Contract No. H2020 – 730539

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

D6.1 – Specification of Virtual Certification principles

Due date of deliverable: 15/02/2017

Actual submission date: 28/09/2018

Leader/Responsible of this Deliverable: Matthias Reinholdt, Siemens AG

Reviewed: Y

Document status		
Revision	Date	Description
1	10/02/2017	First issue
2	10/02/2017	Review Draft
3	27/02/2017	Issue delivery after review - CTA-T6.1-R-SIE-010-01
4	28/03/2017	Conclusions chapter added
5	25/04/2017	Final
6	28/09/2018	Experts' feedback regarcing certification activities added to the document

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: 25 months

ACKNOWLEDGEMENTS

This project has received funding from the Shift2Rail JU under the European Union's Horizon 2020 research and innovation programme. Grant Agreement no. 730539.

REPORT CONTRIBUTORS

Name	Company	Details of Contribution
Mikel Colera	CAF	Co-Author Chapter 2, 3 & 5 / Review Experts' feedback sub-chapter added to Conclusions
Fabian Schneider	BT	Co-Author Chapter 2, 3 & 5/ Review
Carsten Pfeffer	BT	Co-Author Chapter 2, 3 & 5/ Review
Philippe Laporte	SNCF	Co-Author Chapter 2, 3 / Review
Stefan Tesar	DB	Review
Karsten Struck	DB	Review
Arndt Knipping	Siemens	Co-Author (general) / Review

EXECUTIVE SUMMARY

This document specifies the requirements and principles for the usage of simulated environments during a certification process at rolling stock context. The main content of this document defines the following:

1. General philosophy and assumptions.

   This part is a description of the general philosophy and assumptions which define and/or limit the scope of the area of use for simulations in certification processes.

2. Integration in overall certification process.

   The overall certification process is widely complex. There is an obvious need to describe the partial area of use in the overall certification context.

3. Principals for development and validation of a simulation.

   There are basic requirements affecting the creation and testing of the simulation itself which need to be fulfilled to obtain the acceptance by an assessor or regulatory instance.

4. Generic process for development and validation of a simulation.

   Describes and define the process steps for creation and testing a simulation.

ABBREVIATIONS AND ACRONYMS

Abbreviation / Acronym / Glossary	Definition
TCMS	Train control and monitoring system
CONNECTA	Contributing to Shift2Rail's Next generation of high Capable and safe TCMS and brakes.
Qualification	Activity to ensure the ability of a system or tool to fulfil the requirements of the intended use.
Validation	Activity to prove the conformance of the complete functionality to specified requirements and the intended use. Definition according ISO 9001:2008
Certification	Is the granting of approval by an official authority.
Certification	Certification refers to the confirmation of certain characteristics of an object, person, or organization. This confirmation is often, but not always, provided by some form of external review, education, assessment, or audit.
ERTMS	European Rail Traffic Management System
EC	European Community
EU	European Union
NoBo	Notified Body
DeBo	Designated Body
NSA	National Safety Authorities
ERA	European Railway Agency

Table 1: Abbreviations & Acronyms

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

1.1 CONTEXT AND BACKGROUND

The Specification of Virtual Certification principles is a deliverable of task 6.1 of the workpackage 6 “Virtual Placing on the Market” within the CONNECTA project. 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.

1.2 OBJECTIVES AND BACKGROUND

The main goal of the WP6 is to develop a simulation framework in which all subsystems of the train can be simulated, allowing remote and distributed testing including hardware in-the-loop through heterogeneous communication networks.

To Support virtual testing and certification of the TCMS and its applications, task 6.1 will specify and design a certified simulation framework platform which allows

- - virtualizing TCMS communications networks,
- - assuring the same behaviour as of the train,
- - providing the same results and
- - allowing the running of the real software on real hardware or even emulated environment.

The main goal of the subtask 6.1 is to generate a complete definition of a common understanding of a virtual certification principle and process in order to set the bases for the next tasks and to get full agreement with the relevant certification bodies. This document is the deliverable of the subtask 6.1.

1.3 REFERENCES

Ref.	Document ID	Title	Version	Date	Author
[R1]	CTA-GEN-C-CAF-013-01	Technical ANNEX 1 (part A)	1	18/08/2016	Goikoetxea Javier
[R2]	EN 50128	Railway applications – Communication, signalling and processing systems – Software for railway control and protection systems;	2011		DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN and VDE

[R3]	NASA-STD-7009	Standard for models and simulations	2008	07/11/2008	NASA
[R4]	EN 506571	Railway applications - Rolling stock applications - Software onboard of rolling stock	2016	----	CLC/TC 9X SC 9XB

Table 2: References

1.4 DOCUMENT STRUCTURE

Following structure of the document is defined by the DPP of the subtask 6.1:

i. Introductory Pages

Front Sheet (including dissemination level), document summary sheet (including issue status and history), table of contents, table of figures, glossary and definitions

ii. Executive Summary

The purpose of this section is to provide a synthesis of the main contents of the deliverables, giving a brief explanation for each of the main topics included in the document.

1. Introduction

Objective, problem to be solved, input from previous projects and work packages, result and value added, other deliverables to which results will be input, contribution and man-months effort from each partner, paragraph per partner about its contribution

2. General philosophy and assumptions.

This chapter will describe the general philosophy and assumptions which define and/or limit the scope of the area of use for simulations in certification processes.

3. Integration in overall certification process.

The overall certification process is widely complex. There is an obvious need to describe the partial area of use in the overall certification context.

4. Principals for development and validation of a simulation.

There are basic requirements affecting the creation and testing of the simulation itself which need to be fulfilled to obtain the acceptance by an assessor or regulatory instance.

5. Generic process for development and validation of a simulation.

Describes and define the process steps for creation and testing a simulation.

6. Conclusions.

General reflections about found difficulties and learnt lessons are more than welcome.

[1] Upcoming standard – follow up of EN 50128:2011

Open points, if any, should be listed.

