Contract No. H2020 – 730539

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

D1.3 – Function Based Architecture

Due date of deliverable: 31/08/2017

Actual submission date: 12/09/2017

Leader/Responsible of this Deliverable: Stefan Tesar (DBA)

Reviewed: Y

Document status		
Revision	Date	Description
1	13/06/2017	Agreed concept "Logical architecture.pptx" integrated in deliverable, CAF contribution Chapter 3 "architectural principles" added
2	27/07/2017	Chapters completed, Review on Chapter 2 & 3 from SIE, BT, SNCF added;
3	11/08/2017	Agreed comments from the final review call added. Editorial changes
4	12/09/2017	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: 01/03/2017 Duration: 6 months

REPORT CONTRIBUTORS

Name	Company	Details of Contribution
Jorge de Lasala Javier Goikoetxea	CAF	Chapter 3, Review Quality Review
Karsten Köchlin Armin-Hagen Weiss Gernot Hans	BT	Review, Input Final Review
Andreas Winzen Joachim Tiedemann	SIE	Idea Input, Review, Contribution to Annex Final Review
Philippe La Porte	SNCF-M	Review
Mariano Constantino	ASTS	Final Review
Vincent Mayeux	ALS	Final Review
Stefan Tesar Christine Herrick Florian Schießl Wolfgang Benner Christian Schulz	DB Task 1.2 Leader WP1 Leader	Chapters 1,2,4,5, 6,7,8,9 Quality review Final Review

EXECUTIVE SUMMARY

In the deliverable of Task 1.3, a functional view of the systems architecture is defined. It is titled “function based architecture” and it shows the architecture of the NG TCMS system from a functional point of view. The system and its architectural principals and functions are in the focus of the deliverable. The purpose of defining a functional architectural model is to elaborate models and to create views on the functional behaviour of the NG TCMS, without referring to technical implementations.

ABBREVIATIONS AND ACRONYMS

CTA: CONNECTA

D1.3: Deliverable 1.3 Function based architecture

EN: European Standard

FBS: Functional Break Down Structure

NG TCMS: Next Generation TCMS

S2R: Shift2Rail JU

Tx.x: Specific task of another work page within CONNECTA

TCMS: Train control and monitoring system

UC: Use Case

WP: Work Package

A glossary of all terms and expressions used within this deliverable can be found in the CONNECTA Global Glossary.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

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.

The project 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 objectives of the high level requirements management process within WP1 are:

- to describe what the next generation TCMS shall do and which functions it has to fullfill.
- to define the systems functional architecture as a starting point for technical architectures.
- to provide the scope and the value of the system by contributing the basic requirements to all other partners involved. The high level requirements are the base for further technical detailed specification in the different workpackages.

In order to address these objectives, the method of system engineering has been followed by creating the system's functional architecture in Task 1.3. Therefore all functions have been analysed in regard to their risks and their threats. Based on these insights, the functions have been categorised into their SIL level. This has been performed in close cooperation with WP4, to make sure the results are the same.

The deliverable is divided into several parts that need to be viewed a whole:

- The Deliverable D1.3 document itself, explaining the procedure and the method.
- Appendix 1, featuring the function list including the mapping of the epics and the SIL categorisation .

2. BASICS

In the deliverable of Task 1.3, a functional view of the systems architecture is defined. It is titled "function based architecture" and it shows the architecture of the NG TCMS system from a functional point of view. The system and its functions are in the focus of the deliverable. The purpose of defining a functional architectural model is to elaborate models and to create views on the functional behaviour of the NG TCMS, without referring to technical implementations.

This document will feature a draft for a functional architecture of the system that will show the functional structure as well as the functional operation of the system. A behavioural model can also support the understanding of the functional operation. This deliverable is related and builds up on Deliverable 1.2, the TCMS Use Cases. The definitions that have been made for the use cases are still valid for the modelling of the functional architecture. In D1.2 the system boundaries have been defined and an analysis was performed to define the actors that are interacting with the system. Based on this knowledge the user stories as well as the use case collection was created, describing all the functions the NG TCMS system needs to fulfil and perform.

