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

WP3

Deliverable D3.1.1 b: Final proposal for extension of meta-model for hazard and environment modeling

Due date of deliverable: 28/02/13

Actual submission date: 08/03/13

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

Project coordinator name: Stefan Voget

Organization name of lead contractor for this deliverable: OFFIS

Editor: Andreas Baumgart

Contributors: Marion Suerken, Thomas Peikenkamp, Hans-Leo Ross, Stefan Voget, Philippe Cuenot, Christophe Etienne,

Reviewers: Christoph Ainhauser, Philippe Cuenot

Revision chart and history log

Version	Date	Reason
0.1	2013-02-20	Initialization of document
0.2	2013-02-22	Update Scope of WT 3.1.1, Methodology of Hazard and Risk Assessment, and WT 3.1.1 Contribution to SAFE Meta-Model
0.3	2013-02-29	Update Hazard Description Language
0.4	2013-03-04	Review Version of the document
1.0	2013-03-08	Incorporation of review comments, finalization of deliverable

1 Table of contents

2 List of figures

3 Executive Summary

The work task 3.1.1 targets the topics of hazard analysis and risk assessment, determination of safety goals and ASIL definition according to ISO 26262.

Besides giving an overview on the relevant sections of ISO 26262 the requirements allocated to WT 3.1.1, which are resulting from the ISO 26262 analysis of WT 2.1, and the use case descriptions of WT 2.3 are presented. In an additional section, the current achievements on the requirements allocated to WT 3.1.1 are presented.

In addition to the previous mentioned overview, the initial methodology for hazard analysis and risk assessment in accordance with ISO 26262 is presented. Since it is the objective to develop a meta-model extension for hazard analysis and risk assessment, the current version of EAST-ADL is analyzed. Moreover, the contribution of WT 3.1.1 to the SAFE meta-model, which is based on EAST-ADL, is presented.

4 Introduction and overview of document

The document at hand provides information about a final methodology for the hazard analysis and risk assessment and an initial proposal for an extension of the SAFE meta-model that enables a proper hazard and environment modeling which is developed in WT 3.1.1. In the following subsection the scope of the work task as well as the structure of the document is presented.

4.1 Scope of WT 3.1.1

Embedded in work package 3, work task 3.1.1 deals with the hazard and environment modeling including the determination of safety goals and the respective ASIL. The basis for this work task is the dependability part of EAST-ADL which is presented in chapter 7. WT 3.1.1 aims to provide a methodology for the hazard analysis and risk assessment and a meta-model extension suitable for the mentioned topics to WT 3.5. In order to be able to do so, mainly the following artifacts and their interrelations are considered:

Operational Situation

Within WT 3.1.1 a suitable concept for modeling operational situations shall be developed. This includes the representation of the environmental conditions as well as conditions set by the driver or other traffic participants (e.g. other vehicles, pedestrians). The concept shall also enable a formal as well as informal expression of the operational situations.

Hazard

Hazards represent the potential source of harm and form a key aspect of the hazard analysis and risk assessment. WT 3.1.1 shall provide a concept to express hazards in formal as well as informal formulation.

Hazardous Event

Hazardous events are relevant combinations of hazards and operational situations in a given operating mode. It is planned to develop a suitable representation of hazardous events that allows informal as well as formal expression. Moreover, the concept for hazardous events shall enable the classification according to the parameters severity, probability of exposure, and controllability. Based on these parameters the ASIL classification is performed which shall be supported by the meta-model concept.

Safety Goal

Based on the hazardous events safety goals need to be derived. The meta-model extension developed in this work task shall enable to document the safety goals with their respective parameters and to express the safety goals informally and formally. In addition to this it shall be enabled to associate a safe state (“operating mode of an item without an unreasonable level of risk” [1]) with the safety goal. Moreover, it shall be possible to check whether the safety goals correctly address the hazardous event that means that fulfilling the safety goal leads hazard mitigation.

During the requirement elicitation performed in work task WT2.1 and the resulting deliverable D2.1b, requirements were allocated to work task WT3.1.1. These requirements and their coverage in WT 3.1.1 are listed in the following.