Proposals for further activities

1.5 DEPENDENCIES

This section contains an overview of the dependencies and relationships to other tasks, information and deliverables of the CONNECTA project

Dependency	Description
[D1]	Wireless TCMS and Train to Ground WP2
[D2]	Drive by Data WP3 –Communication Architecture of the vehicle
[D3]	Functional Distribution Architecture WP4
[D4]	WP1 – General Specification, e.g. T1.2 – TCMS Use cases or T1.4 - RAMS/Security, safety, legal requirements and norms
[D5]	Safe4Rail WP3
[D6]	PINTA – WP5 Virtual Certification

Table 3: Task dependencies

2. GENERAL PHILOSOPHY AND ASSUMPTIONS

This section will describe the general philosophy and assumptions which define and/or limit the scope of the area of use for simulations in certification processes.

2.1 ASSUMPTIONS FOR USAGE IN CERTIFICATION PROCESS

- Goal of the WP 6 is to have a working prototype which implements a technical prove of concept. The requirements and the corresponding acceptance by regulatory instances are not completely possible because of a lack of involvement in WP6.
- It is possible to use and rely on simulation during the cer process. It is used successfully by other industries, e.g. ERTMS or chemical industry.
- A TCMS functionally validated with or within the test system is sufficiently tested. No further validation steps are necessary for certification of TCMS in other environments (e.g. at the real vehicle).
- The test environment with its simulation functionality is able to handle all different requirements and processes of all national and international (EU) authorities.
- The simulator is able to handle all individual Architectures, interfaces and customizations of any subsystem
- The simulator will be able to simulate the Ethernet network protocols compliant to the IEC-61375 TCN standard
- The hardware platform is generic enough to support common communication interfaces of rolling stock
- Test procedures or test automation for the validation of the TCMS are not part of this WP.

2.2 SCOPE OF TEST SYSTEM AND SIMULATION

Functionality reflected by the Task 6.1 [R1]:

- TCMS Control and subsystems functionality (incl. degraded mode), which is relevant for certification processes
- Architecture should support train to ground communication (easy adoption of simulation), but realization of the train to ground part is out of scope.
- All subsystems in TCMS communication network or which have interfaces via wired connections shall be simulated if they are not physically present. At least an interface simulation shall be provided

- Functionality which is not originally part of TCMS, but part of certification requirements (e.g. Train communication system – Passenger alarms or information)
- The simulation shall be able to support every certification requirement, no matter if it is national or international (EU) (reliable evidences like test reports)
- Allowing remote and distributed testing including hardware in-the-loop through heterogeneous communication networks
- Simulation shall be structured in modules for easy adaption and changing (plug and play functionality)
- Simulation shall provide the interfaces for test automation

2.3 SIMPLIFICATIONS AND BEHAVIOUR OF SIMULATION

Simplifications and the native behaviour of models and simulations lead to an uncertainty of the results. Therefore the development and validation of the entire simulation system need to be assessed. Following aspects could be some of the questions and factors which need to be clarified:

- What kind of abstraction are allowed within the simulation, e.g. simplified behaviour of pneumatic system
- Impact of simplifications cause in interface mock-ups and stubs
- Impact cause by abstraction of real physics and physical behaviour of the simulation
- Error injection shall be basically on signal basis, not as a native function provided by the simulation (API Access to signals)
- etc.

2.4 VALIDATION STRATEGY

A precondition to use a test environment with or without simulation is to qualify and/or validate this environment. Otherwise the test evidences will not be accepted by the regulatory authorities. The general strategy is a declaration of conformity on basis of a tool qualification and/or validation according to the standard EN 50128 [R2].

It is necessary to differentiate between the usage of the simulation for testing of technical standard conform behaviour, safety and non-safety functionality of the tested TCMS system. According to certification regulations in the European Union especially technical standard conformance (e.g. TSI) and safety functionality need to be validated. A qualification and/or validation of the test system and the related simulation are necessary in case of the usage in regards to standard conformity declarations and in regards to test of safety functionality [C1]. If the functionality is not required by

certification processes an explicit validation of the test system and the related simulation is not necessary.

The general procedure of qualification or validation of the test system consists of three main functions, which meet the demands of an attestation of conformance regarding the defined requirements of the test system and the corresponding simulation.

- Selection
- Investigation
- Assessment and confirmation

Each of this bullet points have to be documented is an appropriate way.

The selection and definition of the required tests and conformance declarations of the test system and the corresponding simulation, as well as the basis of the detailed test procedure need to be specified within a validation plan.

The Investigation activities will be executed to get the complete information about the conformance regarding the specified requirements.

The decision if the requirements are fulfilled and the object of the assessment is ready for use can only be done after the analysis of the results of the assessment.

The confirmation and conformance declaration is a statement of proved fulfilment of specified requirements. Specified pass or fail criteria for test or samples are used. Certificates could be used as well.

Deviations according to the specified requirements need to be documented.

The conformance declaration could lose its validity if there are changes or adoptions of the test system of the simulation. This includes:

- Simulation application
- Simulation tools
- Test system hardware
- Requirements

To keep up the validity of the conformance declaration a retest or an assessment on basis of impact analysis could be required.

Following documentation is recommended:

- Specification of the test system and the simulation

- Validation plan - includes requirements, test procedures and restrictions regarding the intended use
- Assessment report – includes test results, deviations and an assessment/conclusion
- Impact analysis in case of changes during or after the qualification/validation

For detailed documentation requirements please refer to the process step descriptions within chapter 4 - “Principles for development and validation of a simulation”

3. INTEGRATION IN OVERALL CERTIFICATION PROCESS

3.1 VEHICLE TYPE APPROVAL / EC TYPE-APPROVAL

The type approval or EC type-approval is the acknowledgement of the regulatory conformance of a vehicle and serves therefore the traffic safety. It is granted on request of the holder of the right of disposal.
There are three kinds of type approvals:

- For types of vehicles
- For single vehicles
- For parts and components of vehicles

The approval is granted without time limits. It can be revoked under special circumstances or can terminate because of modifications of the vehicle.

The EC type-approvals are regulated at EU level. The operating license is granted on national basis and is defined as a national type approval. Granted will be the regulatory confirmation of the conformance of a vehicle, a system, a component or a dedicated technical unit regarding the current regulations.

The European Authorization process based on Directive 2018/57/EC and in the future (mid 2019) on Directive 2016/797/EC. The European and National Notified Rules (remaining national requirements) will be assessed from a NoBo and a DeBo. The result of these assessments will be documented in a Technical File. This Technical File together with the Declaration of Verification will be forwarded to the responsible National Safety Authority or ERA (mid 2019). The NSA / ERA will issue an Authorisation for Placing into Service or an Authorisation for Placing on the Market (after mid 2019).

