS to a subsystem.	approved
CTA-D4.1-286			3.1.3 Diagnostics	approved
CTA-D4.1-40	requirement	Diagnostics (subsystem to TCMS)	The application profile definition shall provide the ability to transfer diagnostics data from a subsystem to the TCMS - including information for corrective maintenance.	approved
CTA-D4.1-28	heading		3.2 Scope of Example	approved
CTA-D4.1-27	requirement	Example application profile: TCMS - HVAC system	The task T4.3 shall define (as an example) the application profile between TCMS and HVAC system.	approved
CTA-D4.1-26	requirement	Example application profile: TCMS - door system	The task T4.3 shall define (as an example) the application profile between TCMS and door system.	approved
CTA-D4.1-50	requirement	Command/Request example scope "provide external access"	The task T4.3 shall define for the example scope "provide external access" the request data, which can be transferred from the TCMS to the subsystem.	approved
CTA-D4.1-49	requirement	Monitoring for example scope "provide external access"	The task T4.3 shall define for the example scope "provide external access" the monitoring data, which can be transferred from the subsystem to the TCMS.	approved
CTA-D4.1-4	heading		4 Requirements for Task T4.4	approved
CTA-D4.1-17	info	Chapter introduction	This chapter contains the requirements for the task T4.4 "Functional Distribution Framework" (shortname "FD framework" abbreviation "FDF").	approved
CTA-D4.1-29	requirement	Security aspects	The task T4.4 shall present aspects regarding security of the functional distribution framework.	approved

CTA-D4.1-30	requirement	Basic architecture	The task T4.4 shall define a basic architecture of the functional distribution framework, which provides the ability to distribute in a flexible way software architecture components over different hardware architecture components.	approved
CTA-D4.1-31	requirement	Interface between architecture elements	The task T4.4 shall define interfaces between architecture elements of the functional distribution framework.	approved
CTA-D4.1-32	requirement	Discovery mechanism	The task T4.4 shall define discovery mechanisms for the functional distribution framework, if they are needed.	approved
CTA-D4.1-156	requirement	Feasibility of main train functions	The task T4.4 shall analyze the feasibility of implementing the main train functions on top of the functional distribution framework.	approved
CTA-D4.1-157	requirement	Methodology for TCMS Certification	The task T4.4 shall present a methodology for TCMS certification, based on the functional distribution framework and considering safety aspects.	approved
CTA-D4.1-158	requirement	Consideration of Safe4Rail WP2 Output	The task T4.4 shall consider the outputs of state of the art study done by Safe4Rail Work Package 2.	approved
CTA-D4.1-159	requirement	Impact Analysis	The task T4.4 shall perform an impact analysis on a number of functions, by doing a detailed analysis of how to implement these functions on top of the functional distribution framework.	approved
CTA-D4.1-33	requirement	Design lifetime	The FD framework shall have a lifetime of at least 30 years.	approved
CTA-D4.1-309	requirement	TCN standard	The task T4.4 shall use the standard IEC 61375-2-5 and IEC61375-2-3.	approved
CTA-D4.1-54	info	Maximum number of consists in a train composition	The maximum number of consists in a train composition of the FD framework shall be [63].	approved
CTA-D4.1-93	heading		4.1 Functional Requirements	approved
CTA-D4.1-328	requirement	Safety Integrity Level	The FD framework shall offer the solution to reach SIL4 to be open for smart solutions. Thus all services of the FD framework shall support SIL4.	draft
CTA-D4.1-94	heading		4.1.1 Partition and process execution	approved
CTA-D4.1-166	info	Partition	Partition shall be defined as an execution environment with an isolated memory address space and limited execution time, which is composed of one or several processes.	approved
CTA-D4.1-95	requirement	Seperation of partitions	The FD framework shall execute one or more partitions concurrently, with complete temporal and spatial separation among them.	approved

