Contract number: ITEA2 – 10039

Safe Automotive soFtware architEcture (SAFE)

ITEA Roadmap application domains:

Major: Services, Systems & Software Creation

Minor: Society

ITEA Roadmap technology categories:

Major: Systems Engineering & Software Engineering

Minor 1: Engineering Process Support

WP 5, WT 5.2

Deliverable D.5.2.c:

Final report including quantitative evaluation results for methods and tools of industrial needs

Due date of deliverable: 30/11/2014

Actual submission date: 03/10/2014

Start date of the project: 01/07/2011 **Duration:** 36 months

Project coordinator name: Stefan Voget

Organization name of lead contractor for this deliverable: Continental Automotive France

Editor: Lionel Guichard, Alexander Rudolph

Contributors: Philippe Cuenot

Version	Date	Reason
0.1	2014-10-03	Initialization of document
0.2	2014-10-30	Document layout updated after harmonization review
0.3	2014-11-23	Update with Result Integration
0.9	2014-11-27	Document finalization before release
1.0	2014-11-28	Final document submitted to SAFE

1 Table of contents

2 Executive Summary

The objective of WP5 (see SAFE FPP [5]) is a) to refine requirements for, b) provide feedback on and c) evaluate methods and tools developed in WP3 and WP4 as well as methodologies and application rules defined in WP6 in context of realistic industrial case studies.

Therefore, Continental automotive has proposed complementary use-cases assessed inside two independent organizations. These uses cases are supported by two main scenarios and two related sub-scenarios as it is depicted after.

One of the use-case is dealing with the ISO 26262 compliancy of an existing product, while the second one is more focusing on the concept phase and the overall safety process regarding the supplier chain of a shared development. Furthermore, as divisions are separated and business oriented, the tailoring of safety methods is necessary.

Hence, PowerTrain and Chassis&Safety divisions come up with the following main scenarios:

- Evaluation of an Engine Management product up to the functional safety concept
- Safety methods assessment for a new Electrical Brake product.

Best practices established during the evaluation will also be documented.

3 Evaluators Introduction

3.1 General description

This section introduces all uses cases perimeter in addition to their contribution to the Work Task 5.2 inside SAFE.

In order to identify the contribution of scenario regarding the WP5, all uses cases are tagged with a **SCxy** acronym that stands for **SCenario** number **x** with sub scenario **y** if needed.

3.2 Engine Management scenario

The objective of this scenario, an Engine Management System (cf. figure 1), will be to demonstrate the safety conformance of the eGas concept with the process defined in the ISO26262. This evaluation will be built using model based technology and the new safety analysis techniques, by comparing potentials benefits from actual experience in "standard" development.

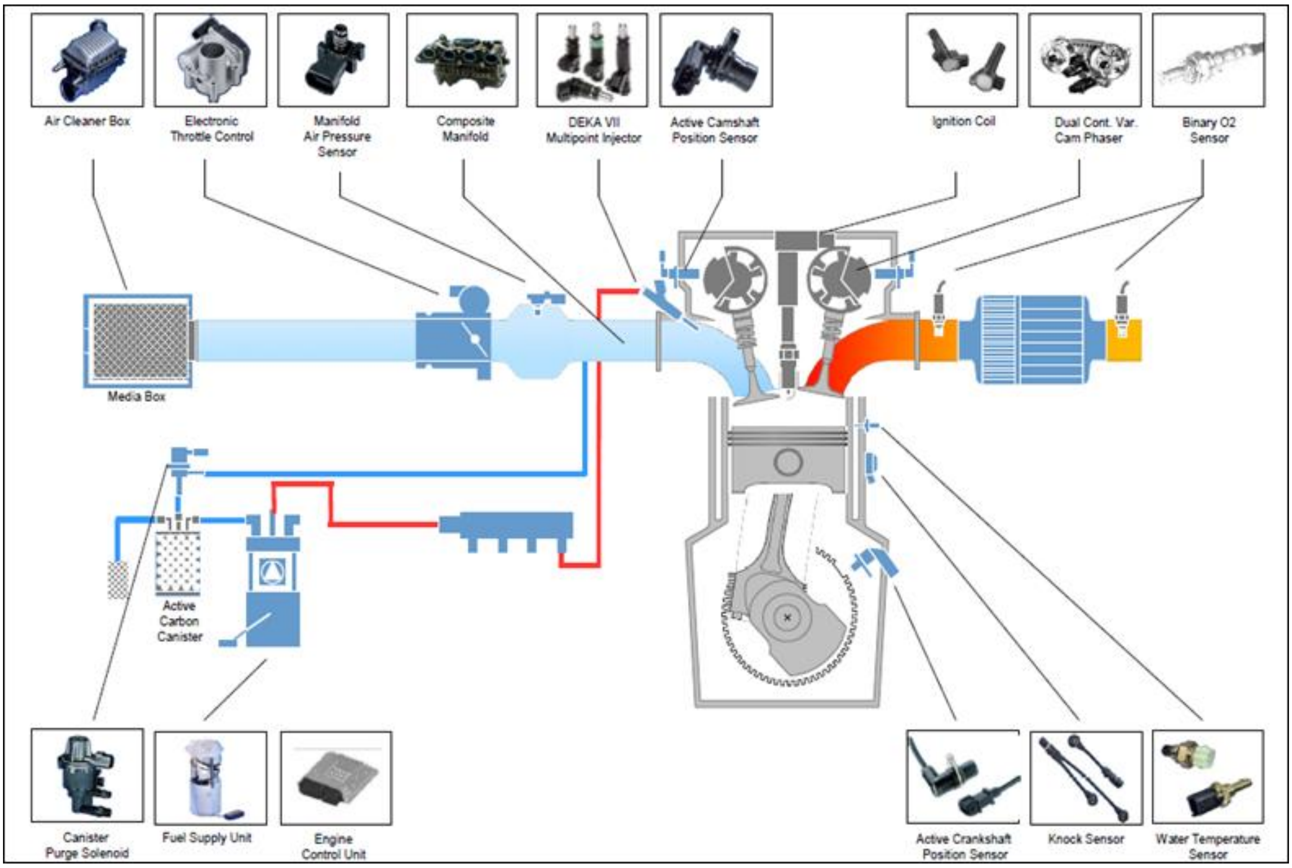


Figure 1

For information, the eGas concept is split in two parts; the torque control function as a hardware independent function; the hardware redundancy function included in the hardware platform (hardware and software driver). For reuse objective of hardware platform reuse, the hardware redundancy function is developed with generic approach capable to fulfill multi customer safety requirements.

Hence the proposed analysis will be performed as:

- The modeling of safety goals of the eGas safety, extracted from OEMs requirements, and then refined down to the level of deriving the hardware platform requirements
- The qualitative safety analysis based on functional architecture and failure modeling relying on the meta model implementation.

Then safety evaluation will be performed to demonstrate the diagnosis coverage using model generation of cut-set analysis and from error hazard occurrence.

The tool implementation of this demonstration will be supported by the PREEvision environment (Vector GmbH) including safety extension features and interoperability capabilities.

This scenario will be referred as **SC1** wherever it makes sense to identify its own contribution within the current document.

3.2.1 Annex E from ISO 26262 standard sub-scenario

As it serves as a reference for the ISO standard, this secondary scenario has been setup in order to act as a representative workbench for special investigation that wouldn’t have been possible within the EMS scenario due to its high level of complexity and missing features inside PREEvision.

Beforehand, this smart example was in particular used to validate a special routine supported by PREEvision as kind of metric that exports the dysfunctional model to HiP-HOPS[1]. This latter is able to realized fast and automatic fault tree or FMEA synthesis out of the dysfunctional model.

Hence the proposed analysis will be performed as:

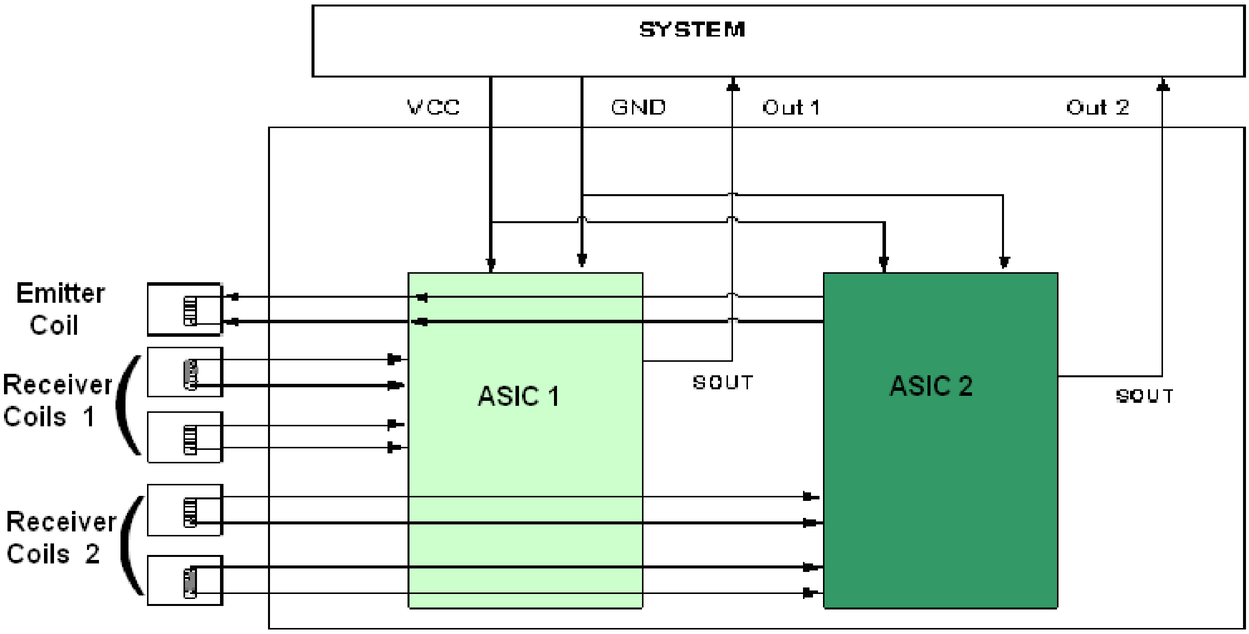
- Capture of architecture elements (system, hardware and software elements) according to Annex E content
- The qualitative safety analysis is performed on different architecture level (including FSC and TSC). The result helps to validate the routine developed by ATOS France

This scenario will be referred as **SC1a** wherever it makes sense to identify its own contribution within the current document.

[1] Hip-Hops is a tool developed by the Dependable Systems Research Group at the University of Hull.

3.2.2 Gear lever position sensor sub-scenario

This scenario completes the main scenario on the quantitative analysis aspect that is required by the ISO 26262. It deals with a gear box leaver position system that comes from another business unit inside Powertain. The leaver's position is dedicated to an automatic gearbox, and provided to the Traction control unit via 2 channels based on PWM according to the following hardware synoptic:



Hence the proposed analysis will be performed as:

- Quantitative safety analysis (hardware metrics computation)

Contrary to the regular method defined inside ISO26262, this analysis is using an alternative methodology proposed by WP3. Mainly, it defines a hierarchal approach that allows hardware metrics computation on hardware block level instead of hardware parts level.

Though early revision of PREEvision only supports hardware metric computation based on hardware parts, this evaluation has been realized anyhow with the help of a special adjustment.

This scenario will be referred as **SC1b** wherever it makes sense to identify its own contribution within the current document.

3.3 Braking System scenario

The objective of the second industrial scenario, as an Electrical Brake System (EBS), will be to improve the overall functional safety process for the development of the product:

1. Especially, the improvement and the definition of interfaces between requirements, architecture, design and its verification during development via Safety Analysis will be highlighted. The definition of the interfaces, the identification of functional and non-functional requirements, technical requirements, design limitations and preliminary architectural assumptions will be assigned to the different hierarchical levels such as vehicle, system or component.
2. As second perspective the representation of the vehicle and system level hazard analyses are considered as top-down entry point for early requirement elicitation and safety goal establishment.

The different elements necessary for this analysis will be modeled using PREEvision extension from WT4.3.

As concrete outcome, the definition of methods and guidelines, on how to support verification at the different design level with Safety Analysis, such as FMEA and FTA and to take safety credit according to ISO 26262 as it is depicted in Task 6.1.

The specific use case to be examined addresses the normal braking function and the antilock braking function of the system, comprising

- the detection of the driver's brake request with dedicated sensors,
- the processing the adequate brake torques and finally,
- the execution of the brake torques with dedicated actuators.

In particular, the graceful degradation concepts of the systems on functional and technical level are rather complex and may serve as ideal test bed for the SAFE platform. Due to the complexity only one degradation level shall be investigated in detail.

The objective of the use case is two-stepped:

1. Product-oriented: SAFE platform evaluation with normal braking function safety concept (this task 5.2)
2. Process-oriented: Implementation of ISO26262 by SAFE (ref. task 6.1)

As final result an evaluation report regarding integrated engineering based upon the SAFE platform shall give indications for the benefit on different levels of brake system design.

This scenario will be referred as **SC2** ("Integration of the FSM Process for an Electronic Brake System") wherever it makes sense to identify its own contribution within the current document.

3.4 Motivation and Argumentation

3.4.1 Development approach before SAFE

On one hand, the safety manager role and procedure are well established in Powertrain division. The engineering of the product itself is partitioned into respective system, hardware and software organization federated by top down process and controlled by a project quality engineer. The technical safety concept applied to the Engine Management product is based on the standardized eGas concept defined by the VDA consortium.

The safety goals and their related ASIL deduced from the hazard and risk analysis are performed by the car manufacturer and reviewed by Continental. This work is mainly based on EXCEL spreadsheet that is the basis for safety requirements enumeration.

The traceability of safety requirements and ASIL propagation is handled within DOOR's but it is almost manual work and could be error-prone.

As function development relies on the eGas concept, our focus for safety is put on hardware development thanks to Electronic FMEDA and overall system FTA analysis.

The FMEA, FMEDA, FTA safety analysis are helped by specialized tool such as FaulTree++ and/or EXCEL template with results are managed in spreadsheet. The traceability with safety requirements and their completeness is observed by human work.

The validation of non safety goals violation is based on huge and costly tests. These tests are performed on software and system product, as safety car reaction test assessed on vehicle, where the software and hardware are instrumented in order to inject fault and validate the failure mitigation of the safety mechanism. As a consequence, these tests are done late within the development and can report defect in coverage of safety mechanism missed during design concept phase despite systematic safety analysis approach.

Besides, each new modification of safety relevant functions implies a complete rework and a late campaign of tests to ensure non-violation of safety goals.

On the other hand, the engineering (management, DD, VV) process for brake systems is widely federated in terms of tooling.

The definition and stipulation of safety requirements, their consideration during design and eventual verification are heterogeneous processes, making system engineering rather difficult in terms of disciplines as configuration and change management, requirement management and verification/test management.

Since Safety engineering is widely predicated on system engineering, a lack of transparency and traceability is directly inherited, making it challenging in terms of

- Information retrieval during analysis
- "frontloading" of Safety requirements, constraints and objectives during synthesis

The expectation towards SAFE is a wider view on the integration of safety engineering in the system development process, in particular from a methodological point of view (what-to-do). The tooling itself, establishing a seamless framework can then be selected (how-to-do).

3.4.2 New approach

SAFE approach and platform is model based oriented. Due to the (semi-)formal representation of architecture element, it can be easily adapted to automate the early analysis of the designed product in order to follow the following descriptions.

The SAFE platform supports hazards analysis, handles relation to the corresponding safety goals with ASIL definition and automatic traces their related requirements for a product.

SAFE platform provides standardized means to build product models based on system definition until hardware and software architecture and links to implementation. It allows capability for interface and consistency check between elements assessed during design.

It provides an exhaustive coverage report of the safety goal until technical safety requirement, and a coverage report on function allocation out of the complete architecture.

Variability of the architecture supported by the SAFE platform allows ensuring a complete check of the product variant of the same family.

Based on a failure propagation model, the SAFE platform is able to automate and provide a complete report of failure and cut set analysis, and to generate the quantitative analysis as hardware metrics computed from hardware failure rate distribution. This would allow interactive safety in the loop analysis during design of new product. It would also facilitate the validation of the boundary condition on the hardware safety requirement during development by evaluating the impact of the failure of the respective element.

Eventually, It makes no doubt that the incorporation of Safety Engineering in the System Engineering process in terms of methodology and tooling shall enable all stakeholders to share their contributions more efficiently, eventually leading to a transparent process and an easier demonstration of product safety.

3.4.3 Expectations towards new approach

3.4.3.1 Benefits of SAFE:

The main benefit is a seamless methodology and tooling allowing closing the gap between system development and safety activities.

Among other things, SAFE provides a systematic and automatic coverage of the traceability starting from the safety goal until function allocation to either software or hardware disciplines. An automatic report of the traceability could be generated.

It allows an early qualitative analysis based on cut-set visualization and hardware quantitative evaluation of the safety concept architecture. This analysis can be automatically built from library component composed into the architecture to build the safety concept (functional and technical). The trace of the various architecture evaluation and failure mitigation can be documented and argued.

Furthermore, the results of the architecture evaluation will bring the initial safety requirement for software and hardware that are formally identified during the system design. This would facilitate the development and impact analysis at the component level development.

In addition the early hardware metrics assessment is based on functional failure allocation and budgeting that can then drive the hardware component development and failure rate distribution. In a second step, the allocation hypothesis is verified according to the architecture level. The impact of the hardware metrics calculation from electronic part is then facilitated as their contribution to the system failure is already bounded by the architecture decomposition view. The main gain expected is productivity for defining and verifying the safety concept of new architecture.