The process of the national and international certification raises requirements on processes of construction and development, the technologic solutions and operation. These requirements could originate in legacy restrictions, regulations of national authorities, standards or certification processes itself. The compliance to these requirements needs to be shown by appropriated evidences.

An adequate management of requirements is highly recommended.

Modelling and simulation have been recognized as a method for teaching in terms of learning exercises as well as risk mitigation for functional aspects. The usage as evidence-based tool for validation of real-world scenarios in certification procedure is a slightly unknown area with a lack of standardization. The reason originates in the natural purpose of the certification. It compares requirements, definitions and design with the realisation. To exchange partly the realization for components, complete functionality or even the surrounding environment and physics contradicts this purpose. A natural uncertainty is applied to the simulation approach.

But using modelling and simulation in a certification workflow is an important step in redesigning processes of software development in rolling stock.

To resolve this conflict a detailed assessment of the validity of the simulation result robustness is required. Additionally it needs to be evaluated which evidence could be provided by using the simulation approach, e.g. functional safety need to reflect several aspects and not all could be covered by simulations.

The functional safety approval needs to show the conformance to following requirements:

1. Evidence of functional correctness in a fault free state
2. Exception handling – Reaching and keep a safe state in case of a not normal operation compliant situation
3. Correct construction, wiring and installation – full hardware coverage
4. Software causal path and interface coverage – full software coverage
5. Correctness of operator and user information
6. Environmental impacts and lifetime influences on functionalities incl. the mounting situation
7. Type of usage and operating conditions

Point 1, 2, 4, 5 and 7 could be supported by modelling and simulations. Point 3 and 6 require a real world setup.

Following schematic figure show the information flow in type approval processes.:

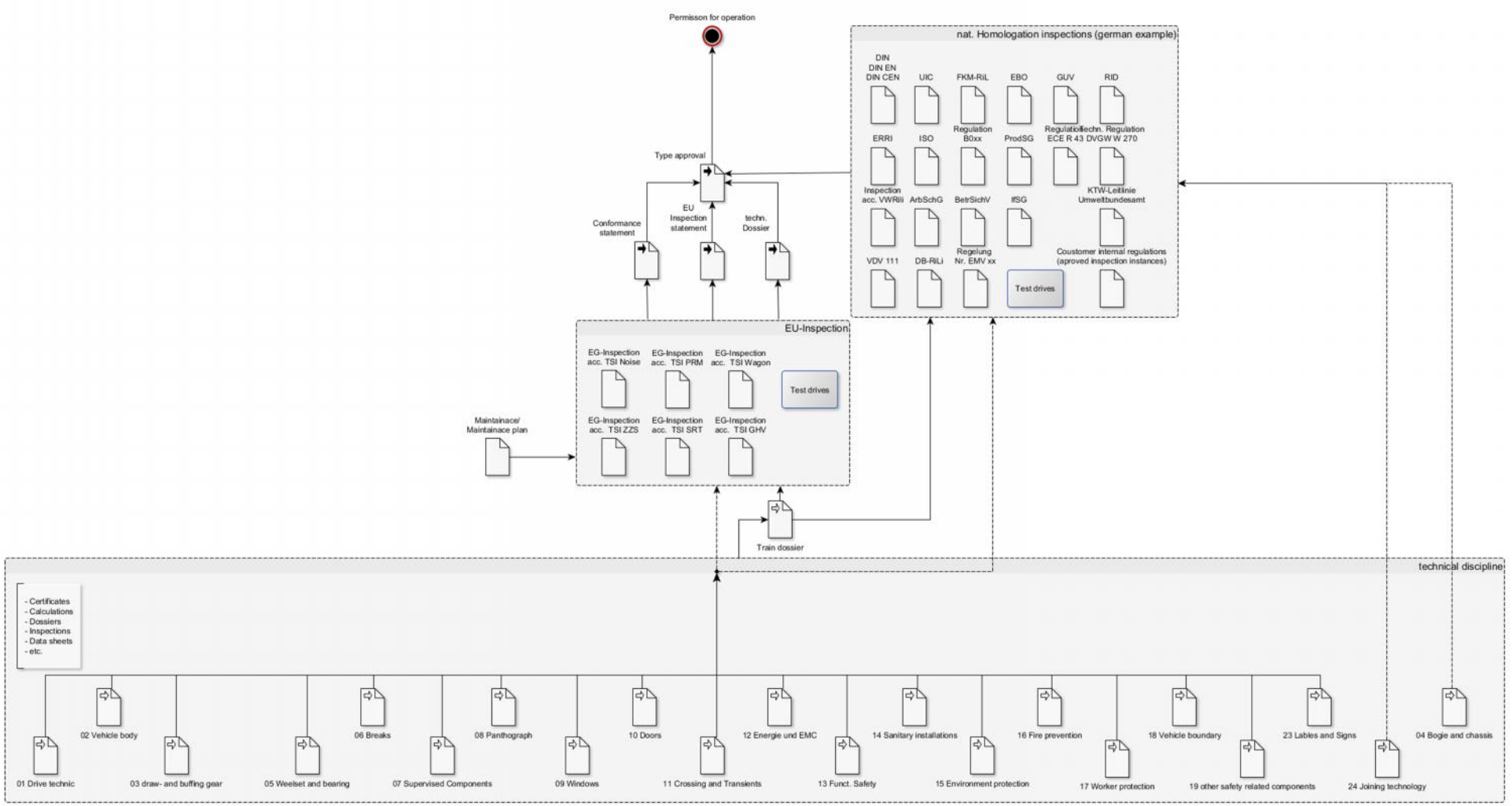

Figure 1: Schematic information flow of type approval

4. PRINCIPLES FOR DEVELOPMENT AND VALIDATION OF A SIMULATION

This chapter describes the requirements for the development and validation of a simulation and test environment.