CTA-D4.1-96	requirement	Partition execution period	The FD framework shall execute each partition with the corresponding period, which shall be defined in the configuration.	approved
CTA-D4.1-311	requirement		The FD framework shall execute each partition within a corresponding time interval, which shall be defined in the configuration.	draft
CTA-D4.1-97	requirement	Process	Partitions shall contain one or more processes with spatial separation among them.	approved
CTA-D4.1-98	requirement	State of partitions	Partitions shall be active or inactive.	approved
CTA-D4.1-99	requirement		The FD framework shall execute only active partitions.	approved
CTA-D4.1-100	requirement		The FD framework shall provide partitions with the ability to deactivate themselves.	approved
CTA-D4.1-101	requirement		The FD framework shall be able to execute processes in two different modes: • sequential (one after the other) AND • concurrent.	approved
CTA-D4.1-160	requirement		The FD framework shall be able to execute partitions redundant in different processing units for availability.	approved
CTA-D4.1-312	requirement		The FD framework shall be able to execute partitions redundant in different processing units to increase availability or to reach SIL3..4 with process segregation e.g. 2oo2 or 2oo3.	draft
CTA-D4.1-275	requirement	Real-time	The FD framework shall provide hard real-time support.	approved
CTA-D4.1-276	requirement		The FD framework shall provide hardware (HW) and operating system (OS) abstraction layer for application FD framework components.	approved
CTA-D4.1-277	requirement		The FD framework shall provide OS-service protection to ensure the independence of services and to support the independence of partitions.	approved
CTA-D4.1-278	requirement	Service discovery and announcement	The FD framework should provide mechanism for service discovery and announcement.	approved
CTA-D4.1-280	requirement	Fault isolation	The FD framework shall provide fault isolation between different partitions to support the independency of partitions.	approved
CTA-D4.1-279	requirement	Memory protection	The FD framework shall provide memory protection between different partitions to support the independency of partitions with different SIL.	approved
CTA-D4.1-102	heading		4.1.2 I/O services	approved
CTA-D4.1-103	requirement		The FD framework shall provide a partition with the ability to access consist network data inputs.	approved
CTA-D4.1-313	requirement		The FD framework shall provide a partition with the ability to access local analog inputs.	draft

CTA-D4.1-329	requirement		The FD framework shall provide a partition with the ability to access local digital inputs.	draft
CTA-D4.1-104	requirement		The FD framework shall provide a partition with the ability to control consist network data outputs.	approved
CTA-D4.1-314	requirement		The FD framework shall provide a partition with the ability to control local analog ouputs.	draft
CTA-D4.1-330	requirement		The FD framework shall provide a partition with the ability to control local digital outputs.	draft
CTA-D4.1-105	requirement	ECN	The FD framework shall support the consist network "Ethernet Consist Network (ECN)" (according to IEC 61375-3-4).	approved
CTA-D4.1-273	requirement	ETB	The FD framework shall support the network "Ethernet Train Backbone (ETB)".	approved
CTA-D4.1-106	requirement		The FD framework shall update the inputs of each partition only before each partition execution.	approved
CTA-D4.1-108	requirement		The FD framework shall write the outputs of each partition only after its complete execution.	approved
CTA-D4.1-162	requirement		The FD framework shall provide the partitions with access to files stored in persistent memory.	approved
CTA-D4.1-163	requirement		The FD framework shall provide the ability to configure the access to files stored in persistent memory either read-only or read-write.	approved
CTA-D4.1-110	heading		4.1.3 Time services	approved
CTA-D4.1-111	requirement		The FD framework shall provide the ability to participate on external time synchronization.	approved
CTA-D4.1-274	requirement		The FD framework shall provide time synchronization via all supported consists networks and based on a standard time synchronization protocol.	approved
CTA-D4.1-112	requirement		The FD framework shall provide the ability to suspend execution of a partition or a process for a certain time.	approved
CTA-D4.1-113	requirement		The FD framework shall provide partitions with the ability to obtain the current time value.	approved
CTA-D4.1-114	heading		4.1.4 Communication services	approved
CTA-D4.1-115	requirement		The FD framework shall provide an interface for inter-process communication.	approved
CTA-D4.1-116	requirement		The FD framework shall provide an interface for inter-partition communication.	approved
CTA-D4.1-117	heading		4.1.5 Replicate local variables on consist network	approved
CTA-D4.1-118	requirement		The FD framework shall be configurable to replicate the value of local input variables on the consist network.	approved
CTA-D4.1-120	heading		4.1.6 Control local variables based on consist network variables	approved