Finally it provides a centralized data set, based on formal model element, to generate the contribution to the safety case document and in particular to the justification of the design choice. This approach would also facilitate the reuse process based on variant management already bounded for the safety aspect by preliminary safety architecture assessment.

The (semi-) formal document introduces further capabilities for interchanging element between customer and supplier. It shall largely improve the quality of the final product, as assumptions are verified by formal exchange of model element including boundary condition, as for example the failure model results or the failure information (Failure rate, propagation impact, …).

In the long run, closing the safety case and demonstrating compliance to ISO26262 will significantly be enhanced by the capability to shed some light on the system design embedded in its safety objectives and verification/analysis campaigns and results.

3.4.3.2 Drawbacks of SAFE:

This new approach requires people experienced in model based development. Indeed, It requires an additional effort for training people to skill them to model based environment tool like PREEvision much more complex today than simple EXCEL spreadsheet utilities.

Strong effort shall be spent on tool environment as PREEvision isn’t yet seamless integrated within the overall product development chain.

Hence, turning the tool complexity into a more user friendly interface could facilitate technical exchange between disciplines and engineering design responsibilities.

The effort for maintenance of architecture model shall not be ignored, especially the first ticket to build the initial model (that then will bring the pay back on the overall concept).

Besides, if the model itself is the item of specification under review it has to be ensured that the implementation exactly follows the model. The approach has therefore to be centralized between design and development. Due to its integrative nature, this is no tooling issue, however it might be challenging on personal level.

3.4.4 Evaluation phase SC1

The final work product regarding the Engine management scenario (SC1) relates to the modeling of the functional safety concept with a special focus on two critical function, alike the engine position and speed determination, and the related qualitative safety analysis.

By the way, the overall safety concept (FSC and TSC) of the Annex E sub-scenario (SC1a) is modeled and its focus was to perform the quantitative analysis of the TSC (Hardware and software) with HiP-HOPS.

Besides, the sub-scenario (SC1b) related to the gear box leaver position sensor deals with quantitative safety analysis, in other words hardware metrics computation.

Eventually, the process proposed by SAFE shall be evaluated according the EMS scenario.Therefore, the complete work product of the scenarios has been separated into 3 parts as follows:

3.4.4.1 Work Product WP52_1: Model definition

This work product will be the model of the existing safety concept used in engine management systems application. This model will be captured in the WP4 platform based on WP3 meta model of the existing technical safety concept use in engine management systems. The tool environment selected is PREEvision.

It should contain, hazard and risks analysis, safety goals, safety requirements, architecture description of functional safety concept, technical safety concept.

It also includes feature for model consistency checks performed on requirements and architecture.

3.4.4.2 Work Product WP52_2: Safety analysis

This work product represents the safety evaluation of the above safety concept. It is built on the capture of the failure mode of the respective safety element and the application of the propagation mechanism developed in the SAFE project. A qualitative safety analysis will be performed on the the functional and technical safety concept view, and analysis results as cut-set visualization will be correlated between the two abstractions levels. Furthermore a final hardware quantitative analysis will be performed to perform an “early” evaluation of hardware metrics as required by the safety standard.

These analyses will be performed on the top of PREEvision extension or using connection established in PREEvision to permit specialized safety analysis.

3.4.4.3 Work Product WP52_3: Variability

The safety concept model element will be extended to support the different variant in the system, and hardware architecture (150% model). The variation will be capture and configured to allow resolution of the variant by the resolver link to tool environment. Then impact on the above WP521_1 and WP521_2 will be assessed to check completeness of the analysis on the 150% model and/or the application for the product variant generated (safety concept) and the associated safety analysis.

The environment selected is still PREEvision.

3.4.5 Evaluation phase SC2

As far as the Braking scenario (SC2) is concerned, the objectives can be divided into a product-oriented and a process-oriented objective. The project-oriented objective deals with the evaluation of the SAFE platform by reference to a safety concept of a by-wire brake system. Regarding the process-oriented purpose the implementation of ISO 26262 by SAFE should be evaluated.

The product-oriented objective can be divided into 3 hierarchical parts which are related to different PREEvision versions:
[1] WT 5.2.2.a: The object under evaluation is PREEvision 6.0.1
[2] WT 5.2.2.b: The object under evaluation is PREEvision 6.5.0
[3] WT 5.2.2.c: The object under evaluation is PREEvision 7.0.0

The evolution and progress of the evaluation itself is briefly summarized in the “project” column of Table 2. The a,b,c notations refer to the above-mentioned PREEVision extensions.

3.5 Implementation

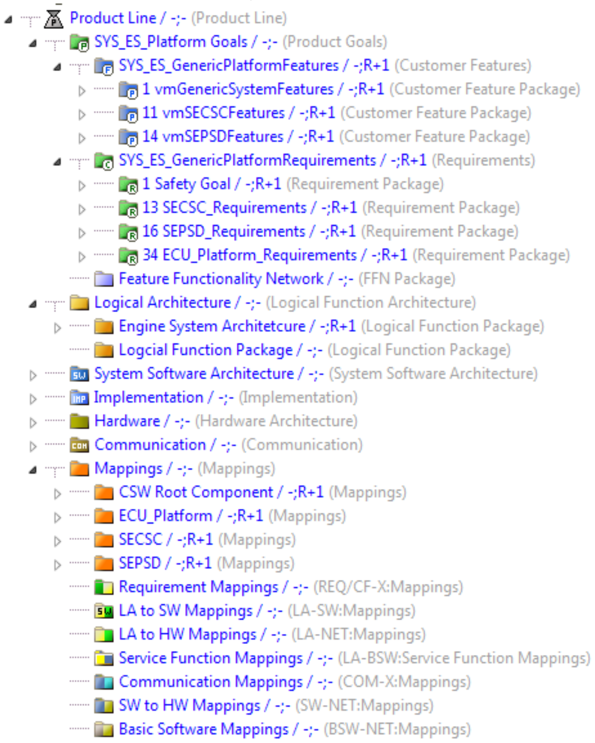
This section deals with the current setup of the evaluators in addition to their dependencies on other work tasks and the items they cover. At last, the actual progress of each evaluator is reported.

First and foremost, let’s focus on each evaluator’s setup within the context of SAFE, as detaile in the sections below.

3.5.1 EMS scenario setup

This scenario has a special focus on the safety assessment of two functions picked from the engine management system. This function is already in serial production and has been developed according to the eGas concept which is the state of the art for safety concept.

To do so the safety requirements are imported from Door’s into PREEvision as follows:



- Product Line / -;- (Product Line)
  - SYS_ES_Platform Goals / -;- (Product Goals)
    - SYS_ES_GenericPlatformFeatures / -;R+1 (Customer Features)
      - 1 vmGenericSystemFeatures / -;R+1 (Customer Feature Package)
      - 11 vmSECSCFeatures / -;R+1 (Customer Feature Package)
      - 14 vmSEPSDFeatures / -;R+1 (Customer Feature Package)
    - SYS_ES_GenericPlatformRequirements / -;R+1 (Requirements)
      - 1 Safety Goal / -;R+1 (Requirement Package)
      - 13 SECSC_Requirements / -;R+1 (Requirement Package)
      - 16 SEPSD_Requirements / -;R+1 (Requirement Package)
      - 34 ECU_Platform_Requirements / -;R+1 (Requirement Package)
    - Feature Functionality Network / -;- (FFN Package)
  - Logical Architecture / -;- (Logical Function Architecture)
    - Engine System Architetcure / -;R+1 (Logical Function Package)
    - Logcial Function Package / -;- (Logical Function Package)
  - System Software Architecture / -;- (System Software Architecture)
  - Implementation / -;- (Implementation)
  - Hardware / -;- (Hardware Architecture)
  - Communication / -;- (Communication)
  - Mappings / -;- (Mappings)
    - CSW Root Component / -;R+1 (Mappings)
    - ECU_Platform / -;R+1 (Mappings)
    - SECSC / -;R+1 (Mappings)
    - SEPSD / -;R+1 (Mappings)
    - Requirement Mappings / -;- (REQ/CF-X:Mappings)
    - LA to SW Mappings / -;- (LA-SW:Mappings)
    - LA to HW Mappings / -;- (LA-NET:Mappings)
    - Service Function Mappings / -;- (LA-BSW:Service Function Mappings)
    - Communication Mappings / -;- (COM-X:Mappings)
    - SW to HW Mappings / -;- (SW-NET:Mappings)
    - Basic Software Mappings / -;- (BSW-NET:Mappings)

Customer Features

System requirements including safety requirements

Preliminary architecture

Mapping between requirements and preliminary architecture

In the meantime, the artifacts corresponding to the hazards and risk analysis were created inside PREEvision. Basically, two safety goals were almost modeled. The first one aims at avoiding an unintended engine start or running while the second avoids an unintentional acceleration. Though both safety goals have been created for the purpose of checking the capabilities of PREEvision, we put a special focus on the second one.

Next, the traceability concept is going to be applied on the model and verified not from safety goals refinement to hardware and software requirements but as well on different architecture allocation.

To conclude, the functional model captured within PREEvision is exported to Hip-HOPS (cf. Annex E regarding model conversion process), in order to perform a qualitative safety analysis based not only on the system topology but on its failure annotation as well.

3.5.2 Annex E scenario setup

This scenario aims at validating the routine[2] developed within PREEvision that performs the dysfunctional model export to HiP-HOPS. This dysfunctional model is composed of the model topology and the failures annotation.

To do so, the functional model of Annex E is first captured under PREEvision as follows:

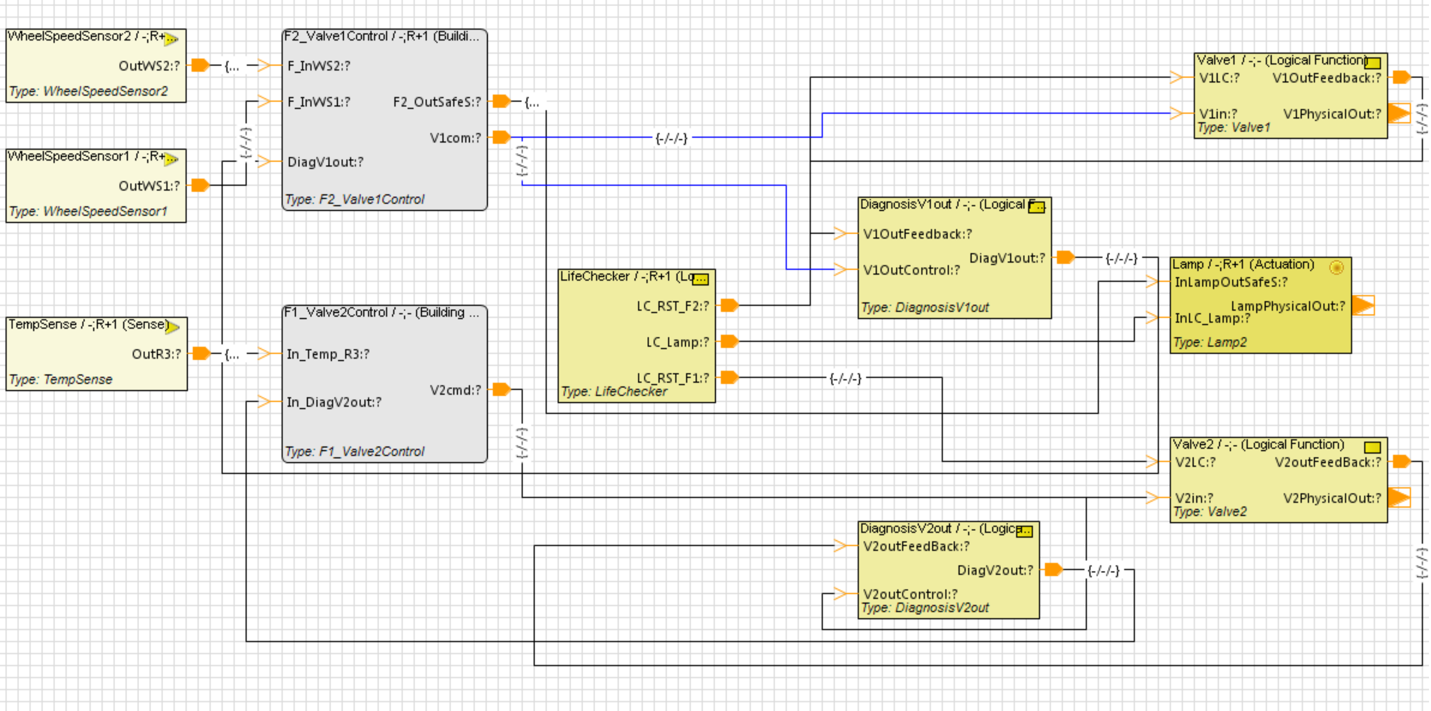
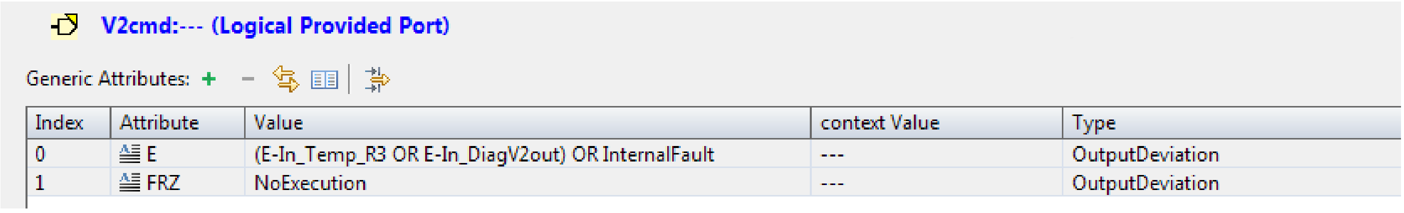


Figure 2: Functional Model

In a second step, all the blocks of this architecture are annotated via the use of generic attributes (cf. figure 3), with their respective failures in a textual manner as required by HiP-HOPS.

[2] Named as metric within PREEvision but used instead for a better understanding.



V2cmd:--- (Logical Provided Port)

Generic Attributes: + −

Index	Attribute	Value	context Value	Type
0	E	(E-In_Temp_R3 OR E-In_DiagV2out) OR InternalFault	---	OutputDeviation
1	FRZ	NoExecution	---	OutputDeviation

Figure 3

As a result, HiP-HOPS provides either a deductive or an inductive view of the failure synthesis in addition to the cut sets and their respective order.

Second, the technical safety architecture has been captured under PREEvision. It shall be noticed that the hardware and software architectures are captured on a logical level which is enough for the quantitative analysis. As far the hardware architecture is concerned, it means that hardware parts are not modeled but their failures are only taken into consideration.

In the same way, the functional architecture is refined, the failures defined on the technical level come more detailed.

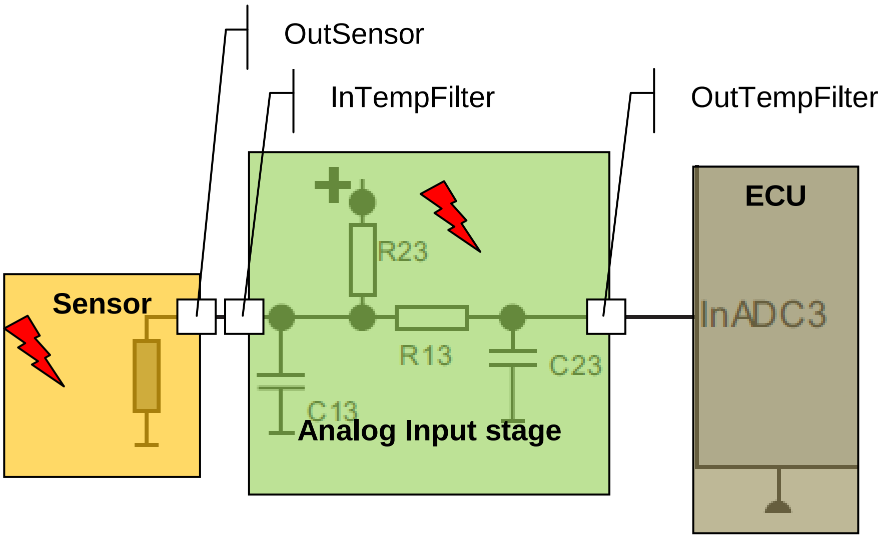


Figure 4: Technical Level of Architecture

Hence, we can define the output failures classes available on each logical hardware block, depending on the hardware parts internal failures. The table that follows contains the failures according to the previous picture:

Component	Related failures classes	Failures description
Sensor	OC	Opened circuit
Sensor	SC	Shortcut circuit
Sensor	DRIFT	Output is drifting

Analog input stage	SCG	Shortcut to ground
Analog input stage	SCB	Shortcut to power supply
Analog input stage	OC	Opened circuit

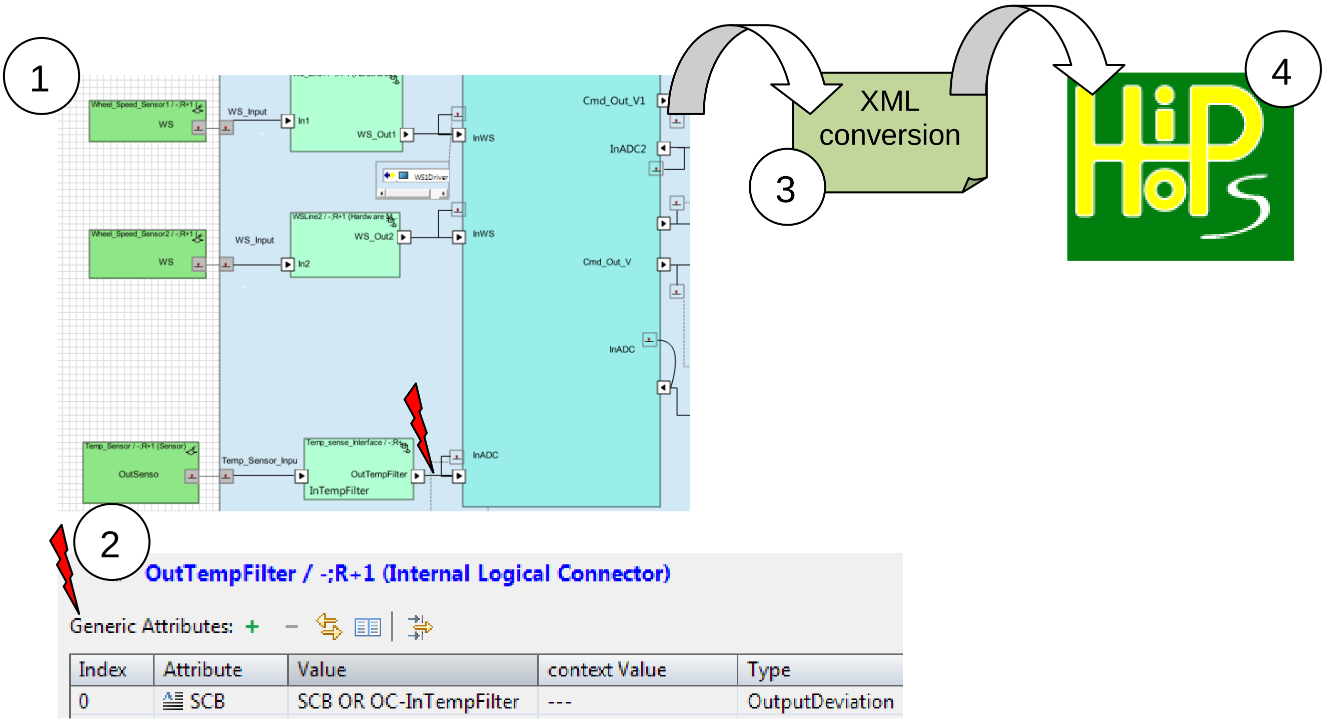
Table 1: Failure Summary

For example, the opened failure (OC) related to the sensor, could lead to a shortcut to the power supply at the output (OutTempFilter) of the Analog input stage. Moreover, the internal shortcut (SCB) of Analog input stage could lead also to the same failure.