4.1 SPECIFICATION AND ARCHITECTURE

Requirement	Description
Req. 4.1.1	Identify and document assumptions and abstractions of the conceptual model
Req. 4.1.2	Identify and document basic structure and mathematics of model
Req. 4.1.3	Identify and document data sets and supporting software for model input and development
Req. 4.1.4	Identify and document units and reference frames
Req. 4.1.5	Identify and document limits of operation of models

Table 4:Requirements for specification and Architecture

4.2 IMPLEMENTATION

Requirement	Description
Req. 4.2.1	Identify and document uncertainly in model-development data
Req. 4.2.2	Document guidance on use of a model
Req. 4.2.3	Identify and document parameter calibrations
Req. 4.2.4	Document updates of the model
Req. 4.2.5	Establish configuration management and maintenance Maintain documentation and models Maintain datasets and supporting software
Req. 4.2.6	Identify and document obsolescence criteria
Req. 4.2.7	Manage feedback for unusual results

Table 5: Requirements for Implementation

4.3 VERIFICATION, VALIDATION AND UNCERTAINTY QUALIFICATION

Requirement	Description
Req. 4.3.1	Identify and document verification techniques and domain of verification
Req. 4.3.2	Identify and document error estimates
Req. 4.3.3	Document verification status
Req. 4.3.4	Identify and document validation techniques and domain of validation
Req. 4.3.5	Identify and document validation metrics, references and data sets
Req. 4.3.6	Document validation studies and results

Req. 4.3.7	Document uncertainty quantification processes
Req. 4.3.8	Identify and document quantified uncertainties
Req. 4.3.9	Document sensitivity analyses
Req. 4.3.10	Document the intended use.

Table 6: Requirements for Verification, validation and uncertainty qualification

4.4 CREDIBILITY ASSESSMENT

Requirement	Description
Req. 4.4.1	Document risk assessment for models and simulations used for evidence in critical certification procedures, e.g. functional safety.
Req. 4.4.2	Identify and document those models and simulations which are in scope of the corresponding evidence-based results (Versions based on configuration management).
Req. 4.4.3	Identify and document the acceptance criteria for model and simulation products
Req. 4.4.4	Document decisions, verification, validation, uncertainty quantifications and the corresponding rationales.

Table 7: Requirements for credibility assessment

5. GENERIC PROCESS FOR DEVELOPMENT AND VALIDATION OF A SIMULATION

The generic process needs to reflect the development and the usage of a simulation environment. Both parts follow independent life cycle aspects. The general development of a simulation should be project independent. It needs to ensure a customization is possible. The project specifically needs to reflect the customization and if the final environment is able to create the necessary results for the intended use.

Following sub chapters defines a process proposal. The mentioned rolls and process step results (artefacts) shall give an idea how the necessary information and result could be created. The described process steps, rolls and artefacts could be merged or divided into sub artefacts as needed [C3].

5.1 IMPLEMENTATION OF A SIMULATION

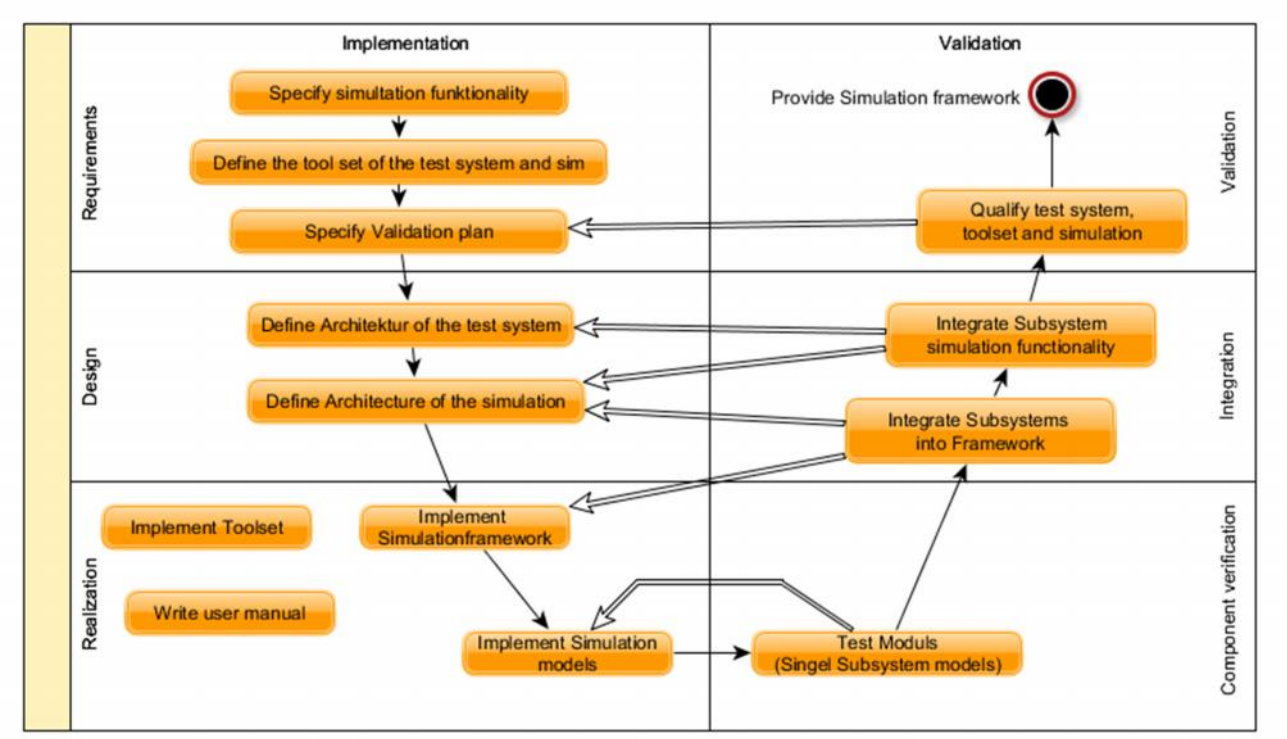

Figure 2: Process schema of simulation development

5.1.1 Implementation

Requirements phase

Process step: Specify simulation functionality	
Input **(Required input to create the output)**	**Output** **(Results of the process step)**
• User requirements • Regulatory requirements	• Simulation Requirement Specification • Risk analysis
Responsible	**Support**
Requirements Manager	stakeholders
Methods	**Phase**
• Requirement engineering • Product risk analysis	Requirements phase
Description	
A Simulation Requirements Specification (abbreviated SRS) is a structured collection of information that embodies the requirements of a simulation. A Requirements Manager is responsible for analyzing the business needs of their clients and stakeholders to help identify problems and propose solutions. Within the development life cycle domain, the SA typically performs a liaison function between the business side of an enterprise and the test department or external service providers.	