CTA-D4.1-121	requirement		The FD framework shall be configurable to modify the value of local output variables based on data received from the consist network.	approved
CTA-D4.1-123	heading		4.1.7 Configuration	approved
CTA-D4.1-124	heading		4.1.7.1 Configuration identifier	approved
CTA-D4.1-125	requirement		The FD framework shall be able to acquire a configuration identifier dynamically.	approved
CTA-D4.1-126	requirement		The configuration identifier shall be selected by one or more local digital inputs, which shall be configured statically.	approved
CTA-D4.1-127	heading		4.1.7.2 Functional configuration	approved
CTA-D4.1-128	requirement		The FD framework shall be configured statically with configuration files or dynamically through the consist network.	approved
CTA-D4.1-129	requirement		The FD framework shall provide the ability to configure the followings aspects: - access to I/Os - consist network configuration - default values for input variables - default values for local and remote output variables - partition execution periods and times - process execution mode (sequential or concurrent, order).	approved
CTA-D4.1-130	heading		4.1.7.3 Consist network variables configuration	approved
CTA-D4.1-164	requirement		The consist network configuration shall be either redundant in all processing units, in which case the FD framework shall assure the consistency of the configurations, or centralized in a single or a few processing units.	approved
CTA-D4.1-132	heading		4.1.8 Internal state monitoring and diagnosis	approved
CTA-D4.1-133	requirement		The FD framework shall provide an Ethernet interface to allow the monitoring of the state of internal variables from the exterior.	approved
CTA-D4.1-134	requirement		The FD framework shall register in a log file internal execution errors.	approved
CTA-D4.1-135	requirement		The FD framework shall provide partitions services with the ability to perform HW integrity checks, in order detect potentially dangerous random failures.	approved
CTA-D4.1-281	requirement		The FD framework shall support monitoring of partitions and processes (e.g. by watchdog or system monitor).	approved
CTA-D4.1-315			The system monitor shall monitor e.g. execution time and period, memory usage, processor load, priorities, overrun, identifiers for all partitions and processes.	draft

CTA-D4.1-140	heading		4.1.9 Partition debugging	approved
CTA-D4.1-141	requirement		The FD framework shall implement a method to externally overwrite values of its local inputs and outputs, to facilitate partition debugging and simulations.	approved
CTA-D4.1-318			The FD framework should implement a method to externally overwrite values of internal variables to facilitate partition debugging and simulations.	draft
CTA-D4.1-142	requirement		The FD framework shall be executable in PC platform, to facilitate simulation and testing.	approved
CTA-D4.1-147	heading		4.1.10 Safety layer for consist network communications	approved
CTA-D4.1-148	requirement		The FD framework shall provide a safety layer on the consist network, if configured to do so. The safety layer is defined in norm IEC61375-2-3.	approved
CTA-D4.1-149	heading		4.2 Non-Functional Requirements	approved
CTA-D4.1-150	heading		4.2.1 Safety requirements	approved
CTA-D4.1-151	requirement		The FD framework shall support the implementation of functions with a safety integrity level 4 according to IEC 61508 standard.	approved
CTA-D4.1-152	heading		4.2.2 Security requirements	approved
CTA-D4.1-60	requirement		The task T4.4 shall perform for the functional distribution framework architecture a security risk assessment to identify: · Relevant threats · Vulnerabilities · Adverse impact to assets that may occur · Probability that harm will occur. * SL for each of the seven following safety foundational requirements to select for each system requirement the right requirement enhancements for each acc. to IEC62443-3-3	approved
CTA-D4.1-256	heading	FR 1 – Identification and authentication control	4.2.2.1 Identification and authentication control	approved