2.1 Goal

The goal of this task is to define an architecture for the next generation TCMS (NG TCMS) system. The function based architecture represents the basis for further technical architectural considerations. It can be a starting point for further development and supports an easier understanding of the system's "big picture".

A functional architecture can be regarded as set and final. For every function there can be several ways of technical implementation. That means at the end there can be several technical models and ways of implementations, all of them fulfilling the functional model.

2.2 Scope

The scope of Task 1.3 stays within the defined WP1 framework, meaning that only a functional view will be taken into account for creating an architecture. Every functional description allows a variety of different technical implementations. How the technical implementations will be done at the end, is left over to the tasks and work packages that are responsible for the prototyping.

Nevertheless, as D1.3 specifies the functional principles of the NG TCMS, it will be used as an input document for the V & V activities (as defined in EN 61508-4) of the global CONNECTA projects in order to verify whether the NG TCMS finally implemented fulfils the requirements written in CONNECTA's Task 1.2. At the end of this document some examples for possible technical implementations are outlined. In Task 1.2 the whole TCMS system is viewed as a black box.

Figure 1: The TCMS blackbox approach

This viewpoint focuses on the IT driven functions of the NG TCMS. Some functions can consist of IT driven functions as well as mechanically driven functions. As an example, the brake control can be named. In the context of the train it consists of the electrical control part and the mechanical control part. For CONNECTA only the IT driven functions of the NG TCMS are of interest. So when we are talking about the brake control it is only referring to the IT driven part of the brake control.

2.3 Functional architecture model

The functional architecture shows the functional structure of the system. The functions of the system are displayed and described and their functional links are documented as a drawing. This will also show the data flows in the system and the system relevant interfaces.

A functional architecture model is a set of functions and their sub-functions that defines the transformations performed by the system to complete its mission. [4]

A function transfers input parameters into aim related output parameters. These inputs and outputs are the "flow-items" exchanged between functions. In order to define the complete set of functions of the system, all the functions necessitated by the system and its derived requirements must be identified, as well as the related inputs and outputs of those functions. That means a model can also feature the functional behavior of the system.

There are functions that are directly deduced from functional and interface requirements. These functions express the expected services of the NG TCMS necessary to meet its system requirements.

As outlined in Task 1.2's TCMS Use Cases, the TCMS system is viewed as a blackbox. All functions of the TCMS are within the systems boundaries. There are input actions that are the trigger for certain output actions of the system. Input actions are performed by the actors who interact with the system. The output actions affect one of the actors or other subsystems on the rail vehicle.

A function is specified or described without referencing to the physical mean of achieving it.

The architecture will include functions which cover future needs to make sure a system is developed that is ahead of technology when it is implemented. The scope will cover all IT driven functions of rail vehicles. This includes safety related functions such as brakes or non-safety related functions such as infotainment or WLAN access for passengers.

2.1 DESOMPOSITION OF FUNCTIONS

The TCMS black box approach considered for the TCMS Use Cases will be improved and broken down to the specific functions of the NG TCMS. A functional breakdown structure has been defined by the EN 15380-4. In this norm the functions of a train are defined and broken down into detailed sub-functions. The EN 15380-4 will be used as a reference and an input for the work in CONNECTA. Existing norms and standards shall be used and taken into account as long as it makes sense in the context of the CONNECTA project.

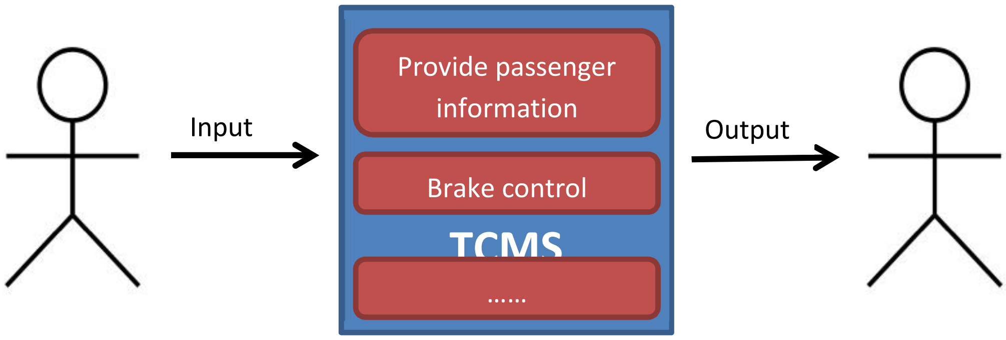

Figure 2: From blackbox to white box by defining the functional level

Figure 2 shows a few examples how the TCMS can be broken down into functions. For example, it has to provide passenger information as well as brake control.. The functions will be displayed in detail on the list, which is attached as Annex 1.