Process step: Define the tool set of the test system and simulation	
Input **(Required input to create the output)**	**Output** **(Results of the process step)**
• Simulation Requirement Specification	• Toolset Requirement Specification
Responsible	**Support**
Requirements Manager	• Implementer (Simulation) • User (Tester)
Methods	**Phase**
• Requirement engineering	Requirements phase
Description	
The Toolset requirement specification (abbreviated TRS) describe is a structured collection of information that embodies the requirements needed to implement a simulation, administrate the test system and execute the test procedures.	

Process step: Specify Validation plan	
Input **(Required input to create the output)**	**Output** **(Results of the process step)**
• Simulation Requirement Specification • Toolset Requirement Specification • Risk analysis	• Simulation Validation Plan (Basic simulation)
Responsible	**Support**
Tester (Simulation)	Requirements Manager
Methods	**Phase**
• Tool Validation strategies • Test coverage concepts • Uncertainty evaluation methods • Credibility assessment methods	Requirements phase
Description	
The Simulation Validation plan describes the acceptance procedure and criteria for the simulation tool set and the simulation environment.	

Design phase

Process step: Define Architecture of the test system and simulation	
Input **(Required input to create the output)**	**Output** **(Results of the process step)**
• Simulation Requirement Specification • Toolset requirement specification	• Simulation Architecture Specification
Responsible	**Support**
Simulation Designer	• Requirements Manager • User (Tester)
Methods	**Phase**
• system architecture engineering	Design phase
Description	
In (hardware, software, or enterprise) systems development, an architectural specification (abbreviated ARS) is the set of documentation that describes the structure, behaviour, dependency and interface views of that system.	

Realization phase

Process step: Implement Toolset	
Input **(Required input to create the output)**	**Output** **(Results of the process step)**
• Toolset Requirement Specification • Simulation Architecture Specification • Coding Guideline	• Toolset for development, administration and usage
Responsible	**Support**
Implementer	• Simulation Designer • User
Methods	**Phase**
• Usability • Installability • Performance • Robustness • Prototyping	Realization phase
Description	
The toolset is a collection for tool with specific intended usage. There are tools for development, administration, analysis and test tasks.	

Process step: Implement Simulation framework and simulation models	
Input **(Required input to create the output)**	**Output** **(Results of the process step)**
• Simulation Requirement Specification • Simulation Architecture Specification • Coding Guideline • Modelling Guideline • Toolset for development	• Simulation framework • Simulation models
Responsible	**Support**
Implementer	• Simulation Designer • Requirements Manager
Methods	**Phase**
• Modelling • Coding	Realization phase
Description	
Implementation of the simulation product. Corresponding to the architecture there might be segregated components and architectural elements which can be implemented and validated independently.	

Process step: Write user manual	
Input **(Required input to create the output)**	**Output** **(Results of the process step)**
• Configuration features • Workarounds • Restrictions • Known Bugs • Simulation Requirement Specification	• Toolset User Manual • Simulation Administration Manual • Simulation User Manual • Data sheets (Hardware) • Construction plan (Basic hardware Setup)
Responsible	**Support**
Implementer	• User (Tester) • Requirements Manager
Methods	**Phase**
• User oriented documentation	Realization phase
Description	
The user documentation need to address the specific needs of information for the individual use cases (utilisation, administration, etc.).	

5.1.2 Validation

Component verification phase

Process step: Test Modules	
Input **(Required input to create the output)**	**Output** **(Results of the process step)**
• Simulation Architecture Specification • Toolset Requirement specification • Simulation Validation Plan (Basic simulation)	• Deviation Report • Component Verification Log
Responsible	**Support**
Implementer (4-Eyes)	• Implementer
Methods	**Phase**
• Unit test methods (e.g. automated test) • Parameterized unit testing • Boundary test • etc.	Component verification phase
Description	
Intuitively, one can view a module or unit as the smallest testable part of an application. In procedural programming, a unit could be an entire module, but it is more commonly an individual function or procedure. Unit tests are usually short code fragments created by Implementers or occasionally by white box testers during the development process.	

Integration phase

Process step: Integrate Subsystems into framework	
Input **(Required input to create the output)**	**Output** **(Results of the process step)**
• Simulation Architecture Specification • Simulation framework	• Simulation runtime with integrated interfaces • Deviation Report • Component Integration Log
Responsible	**Support**
Implementer	• Simulation Designer
Methods	**Phase**
n.a.	Integration phase
Description	
The goal is to create a running simulation product. It should be installable and usable without runtime errors.	

Process step: Integrate Subsystem functionality	
Input **(Required input to create the output)**	**Output** **(Results of the process step)**
• Simulation Architecture Specification	• Simulation runtime with integrated subsystem functionality • Deviation Report • Software Integration Log
Responsible	**Support**
Integrator	• Implementer
Methods	**Phase**
• Dependency analysis • Equivalence class • Boundary analyses	Integration phase
Description	
Software system integration refers to the practice of combining individually tested software components into an integrated whole. Software is integrated when subsystems are combined into products. Components may be integrated after all are implemented and tested as in a waterfall model or a "big bang" approach. In either, software system integration appears as a discrete step toward the end of the development life cycle between component development and integration testing. Continuous integration is a much less risky approach wherein the components and subsystems are integrated as they are developed into multiple working mini-versions of the system.	

Validation phase

Process step: Qualify test system, toolset and simulation	
Input **(Required input to create the output)**	**Output** **(Results of the process step)**
• Simulation & Test system environment • Simulation Validation Plan (Basic simulation) • Simulation Requirement Specification • Toolset User Manual • Simulation Administration Manual • Simulation User Manual • Workarounds • Restrictions • Known Bugs	• Deviation Report • Validation Logs (Toolset, Simulation & Simulation environment, Administration) • Validation Report
Responsible	**Support**
Tester	• Requirements Manager • Simulation Designer • Implementer
Methods	**Phase**
• Formal Test methods • Technical reviews • Configuration Management audits • Monitor progression during software integration • Plans, procedures and documentation reviews • Qualification and Acceptance testing	Validation phase
Description	
Definition according ISO 9001: The verification aspect is a set of tasks that ensure correct implementations techniques are in place to verify that the right work product is being integrated correctly. The validation concept ensures that the correct work product is the right product to validate.	