CTA-D4.1-263	info	Purpose and SL-C(IAC) descriptions	Identify and authenticate all users (humans, software processes and devices) before allowing them to access to the control system. • SL 1 – Identify and authenticate all users (humans, software processes and devices) by mechanisms which protect against casual or coincidental access by unauthenticated entities. • SL 2 – Identify and authenticate all users (humans, software processes and devices) by mechanisms which protect against intentional unauthenticated access by entities using simple means with low resources, generic skills and low motivation. • SL 3 – Identify and authenticate all users (humans, software processes and devices) by mechanisms which protect against intentional unauthenticated access by entities using sophisticated means with moderate resources, IACS specific skills and moderate motivation. • SL 4 – Identify and authenticate all users (humans, software processes and devices) by mechanisms which protect against intentional unauthenticated access by entities using sophisticated means with extended resources, IACS specific skills and high motivation.	approved
CTA-D4.1-169	requirement	SR 1.1 – Human user identification and authentication	The control system shall provide the capability to identify and authenticate all human users. This capability shall enforce such identification and authentication on all interfaces which provide human user access to the control system to support segregation of duties and least privilege in accordance with applicable security policies and procedures.	approved
CTA-D4.1-174	requirement	SR 1.2 – Software process and device identification and authentication	The control system shall provide the capability to identify and authenticate all software processes and devices. This capability shall enforce such identification and authentication on all interfaces which provide access to the control system to support least privilege in accordance with applicable security policies and procedures.	approved
CTA-D4.1-177	requirement	SR 1.3 – Account management	The control system shall provide the capability to support the management of all accounts by authorized users, including adding, activating, modifying, disabling and removing accounts.	approved
CTA-D4.1-181	requirement	SR 1.4 – Identifier management	The control system shall provide the capability to support the management of identifiers by user, group, role or control system interface.	approved

CTA-D4.1-183	requirement	SR 1.5 – Authenticator management	The control system shall provide the capability to: h) initialize authenticator content; i) change all default authenticators upon control system installation; j) change/refresh all authenticators; and k) protect all authenticators from unauthorized disclosure and modification when stored and transmitted.	approved
CTA-D4.1-186	requirement	SR 1.6 Wireless access management	The control system shall provide the capability to identify and authenticate all users (humans, software processes or devices) engaged in wireless communication.	approved
CTA-D4.1-189	requirement	SR 1.7 Strength of password-based authentication	For control systems utilizing password-based authentication, the control system shall provide the capability to enforce configurable password strength based on minimum length and variety of character types.	approved
CTA-D4.1-193	requirement	SR 1.8 – Public key infrastructure (PKI) certificates	Where PKI is utilized, the control system shall provide the capability to operate a PKI according to commonly accepted best practices or obtain public key certificates from an existing PKI.	approved
CTA-D4.1-195	requirement	SR 1.9 – Strength of public key authentication	For control systems utilizing public key authentication, the control system shall provide the capability to: a) validate certificates by checking the validity of the signature of a given certificate; b) validate certificates by constructing a certification path to an accepted CA or in the case of self-signed certificates by deploying leaf certificates to all hosts which communicate with the subject to which the certificate is issued; c) validate certificates by checking a given certificate's revocation status; d) establish user (human, software process or device) control of the corresponding private key; and e) map the authenticated identity to a user (human, software process or device).	approved
CTA-D4.1-198	requirement	SR 1.10 – Authenticator feedback	The control system shall provide the capability to obscure feedback of authentication information during the authentication process.	approved
CTA-D4.1-201	requirement	SR 1.11 Unsuccessful login attempts	The control system shall provide the capability to enforce a limit of a configurable number of consecutive invalid access attempts by any user (human, software process or device) during a configurable time period. The control system shall provide the capability to deny access for a specified period of time or until unlocked by an administrator when this limit has been exceeded.	approved