4.1.1 Scope with regard to ISO 26262 part 3

Requirement 03_005 (relates to ISO 26262 part 3, clause 5.4.1)

Safe product shall allow to capture dependencies of the items with its environment

Status: Covered

Requirement 03_007 (relates to ISO 26262 part 3, clause 5.4.2 c) d) e))

Safe product shall allow to model the interface of the items and interaction between them or with the environment

Status: Covered

Requirement 03_009 (relates to ISO 26262 part 3, clause 5.4.2 b), g))

Safe product shall allow to capture bevioural interaction between items and environment describing operating scenario and effects on items

Status: Covered

Requirement 03_012 (relates to ISO 26262 part 3, clause 6.4.1)

Safe product shall support categorization of item and environment as a) new development b) modification of existing items or environment

Status: Covered

Requirement 03_017 (relates to ISO 26262 part 3, clause 6.4.2.1)

Safe product shall support categorization of item and environment as a) new development b) modification of existing items or environment

Status: Partially Covered

- WT 3.1.1 only addresses dependencies between hazards, safety goals, safety requirements, operational situations. The requirement should not be excluded because SAFE methods provide outstanding facilities to do semantically founded impact analysis. System model can identify the new, existent and modification product.

Requirement 03_019 (relates to ISO 26262 part 3, clause 6.4.2.2 / 6.4.2.3 / 6.4.2.3)

Safe process shall allow to trace all items areas and work product affected by a modification as a) operational situtation and operating modes, b) interface with the environment c) installations characteristics, d) range of environmental conditions [impact analysis]

Status: Partially Covered

- The environmental condition are not necessarily part of the model properties ? (others then in requirement classification from 5.4.1 b)

Requirement 03_020 (relates to ISO 26262 part 3, clause 6.4.2.2)

Safe process shall support identification of differences between previous and future conditions of use of the item.

Status: Covered

Requirement 03_035 (relates to ISO 26262 part 3, clause 7.4.1)

Safe processes for hazard analysis and risk assessment shall be based on the item definition.

Status: Covered

Requirement 03_36 (relates to ISO 26262 part 3, clause 7.4.1.1 / 7.4.2.2.2)

Safe product shall allow to represent hazards of the item on the vehicle level.

Status: Covered

Requirement 03_37 (relates to ISO 26262 part 3, clause 7.4.1.2)

Safe product shall distinguish between the representation of the item and its safety mechanism

Status: Partially Covered

- WT 3.1.1 does not address the representation of safety mechanisms.

Requirement 03_38 (relates to ISO 26262 part 3, clause 7.4.1.2)

Safe process shall allow evaluation of item in context of hazard analysis and risk assessment with and without safety mechanisms.

Status: Covered

Requirement 03_39 (relates to ISO 26262 part 3, clause 7.4.2.1)

Safe product shall support description of operational situation and operating modes for malfunction behavioural description resulting to a hazard event (for correct usage of the vehicle but also incorrect usage)

Status: Covered

Requirement 03_40 (relates to ISO 26262 part 3, clause 7.4.2.2.1 / 7.4.2.2.2)

Safe process shall allow to determine hazard defined in term and condition or behavior observed at vehicle level (a usage of model information is expected from project scope)

Status: Covered

Requirement 03_41 (relates to ISO 26262 part 3, clause 7.4.2.2.1)

Safe product shall allow to represent the results of activities listed in 7.4.2.2.1.

Status: Covered

Requirement 03_42 (relates to ISO 26262 part 3, clause 7.4.2.2.3)

Safe product shall support to capture hazards and hazardous events

Status: Covered

Requirement 03_43 (relates to ISO 26262 part 3, clause 7.4.2.2.3)

Safe product shall allow to represent hazardous events which are the outcome of combinations of hazards and operational situations.