3. ARCHITECTURAL PRINCIPLES

Principles are the foundation of every architectural model. They are defined prior to the modelling process, to make sure that architects and contributors of the model will follow the same rules and guidelines while creating the model. The principles shall enable the architect to achieve his goals by creating the systems architecture. Therefore, the principles shall be easily understandable.

3.1 FUNCTION ORIENTED

The basic abstractions given to the user are functions. The control over the whole train is done using distributed functions. Therefore, the architecture shall follow the function oriented approach, not referencing to the technical implementation.

3.2 FUNCTIONAL CLUSTERING

Clustering is the task of grouping a set of functions in such a way that objects in the same group (cluster) that are similar to each other than to those in other groups (clusters). For the NG TCMS there is no strict definition of the clusters, it will be more or less defined by the main functions provided by the IT system. From the technical point of view, grouping functions into clusters can support efficiency for the technical implementation by avoiding the implementation of similar functions. It can help reduce the amount of wires and controllers in the whole network. Another criteria for clustering can be the security level of the related function/function domain. Here security requirements according IEC 62443-3-3 [6] can be followed.

3.3 SEPARATION OF FUNCTIONS

The safety goals of the functions have an important impact on the architecture of the NG TCMS. These safety goals (i.e. Safety Integrity Levels – SIL) are defined per function. Functions with different SIL shall not interfere no matter what SIL level is considered (e.g. application, communication, etc.) in order not to risk the overall safety of the NG TCMS. A key point is that if safety and non-safety related functions are mixed in one communication network, there must be architectural restrictions to make sure that the data exchange is completely controlled. Furthermore, the architectural design must guarantee that any change made to a function will not affect other functions. For example: a SW update of the passenger information system shall not affect any software of the safety related functions in the architecture (e.g. brake control).

Functions shall be independent from communication technology and hardware so that functions will not change after a communication technology or hardware change.

Temporal and spatial partitioning can have the effect of isolating distributed functions (functional partitions). As TCMS is deeply involved in the homologation processes, these principles help its assessment by an authorised assessor.

3.4 MINIMISE INTERFACES

The architecture shall feature a minimum of interfaces between the functions. Careful planning of the functional architecture will support a minimum number of necessary interfaces for the technical implementation.

3.5 SECURITY BY DESIGN

Security must be taken into account from the beginning. The functional architecture shall be designed to be secure from the ground up. Designers must cope with different kinds of security vulnerabilities and extreme events. The architecture shall provide control mechanisms to protect and secure the functionality of the NG TCMS or its sub-systems functions. System Security Requirements and Security Levels are defined in IEC 62443-3-3 [6].

3.6 SCALABILITY

The NG TCMS shall provide flexibility and scalability to make sure it will be adaptable to future requirements of the different stakeholders.

Scalability means the following features in specific:

- Adding new functionality easily.
- The coupling of different trains shall be considered as a use case and the proposed architecture shall be able to deal with this situation. Coordination with the tasks in WP4 is performed.
- Easy component exchangeability through standardised interfaces.
- Increase the number of instances of objects (units, cars, carriers of functions/subsystems) usually referred to as horizontal scaling or scale out.
- Increase the performance of instances of objects (units, cars, carriers of functions/subsystems) usually referred to as vertical scaling or scale up.

The NG TCMS is open to adapt to upcoming requirements effortlessly. Scaling the system's non-safety related functions is performed without the necessity of a re-homologation of the TCMS or sub-systems of it.