Thus, the HiP-HOPS equation is expressed as follows:

SCB-OutTempFilter = SCB-Analog Input Stage OR OC-InTempFilter

Eventually, the Fault trees of the technical architecture could be synthesized within HiP-HOPS according to the following process:



OutTempFilter / -;R+1 (Internal Logical Connector)

Index	Attribute	Value	context Value	Type
0	SCB	SCB OR OC-InTempFilter	---	OutputDeviation

Figure 5: Hip-HOPS Process

<u>Process steps:</u>

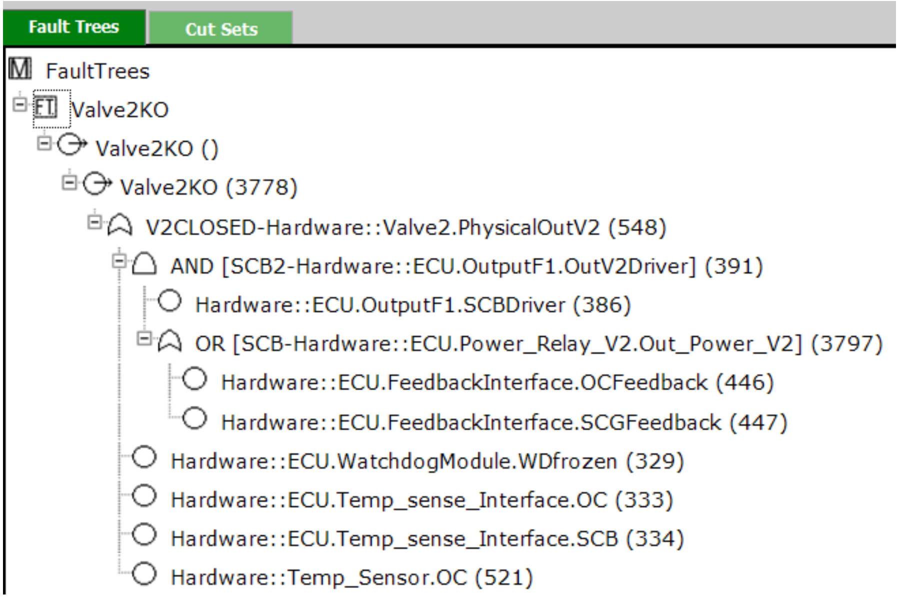
1: Functional safety model

2: Failure annotation

3: Model conversion via XML

4: FTA, FMEA and cut-sets generation thanks to HiP-HOPS

- Instance of process steps



```
FaultTrees
  Valve2KO
    Valve2KO ()
      Valve2KO (3778)
        V2CLOSED-Hardware::Valve2.PhysicalOutV2 (548)
          AND [SCB2-Hardware::ECU.OutputF1.OutV2Driver] (391)
            Hardware::ECU.OutputF1.SCBDriver (386)
            OR [SCB-Hardware::ECU.Power_Relay_V2.Out_Power_V2] (3797)
              Hardware::ECU.FeedbackInterface.OCFeedback (446)
              Hardware::ECU.FeedbackInterface.SCGFeedback (447)
          Hardware::ECU.WatchdogModule.WDfrozen (329)
          Hardware::ECU.Temp_sense_Interface.OC (333)
          Hardware::ECU.Temp_sense_Interface.SCB (334)
          Hardware::Temp_Sensor.OC (521)
```

Figure 6: Fault Tree View in HiP-HOPS

3.5.3 Gear box leaver position sensor setup

This scenario has been especially introduced in last year of the SAFE project in order to cope with the delay accumulated on PREEvision regarding the quantitative safety analysis feature. Nevertheless, as the bill of material is smaller than an EMS, evaluation and conclusion are easier to be drawn.

Hence, the purpose of this scenario is to evaluate the hardware metrics computation methodology as proposed by the alternative 1 within the workpackage WP3.3, in addition to the associated process. This scenario has still a particular interest has it deals not only with the hardware metric computation on hardware part level, which is the current method described within ISO standard, but also on the hardware block level which is an alternative proposed by Valeo.

To do so, one of the two safety goals has been selected and captured inside PREEvision in addition to its respective safety mechanism artifacts.

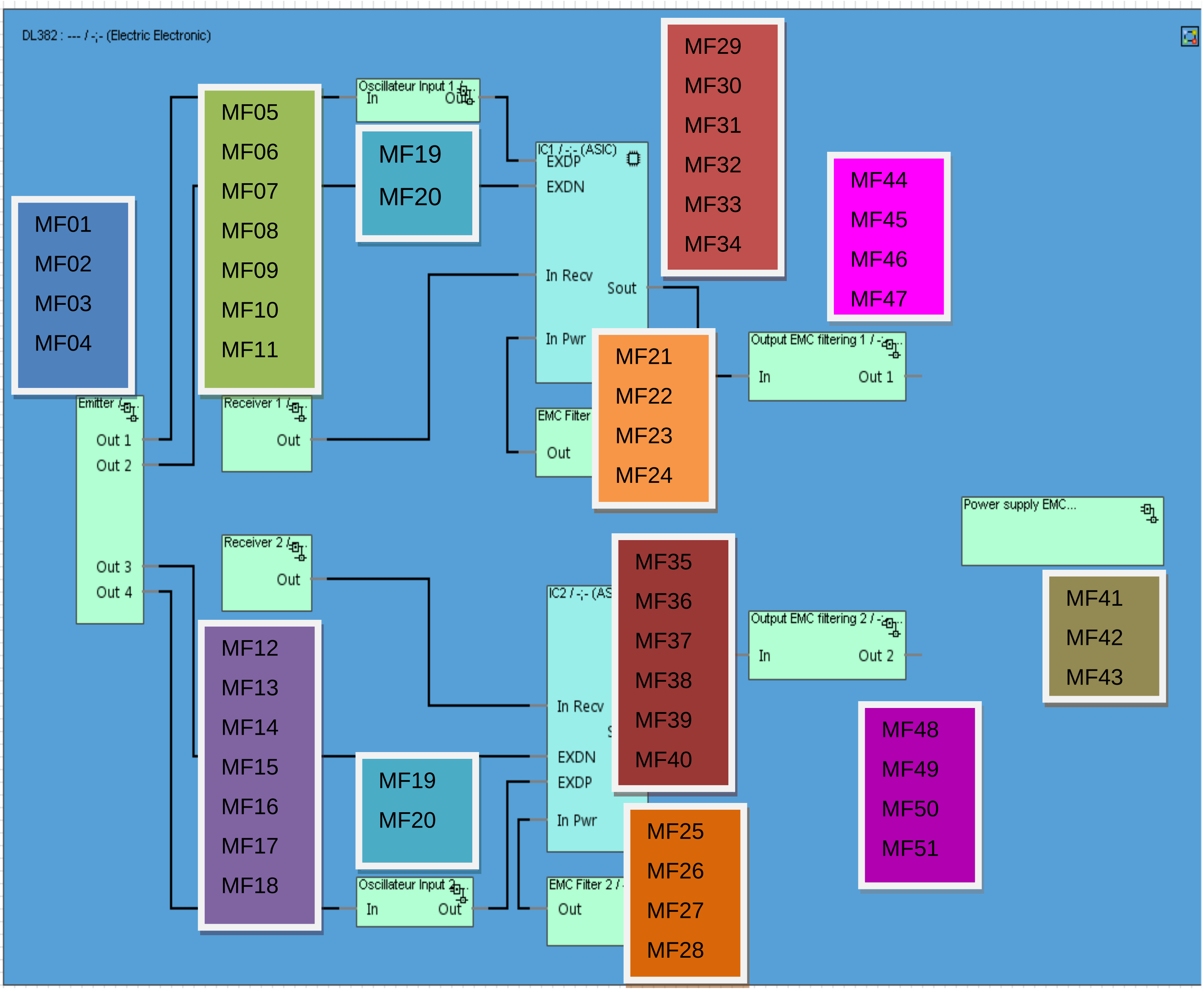
This safety goal is expressed as follows: “If one channel is detected as faulty, the sensor shall not deliver an erroneous plausible signal on the other channel”.

The hardware schematic is captured on the hardware logical level. In other words, it means that hardware parts are aggregated by functionality.

In a second step, the malfunctions that have been identified during the preliminary qualitative safety analysis and mapped to the respective hardware blocks and classified (e.g. single point fault, multiple point fault, or residual point fault), according to their possible involvement in a safety goal violation.

The hardware parts with their failure rate, their failure mode and distribution are captured under PREEvision.

Regarding our scenario, 51 malfunctions were identified and mapped to the corresponding hardware block level under PREEvision environment:



Then, the failure rate related to the top malfunction is determined according to the contribution of the failure modes determined on hardware part level.

For instance, if we consider one Receiver, internal failures are bound to local malfunction according to the following table.
Though the receiver is composed of two identical coils and two resistors, only one set is described.

Hardware parts related to Receiver 1	Failure mode	FIT	Distribution	Event FIT	Malfunction
Coil1	opened circuit	0,17	10,00%	0,02	MF05
	shortcut to ground	0,17	10,00%	0,02	MF06
	shortcut with another coil	0,17	10,00%	0,02	MF07
	internal shortcut	0,17	30,00%	0,05	MF08
	shortcut to Vdd	0,17	10,00%	0,02	MF09
	shortcut with emitter	0,17	30,00%	0,05	MF10
Resistor 1	Open circuit	0,65	40,00%	0,26	MF05
	Drift	0,65	60,00%	0,39	MF11
Resistor 2	Open circuit	0,65	40,00%	0,26	MF05
	Drift	0,65	60,00%	0,39	MF11

Table 2: e-fmea

∑ FIT per malfunction

Malfunction	FIT	SG violation	Classification	Safety Mechanism	Coverage	Latent fault (FIT)
MF05	1,07	Y	MPF	SM5	99%	0,010668
MF06	0,03	Y	MPF	SM6	99%	0,000348
MF07	0,00	N	SF	N/A	N/A	N/A
MF08	0,10	Y	MPF	SM8	99%	0,001044
MF09	0,03	Y	MPF	SM9	99%	0,000348
MF10	0,10	Y	MPF	SM10	99%	0,001044
MF11	0,00	N	SF	N/A	N/A	N/A

Table 3: Quantitative FMEDA at hardware block

Eventually, the hardware metrics required by ISO 26-262, namely SPFM and LFM are computed in a conservative manner according to method proposed inside WP331. Mainly, only failures mode of safety related hardware parts that are involved in a malfunction on higher level are considered for the computation of the total failure rates ($\sum \lambda_{SR,HW}$).

3.5.4 Braking scenario setup

The brake system scenario in terms of

- Scope and objectives
- Work products and usage for evaluated
- Results incl. Feedback
- Summary and Conclusion

is completely described in the technical Report “WT 5.2.2 Evaluation Scenario - Electrical Brake System” [15]. In the following, it is briefly described.

The general system used for evaluation is depicted in 7 below from a rather hydraulic point of view. It is the MKC1 brake system which is currently under series development.

Three ground rules shall apply for evaluation:

1. The evaluation shall comprise the entire development lifecycle of the system.
2. The evaluation shall only be based on series artefacts AND not make use of any sideways.
3. The evaluation shall comprise selected and agreed SAFE project requirements.

The scope is wider than depicted and includes also the functional behavior of the system in terms of the service brake function and the antilock brake function.

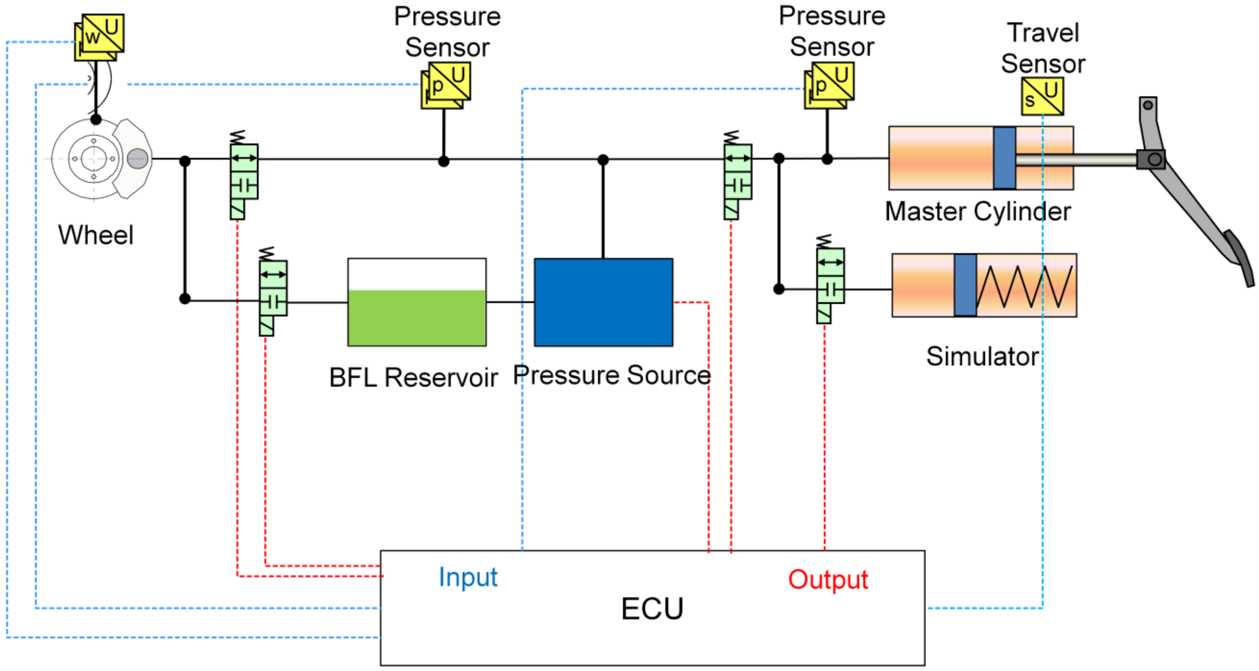


Figure 7: General Brake System used for Evaluation

As described in [15], PREEVision including its extensions as provided to the SAFE project is used as integrated frontend for evaluation. In Figure 8, the general evaluation objective is summarized. Is is three-stepped:

1. INPUT: The indicated artefacts are generated from series development and submitted as evaluation input.
2. EVALUATION: The artefacts are applied to the framework and it’s the general usability in particular in terms of safety issues is assessed. Base shall
3. OUTPUT: The fulfillment in terms of the agreed SAFE project requirements is documented.

A general modeling guidance [19] is generated in order to demonstrate how the model integration has been done and can be maintained.