CTA-D4.1-205	requirement	SR 1.12 – System use notification	The control system shall provide the capability to display a system use notification message before authenticating. The system use notification message shall be configurable by authorized personnel.	approved
CTA-D4.1-207	requirement	SR 1.13 – Access via untrusted networks	The control system shall provide the capability to monitor and control all methods of access to the control system via untrusted networks.	approved
CTA-D4.1-260	heading	FR2 - Use control	4.2.2.2 Use control	approved
CTA-D4.1-264	info	Purpose and SL-C(UC) descriptions	Enforce the assigned privileges of an authenticated user (human, software process or device) to perform the requested action on the IACS and monitor the use of these privileges. • SL 1 – Restrict use of the IACS according to specified privileges to protect against casual or coincidental misuse. • SL 2 – Restrict use of the IACS according to specified privileges to protect against circumvention by entities using simple means with low resources, generic skills and low motivation. • SL 3 – Restrict use of the IACS according to specified privileges to protect against circumvention by entities using sophisticated means with moderate resources, IACS specific skills and moderate motivation. • SL 4 – Restrict use of the IACS according to specified privileges to protect against circumvention by entities using sophisticated means with extended resources, IACS specific skills and high motivation.	approved
CTA-D4.1-210	requirement	SR 2.1 – Authorization enforcement	On all interfaces, the control system shall provide the capability to enforce authorizations assigned to all human users for controlling use of the control system to support segregation of duties and least privilege	approved
CTA-D4.1-217	requirement	SR 2.2 – Wireless use control	The control system shall provide the capability to authorize, monitor and enforce usage restrictions for wireless connectivity to the control system according to commonly accepted security industry practices.	approved
CTA-D4.1-223	requirement	SR 2.3 – Use control for portable and mobile devices	The control system shall provide the capability to automatically enforce configurable usage restrictions that include: a) preventing the use of portable and mobile devices; b) requiring context specific authorization; and c) restricting code and data transfer to/from portable and mobile devices.	approved

CTA-D4.1-222	requirement	SR 2.4 – Mobile code	The control system shall provide the capability to enforce usage restrictions for mobile code technologies based on the potential to cause damage to the control system that include: a) preventing the execution of mobile code; b) requiring proper authentication and authorization for origin of the code; c) restricting mobile code transfer to/from the control system; and d) monitoring the use of mobile code.	approved
CTA-D4.1-221	requirement	SR 2.5 – Session lock	The control system shall provide the capability to prevent further access by initiating a session lock after a configurable time period of inactivity or by manual initiation. The session lock shall remain in effect until the human user who owns the session or another authorized human user re-establishes access using appropriate identification and authentication procedures.	approved
CTA-D4.1-220	requirement	SR 2.6 – Remote session termination	The control system shall provide the capability to terminate a remote session either automatically after a configurable time period of inactivity or manually by the user who initiated the session.	approved
CTA-D4.1-219	requirement	SR 2.7 – Concurrent session control	The control system shall provide the capability to limit the number of concurrent sessions per interface for any given user (human, software process or device) to a configurable number of sessions.	approved
CTA-D4.1-218	requirement	SR 2.8 – Auditable events	The control system shall provide the capability to generate audit records relevant to security for the following categories: access control, request errors, operating system events, control system events, backup and restore events, configuration changes, potential reconnaissance activity and audit log events. Individual audit records shall include the timestamp, source (originating device, software process or human user account), category, type, event ID and event result.	approved
CTA-D4.1-224	requirement	SR 2.9 – Audit storage capacity	The control system shall allocate sufficient audit record storage capacity according to commonly recognized recommendations for log management and system configuration. The control system shall provide auditing mechanisms to reduce the likelihood of such capacity being exceeded.	approved