3.7 SUPPORT DEPENDABILITY

Dependability is closely related to RAMS as it considers the system's availability, reliability, maintainability and further on also durability, safety and security aspects. For TCMS attention also needs to be paid to a potentially required trade-off between different characteristics of dependability, e.g. safety vs. reliability, where increasing safety may lead to reduced reliability.

4. FROM EPIC TO FUNCTION

Every rail vehicle features IT functions. A function describes what a system shall be able to do.

In Task 1.1 a first approach for epics in the context of a collective term for functions has been performed. For the TCMS use cases in Task 1.2, the epics have been adapted in several iteration loops.

4.1 EPICS

An epic in the context of requirement management is the description of requirements on a very high level of abstraction. Everyday language is used to formulate an epic.

In the requirement development process it features a very summarised and rough overview of the system requirements, without going into details. In the case of CONNECTA, an example could be the function of “braking”, “providing information to passengers” or “surveillance”.

In the process of story decomposing, an epic can be broken down into several user stories, as well as use cases to describe the epic somewhat more detailed.

The insights that have been made within D1.1 can undergo some iteration loops and will be improved to suit the needs for CONNECTA and WP1.

The following figure shows roughly the structure from an epic via user stories to use cases and their link to functional requirements. Viewed vertically it describes a function step-by-step in more details.

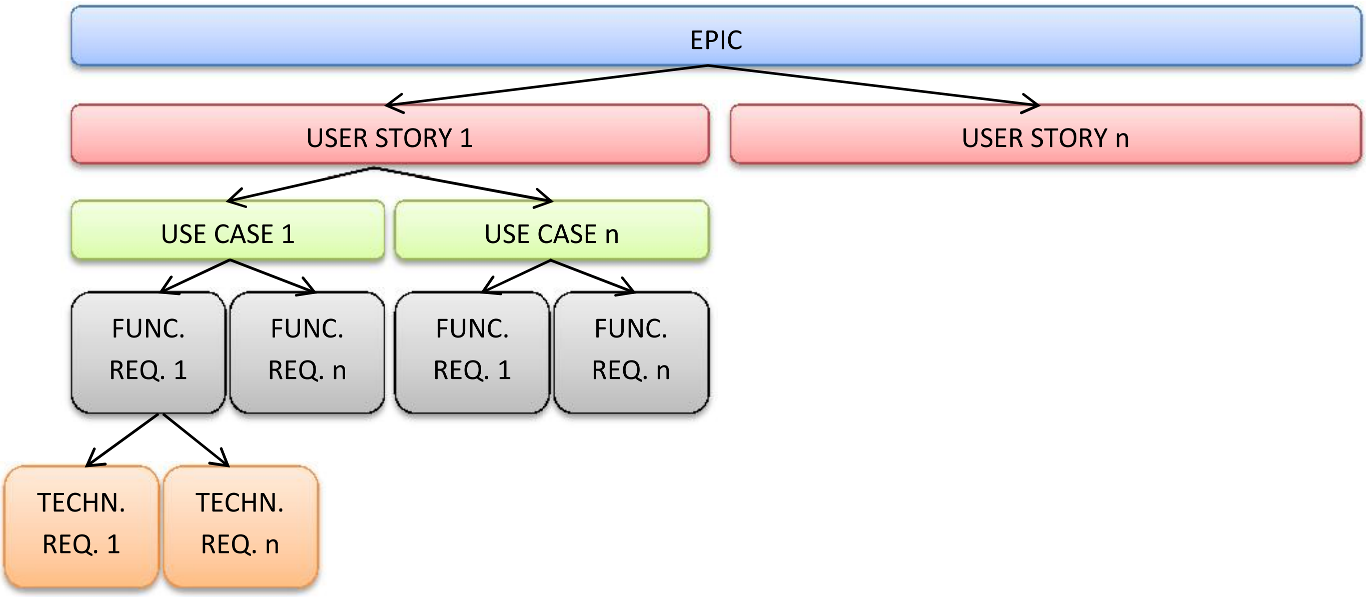

Figure 3: From Epic to Requirement

4.2 EN15380-4 Functions

The standard EN 15380-4 provides a classification system for rail vehicle functions. Part 4 focuses on the function groups. The document was prepared by the European Committee for Standardisation CEN/TC 256 as well as the WG19.