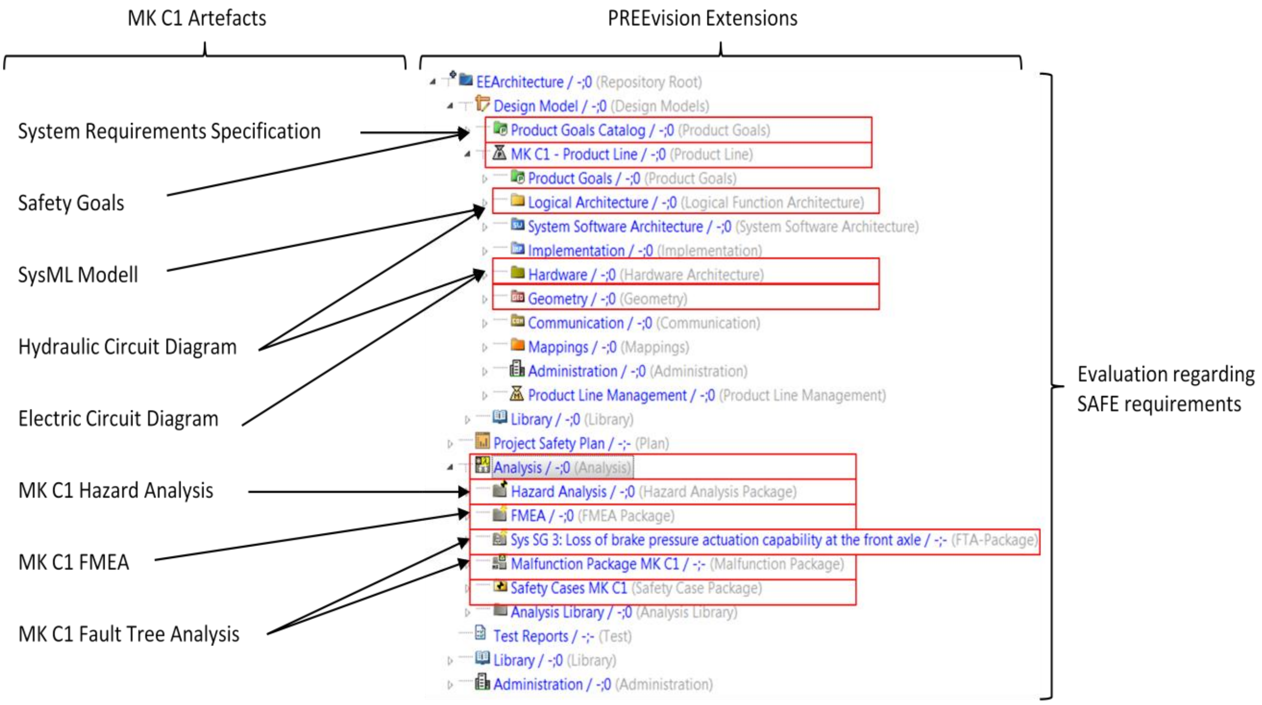

MK C1 Artefacts
PREEvision Extensions
System Requirements Specification
Safety Goals
SysML Modell
Hydraulic Circuit Diagram
Electric Circuit Diagram
MK C1 Hazard Analysis
MK C1 FMEA
MK C1 Fault Tree Analysis
EEArchitecture / -;0 (Repository Root)
Design Model / -;0 (Design Models)
Product Goals Catalog / -;0 (Product Goals)
MK C1 - Product Line / -;0 (Product Line)
Product Goals / -;0 (Product Goals)
Logical Architecture / -;0 (Logical Function Architecture)
System Software Architecture / -;0 (System Software Architecture)
Implementation / -;0 (Implementation)
Hardware / -;0 (Hardware Architecture)
Geometry / -;0 (Geometry)
Communication / -;0 (Communication)
Mappings / -;0 (Mappings)
Administration / -;0 (Administration)
Product Line Management / -;0 (Product Line Management)
Library / -;0 (Library)
Project Safety Plan / -;- (Plan)
Analysis / -;0 (Analysis)
Hazard Analysis / -;0 (Hazard Analysis Package)
FMEA / -;0 (FMEA Package)
Sys SG 3: Loss of brake pressure actuation capability at the front axle / -;- (FTA-Package)
Malfunction Package MK C1 / -;- (Malfunction Package)
Safety Cases MK C1 (Safety Case Package)
Analysis Library / -;0 (Analysis Library)
Test Reports / -;- (Test)
Library / -;0 (Library)
Administration / -;0 (Administration)
Evaluation regarding SAFE requirements

Figure 8: Modelling Objectives: Input-Doing-Output

The precise input is summarized in Table 22 below.

ID	Type of Input		Format of Input	Project	See Details in
/1/	System Requirements Specification	Concept	MKS Export -> MS Excel	a	[16]
/2/	Safety Goals	Concept	MS Excel	a	[16]
/3/	SysML Modell	Design	IBM Rhapsody	a	[17]
/4/	Hydraulic Circuit Diagram	Design	MS Power Point	a	[17]
/5/	Electrical Circuit Diagram	Design	MS Power Point (Architecture), Zuken (Circuit Diagram)	a	[17]
/6/	MK C1 Hazard Analysis	Concept	MKS Export -> MS Excel	a	[16]
/7/	MK C1 FMEA (Failure Net)	Analysis	APIS IQ Export -> MS Excel	a	[16]
/8/	MK C1 Fault Tree Analysis	Concept	Isograph Reliability Workbench	b	[18], [15]
/9/	MK C1 FMEDA (HW Metrics)	Analysis	Zuken (circuit data), Failure Modes, etc	c	[16]

Table 2: Detailed Input for Evaluation

As can be seen in the third column, their integration to the evaluation scenario grew along with the capabilities and maturity of the PREEVision extensions.

3.5.5 Dependencies

All the work-products developed in other work tasks but applied in the different scenarios of the current work task WT5.2 are the following:

- WT3_1_1_Safety_goals_Modelling
- WT3_1_2_Safety Requirements Expression
- WT3_1_3_Safety_Case_Generation
- WT3_2_1_System_and_Software_Models_Enhancement
- WT3_2_2_Hardware_Modeling
- WT3_3_1_Failure_and_cutsets_analyses
- WT4_3_PREEVision_Extension
- WT3_4_Variant_Management(1)
- WT6_1_Methodology_Definition

(1): This work task dependence only concerns the engine management system scenario (SC1).

3.5.6 Final implementation of the evaluators

3.5.6.1 EMS scenario final implementation

First of all, the EMS model has been captured in PREEvision V5.5.2. The safety requirements have been imported from DOORS into PREEvision V5.5.2 . A set of rules for traceability verification have been created in PREEvision language. So, the links has been successfully verified on requirements traceability (from safety goal to technical requirements) and architecture allocation (requirements allocation to architecture elements).

Though, this part was not re-evaluated according to earlier release of PREEvision, it shall be noticed that the investigation realized on the example by PREEvision 7 brings a lots of improvement especially on the safety goals definition and their refinement until technical safety requirements, but also on the traceability safety rules that are natively embedded.

The hazard and risk analysis have been evaluated two times. One time on the PREEvision version 6.0, where several deviations were reported not only according to Continental's expectations but also with the SAFE meta-model's requirements. Eventually, a fast evaluation loop was performed on PREEvision 7 that demonstrates the fulfillment of the missing requirements.
Secondly, the functional safety concept of the EMS was annotated with the failures with a special focus on the engine position speed and speed determination, besides the driver pedal input item. In the same way of qualitative safety analysis of Annex E, the model of the FSC was synthesized with HiP-HOPS.
As we considered only a part of the item for the dysfunctional model, it wasn't possible to prove the whole conformance of the e-gas concept. However the focus was put on two safety relevant function that need to be monitored according to the e-gas safety concept

If we assume that the engine management system implementation relies on a 3 layers approach. That is to say, one functional, a second one that monitors the first one and a third one that monitors hardware error, we have demonstrated the influence of the e-gas concept by introducing step by step the different layers within the architecture.

Actually we successively obtained the following results:

Cut-sets / Layers	1st order cut	2nd order cut independent errors	2nd order cut uncovered error	3rd order cut uncovered error(s)	Total
L1	11	0	30	66	107
L1 + L2	0	4	27	64	95
L1 + L2 + L3	0	4	0	27	31

Lx corresponds to the three layers described above. First order cuts are already limited by the diagnosis available on the layer 1.
By adding the layer 2, first order cuts are deleted. In fact they are turned into second order either by combination with each other (independent errors) or by coverage by layer two elements (uncovered error). By adding the layer 3, the cuts get one order more. Second order cuts become third order.

Eventually, the model of the TSC of the engine management system was captured under PREEvision but it remains incomplete for two main reasons. The first one concerns the delay accumulated on PREEvision while the second one deals with the difficulty to see the system as a white box, and it especially concerns the way to model the software in order to define the right annotations for the failure propagation.

However, the concept was evaluated on the Annex E that is described in the next section.

Due to accumulated delays on previous topics evaluation, it wasn't possible to perform the variability evaluation.

3.5.6.2 Annex E scenario final implementation

The functional and the technical safety concept system of the system described in Annex E have been captured under PREEvision 6.5.x (originally implemented on the 6.5.2) and eventually migrated to release 7.0.

This model is annotated with the related failure on the functional and technical architecture's level.

Hence the safety analysis have been successfully completed on the model with the help of HiP-HOPS and the plug-in developed as a metric.

As the features to perform FTA and to model malfunctions were implemented late in PREEvision, the Fault tree analysis of the FSC has been captured inside PREEvision.

3.5.6.3 Gear box leaver position sensor final implementation

As PREEvision 7.0 only comes with the hardware metric computation on hardware part level (Atlernative 2 depicted D331), the computation method was preliminary checked according to the exemple provided, which is no more than the Annex E.

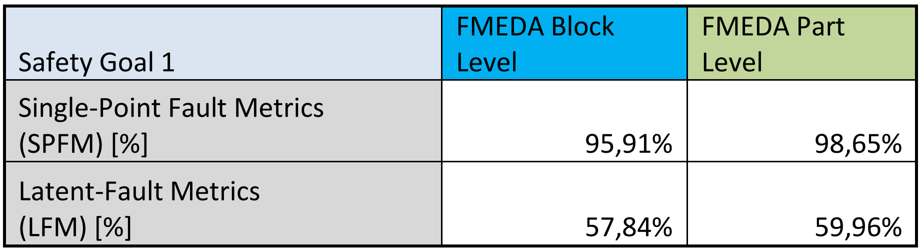
In order to evaluate the hardware metric on hardware block level (Alternative 1 depicted in D331), a temporary workaround was found in order to cope with the following restriction:

- Only one Malfunction could be mapped to an hardware component

This issue is in particular a blocking point for the Alternative 1 evaluation, as failure mode of an hardware component are bound to the top malfunctions defined on hardware block level.

Secondly, the hardware metric computation on hardware block was setup within Excel not only for method evaluation, but also to build a basis for later comparison after implementation inside PREEvison.

Finally, the hardware metric computed inside PREEvision didn't show any difference compared to the Excel sheet. Of course, the results are worse compared the project's (cf. Figure 9) ones but it was predictable according to computation methodology.



Safety Goal 1	FMEDA Block Level	FMEDA Part Level
Single-Point Fault Metrics (SPFM) [%]	95,91%	98,65%
Latent-Fault Metrics (LFM) [%]	57,84%	59,96%

Figure 9 : metrics results at block vs metrics results from project

3.5.6.4 Braking scenario final implementation

3.5.6.4.1 *Design Space*

The functional/technical model for brake system scenario as generated from the evaluation inputs /3/, /4/, /5/ includes the following parts:

1. Item Definition for Brake System (Figure 9)
2. Brake System Model (Figure 10)
3. Functional Description of Brake System (Figure 11)

In general, the scope of Figure has been slightly expanded towards the entire brake architecture incorporating all wheels. Moreover the vehicle context of the brake system is part of the model in order to capture functional consequences.

As can seen, the level of detail is rather high, allowing in-depth evaluation of the PREEVision Extension against the selected project requirements.

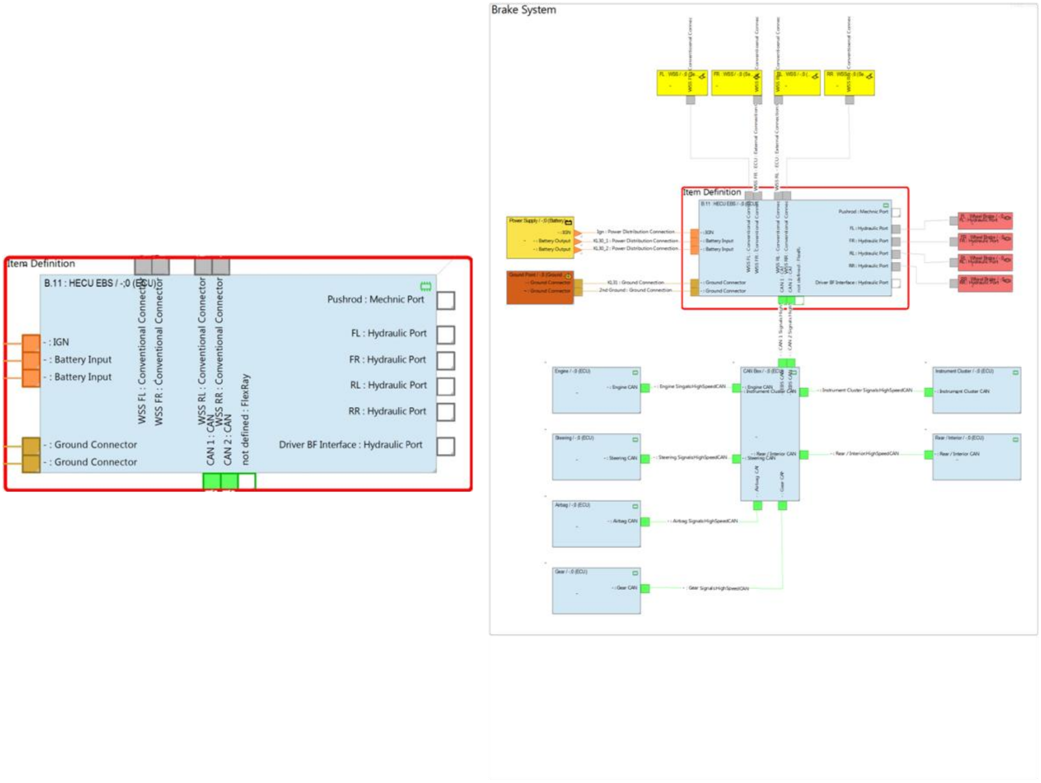


Figure 9: Item Definition for Brake System /3/

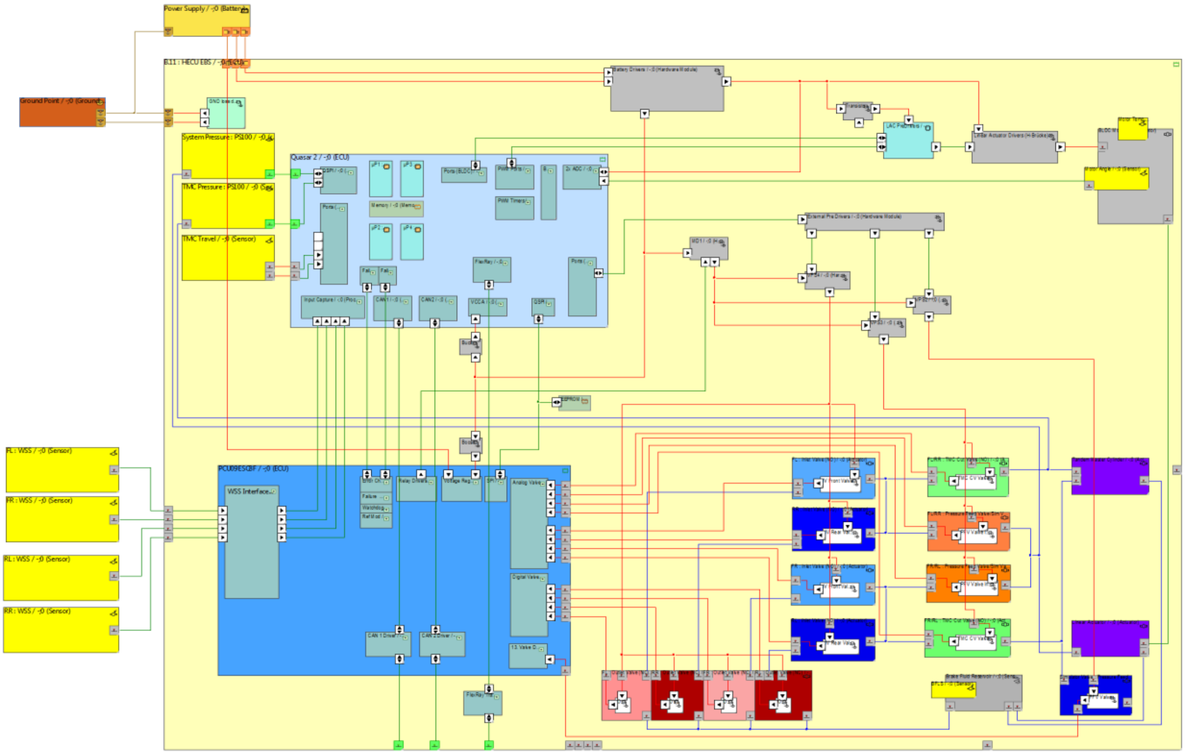

Power Supply / -;0 (Battery)
B.11 : HECU EBS / -;0 (ECU)
Ground Point / -;0 (Ground)
GND board
System Pressure : PS100 / -;0
TMC Pressure : PS100 / -;0
TMC Travel / -;0 (Sensor)
Quasar 2 / -;0 (ECU)
QSPI / -:0
Ports (BLDC)
PWM Ports
PWM Timers
2x ADC / -:0
Memory / -:0
Ports
Fail
FlexRay / -:0
Input Capture / -:0
CAN1 / -:0
CAN2 / -:0
VCCA / -:0
QSPI
EEPROM
Battery Drivers / -:0 (Hardware Module)
Transistor
LAC PreDrivers
Linear Actuator Drivers (H-Brücke)
Motor Temp
Motor Angle / -:0 (Sensor)
External Pre Drivers / -:0 (Hardware Module)
MD1 / -:0
VPS4 / -:0
VPS2 / -:0
VPS3 / -:0
FL : WSS / -;0 (Sensor)
FR : WSS / -;0 (Sensor)
RL : WSS / -;0 (Sensor)
RR : WSS / -;0 (Sensor)
PCU09ESCBF / -;0 (ECU)
WSS Interface
Failure
Watchdog
Ref Mod
Relay Drivers
Voltage Reg
SPI
Analog Valve
Digital Valve
13. Valve D
CAN 1 Driver
CAN 2 Driver
FlexRay Tra
FL : Inlet Valve (NO) / -:0 (Actuator)
IV Front Valve
IV Rear Valve
FR : Inlet Valve (NO) / -:0 (Actuator)
FL/RR : TMC Cut Valve (NO) / -:0
TMC CV Valve
FL/RR : Pressure Feed Valve/Sim V
PFV Valve
FR/RL : Pressure Feed Valve/Sim V
FR/RL : TMC Cut Valve (NO) / -:0
Tandem Master Cylinder / -:0
Linear Actuator / -:0 (Actuator)
Outlet Valve (NC)
Brake Fluid Reservoir / -:0
BFLS / -:0 (Sensor)
PFV Valve
Booster