5.2 USAGE OF SIMULATION

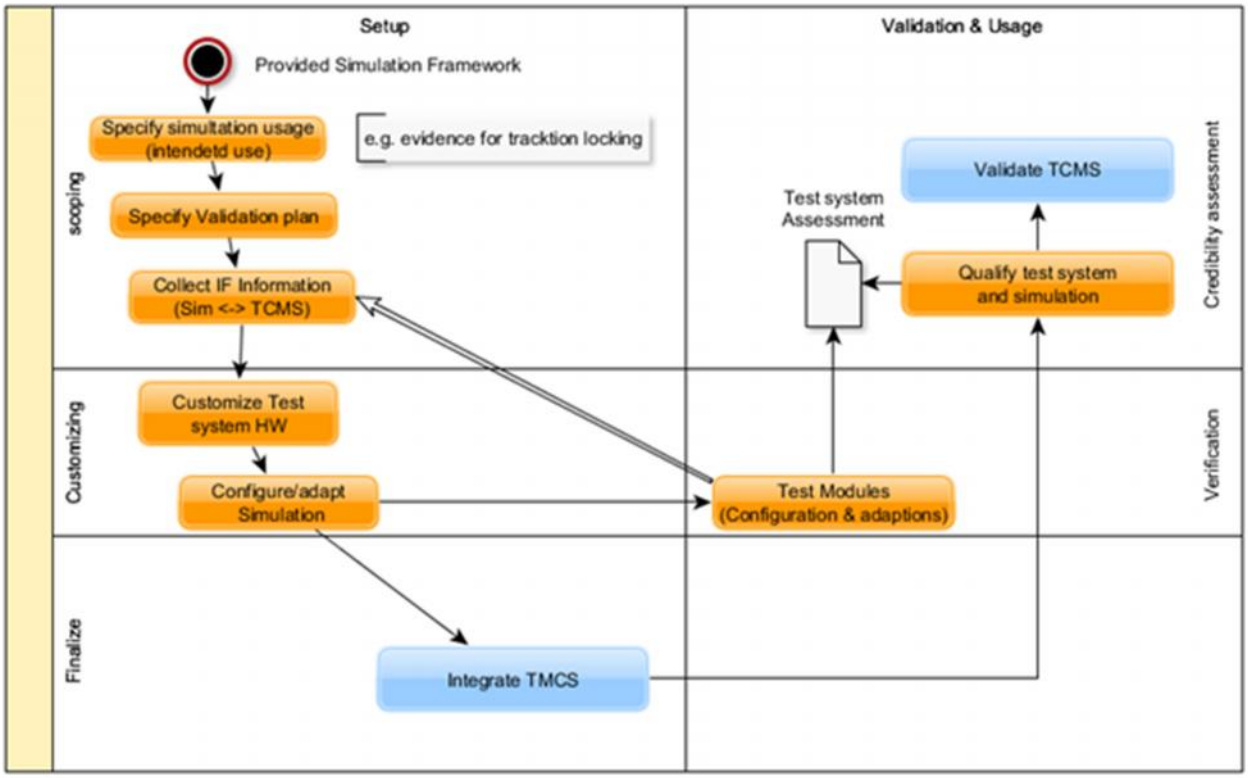

Figure 3: Process schema of simulation usage

5.2.1 Setup

Scoping phase

Process step: Specify simulation usage	
Input **(Required input to create the output)**	**Output** **(Results of the process step)**
• "Product" Basic Simulation • Project specific information / goals	• Scoping Documentation • Simulation Environment Requirements
Responsible	**Support**
Tester	• Project Management • Certification Management
Methods	**Phase**
• Risk analysis • Impact analysis	Scoping phase
Description	
During the Scoping phase the department of user group identify intended use, the derived requirements and conduct preliminary site. This phase includes needs assessments and definition of project parameters. The Simulation Environment Requirements describe the properties of the simulation environment needed to execute the test procedures.	

Process step: Specify validation plan	
Input **(Required input to create the output)**	**Output** **(Results of the process step)**
• Scoping Documentation • Toolset User Manual • Simulation Administration Manual • Simulation User Manual • Workarounds (Simulation) • Restrictions (Simulation) • Known Bugs (Simulation) • Risk analysis	• Validation Plan (Simulation environment)
Responsible	**Support**
Tester	Requirements Manager
Methods	**Phase**
• Tool Validation strategies • Test coverage concepts • Uncertainty evaluation methods • Credibility assessment methods	Scoping phase
Description	
The Simulation Validation plan describes the acceptance procedure and criteria for the simulation tool set and the simulation environment.	

Process step: Collect interface Information	
Input **(Required input to create the output)**	**Output** **(Results of the process step)**
• Simulation Environment Requirements • Toolset User Manual • Simulation Administration Manual • Simulation User Manual • Data sheets (Hardware) • Test Object Architecture Documentation • Reference data	• Simulation Environment Data Requirements • Simulation Environment Specification
Responsible	**Support**
Administrator	• Tester • Test Object Designer
Methods	**Phase**
n.a.	Scoping phase
Description	
The simulation environment setup is defined in hardware, software, boundaries and interfaces to the test object. It is specified which customizations are required. The simulation environment Data Requirements describe the properties of the data needed to setup the simulation environment.	

Customizing phase

Process step: Customize test system hardware	
Input **(Required input to create the output)**	**Output** **(Results of the process step)**
• Simulation Administration Manual • Simulation Environment Specification • Construction plan (Basic hardware Setup)	• Construction documentation (Customizing) • Physical Simulation Environment
Responsible	**Support**
Tester	n.a.
Methods	**Phase**
• Commissioning	Customizing phase
Description	
The result of this step is the physical test system part and the corresponding documentation like electrical schemas and construction plans.	

Process step: Configure / adapt simulation	
Input **(Required input to create the output)**	**Output** **(Results of the process step)**
• Simulation User Manual • Simulation Administration Manual • Simulation Environment Data Requirements • Simulation Environment Specification	• Project specific environment data • Project specific models • Customization documentation
Responsible	**Support**
• Implementer	• Tester
Methods	**Phase**
• Modelling • Coding	Customizing phase
Description	
The result of this step is the logical test system part and the corresponding documentation like parameter configurations and model documentation.	