The FBS standard describes all functions a train features and is used to obtain a correlation between functional requirements and the structure of functions and the related use cases. It can help in structuring functional requirements and use cases according to a standardised list of functions.

In all cases in which functionality is a key issue (e.g. safety and reliability analyses, inspections and testing, maintenance programmes, field data acquisition and related documentation), communication is based on a functional vehicle structure composed of functional groups – particularly when cross-system or interdisciplinary considerations are important.

Functions are grouped into levels regardless of their vehicle specific technical realisation. Hence the function groups and function descriptions were developed without considering how each function may be achieved in practice. At the end of the list the link to the physical structure is made, without referring to the technical implementation. There is not necessarily a simple one-to-one relationship between each function and its technical realisation. A system or item of equipment can contribute to different functions at the same time or in sequence.

In the context of CONNECTA's WP1, mainly the IT functions are of interest.

5. FUNCTION BREAKDOWN ANALYSIS

The function breakdown analysis can be found in ANNEX 1 to the document.

The basis for the analysis was the functional breakdown structure of the EN15380-4 list. Based on this list, every IT related function has been mapped to an epic. Additionally, the different functions were categorised into their safety integrity level (SIL).

In a second step, the functions of the EN15380-4 have been categorised into their level of potential hazard. The right categorisation for it is the safety integrity level (SIL) categorisation. Every function needs to be analysed in regard of its potential risks as well as its potential hazards that can occur during operation or malfunctioning.

The safety integrity level (SIL) is defined as a relative level of risk-reduction provided by a safety function, or to specify a target level of risk reduction.

The requirements for a given SIL are not consistent among all of the functional safety standards. In the functional safety standards based on the IEC 61508 standard, four SILs are defined, with SIL 4 which is the most dependable and SIL 1 is the least dependable. For the work in CONNECTA the SIL levels for software have been reduced to SIL 2 and SIL 4. Technically speaking for software there are no differences in implementation when implementing SIL 3 in comparison to a SIL 4 function.

During the development and design of systems it gradually provides the safety-related criteria, which must be adhered to in order to minimise the risk of malfunctions. The higher the level (1-4), the higher the criteria are that need to be met. The term safety requirement level originates from the field of functional safety and serves both the assessment of electrical and electronic systems as well as the evaluation of software. For TCMS the Safety integrity level (SIL) aspects the European norms EN 50126 [8], 50128 [9] (50657 [10]), 50129 [11], 50159 [12] and the international norm IEC 62443 [6] shall be applied.

The term security integrity level has been defined by Josef Börcsök as follows:

> *"There are four well-defined levels for specifying the requirement for the security integrity of security functions associated with the E/E/PE security-related system, whereby the Security Integrity Level 4 represents the highest level of security integrity and Security Integrity Level 1 represents the lowest level of security".* [5]

The level of the safety integrity of the individual component or the subsystem of a railway vehicle is determined on the basis of a hazard assessment. In this case, the perspective is focused on components which are in indirect interaction with one another and interact. This includes in particular sensors, control circuits and feedback loops, which are installed for the self-checking of a control circuit. The structure of the technical architecture and the selection of suitable components result from the basis of the specification. The system manufacturer is established up to level 2. From level 3, the system must be certified by experts or representatives of the German Federal Railway Authorities. Several factors are used for the classification assessment.

Below are some examples:

- Ratio of safe errors to unsafe errors

- The safety function must be monitored continuously as requested
- Structural redundancy
- Failure performance
- Consideration of the entire service life.

  The assessment of software components is more complex.

  Two different types of errors can be distinguished:

  - Errors that originate from the program code creation
  - Errors that originate from software tools such as compilers.

In addition, measures must be taken on how to react to such errors. [5]

The IT functions of the NG TCMS have different basic requirements. Some of them can be categorised as safety related (e.g. braking), some are not safety related (e.g. provide passenger information) as one simple example.