CTA-D4.1-229	requirement	SR 2.10 – Response to audit processing failures	The control system shall provide the capability to alert personnel and prevent the loss of essential services and functions in the event of an audit processing failure. The control system shall provide the capability to support appropriate actions in response to an audit processing failure according to commonly accepted industry practices and recommendations.	approved
CTA-D4.1-228	requirement	SR 2.11 – Timestamps	The control system shall provide timestamps for use in audit record generation.	approved
CTA-D4.1-227	requirement	SR 2.12 – Non-repudiation	The control system shall provide the capability to determine whether a given human user took a particular action.	approved
CTA-D4.1-262	heading	FR 3 – System integrity	4.2.2.3 System integrity	approved
CTA-D4.1-265	info	Purpose and SL-C(SI) descriptions	Ensure the integrity of the IACS to prevent unauthorized manipulation. • SL 1 – Protect the integrity of the IACS against casual or coincidental manipulation. • SL 2 – Protect the integrity of the IACS against manipulation by someone using simple means with low resources, generic skills and low motivation. • SL 3 – Protect the integrity of the IACS against manipulation by someone using sophisticated means with moderate resources, IACS specific skills and moderate motivation. • SL 4 – Protect the integrity of the IACS against manipulation by someone using sophisticated means with extended resources, IACS specific skills and high motivation.	approved
CTA-D4.1-226	requirement	SR 3.1 – Communication integrity	The control system shall provide the capability to protect the integrity of transmitted information.	approved
CTA-D4.1-225	requirement	SR 3.2 – Malicious code protection	The control system shall provide the capability to employ protection mechanisms to prevent, detect, report and mitigate the effects of malicious code or unauthorized software. The control system shall provide the capability to update the protection mechanisms.	approved
CTA-D4.1-233	requirement	SR 3.3 – Security functionality verification	The control system shall provide the capability to support verification of the intended operation of security functions and report when anomalies are discovered during FAT, SAT and scheduled maintenance. These security functions shall include all those necessary to support the security requirements specified in this standard.	approved

CTA-D4.1-232	requirement	SR 3.4 – Software and information integrity	The control system shall provide the capability to detect, record, report and protect against unauthorized changes to software and information at rest.	approved
CTA-D4.1-231	requirement	SR 3.5 – Input validation	The control system shall validate the syntax and content of any input which is used as an industrial process control input or input that directly impacts the action of the control system.	approved
CTA-D4.1-230	requirement	SR 3.6 – Deterministic output	The control system shall provide the capability to set outputs to a predetermined state if normal operation cannot be maintained as a result of an attack.	approved
CTA-D4.1-234	requirement	SR 3.7 – Error handling	The control system shall identify and handle error conditions in a manner such that effective remediation can occur. This shall be done in a manner which does not provide information that could be exploited by adversaries to attack the IACS unless revealing this information is necessary for the timely troubleshooting of problems.	approved
CTA-D4.1-239	requirement	SR 3.8 – Session integrity	The control system shall provide the capability to protect the integrity of sessions. The control system shall reject any usage of invalid session IDs.	approved
CTA-D4.1-238	requirement	SR 3.9 – Protection of audit information	The control system shall protect audit information and audit tools (if present) from unauthorized access, modification and deletion.	approved
CTA-D4.1-261	heading	FR 4 – Data confidentiality	4.2.2.4 Data confidentiality	approved
CTA-D4.1-266	info	Purpose and SL-C(DC) descriptions	Ensure the confidentiality of information on communication channels and in data repositories to prevent unauthorized disclosure. • SL 1 – Prevent the unauthorized disclosure of information via eavesdropping or casual exposure. • SL 2 – Prevent the unauthorized disclosure of information to an entity actively searching for it using simple means with low resources, generic skills and low motivation. • SL 3 – Prevent the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with moderate resources, IACS specific skills and moderate motivation. • SL 4 – Prevent the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with extended resources, IACS specific skills and high motivation.	approved
CTA-D4.1-237	requirement	SR 4.1 – Information confidentiality	The control system shall provide the capability to protect the confidentiality of information for which explicit read authorization is supported,	approved