Figure 10: Brake System Model /3/, /4/, /5/

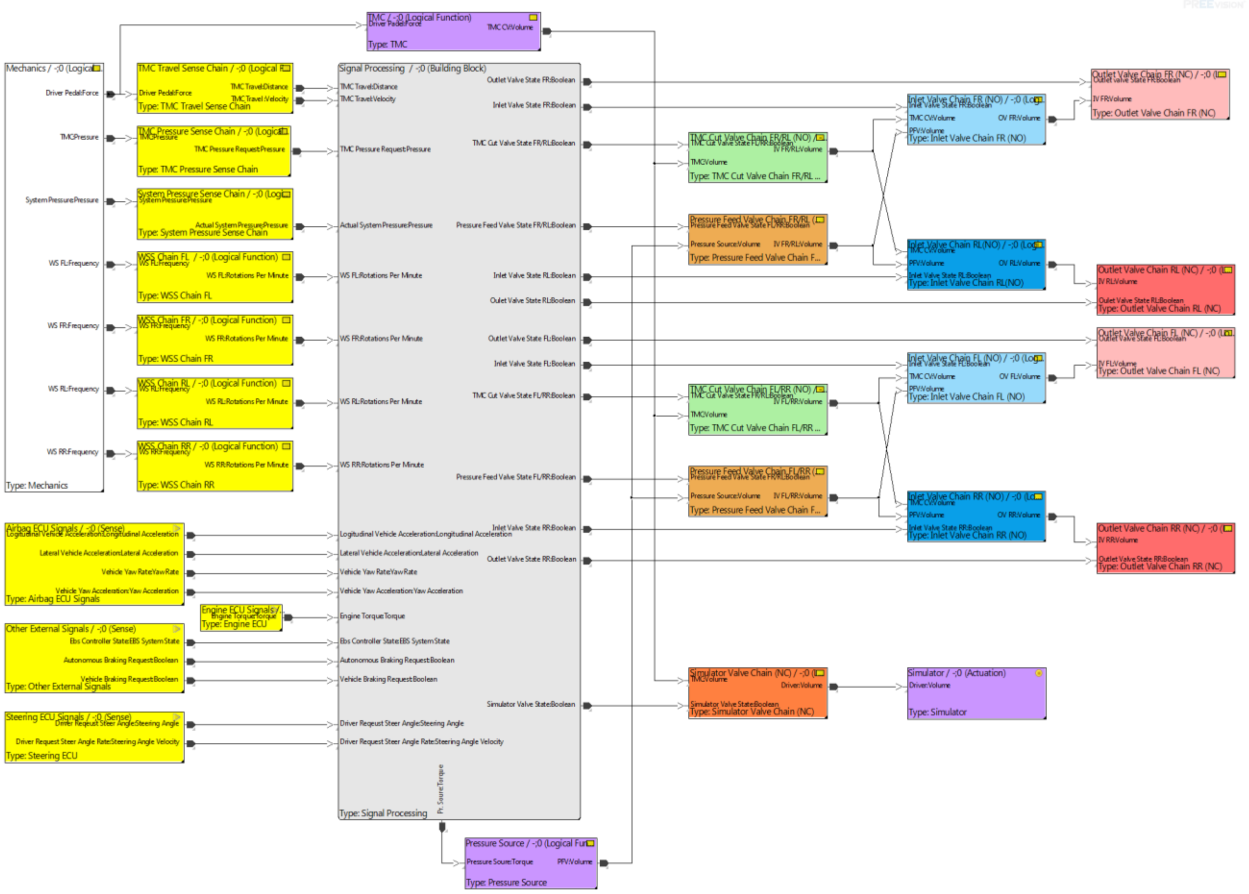
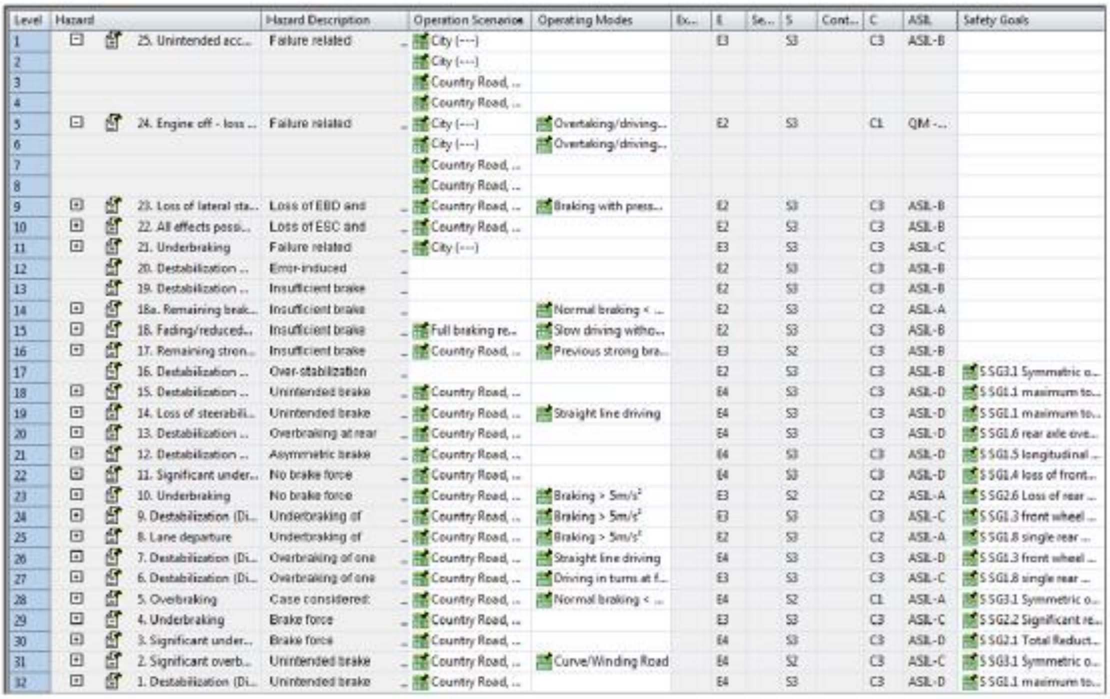

PREEvision
TMC / -;0 (Logical Function)
Driver Padel:Force
TMC CV:Volume
Type: TMC
Mechanics / -;0 (Logical...
Driver Pedal:Force
TMC:Pressure
System Pressure:Pressure
WS FL:Frequency
WS FR:Frequency
WS RL:Frequency
WS RR:Frequency
Type: Mechanics
TMC Travel Sense Chain / -;0 (Logical F...
Driver Pedal:Force
TMC Travel:Distance
TMC Travel:Velocity
Type: TMC Travel Sense Chain
TMC Pressure Sense Chain / -;0 (Logical...
TMC:Pressure
TMC Pressure Request:Pressure
Type: TMC Pressure Sense Chain
System Pressure Sense Chain / -;0 (Logi...
System Pressure:Pressure
Actual System Pressure:Pressure
Type: System Pressure Sense Chain
WSS Chain FL / -;0 (Logical Function)
WS FL:Frequency
WS FL:Rotations Per Minute
Type: WSS Chain FL
WSS Chain FR / -;0 (Logical Function)
WS FR:Frequency
WS FR:Rotations Per Minute
Type: WSS Chain FR
WSS Chain RL / -;0 (Logical Function)
WS RL:Frequency
WS RL:Rotations Per Minute
Type: WSS Chain RL
WSS Chain RR / -;0 (Logical Function)
WS RR:Frequency
WS RR:Rotations Per Minute
Type: WSS Chain RR
Airbag ECU Signals / -;0 (Sense)
Logitudinal Vehicle Acceleration:Longitudinal Acceleration
Lateral Vehicle Acceleration:Lateral Acceleration
Vehicle Yaw Rate:Yaw Rate
Vehicle Yaw Acceleration:Yaw Acceleration
Type: Airbag ECU Signals
Engine ECU Signals /...
Engine Torque:Torque
Type: Engine ECU
Other External Signals / -;0 (Sense)
Ebs Controller State:EBS System State
Autonomous Braking Request:Boolean
Vehicle Braking Request:Boolean
Type: Other External Signals
Steering ECU Signals / -;0 (Sense)
Driver Reqeust Steer Angle:Steering Angle
Driver Request Steer Angle Rate:Steering Angle Velocity
Type: Steering ECU
Signal Processing / -;0 (Building Block)
TMC Travel:Distance
TMC Travel:Velocity
TMC Pressure Request:Pressure
Actual System Pressure:Pressure
WS FL:Rotations Per Minute
WS FR:Rotations Per Minute
WS RL:Rotations Per Minute
WS RR:Rotations Per Minute
Logitudinal Vehicle Acceleration:Longitudinal Acceleration
Lateral Vehicle Acceleration:Lateral Acceleration
Vehicle Yaw Rate:Yaw Rate
Vehicle Yaw Acceleration:Yaw Acceleration
Engine Torque:Torque
Ebs Controller State:EBS System State
Autonomous Braking Request:Boolean
Vehicle Braking Request:Boolean
Driver Reqeust Steer Angle:Steering Angle
Driver Request Steer Angle Rate:Steering Angle Velocity
Outlet Valve State FR:Boolean
Inlet Valve State FR:Boolean
TMC Cut Valve State FR/RL:Boolean
Pressure Feed Valve State FR/RL:Boolean
Inlet Valve State RL:Boolean
Oulet Valve State RL:Boolean
Outlet Valve State FL:Boolean
Inlet Valve State FL:Boolean
TMC Cut Valve State FL/RR:Boolean
Pressure Feed Valve State FL/RR:Boolean
Inlet Valve State RR:Boolean
Outlet Valve State RR:Boolean
Simulator Valve State:Boolean
Pr. Soure:Torque
Type: Signal Processing
Pressure Source / -;0 (Logical Fun...
Pressure Soure:Torque
PFV:Volume
Type: Pressure Source
TMC Cut Valve Chain FR/RL (NO) /...
TMC Cut Valve State FL/RR:Boolean
IV FR/RL:Volume
TMC:Volume
Type: TMC Cut Valve Chain FR/RL ...
Pressure Feed Valve Chain FR/RL (...
Pressure Feed Valve State FL/RR:Boolean
Pressure Source:Volume
IV FR/RL:Volume
Type: Pressure Feed Valve Chain F...
TMC Cut Valve Chain FL/RR (NO) /...
TMC Cut Valve State FR/RL:Boolean
IV FL/RR:Volume
TMC:Volume
Type: TMC Cut Valve Chain FL/RR ...
Pressure Feed Valve Chain FL/RR (...
Pressure Feed Valve State FR/RL:Boolean
Pressure Source:Volume
IV FL/RR:Volume
Type: Pressure Feed Valve Chain F...
Simulator Valve Chain (NC) / -;0 (I...
TMC:Volume
Driver:Volume
Simulator Valve State:Boolean
Type: Simulator Valve Chain (NC)
Simulator / -;0 (Actuation)
Driver:Volume
Type: Simulator
Inlet Valve Chain FR (NO) / -;0 (Log...
Inlet Valve State FR:Boolean
TMC CV:Volume
OV FR:Volume
PFV:Volume
Type: Inlet Valve Chain FR (NO)
Inlet Valve Chain RL(NO) / -;0 (Log...
TMC CV:Volume
PFV:Volume
OV RL:Volume
Inlet Valve State RL:Boolean
Type: Inlet Valve Chain RL(NO)
Inlet Valve Chain FL (NO) / -;0 (Log...
Inlet Valve State FL:Boolean
TMC CV:Volume
OV FL:Volume
PFV:Volume
Type: Inlet Valve Chain FL (NO)
Inlet Valve Chain RR (NO) / -;0 (Lo...
TMC CV:Volume
PFV:Volume
OV RR:Volume
Inlet Valve State RR:Boolean
Type: Inlet Valve Chain RR (NO)
Outlet Valve Chain FR (NC) / -;0 (L...
Outlet valve State FR:Boolean
IV FR:Volume
Type: Outlet Valve Chain FR (NC)
Outlet Valve Chain RL (NC) / -;0 (L...
IV RL:Volume
Oulet Valve State RL:Boolean
Type: Outlet Valve Chain RL (NC)
Outlet Valve Chain FL (NC) / -;0 (L...
Outlet Valve State FL:Boolean
IV FL:Volume
Type: Outlet Valve Chain FL (NC)
Outlet Valve Chain RR (NC) / -;0 (L...
IV RR:Volume
Outlet Valve State RR:Boolean
Type: Outlet Valve Chain RR (NC)

Figure 11: Functional Description of Brake System /3/

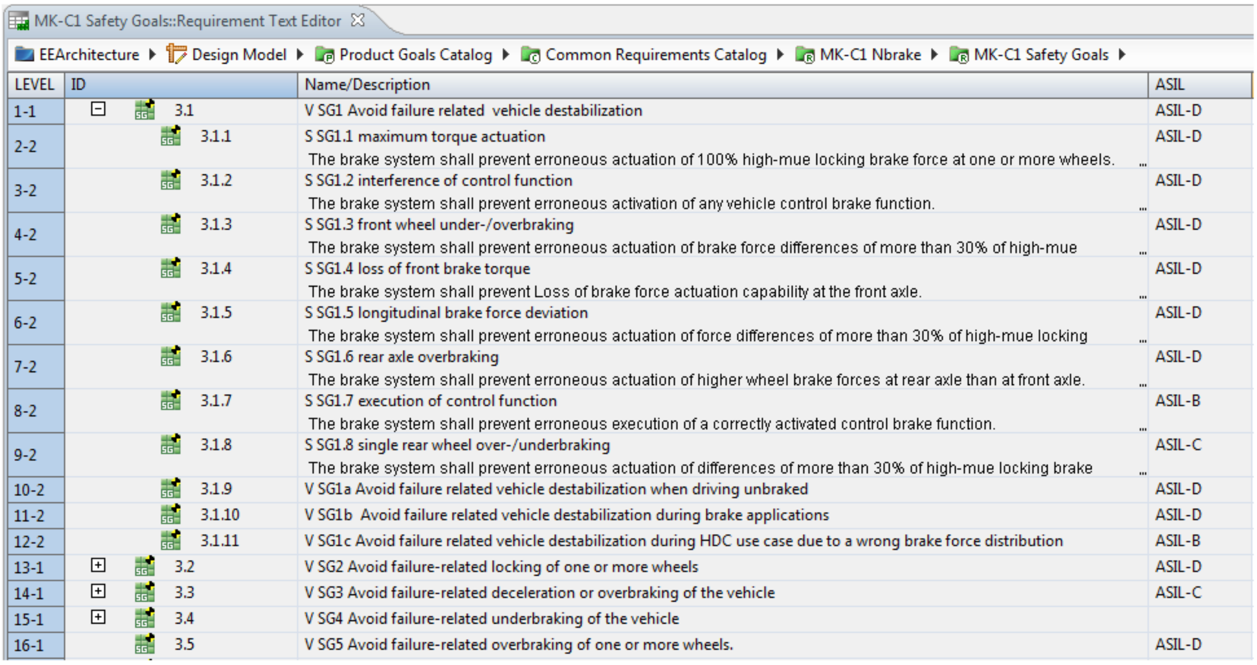
3.5.6.4.2 *Concept Space*

The conceptual inputs /1/, /2/, /6/ are also incorporated and summarized in the following. More information on their detailed incorporation can be derived from [15].