Finalization phase

Process step: Integrate TCMS	
Input **(Required input to create the output)**	**Output** **(Results of the process step)**
• Simulation Environment Specification • Simulation Environment Requirements • Project specific environment data • Project specific models • Construction documentation (Customizing) • Customization documentation	• Completed test environment • Environment readiness report • Deviation Report
Responsible	**Support**
Tester	• Implementer
Methods	**Phase**
• Commissioning	Finalization phase
Description	
This step focuses on the integration of the test object into the previously provided simulation environment.	

5.2.2 Validation & Usage

Verification phase

Process step: Test modules	
Input **(Required input to create the output)**	**Output** **(Results of the process step)**
• Simulation Environment Specification • Simulation Environment Requirements • Simulation Environment Data Requirements • Project specific environment data • Project specific models • Customization documentation	• Customization Verification Log • Deviation Report
Responsible	**Support**
Tester	• Administrator • Implementer
Methods	**Phase**
• Unit test methods (e.g. automated test) • Parameterized unit testing • Boundary test • etc.	Verification phase
Description	
This process step verifies the project specific customizations (models, parameter configurations and datasets)	

Credibility assessment

Process step: Qualify test system and simulation	
Input **(Required input to create the output)**	**Output** **(Results of the process step)**
• Scoping Documentation • Toolset User Manual • Simulation Administration Manual • Simulation User Manual • Workarounds • Restrictions • Known Bugs • Risk analysis • Validation Plan • Simulation Environment Specification • Simulation Environment Requirements • Simulation Environment Data Requirements • Project specific environment data • Reference data • Project specific models • Customization documentation • Customization Verification Log • Environment readiness report	• Test System Assessment Report • Deviation Report
Responsible	**Support**
Tester	• all
Methods	**Phase**
• Uncertainty Quantification • Sensitivity Analysis	Credibility assessment
Description	
This process step shows the uncertainty of the simulation, the test environment, the test data and the robustness of the simulation output / results. The result is a Test System Assessment Report which includes all known issues, deviation from Validation Plan, rationales, uncertainty quantifications and the approval decision.	

Process step: Validate TCMS	
Input **(Required input to create the output)**	**Output** **(Results of the process step)**
• Simulation User Manual • Customization documentation • Known Bugs • Workarounds • Restrictions	• Deviation Report for Simulation • Impact analysis (reg. test result)
Responsible	**Support**
TCMS Tester	• Administrator
Methods	**Phase**
• Impact analysis • Defined in test strategy of the customer project.	Credibility assessment
Description	
This process step reflects the usage of the simulation environment during the dynamic test process within the customer project. It is important that all errors and failures of the simulation and test environment are documented and assessed because they could have impact on the test results.	

5.3 CREDIBILITY ASSESSMENT (PROPOSAL)

An assessment could be done according to NASA standard NASA-STD-7009 [R3]. This only proposal. A valid method needs to be defined in the Validation Plan document.

Level	Verification*	Validation*	Input pedigree*	Result uncertainty*	Result robustness*	Use history	Management	People qualification
4	Reliable error estimation methods are used to quantitatively assess numerical errors. These estimates show that the errors are small from test suites, which exercise all important algorithms, all important features and capabilities, and all important couplings (physics, modules, etc.) of the full computational model.	Model and simulation results are compared favourable for the real-world system at validation points by comparison of the model and simulation results to acceptable references, which are measurements on the real-world system.	The input data compare favourably with measured data from the real-world system, or the input data came with a summary credibility rating above 3.5. Uncertainty associated with the input data is known.	Uncertainty estimates are quantitative and base upon nondeterministic and numerical analysis.	Sensitivity of the model and simulation results for the real-world system is quantitatively known for many variables and parameters, including all of the most sensitive variables and parameters.	De facto standard.	Continuing process improvement: The effort is using measurements on processes to improve the repeatability of the model and simulation results.	Possesses an advanced engineering or science degree or extensive work experience in modelling and simulation. Has extensive experience with the development and use of the models and simulations being reviewed, and has employed specific recommended practices relevant to current application.

Level	Verification*	Validation*	Input pedigree*	Result uncertainty*	Result robustness*	Use history	Management	People qualification
3	Some formal method is used to assess numerical errors associated with unit testing with significant coverage of the code.	Model and simulation results are compared favourably for problems of interest at validation points by comparison of the model and simulation results to acceptable references, which are experimental measurements on problems of interest.	The input data compare favourably with acceptable measured reference data from problems of interest, or the input data came with a summary credibility rating above 3.0. Uncertainty associated with the input data is known.	Uncertainty estimates are quantitative and base upon nondeterministic analysis.	Sensitivity of the model and simulation results for the real-world system is quantitatively known for many variables and parameters.	Post-decision real-world events have been accurately represented in model and simulation results (e.g. validated by field data)	Predictable process: The effort is measuring repeatability of the model and simulation results generated by the processes.	Possesses an advanced engineering or science degree or extensive work experience in modelling and simulation. Has general modelling and simulation training. Has specific experience with the models and simulations being reviewed, and has been trained on specific recommended practices relevant to current application.

Level	Verification*	Validation*	Input pedigree*	Result uncertainty*	Result robustness*	Use history	Management	People qualification
2	Favourable results from unit and regression testing of key features of the computational model.	Model and simulation results are compared favourably for unit problems at validation points by comparison of the model and simulation results to acceptable references, which are experimental measurements of higher fidelity results.	The input data is traceable to formal documentation, or the input data came with a summary credibility rating above 2.0	Uncertainty estimates are quantitative and base upon deterministic analysis or expert opinion.	Sensitivity of the model and simulation results for the real-world system is quantitatively known for a few variables and parameters.	Used previously upon which critical decisions have been made.	Established process: The effort has established a documented process for development and operations.	Possesses an engineering or science degree. Has received formal training in formulation of modelling and simulation and generic training on recommended practices relevant to current application. Has developed models and simulations.
1	Favourable evidence of verification for conceptual and mathematical models.	Conceptual and mathematical models compare favourably with "general problem" and "textbook" referents.	The input data is traceable to informal documentation, or the input data came with a summary credibility rating above 1.0	Uncertainty estimates are quantitative.	Sensitivity of the model and simulation results for the real-world system is estimated by analogy with the quantified sensitivity of similar problems of interest	Specific scenarios have been created to test application, or model and simulation results compare favourably with outputs from other similar tools.	Managed process: The roles and responsibilities have been defined.	Possesses an engineering or science degree. Has been introduced to the topic of modelling and simulation and has been exposed to generic recommended practices in modelling and simulations.