			whether at rest or in transit.	
CTA-D4.1-236	requirement	SR 4.2 – Information persistence	The control system shall provide the capability to purge all information for which explicit read authorization is supported from components to be released from active service and/or decommissioned.	approved
CTA-D4.1-235	requirement	SR 4.3 – Use of cryptography	If cryptography is required, the control system shall use cryptographic algorithms, key sizes and mechanisms for key establishment and management according to commonly accepted security industry practices and recommendations.	approved
CTA-D4.1-259	heading	FR 5 – Restricted data flow	4.2.2.5 Restricted data flow	approved
CTA-D4.1-267	info	Purpose and SL-C(RDF) descriptions	Segment the control system via zones and conduits to limit the unnecessary flow of data. • SL 1 – Prevent the casual or coincidental circumvention of zone and conduit segmentation. • SL 2 – Prevent the intended circumvention of zone and conduit segmentation by entities using simple means with low resources, generic skills and low motivation. • SL 3 – Prevent the intended circumvention of zone and conduit segmentation by entities using sophisticated means with moderate resources, IACS specific skills and moderate motivation. • SL 4 – Prevent the intended circumvention of zone and conduit segmentation by entities using sophisticated means with extended resources, IACS specific skills and high motivation.	approved
CTA-D4.1-240	requirement	SR 5.1 – Network segmentation	The control system shall provide the capability to logically segment control system networks from non-control system networks and to logically segment critical control system networks from other control system networks.	approved
CTA-D4.1-244	requirement	SR 5.2 – Zone boundary protection	The control system shall provide the capability to monitor and control communications at zone boundaries to enforce the compartmentalization defined in the risk-based zones and conduits model.	approved
CTA-D4.1-242	requirement	SR 5.3 – General purpose person-to-person communication restrictions	The control system shall provide the capability to prevent general purpose person-to-person messages from being received from users or systems external to the control system.	approved
CTA-D4.1-243	requirement	SR 5.4 – Application partitioning	The control system shall provide the capability to support partitioning of data, applications and services based on criticality to facilitate implementing	approved

			a zoning model.	
CTA-D4.1-258	heading	FR 6 – Timely response to events	4.2.2.6 Timely response to events	approved
CTA-D4.1-268	info	Purpose and SL-C(TRE) descriptions	Respond to security violations by notifying the proper authority, reporting needed evidence of the violation and taking timely corrective action when incidents are discovered. • SL 1 – Monitor the operation of the IACS and respond to incidents when they are discovered by collecting and providing the forensic evidence when queried. • SL 2 – Monitor the operation of the IACS and respond to incidents when they are discovered by actively collecting and periodically reporting forensic evidence. • SL 3 – Monitor the operation of the IACS and respond to incidents when they are discovered by actively collecting and pushing forensic evidence to the proper authority. • SL 4 – Monitor the operation of the IACS and respond to incidents when they are discovered by actively collecting and pushing forensic evidence to the proper authority in near real-time.	approved
CTA-D4.1-241	requirement	SR 6.1 – Audit log accessibility	The control system shall provide the capability for authorized humans and/or tools to access audit logs on a read-only basis.	approved
CTA-D4.1-245	requirement	SR 6.2 – Continuous monitoring	The control system shall provide the capability to continuously monitor all security mechanism performance using commonly accepted security industry practices and recommendations to detect, characterize and report security breaches in a timely manner.	approved
CTA-D4.1-257	heading	FR 7 – Resource availability	4.2.2.7 Resource availability	approved