In fact, relevant questions for a possible categorisation concern the following points:

- Safety assessment - Does the function provide any safety risks to the passengers or actors involved?
- Security assessment – Does the function provide any security risks to the passengers or actors involved?
- IT security assessment – Can there be any IT threats to the function? The question to be asked is also about the severity as well as risk and danger for the passengers of the vehicle.
- User benefit – Does the function provides a benefit for the passenger, such as information about the travel, infotainment or similar.
- Effort for initial homologation – How high is the effort to assess the function for the first time to receive an assessment for the whole vehicle.
- Effort for re-homologation after hardware or software changes – are there assessment efforts needed after applying changes to hardware or software. This can be simple software updates to fix security issues, adding new functionality or changing hardware after malfunction or defects.
- Lifespan of function: IT driven functions have a much shorter innovation cycle than, for example mechanical functions. The further development of computers as well as personal devices require short innovation cycles for passenger related functions.. On the other hand, there are functions such as braking that will not have the need for any change or update during the lifetime of a vehicle.

After a first high level analysis certain characteristics can be defined in the different categories:

Category	State 1	State 2
Safety integrity Level (SIL)	0 – no safety relation	2, 4 – safety relation
IT security	low – no security relation	multiple levels of security, depending on attacker type and severity of the attack
Passenger benefit	Benefit for passenger	No benefit for passenger
Effort for initial homologation	Low effort is required	High effort is required due to safety relation
Effort for re-homologation	No re-homologation or re-assessment by railway authorities required	Re-homologation or re-assessment after any hardware or software changes

		required.
Lifespan of function	0,5-3 years – functions with short innovation cycles	5-30 years – functions that do not require updates at all or will only once require updates during the lifetime of a vehicle.

Table 1: Categories and States

For each category there can be more or less two different states defined. This will be a major input for the domain model as a starting point. In first step, reasonable domains shall be defined to make sure the functions are aggregated into the domains. In one domain all functions that have similar requirements shall be collected, as listed in Table 1 above. They shall be named "top domains" then and be one of the major architectural guidelines. Some of the architectural principles as found in Chapter 3 will be fulfilled with this approach.

7.1 Top Domains

Concluding from the insights of the last chapter, it can be said that the functions of the NG TCMS can be aggregated into two different groups.

On one side there are the functions that feature a benefit to the passenger, require very short innovation cycles and are not safety related. A very good example for such a function would be the infotainment on-board or passengers' access to internet services.

On the other side there are functions, such as braking, where no changes after the initial homologation are required. It doesn't feature a direct benefit to the passenger and the lifespan of the function is as long as the lifetime of the vehicle.

Based on these assumptions two domains can be defined. 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. These are not safety related and have relative short innovation cycles.

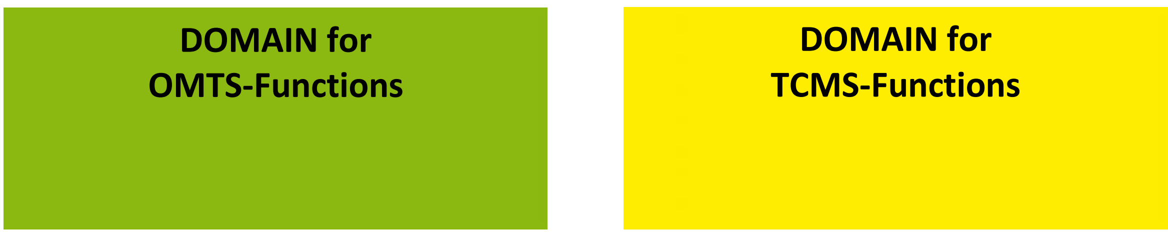

Figure 4: Top Domain Model

In the next step the functions according to their SIL level and their other requirements are assigned to the different domains. Every function needs to be analysed in detail. The major category - the SIL levels can be found in the Annex 1 list.

Figure 5: Domain Model with Functions

Figure 6 show the idea of assigning the functions to the different domains. There are several approaches for doing so, meaning there is no single solution. The result can be more or less several different approaches and models.

On the other side in Roll2Rail deliverable D2.1 – Specification of the Wireless TCMS [7] a different decomposition into domains was followed. Here TCMS was segregated into three domains.

Therefore TCMS shall be open for a best suited tailoring in further detailing.