Level	Verification*	Validation*	Input pedigree*	Result uncertainty*	Result robustness*	Use history	Management	People qualification
0	Insufficient evidence.	Insufficient evidence.	Insufficient evidence.	Insufficient evidence.	Insufficient evidence.	Insufficient evidence.	Insufficient evidence.	Insufficient evidence.

Figure 4: Principle assessment matrix according to NASA-STD-7009

	Verification*	Validation*	Input pedigree*	Result uncertainty*	Result robustness*	Use history	Management	People qualification	
Level	4	3	3	3	1	4	3	3	
Weight	0,7	0,7	0,5	0,5	0,5	1	1	1	
	Technical Review	Technical Review	Technical Review	Technical Review	Technical Review				
Level	2	3,5	3,5	3	2				
Weight	0,3	0,3	0,5	0,5	0,5				Overall Score
Total	3,4	3,15	3,25	3	1,5	4	3	3	
Threshold	3	3	3	3	3	4	4	3	1,5
	OK	OK	OK	OK	NOK	OK	WARN	OK	

* Total <-> Threshold: Gap<0,5 (OK); 0,5<=Gap<=1 (WARN); Gap>1 (NOK)

Figure 5: Assessment example with weak credibility according to NASA-STD-7009

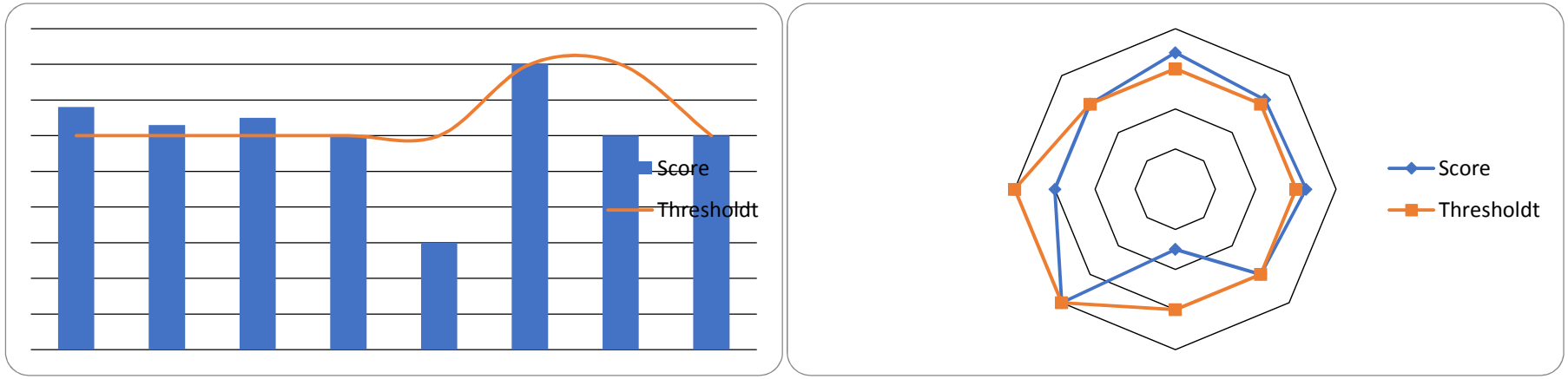

Figure 6: Graphic schema of example assessment

6. CONCLUSIONS

- The participation of the NoBos is going to be mandatory if we want to be able to certificate /re-certificate.
- Not all the requirements will be possible to be certificate through the simulation framework. For several reasons:
  - Not possible to be represented in the simulation framework (technical limitations)
  - The NoBos will not accept for safety reasons.
  - Not interesting from the cost/benefit ratio point of view
- The time issue regarding remote tests is impossible to solve
- Even if FW is not used for certification, it will be useful otherwise.

Assumption	Description
[C1]	A qualification and/or validation of the test system and the related simulation is only necessary in case of the usage in regards to standard conformity declarations and test of safety functionality.
[C2]	The reflecting the requirements and the corresponding acceptance by regulatory instances is not completely possible because of a lack of involvement in WP6
[C3]	The described process steps, rolls and artefacts could be merged or divided into sub artefacts as needed
[C4]	Detailed role descriptions and structure of documentation need to be defined in the simulation development project.

6.1 EXPERTS' FEEDBACK ON THE VIRTUAL CERTIFICATION PRINCIPAL

As WP6 activities progressed we have received feedback from experts from different areas related to certification. This feedback was provided by expertes during Advisory Board meetings and by experts from the Open Call S4R. Since this feedback was very enriching and the D6.1 was already closed we were sugested by the JU to reopen it and add this new information in the deliverabl. We decided to formaly gather it in a more formal way this feedback and for that matter we had a conference meeting with some experts. Below is a sample of the coments we received on our deliverable.

The TCMS is an essential subsystem of a rolling stock but it is not in itself subject to any authorisation. Increasing the amount of virtual testing vs field testing of the TCMS will facilitate the authorisation of rolling stock and reduce its cost and duration but this should not be considered a direct objective of the project.

The objective should be the development of reliable virtual testing of the TCMS and its applications. Once this is objective is reached and the reliability is confirmed (by an assessment, certification or accreditation body like for the ICE4 test system presented on the PowerPoint and not by authorities in charge of authorising rolling stock), it will be a task for the relevant authorities, and not for CTA/S4R or their successors, to take this output on-board for the evolution of the authorisation process of rolling stock.

The principles for the development and validation of a simulation described in chapters 4 and 5 of D6.1 are clear and constitute a good starting point to get the virtual testing recognised a reliable alternative to field test. D6.2 is also a good starting point for specifying the virtual testing equipment.

Note: ERTMS is mentioned in the document 6.1 § 2.1 as an example of product authorised on the basis of simulations. Simulations are used in the certification of a component of ERTMS, that is the on-board ETCS which is an Interoperability Constituent (I.C, i.e. a part of a subsystem that can be assessed independently from the subsystem). TCMS is currently not an I.C and consequently it is not assessed independently from the rolling stock. Considering the TCMS as an I.C may be an option for the future in case it is deemed appropriate, in order to permit the placing of the market of authorised and virtually tested TCMS.