CTA-D4.1-269	info	Purpose and SL-C(RA) descriptions	Ensure the availability of the control system against the degradation or denial of essential services. • SL 1 – Ensure that the control system operates reliably under normal production conditions and prevents DoS situations caused by the casual or coincidental actions of an entity. • SL 2 – Ensure that the control system operates reliably under normal and abnormal production conditions and prevents DoS situations by entities using simple means with low resources, generic skills and low motivation. • SL 3 – Ensure that the control system operates reliably under normal, abnormal, and extreme production conditions and prevents DoS situations by entities using sophisticated means with moderate resources, IACS specific skills and moderate motivation. • SL 4 – Ensure that the control system operates reliably under normal, abnormal, and extreme production conditions and prevents DoS situations by entities using sophisticated means with extended resources, IACS specific skills and high motivation.	approved
CTA-D4.1-247	requirement	SR 7.1 – Denial of service protection	The control system shall provide the capability to operate in a degraded mode during a DoS event.	approved
CTA-D4.1-248	requirement	SR 7.2 – Resource management	The control system shall provide the capability to limit the use of resources by security functions to prevent resource exhaustion.	approved
CTA-D4.1-246	requirement	SR 7.3 – Control system backup	The identity and location of critical files and the ability to conduct backups of user-level and system-level information (including system state information) shall be supported by the control system without affecting normal train operations.	approved
CTA-D4.1-249	requirement	SR 7.4 – Control system recovery and reconstitution	The control system shall provide the capability to recover and reconstitute to a known secure state after a disruption or failure.	approved
CTA-D4.1-253	requirement	SR 7.5 – Emergency power	The control system shall provide the capability to switch to and from an emergency power supply without affecting the existing security state or a documented degraded mode.	approved
CTA-D4.1-252	requirement	SR 7.6 – Network and security configuration settings	The control system shall provide the capability to be configured according to recommended network and security configurations as described in guidelines provided by the control system supplier. The control system shall provide an interface to the currently deployed network and security configuration settings.	approved

CTA-D4.1-251	requirement	SR 7.7 – Least functionality	The control system shall provide the capability to specifically prohibit and/or restrict the use of unnecessary functions, ports, protocols and/or services.	approved
CTA-D4.1-250	requirement	SR 7.8 – Control system component inventory	The control system shall provide the capability to report the current list of installed components and their associated properties.	approved
CTA-D4.1-153	heading		4.2.3 Performance requirements	approved
CTA-D4.1-165	requirement		The FD framework architecture and its implementation shall support the following parameters: - number of supported local inputs - number of supported local outputs - time required for an input variable to be available to partitions - time required for an output variable from the time point it is set by a partition until it reaches the output - number of variables that can be read with a certain frequency - number of variables that can be written with a certain frequency.	approved
CTA-D4.1-319			- number of supported local inputs, at least tbd/consist	draft
CTA-D4.1-322			- number of supported local outputs, at least tbd/consist	draft
CTA-D4.1-323			- max. time tbd required for an input variable to be available to partitions	draft
CTA-D4.1-324			- max. time tbd required for an output variable from the time point it is set by a partition until it reaches the output	draft
CTA-D4.1-326			- max. number tbd of variables that can be read with a certain tbd frequency	draft
CTA-D4.1-327			- max. number tbd of variables that can be written with a certain tbd frequency	draft
CTA-D4.1-154	heading		4.2.4 Interface requirements	approved
CTA-D4.1-155	requirement		The FD framework shall provide an interface to the partitions. The interface shall be defined within task 4.4 in Connecta WP4.	approved

7. CONCLUSIONS

The task T4.1 Requirements and specification delivers with this document the requirements for the tasks T4.2 Function standardisation and Functional Open Coupling, T4.3 Application Profile and T4.4 Functional Distribution Framework.

User stories and use cases (from task T1.2 TCMS Use Cases) and high level requirements (from T1.5 Functional requirements (High level requirements)) are considered as they are available at the moment of the deliverable of this document.

The exchange of the requirements and their review comments, often based on Excel files, was not always an easy way of working. For the future is should be attempt to have a two-way exchange based on ReqIF with tool support.

In general it is important to define the system-of-interest at the beginning of work. While the definition of the requirements, there was the wish to introduce new term “(operational) consist” for the functional open coupling beside the term “consist”.

This deliveralabe enable the tasks T4.2 Functional Open Coupling, T4.3 Application Profile and T4.4 Functional Distribution Framework to start and detail their work on a defined set of requirements.