Level	Hazard	Hazard Description	Operation Scenarios	Operating Modes	Ex...	E	Se...	S	Cont...	C	ASIL	Safety Goals
1	⊟ 25. Unintended acc...	Failure related	City (---)			E3		S3		C3	ASIL-B	
2			City (---)									
3			Country Road, ...									
4			Country Road, ...									
5	⊟ 24. Engine off - loss ...	Failure related	City (---)	Overtaking/driving...		E2		S3		C1	QM -...	
6			City (---)	Overtaking/driving...								
7			Country Road, ...									
8			Country Road, ...									
9	⊞ 23. Loss of lateral sta...	Loss of EBD and	Country Road, ...	Braking with press...		E2		S3		C3	ASIL-B	
10	⊞ 22. All effects possi...	Loss of ESC and	Country Road, ...			E2		S3		C3	ASIL-B	
11	⊞ 21. Underbraking	Failure related	City (---)			E3		S3		C3	ASIL-C	
12	20. Destabilization ...	Error-induced				E2		S3		C3	ASIL-B	
13	19. Destabilization ...	Insufficient brake				E2		S3		C3	ASIL-B	
14	⊞ 18a. Remaining brak...	Insufficient brake		Normal braking < ...		E2		S3		C2	ASIL-A	
15	⊞ 18. Fading/reduced...	Insufficient brake	Full braking re...	Slow driving witho...		E2		S3		C3	ASIL-B	
16	⊞ 17. Remaining stron...	Insufficient brake	Country Road, ...	Previous strong bra...		E3		S2		C3	ASIL-B	
17	16. Destabilization ...	Over-stabilization				E2		S3		C3	ASIL-B	S SG3.1 Symmetric o...
18	⊞ 15. Destabilization ...	Unintended brake	Country Road, ...			E4		S3		C3	ASIL-D	S SG1.1 maximum to...
19	⊞ 14. Loss of steerabili...	Unintended brake	Country Road, ...	Straight line driving		E4		S3		C3	ASIL-D	S SG1.1 maximum to...
20	⊞ 13. Destabilization ...	Overbraking at rear	Country Road, ...			E4		S3		C3	ASIL-D	S SG1.6 rear axle ove...
21	⊞ 12. Destabilization ...	Asymmetric brake	Country Road, ...			E4		S3		C3	ASIL-D	S SG1.5 longitudinal ...
22	⊞ 11. Significant under...	No brake force	Country Road, ...			E4		S3		C3	ASIL-D	S SG1.4 loss of front...
23	⊞ 10. Underbraking	No brake force	Country Road, ...	Braking > $5m/s^2$		E3		S2		C2	ASIL-A	S SG2.6 Loss of rear ...
24	⊞ 9. Destabilization (Di...	Underbraking of	Country Road, ...	Braking > $5m/s^2$		E3		S3		C3	ASIL-C	S SG1.3 front wheel ...
25	⊞ 8. Lane departure	Underbraking of	Country Road, ...	Braking > $5m/s^2$		E2		S3		C2	ASIL-A	S SG1.8 single rear ...
26	⊞ 7. Destabilization (Di...	Overbraking of one	Country Road, ...	Straight line driving		E4		S3		C3	ASIL-D	S SG1.3 front wheel ...
27	⊞ 6. Destabilization (Di...	Overbraking of one	Country Road, ...	Driving in turns at f...		E3		S3		C3	ASIL-C	S SG1.8 single rear ...
28	⊞ 5. Overbraking	Case considered:	Country Road, ...	Normal braking < ...		E4		S2		C1	ASIL-A	S SG3.1 Symmetric o...
29	⊞ 4. Underbraking	Brake force	Country Road, ...			E3		S3		C3	ASIL-C	S SG2.2 Significant re...
30	⊞ 3. Significant under...	Brake force	Country Road, ...			E4		S3		C3	ASIL-D	S SG2.1 Total Reduct...
31	⊞ 2. Significant overb...	Unintended brake	Country Road, ...	Curve/Winding Road		E4		S2		C3	ASIL-C	S SG3.1 Symmetric o...
32	⊞ 1. Destabilization (Di...	Unintended brake	Country Road, ...			E4		S3		C3	ASIL-D	S SG1.1 maximum to...

Figure 12: Hazard Analysis /6/

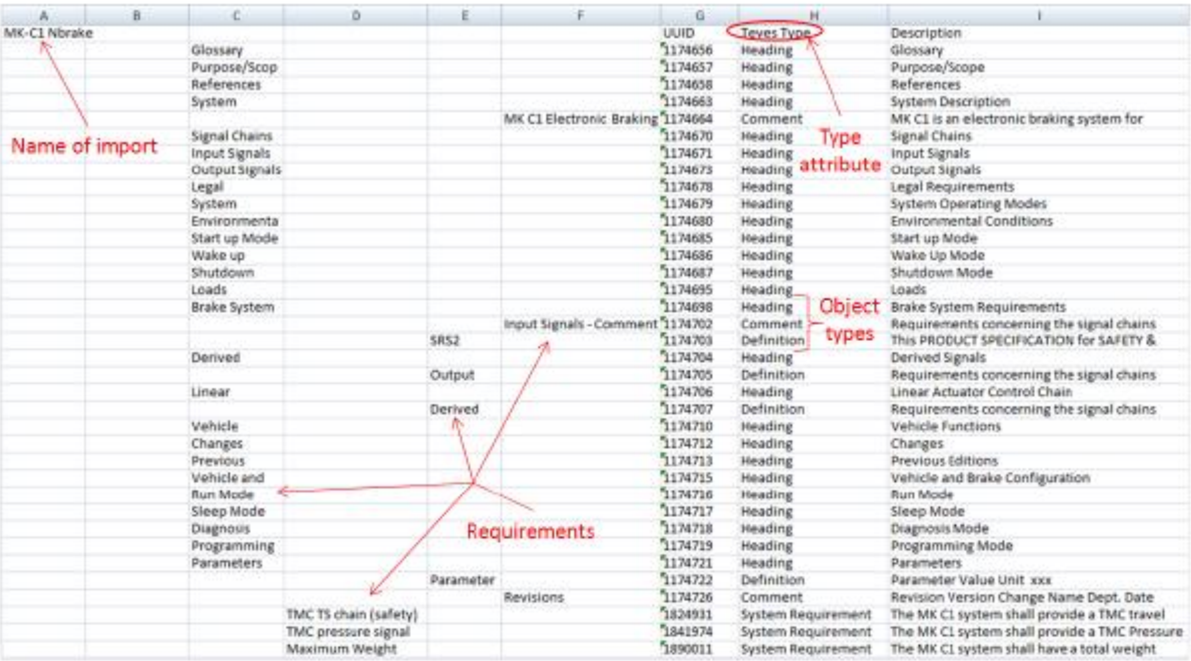


MK-C1 Safety Goals::Requirement Text Editor ☒

EEArchitecture ▸ Design Model ▸ Product Goals Catalog ▸ Common Requirements Catalog ▸ MK-C1 Nbrake ▸ MK-C1 Safety Goals ▸

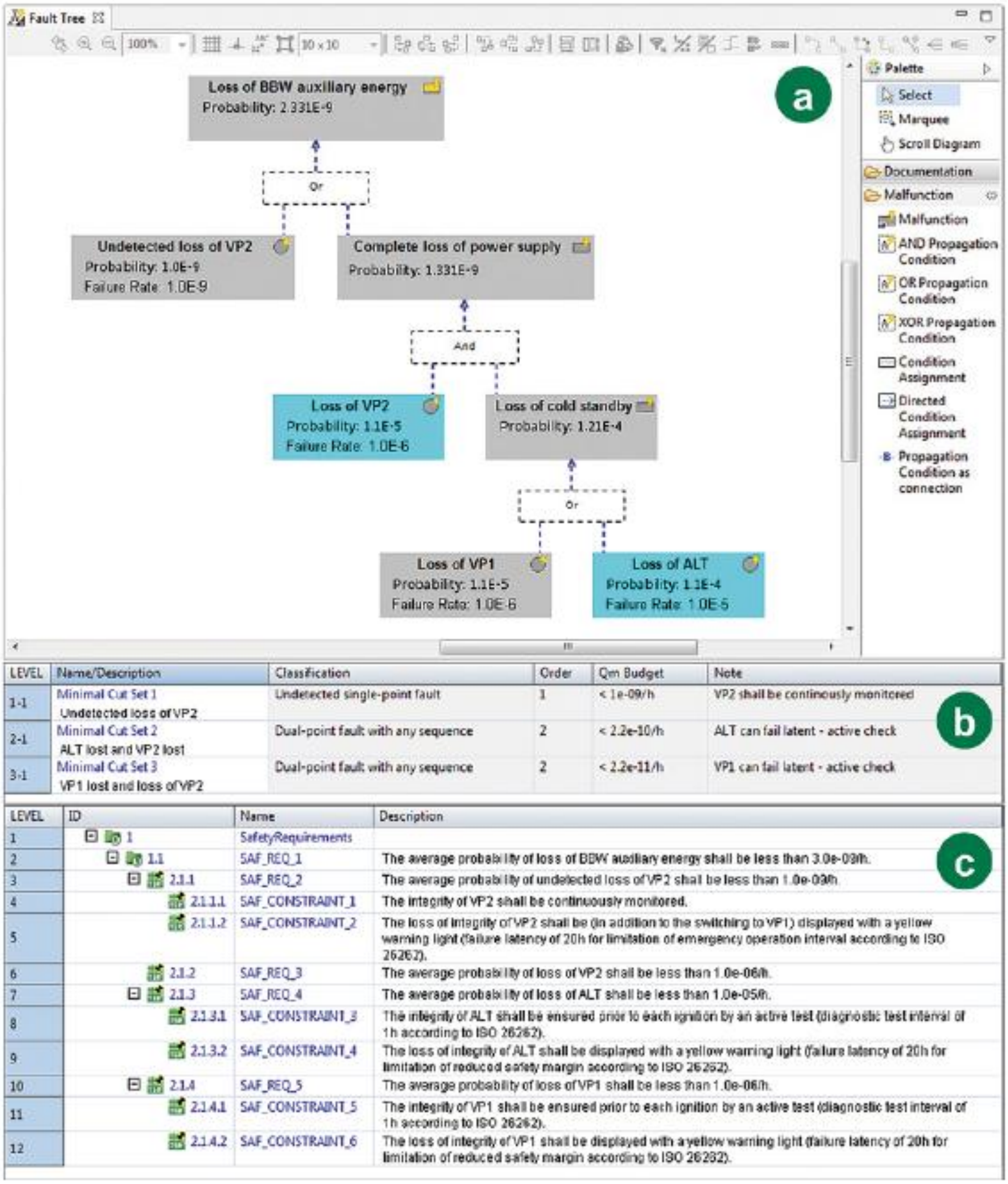
LEVEL	ID	Name/Description	ASIL
1-1	⊟ 3.1	V SG1 Avoid failure related vehicle destabilization	ASIL-D
2-2	3.1.1	S SG1.1 maximum torque actuation The brake system shall prevent erroneous actuation of 100% high-mue locking brake force at one or more wheels. ...	ASIL-D
3-2	3.1.2	S SG1.2 interference of control function The brake system shall prevent erroneous activation of any vehicle control brake function. ...	ASIL-D
4-2	3.1.3	S SG1.3 front wheel under-/overbraking The brake system shall prevent erroneous actuation of brake force differences of more than 30% of high-mue ...	ASIL-D
5-2	3.1.4	S SG1.4 loss of front brake torque The brake system shall prevent Loss of brake force actuation capability at the front axle. ...	ASIL-D
6-2	3.1.5	S SG1.5 longitudinal brake force deviation The brake system shall prevent erroneous actuation of force differences of more than 30% of high-mue locking ...	ASIL-D
7-2	3.1.6	S SG1.6 rear axle overbraking The brake system shall prevent erroneous actuation of higher wheel brake forces at rear axle than at front axle. ...	ASIL-D
8-2	3.1.7	S SG1.7 execution of control function The brake system shall prevent erroneous execution of a correctly activated control brake function. ...	ASIL-B
9-2	3.1.8	S SG1.8 single rear wheel over-/underbraking The brake system shall prevent erroneous actuation of differences of more than 30% of high-mue locking brake ...	ASIL-C
10-2	3.1.9	V SG1a Avoid failure related vehicle destabilization when driving unbraked	ASIL-D
11-2	3.1.10	V SG1b Avoid failure related vehicle destabilization during brake applications	ASIL-D
12-2	3.1.11	V SG1c Avoid failure related vehicle destabilization during HDC use case due to a wrong brake force distribution	ASIL-B
13-1	⊞ 3.2	V SG2 Avoid failure-related locking of one or more wheels	ASIL-D
14-1	⊞ 3.3	V SG3 Avoid failure-related deceleration or overbraking of the vehicle	ASIL-C
15-1	⊞ 3.4	V SG4 Avoid failure-related underbraking of the vehicle	
16-1	3.5	V SG5 Avoid failure-related overbraking of one or more wheels.	ASIL-D

Figure 13: Safety Goals /2/



A	B	C	D	E	F	G	H	I
MK-C1 Nbrake						UUID	Teves Type	Description
		Glossary				1174656	Heading	Glossary
		Purpose/Scop				1174657	Heading	Purpose/Scope
		References				1174658	Heading	References
		System				1174663	Heading	System Description
					MK C1 Electronic Braking	1174664	Comment	MK C1 is an electronic braking system for
		Signal Chains				1174670	Heading	Signal Chains
		Input Signals				1174671	Heading	Input Signals
		Output Signals				1174673	Heading	Output Signals
		Legal				1174678	Heading	Legal Requirements
		System				1174679	Heading	System Operating Modes
		Environmenta				1174680	Heading	Environmental Conditions
		Start up Mode				1174685	Heading	Start up Mode
		Wake up				1174686	Heading	Wake Up Mode
		Shutdown				1174687	Heading	Shutdown Mode
		Loads				1174695	Heading	Loads
		Brake System				1174698	Heading	Brake System Requirements
					Input Signals - Comment	1174702	Comment	Requirements concerning the signal chains
				SRS2		1174703	Definition	This PRODUCT SPECIFICATION for SAFETY &
		Derived				1174704	Heading	Derived Signals
				Output		1174705	Definition	Requirements concerning the signal chains
		Linear				1174706	Heading	Linear Actuator Control Chain
				Derived		1174707	Definition	Requirements concerning the signal chains
		Vehicle				1174710	Heading	Vehicle Functions
		Changes				1174712	Heading	Changes
		Previous				1174713	Heading	Previous Editions
		Vehicle and				1174715	Heading	Vehicle and Brake Configuration
		Run Mode				1174716	Heading	Run Mode
		Sleep Mode				1174717	Heading	Sleep Mode
		Diagnosis				1174718	Heading	Diagnosis Mode
		Programming				1174719	Heading	Programming Mode
		Parameters				1174721	Heading	Parameters
				Parameter		1174722	Definition	Parameter Value Unit xxx
					Revisions	1174726	Comment	Revision Version Change Name Dept. Date
			TMC TS chain (safety)			1824931	System Requirement	The MK C1 system shall provide a TMC travel
			TMC pressure signal			1841974	System Requirement	The MK C1 system shall provide a TMC Pressure
			Maximum Weight			1890011	System Requirement	The MK C1 system shall have a total weight

Figure 14: System Requirement Specification /1/



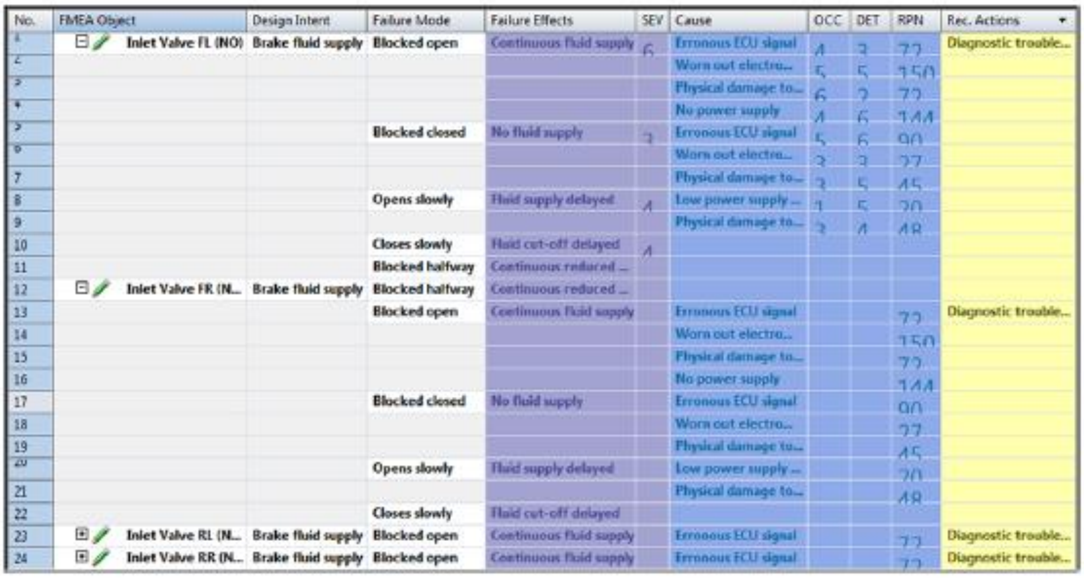
LEVEL	Name/Description	Classification	Order	Qm Budget	Note
1-1	Minimal Cut Set 1 Undetected loss of VP2	Undetected single-point fault	1	< 1e-09/h	VP2 shall be continously monitored
2-1	Minimal Cut Set 2 ALT lost and VP2 lost	Dual-point fault with any sequence	2	< 2.2e-10/h	ALT can fail latent - active check
3-1	Minimal Cut Set 3 VP1 lost and loss of VP2	Dual-point fault with any sequence	2	< 2.2e-11/h	VP1 can fail latent - active check

LEVEL	ID	Name	Description
1	⊟ 1	SafetyRequirements	
2	⊟ 1.1	SAF_REQ_1	The average probability of loss of BBW auxiliary energy shall be less than 3.0e-09/h.
3	⊟ 2.1.1	SAF_REQ_2	The average probability of undetected loss of VP2 shall be less than 1.0e-09/h.
4	2.1.1.1	SAF_CONSTRAINT_1	The integrity of VP2 shall be continuously monitored.
5	2.1.1.2	SAF_CONSTRAINT_2	The loss of integrity of VP2 shall be (in addition to the switching to VP1) displayed with a yellow warning light (failure latency of 20h for limitation of emergency operation interval according to ISO 26262).
6	2.1.2	SAF_REQ_3	The average probability of loss of VP2 shall be less than 1.0e-06/h.
7	⊟ 2.1.3	SAF_REQ_4	The average probability of loss of ALT shall be less than 1.0e-05/h.
8	2.1.3.1	SAF_CONSTRAINT_3	The integrity of ALT shall be ensured prior to each ignition by an active test (diagnostic test interval of 1h according to ISO 26262).
9	2.1.3.2	SAF_CONSTRAINT_4	The loss of integrity of ALT shall be displayed with a yellow warning light (failure latency of 20h for limitation of reduced safety margin according to ISO 26262).
10	⊟ 2.1.4	SAF_REQ_5	The average probability of loss of VP1 shall be less than 1.0e-06/h.
11	2.1.4.1	SAF_CONSTRAINT_5	The integrity of VP1 shall be ensured prior to each ignition by an active test (diagnostic test interval of 1h according to ISO 26262).
12	2.1.4.2	SAF_CONSTRAINT_6	The loss of integrity of VP1 shall be displayed with a yellow warning light (failure latency of 20h for limitation of reduced safety margin according to ISO 26262).