8. DATA FLOWS

Some of the functions need to exchange information. This can be directly from one function to the other or in a broadcast manner to provide information from one source to several components (e.g. global time, actual position).

Functions within the same domain shall be able to communicate without restrictions. This is more or less the main purpose of the domain model.

The communication between the domains undergoes certain restrictions. They depend on questions about safety and IT security. The communication needs to be monitored and controlled by a higher instance in the architecture. This will ensure that only predefined messages with predefined values in a predefined time interval can be exchanged. Any other message exchange with invalid values or other time intervals can be categorised as a possible attack on the system.

A given use case is that any changes in hardware or software in one of the domains shall not have any effect on functions of the other domain. This can be fulfilled by the domain driven approach, meaning that changes in the OMTS domain shall not have assessment questions as long as the communication to the TCMS domain is under control.

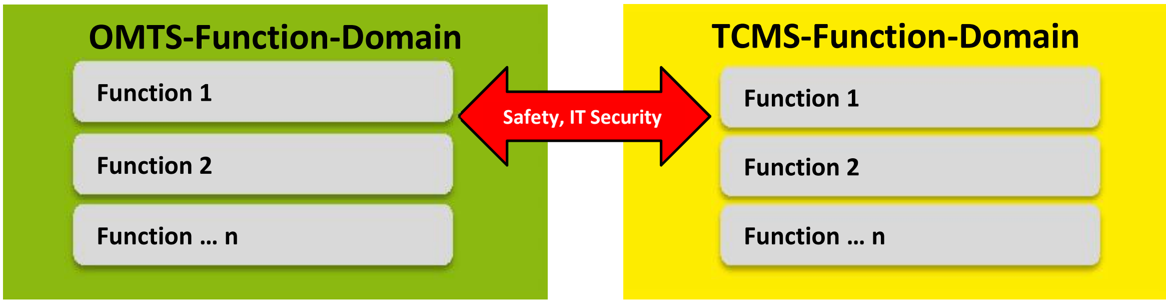

Figure 6: Communication of Functions between Domains

9. CONCLUSIONS

One of the major points in this deliverable are the architectural principles, which have to be respected for the creation of the function based architecture as well as for the design of the technical architecture. Beside use cases, functional and non-functional requirements, the architectural principles express some of the basic technical demands requirements that the rail vehicle operators have.

Setting up the domain model will be of support to have an open, flexible and scalable NG TCMS that will be adaptable to future requirements. The short innovation cycles in the IT and smartphone world are pressuring the rail vehicle operators to move to easily adaptable passenger information solutions.

All in all it can be said, that the insights made during the creation phase of Deliverable 1.3 are a very valuable basis for the further development in other tasks and work packages of the NG TCMS system.

REFERENCES

[1] EN 15380-4:2013 Railway applications — Classification system for railway vehicles — Part 4: Function groups

[2] A Practical Guide to SysML, Sanford Friedenthal, 3rd edition, The MK/OMG PRESS

[3] EN 61508-4:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 4: Definitions and abbreviations

[4] http://sebokwiki.org - *Systems Engineering Body of Knowledge (SEBoK v1.8), 2017*

[5] Adaption von Schienenfahrzeug IT an gegenwärtige Anforderungen der Betreiber, Master Thesis, Stefan Tesar, 15.11.2014

[6] IEC 62443-3-3 Security for industrial automation and control systems - System Security Requirements and Security Levels

[7] Roll2Rail D2.1 R2R-T2.1-D-TRI-053-11 Specification of the Wireless TCMS - R2R-T2.1-D-TRI-053-11

[8] EN 50126 Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)

[9] EN 50128 Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems

[10] EN 50657 Railway applications - Rolling stock applications - Software on board of rolling stock, excluding railway control and protection applications

[11] EN 50129 Railway applications - Communications, signalling and processing systems - Safety related electronic systems for signalling

[12] EN 50159 Railway applications - Communication, signalling and processing systems - Safety-related communication in transmission systems

ANNEX 1

List with EN15380-4 functions featuring their epic and SIL categorisation.

This list will be added as Annex 1 when the consolidated mapping list will be available from WP4.