Figure 15: Fault Tree Analysis /8/

For /9/ no visualized artefact is available – please refer to [15] for details.

3.5.6.4.3 *Analysis Space:*



No.	FMEA Object	Design Intent	Failure Mode	Failure Effects	SEV	Cause	OCC	DET	RPN	Rec. Actions
1	⊟ Inlet Valve FL (NO)	Brake fluid supply	Blocked open	Continuous fluid supply	6	Erronous ECU signal	4	3	72	Diagnostic trouble...
2						Worn out electro...	5	5	150	
3						Physical damage to...	6	2	72	
4						No power supply	4	6	144	
5			Blocked closed	No fluid supply	3	Erronous ECU signal	5	6	90	
6						Worn out electro...	3	3	27	
7						Physical damage to...	3	5	45	
8			Opens slowly	Fluid supply delayed	4	Low power supply ...	1	5	20	
9						Physical damage to...	3	4	48	
10			Closes slowly	Fluid cut-off delayed	4					
11			Blocked halfway	Continuous reduced ...						
12	⊟ Inlet Valve FR (N...	Brake fluid supply	Blocked halfway	Continuous reduced ...						
13			Blocked open	Continuous fluid supply		Erronous ECU signal			72	Diagnostic trouble...
14						Worn out electro...			150	
15						Physical damage to...			72	
16						No power supply			144	
17			Blocked closed	No fluid supply		Erronous ECU signal			90	
18						Worn out electro...			27	
19						Physical damage to...			45	
20			Opens slowly	Fluid supply delayed		Low power supply ...			20	
21						Physical damage to...			48	
22			Closes slowly	Fluid cut-off delayed						
23	⊞ Inlet Valve RL (N...	Brake fluid supply	Blocked open	Continuous fluid supply		Erronous ECU signal			72	Diagnostic trouble...
24	⊞ Inlet Valve RR (N...	Brake fluid supply	Blocked open	Continuous fluid supply		Erronous ECU signal			72	Diagnostic trouble...

Figure 16: FMEA of a Valve /7/

4 Evaluation Results

In the following the evaluation results are summarized. As they are primarily obtained from both evaluation scenarios a common representation is selected to highlight the outcome and the feedback to the work task during the runtime of the SAFE projects. Dedicated results regarding the individual evaluation results are available in the project documentation [15],[21].

4.1 Fulfillment of WP 3/4/6 requirements

The matrix below depicts the overall result of the requirements coming from other work task and evaluated by the hereby scenarios. As a matter of fact, the status of requirements presented here reflects the achievement of the evaluation process, that was iterative according to succeeding version of PREEvision and progress of the different related work task

As the different scenarios may address separate topics, the requirements are likely to be tagged with the corresponding one.

For the sake of understanding, all single requirements are collected in meta-requirement as follows:

- **WT52_REQ_1:** The PREEvision environment shall implement the Safe project methods defined in WT311, WT312, WT313, WT321, WT331, and useful to architecture modeling and analysis
- **WT52_REQ_2:** The safe project methods shall demonstrate the capability to model hazards and safety goals including related traceability
- **WT52_REQ_3:** The Safe project methods shall demonstrate the capability to model and trace safety requirement to the system safety goals
- **WT52_REQ_4:** The Safe project methods shall demonstrate the capability to generate safety case for an architecture model and to represent safety goal
- **WT52_REQ_5:** The Safe project methods shall demonstrate the capability to capture and refine the safety related system architecture including safety software components
- **WT52_REQ_6:** The Safe project methods shall demonstrate the capability to capture the hardware component and associated failure rate of an hardware safety architecture
- **WT52_REQ7:** The Safe project methods shall demonstrate the capability to support qualitatively and quantitatively safety analysis
- **WT52_REQ8:** The Safe project methods shall demonstrate the capability to support variant in the safety architecture of system products coming from the same family

Thus the matrix below gathers the status of requirements that are colored according to the legend next to the table.

In order to get more details about single requirements, please refer to

- [15] regarding the brake-system Use Case
- [21] regarding the EMS Use Case

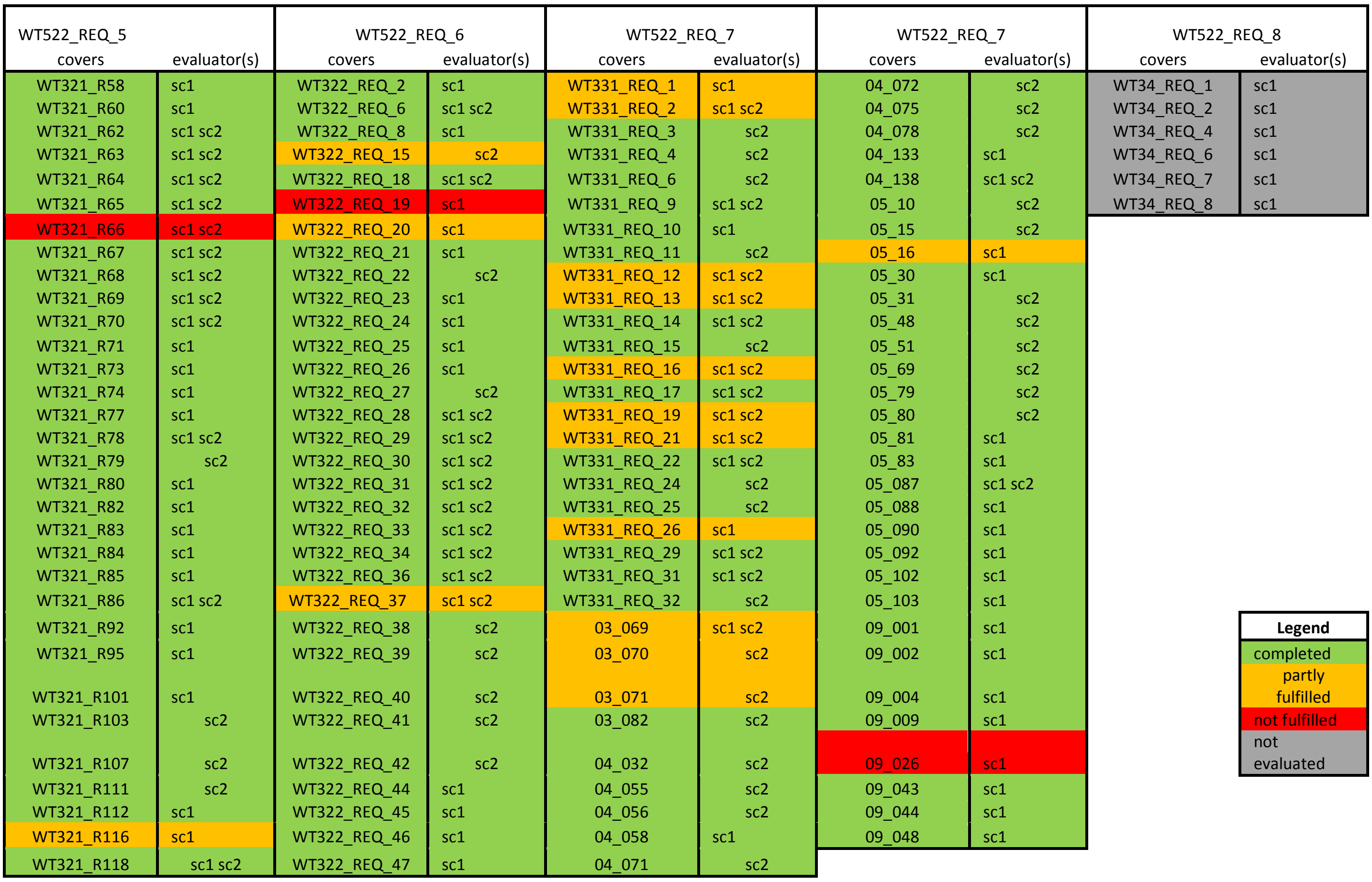
Eventually, the picture below deals with a synthesis of the main findings that are reported to their respective owner work task. Furthermore, the results are reflected to Vector Informatik, to improve the meta-model.

4.2 Detailed Evaluation Result

Table 3 and Table 4 summarize the overall outcome of the two evaluation scenarios.

WT522_REQ_1		WT522_REQ_2		WT522_REQ_3		WT522_REQ_4		WT522_REQ_5	
covers	evaluator(s)	covers	evaluator(s)	covers	evaluator(s)	covers	evaluator(s)	covers	evaluator(s)
02_001	sc1 sc2	WT311_REQ_1	sc1 sc2	WT312_REQ_1	sc1	WT313_REQ_1	sc1 sc2	WT321_R1	sc2
02_002	sc1 sc2	WT311_REQ_2	sc1 sc2	WT312_REQ_2	sc1 sc2	WT313_REQ_2	sc2	WT321_R2	sc1
02_003	sc2	WT311_REQ_3	sc1 sc2	WT312_REQ_3	sc1	WT313_REQ_3	sc2	WT321_R3	sc1 sc2
02_004	sc1 sc2	WT311_REQ_4	sc1	WT312_REQ_4	sc1	WT313_REQ_4	sc2	WT321_R7	sc1
02_006	sc1 sc2	WT311_REQ_5	sc2	WT312_REQ_5	sc1 sc2	WT313_REQ_5	sc2	WT321_R9	sc2
		WT311_REQ_7	sc1 sc2	WT312_REQ_6	sc1	WT311_REQ_7	sc2	WT321_R14	sc1 sc2
		WT311_REQ_8	sc1	WT312_REQ_7	sc1 sc2	WT311_REQ_9	sc2	WT321_R15	sc1
		WT311_REQ_9	sc1	WT312_REQ_8	sc1 sc2	WT311_REQ_13	sc2	WT321_R18	sc1
		WT311_REQ_10	sc1	WT312_REQ_9	sc1 sc2	WT311_REQ_25	sc2	WT321_R20	sc1
		WT311_REQ_12	sc1	WT312_REQ_12	sc1 sc2	WT311_REQ_38	sc2	WT321_R21	sc1
		WT311_REQ_13	sc1	WT312_REQ_13	sc1 sc2	WT311_REQ_46	sc2	WT321_R25	sc2
		WT311_REQ_14	sc1	WT312_REQ_17	sc1 sc2	WT32_R115	sc2	WT321_R26	sc2
		WT311_REQ_15	sc1	WT312_REQ_18	sc1 sc2			WT321_R27	sc2
		WT311_REQ_17	sc1	WT312_REQ_19	sc1			WT321_R30	sc1
		WT311_REQ_20	sc1	WT312_REQ_20	sc1 sc2			WT321_R32	sc1
		WT311_REQ_21	sc1	WT312_REQ_21	sc1			WT321_R33	sc1
		WT311_REQ_22	sc1	WT312_REQ_22	sc1			WT321_R34	sc1
		WT311_REQ_23	sc1 sc2	WT312_REQ_23	sc1			WT321_R35	sc1
		WT311_REQ_26	sc1	WT312_REQ_24	sc1			WT321_R36	sc1
		WT311_REQ_27	sc1	WT312_REQ_26	sc1 sc2			WT321_R37	sc1
		WT311_REQ_28	sc1	WT312_REQ_27	sc1			WT321_R38	sc1
		WT311_REQ_32	sc1 sc2	WT312_REQ_29	sc2			WT321_R40	sc1
		WT311_REQ_33	sc1	WT312_REQ_31	sc2			WT321_R41	sc1
		WT311_REQ_34	sc1	WT312_REQ_32	sc2			WT321_R42	sc1
		WT311_REQ_35	sc1	WT312_REQ_33	sc2			WT321_R43	sc1
		WT311_REQ_36	sc1	WT312_REQ_34	sc2			WT321_R44	sc1
		WT311_REQ_37	sc1					WT321_R45	sc1
		WT311_REQ_38	sc1					WT321_R48	sc1
		WT311_REQ_45	sc1					WT321_R50	sc2
		WT311_REQ_47	sc1					WT321_R51	sc1 sc2
		WT311_REQ_48	sc1					WT321_R52	sc1 sc2
		WT311_REQ_49	sc1					WT321_R53	sc1 sc2
		WT311_REQ_51	sc2					WT321_R54	sc1
		WT311_REQ_52	sc2					WT321_R55	sc1
		WT311_REQ_53	sc2					WT321_R56	sc1

Table 3: Evaluation Result 1



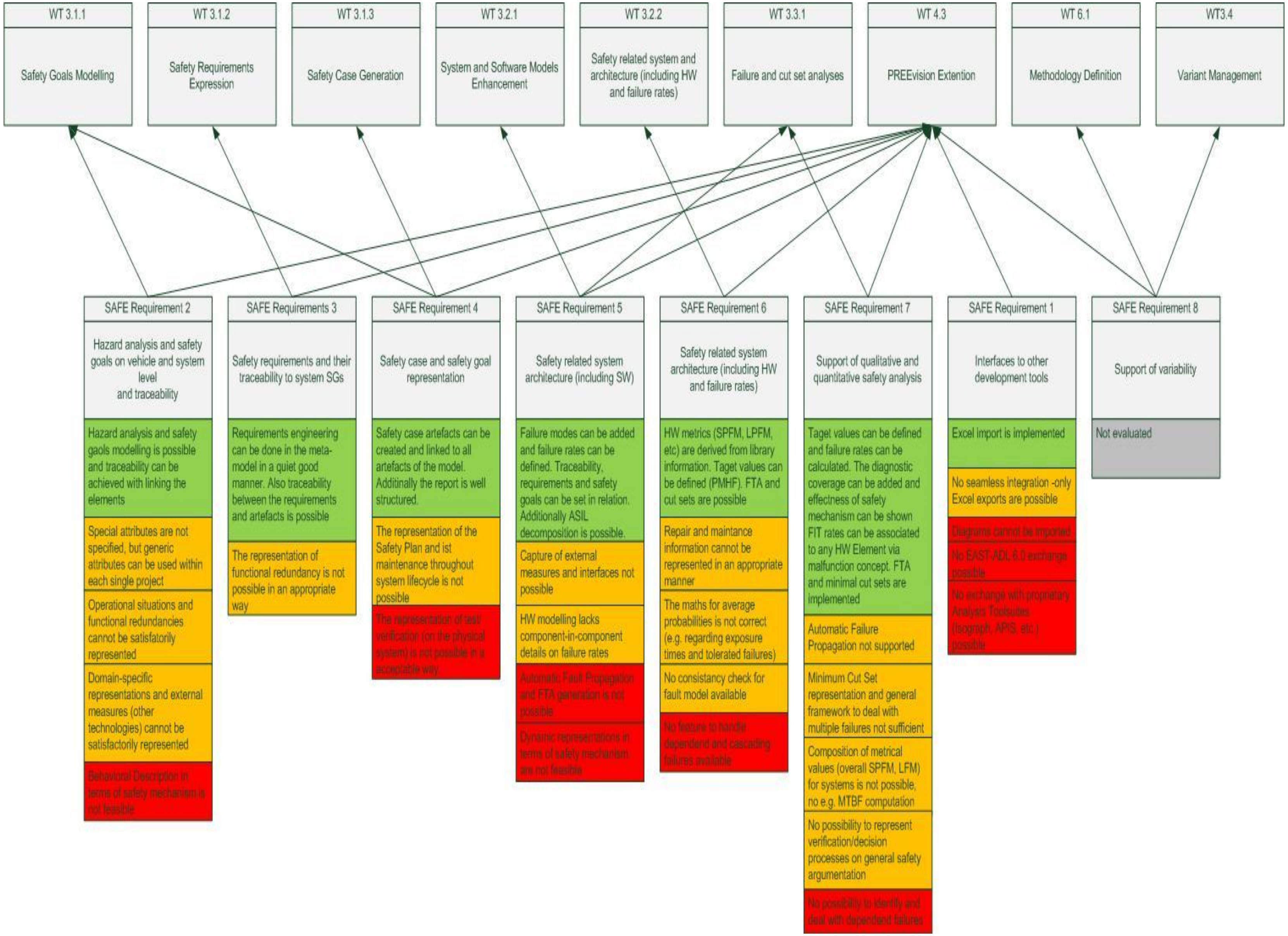
WT522_REQ_5		WT522_REQ_6		WT522_REQ_7		WT522_REQ_7		WT522_REQ_8	
covers	evaluator(s)	covers	evaluator(s)	covers	evaluator(s)	covers	evaluator(s)	covers	evaluator(s)
🟩 WT321_R58	sc1	🟩 WT322_REQ_2	sc1	🟨 WT331_REQ_1	sc1	🟩 04_072	sc2	⬜ WT34_REQ_1	sc1
🟩 WT321_R60	sc1	🟩 WT322_REQ_6	sc1 sc2	🟨 WT331_REQ_2	sc1 sc2	🟩 04_075	sc2	⬜ WT34_REQ_2	sc1
🟩 WT321_R62	sc1 sc2	🟩 WT322_REQ_8	sc1	🟩 WT331_REQ_3	sc2	🟩 04_078	sc2	⬜ WT34_REQ_4	sc1
🟩 WT321_R63	sc1 sc2	🟨 WT322_REQ_15	sc2	🟩 WT331_REQ_4	sc2	🟩 04_133	sc1	⬜ WT34_REQ_6	sc1
🟩 WT321_R64	sc1 sc2	🟩 WT322_REQ_18	sc1 sc2	🟩 WT331_REQ_6	sc2	🟩 04_138	sc1 sc2	⬜ WT34_REQ_7	sc1
🟩 WT321_R65	sc1 sc2	🟥 WT322_REQ_19	sc1	🟩 WT331_REQ_9	sc1 sc2	🟩 05_10	sc2	⬜ WT34_REQ_8	sc1
🟥 WT321_R66	sc1 sc2	🟨 WT322_REQ_20	sc1	🟩 WT331_REQ_10	sc1	🟩 05_15	sc2		
🟩 WT321_R67	sc1 sc2	🟩 WT322_REQ_21	sc1	🟩 WT331_REQ_11	sc2	🟨 05_16	sc1		
🟩 WT321_R68	sc1 sc2	🟩 WT322_REQ_22	sc2	🟨 WT331_REQ_12	sc1 sc2	🟩 05_30	sc1		
🟩 WT321_R69	sc1 sc2	🟩 WT322_REQ_23	sc1	🟨 WT331_REQ_13	sc1 sc2	🟩 05_31	sc2		
🟩 WT321_R70	sc1 sc2	🟩 WT322_REQ_24	sc1	🟩 WT331_REQ_14	sc1 sc2	🟩 05_48	sc2		
🟩 WT321_R71	sc1	🟩 WT322_REQ_25	sc1	🟩 WT331_REQ_15	sc2	🟩 05_51	sc2		
🟩 WT321_R73	sc1	🟩 WT322_REQ_26	sc1	🟨 WT331_REQ_16	sc1 sc2	🟩 05_69	sc2		
🟩 WT321_R74	sc1	🟩 WT322_REQ_27	sc2	🟩 WT331_REQ_17	sc1 sc2	🟩 05_79	sc2		
🟩 WT321_R77	sc1	🟩 WT322_REQ_28	sc1 sc2	🟨 WT331_REQ_19	sc1 sc2	🟩 05_80	sc2		
🟩 WT321_R78	sc1 sc2	🟩 WT322_REQ_29	sc1 sc2	🟨 WT331_REQ_21	sc1 sc2	🟩 05_81	sc1		
🟩 WT321_R79	sc2	🟩 WT322_REQ_30	sc1 sc2	🟩 WT331_REQ_22	sc1 sc2	🟩 05_83	sc1		
🟩 WT321_R80	sc1	🟩 WT322_REQ_31	sc1 sc2	🟩 WT331_REQ_24	sc2	🟩 05_087	sc1 sc2		
🟩 WT321_R82	sc1	🟩 WT322_REQ_32	sc1 sc2	🟩 WT331_REQ_25	sc2	🟩 05_088	sc1		
🟩 WT321_R83	sc1	🟩 WT322_REQ_33	sc1 sc2	🟨 WT331_REQ_26	sc1	🟩 05_090	sc1		
🟩 WT321_R84	sc1	🟩 WT322_REQ_34	sc1 sc2	🟩 WT331_REQ_29	sc1 sc2	🟩 05_092	sc1		
🟩 WT321_R85	sc1	🟩 WT322_REQ_36	sc1 sc2	🟩 WT331_REQ_31	sc1 sc2	🟩 05_102	sc1		
🟩 WT321_R86	sc1 sc2	🟨 WT322_REQ_37	sc1 sc2	🟩 WT331_REQ_32	sc2	🟩 05_103	sc1		
🟩 WT321_R92	sc1	🟩 WT322_REQ_38	sc2	🟨 03_069	sc1 sc2	🟩 09_001	sc1		
🟩 WT321_R95	sc1	🟩 WT322_REQ_39	sc2	🟨 03_070	sc2	🟩 09_002	sc1		
🟩 WT321_R101	sc1	🟩 WT322_REQ_40	sc2	🟨 03_071	sc2	🟩 09_004	sc1		
🟩 WT321_R103	sc2	🟩 WT322_REQ_41	sc2	🟩 03_082	sc2	🟩 09_009	sc1		
🟩 WT321_R107	sc2	🟩 WT322_REQ_42	sc2	🟩 04_032	sc2	🟥 09_026	sc1		
🟩 WT321_R111	sc2	🟩 WT322_REQ_44	sc1	🟩 04_055	sc2	🟩 09_043	sc1		
🟩 WT321_R112	sc1	🟩 WT322_REQ_45	sc1	🟩 04_056	sc2	🟩 09_044	sc1		
🟨 WT321_R116	sc1	🟩 WT322_REQ_46	sc1	🟩 04_058	sc1	🟩 09_048	sc1		
🟩 WT321_R118	sc1 sc2	🟩 WT322_REQ_47	sc1	🟩 04_071	sc2				

Legend
🟩 completed
🟨 partly fulfilled
🟥 not fulfilled
⬜ not evaluated

Table 4: Evaluation Result 2

4.3 Final Evaluation Outcome and Feedback to other Worktasks

Figure 17 below summarized the outcome and the feedback provided to the individual work tasks of the SAFE project.



WT 3.1.1 Safety Goals Modelling

WT 3.1.2 Safety Requirements Expression

WT 3.1.3 Safety Case Generation

WT 3.2.1 System and Software Models Enhancement

WT 3.2.2 Safety related system and architecture (including HW and failure rates)

WT 3.3.1 Failure and cut set analyses

WT 4.3 PREEvision Extention

WT 6.1 Methodology Definition

WT3.4 Variant Management

SAFE Requirement 2 – Hazard analysis and safety goals on vehicle and system level and traceability

- Hazard analysis and safety gaols modelling is possible and traceability can be achieved with linking the elements
- Special attributes are not specified, but generic attributes can be used within each single project
- Operational situations and functional redundancies cannot be satisfatorily represented
- Domain-specific representations and external measures (other technologies) cannot be satisfactorily represented
- Behavioral Description in terms of safety mechanism is not feasible

SAFE Requirements 3 – Safety requirements and their traceability to system SGs

- Requirements engineering can be done in the meta-model in a quiet good manner. Also traceability between the requirements and artefacts is possible
- The representation of functional redundancy is not possible in an appropriate way

SAFE Requirement 4 – Safety case and safety goal representation

- Safety case artefacts can be created and linked to all artefacts of the model. Additinally the report is well structured.
- The representation of the Safety Plan and ist maintenance throughout system lifecycle is not possible
- The representation of test verification (on the physical system) is not possible in a acceptable way.

SAFE Requirement 5 – Safety related system architecture (including SW)

- Failure modes can be added and failure rates can be defined. Traceability, requirements and safety goals can be set in relation. Additionally ASIL decomposition is possible.
- Capture of external measures and interfaces not possible
- HW modelling lacks component-in-component details on failure rates
- Automatic Fault Propagation and FTA generation is not possible
- Dynamic representations in terms of safety mechanism are not feasible

SAFE Requirement 6 – Safety related system architecture (including HW and failure rates)

- HW metrics (SPFM, LPFM, etc) are derived from library information. Taget values can be defined (PMHF). FTA and cut sets are possible
- Repair and maintance information cannot be represented in an appropriate manner
- The maths for average probabilities is not correct (e.g. regarding exposure times and tolerated failures)
- No consistancy check for fault model available
- No feature to handle dependend and cascading failures available

SAFE Requirement 7 – Support of qualitative and quantitative safety analysis

- Taget values can be defined and failure rates can be calculated. The diagnostic coverage can be added and effectness of safety mechanism can be shown FIT rates can be associated to any HW Element via malfunction concept. FTA and minimal cut sets are implemented
- Automatic Failure Propagation not supported
- Minimum Cut Set representation and general framework to deal with multiple failures not sufficient
- Composition of metrical values (overall SPFM, LFM) for systems is not possible, no e.g. MTBF computation
- No possibility to represent verification/decision processes on general safety argumentation
- No possibility to identify and deal with dependend failures

SAFE Requirement 1 – Interfaces to other development tools

- Excel import is implemented
- No seamless integration -only Excel exports are possible
- Diagrams cannot be imported
- No EAST-ADL 6.0 exchange possible
- No exchange with proprietary Analysis Toolsuites (Isograph, APIS, etc.) possible

SAFE Requirement 8 – Support of variability

- Not evaluated

Figure 17: Summary

5 Conclusion

The following conclusions represent a common viewpoint synthesized from both evaluation scenarios.

5.1 SAFE Criteria

With the results of the previous chapters, the overall performance of the SAFE platform in terms of pre-defined project criteria is assessed as follows:

Evaluation Criterium	Qualitative statement	Rationale
Correct and comprehensible documentation	good	Documentation is clear and understandable
Compliant with SAFE meta-model	incomplete	Mains features seems to be in, but there is no interchange format available with SAFE meta model PREEvision support feature for transformation and import mechanism but not instantiated for SAFE meta model (and EAST-ADL model)
Correct implementation of SAFE methods	sufficient	Hazard analysis and Requirement capture and tracing concept are incorporated and valid. System modeling is possible and interrelations with requirements are adequate. Failure propagation methodology are partly implemented therefore FTA and FMEA suffers the lack of automation and dependency failures identification. Safety Planning, Safety Assessment and Safety Argumentation are hardly possible in a model. So there is urgent need to incorporate the model in an overall planning, assessment, decision and conclusion process.
Correct and seamless interoperability with other SAFE work products	N/A	
Reasonable support for manual or semi-automated activities	sufficient	PREEvision offers various capabilitites for the user for writing queries. However automation of FTA/ FMEA are missing.
Training level and expertise required for usage	incomplete	With today user interface and mechanism PREEvision technology is only adequate to modeling and programming specialist. Any mechanical/automation engineers would need a strong training to be able to model and configure the environment (5 days training actually in the Vector catalog).

Evaluation Criterium	Qualitative statement	Rationale
Tailoring capabilities	perfect	High level of tailoring of the environment for applying methods as rules can define to verify or generate model, and plug-in can be created for more complex function (but require high level of expertise)

Table 5: Fulfillment of predefined SAFE Criteria

5.2 Automotive Development Criteria

The general benefit of the SAFE platform within the automotive development cycle is judged as follows. Beyond the estimated efficiency increase it has to emphasized that the safety argumentation itself is not possible within the conventional engineering framework. So arguing Safety is a stake itself, irrespective of any efficiency claim.

	Tier 1
HW Development	
Effort Reduction	5%-10%
Rationale	• Early requirement elicitation and metrics compliance prediction (“frontloading”)
SW Development	
Effort Reduction	5%-10%
Rationale	• Early fault isolation definition • Early definition of monitoring and intrusion check concept
Safety Analysis	
Effort Reduction	2%-5%
Rationale	• Less Interface through seemless representation • Concurrent design/analysis • Potential semi-automatic analysis
System Design	
Effort Reduction	20% -25%
Rationale	• Better understanding through hierarchical approach • Better organisation of systems engineering methodology (prerequisite for safety engineering) • Re-use of architecture
Concept Phase	
Effort Reduction	20% - 25%
Rationale	• Graphical „all-in-one“ tooling alone the ISO26262 lifecycle • Graphical HA/SG representation as „initalisation“ of lifecycle

Table 6: Quantified benefit of SAFE versus engineering domain

The following comments are significant in terms of safety argumentation:

- The SAFE platform and in particular the PREEVision Extensions are highly appreciated
- A final Safety argumention is however achieved
- Incorporation of FSM expert work needs to be detailed (rather from requirement point of view):
  - Linking/Mapping alone is no Safety argument
  - Extent of automated approaches needs to be settled
- In general, the structured provision of safety arguments and justifications as required by ISO26262 is not achievable with any model-based approach.

- So there must be some justification/argumentation document compiled by safety experts, to which a model might provide inputs. The model cannot be this document

5.3 Final quantification of the work product

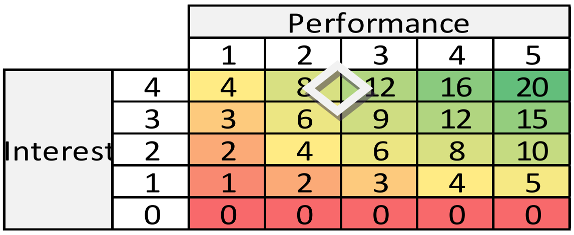
The performance vs. interest square for the SAFE product is judged from an evaluation outcome point of view as illustrated in Figure 1 below.

The metric *performance* is setup rating how well the expectations given in the work product description have been met (level 1-5):

- Level 5: Beyond expectations described in the Full Project Proposal and evaluation criteria
- Level 4: Expectation from Full Project Proposal and good level evaluation criteria met
- Level 3: Expectations not fully met or some evaluation criteria not reached sufficient level but significant improvement achieved
- Level 2: No significant improvement achieved or some evaluation criteria are rated incomplete
- Level 1: Negative impact (performance degraded) and all evaluation criteria are incomplete

This evaluation is crossed with a metric *industrial interest* qualifying the relevance of the method (or tool or methodology, respectively, level 1-4) covered by the corresponding evaluation scenario:

- Level 4: Interesting for evaluation scenario and ready for application in the field
- Level 3: Interesting for evaluation scenario but needs to be slightly matured for application in the field
- Level 2: Interesting for evaluation scenario but needs to be significantly matured for application in the field
- Level 1: Not of interest for the specific evaluation scenario but interesting anyway for application in the field (not considered further for project evaluation – no detailed evaluation result available)
- Level 0: Out of scope of evaluation scenario, not of interest for application in the field.



		Performance				
		1	2	3	4	5
Interest	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
	0	0	0	0	0	0

Figure 1: Performance vs. Interest Square

Besides the issues fed back to the work task, the general position of any model-based approach within the safety assessment process has to be clarified and defined.

6 References

[1] SAFE Requirements

https://safe.offis.de/svn/svndav/40_Deliverables/SAFE_D2.1.a/SAFE_D2.1.a.pdf

[2] SAFE Report of WT3.6

https://safe.offis.de/svn/svndav/33_WP3_Model_Based_Development/WT3_6_Safety_Code_Generation/Deliverables/SAFE_WT3.6_Report.doc

[3] Classification of safety mechanisms

https://safe.offis.de/svn/svndav/33_WP3_Model_Based_Development/WT3_6_Safety_Code_Generation/Documents/safetymechanismclustering/safetymechanismclustering.eap

[4] SAFE Risk List

https://safe.offis.de/svn/svndav/10_Project_Management/SAFE_Plus-Minus-Risks.xlsx

[5] SAFE FPP

https://safe.offis.de/svn/svndav/10_Project_Management/FPP/!Actual_Official_Version/SAFE_FPP.docx

[6] SAFE_D2.1.a-ISO-Part_2.pdf (Management of functional safety)

[7] SAFE_D2.1.a-ISO-Part_3.pdf (Concept Phase)

[8] SAFE_D2.1.a-ISO-Part_4.pdf (Product development at the system level)

[9] SAFE_D2.1.a-ISO-Part_5.pdf (Product development at the hardware level)

[10] SAFE_D2.1.a-ISO-Part_6.pdf (Product development at the software level)

[11] SAFE_D2.1.a-ISO-Part_7.pdf (Production and operation)

[12] SAFE_D2.1.a-ISO-Part_8.pdf (Supporting Processes)

[13] SAFE_D2.1.a-ISO-Part_9.pdf (Automotive Safety Integrity Level (ASIL)-oriented safety-oriented analysis

[14] ISO/FDIS 26262 parts 2-9: 2011.

[15] WT 5.2.2 Evaluation Scenario - Electrical Brake System

[16] Vikram Kothari. Model based representation of safety concept of an electronic “By-Wire” brake system using extended PREEvision development environment. Diploma Thesis. Continental AG, Kaiserslautern University.

[17] Stefan Buch. Modellerstellung eines elektonischen By-Wire Bremssystems in einer erweiterten PREEvision Entwurfsumgebung. Dipolma Thesis. Continental AG, Rhein-Main University of Applied Sciences.

[18] Bessem Ben Arbia. Fehlerbaumanalyse eines zukünftigen Bremssystems. Diploma Thesis. Continental AG, Darmstadt University of Technology.

[19] Stefan Buch, Vikram Kothari, Modeling with PREEvision Extentions. Continental AG.

[20] Adler, Metzker, Otten, Rudolph. ISO26262 DESIGN UND ANALYSE FUNKTIONAL SICHERER HARDWARE IN EINEM elektronische Bremssystem. Submitted for Publication.

[21] EMS_requirements_evaluation

7 Acknowledgments

This document is based on the SAFE project in the framework of the ITEA2, EUREKA cluster program Σ! 3674. The work has been funded by the German Ministry for Education and Research (BMBF) under the funding ID 01IS11019, and by the French Ministry of the Economy and Finance (DGCIS). The responsibility for the content rests with the authors.