Status: Covered

Requirement 03_44 (relates to ISO 26262 part 3, clause 7.4.2.2.4)

Safe product shall support traceability of hazardous event to operation situation and hazard

Status: Covered

Requirement 03_45 (relates to ISO 26262 part 3, clause 7.4.2.2.4)

Safe product shall allow to capture consequence of hazardous event on the item and the function, as associated functional failure and propagation ton the different items

Status: Partially Covered

- Capturing functional failures (functional models) and capturing propagation (propagation model) is addressed by WT 3.3.1

Requirement 03_47 (relates to ISO 26262 part 3, clause 7.4.2.2.4)

Safe process shall support identification of consequences of hazardous events.

Status: Partially Covered

- WT 3.1.1 addresses specification of safety goal.

Requirement 03_48 (relates to ISO 26262 part 3, clause 7.4.2.2.5)

Safe product shall allow to categorize the hazard and hazardous event as E/E related or others domain (in order to highlight them to responsible person to take appropriates measures)

Status: Covered

Requirement 03_49 (relates to ISO 26262 part 3, clause 7.4.2.2.5)

Safe process shall allow to identify and highlight hazards which are outside the scope of ISO 26262.

Status: Partially Covered

- Relationship to other items which are out of scope of the ISO 26262 is possible.

Requirement 03_50 (relates to ISO 26262 part 3, clause 7.4.3)

Safe product shall provide the possibility to represent the parameters for severity, probability of exposure, and controllability for each hazardous event.

Status: Covered

Requirement 03_51 (relates to ISO 26262 part 3, clause 7.4.3.1)

Safe product shall support the classification of hazardous events

Status: Covered

Requirement 03_52 (relates to ISO 26262 part 3, clause 7.4.3.1)

Safe process shall allow to check whether all hazardous events which are in scope of ISO 26262 are classified.

Status: Covered

Requirement 03_53 (relates to ISO 26262 part 3, clause 7.4.3.2 / 7.4.3.3)

Safe product shall allow to capture Severity level (S0 to S3) for each potential hazardous event and help context shall be provided for selection of the level (e.g. table 1 value and recommendation for S0 to impact only on material damage)

Status: Covered

Requirement 03_54 (relates to ISO 26262 part 3, clause 7.4.3.2 / 7.4.3.3)

Safe process shall support the severity classification for each hazardous event based on an operational scenario. The severity shall be assigned to one of the classes presented in table 1, ISO 26262-3:2011.

Status: Covered

Requirement 03_55 (relates to ISO 26262 part 3, clause 7.4.3.4 / 7.4.3.5 / 7.4.3.6)

Safe product shall allow to capture Exposure level (E0 to E4) for each potential hazardous event and help context shall be provided for selection of the level (e.g. table 2 value and consideration of number of vehicle equipped with the item, recommendation for E0 about incredible situation)

Status: Covered

Requirement 03_56 (relates to ISO 26262 part 3, clause 7.4.3.4 / 7.4.3.5 / 7.4.3.6)

Safe process shall support determination of probability of exposure for each hazardous event based on an operational scenario. The probability of exposure shall be assigned to one of the classes presented in table 2, ISO 26262-3:2011.

Status: Covered

Requirement 03_57 (relates to ISO 26262 part 3, clause 7.4.3.7 / 7.4.3.8)

Safe product shall allow to capture the Controllability level (C0 to C3) for each potential hazardous event and help context shall be provided for selection of the level (e.g. table 3 value and recommendation for C0 where existing recommendation are defined by standards)

Status: Covered

Requirement 03_58 (relates to ISO 26262 part 3, clause 7.4.3.7 / 7.4.3.8)

Safe process shall support determination of controllability for each hazardous event based on an operational scenario. The controllability shall be assigned to one of the classes presented in table 3, ISO 26262-3:2011.

Status: Covered

Requirement 03_59 (relates to ISO 26262 part 3, clause 7.4.4.1)

Safe process shall support automatic calculation of ASIL level from Severity, Exposure and Controllability and propagate ASIL level (from Table 4 - ASIL determination) to hazardous event and related elements (items, requirement, scenario…)

Status: Partially Covered

- Definition of Hazardous Event allows determination of ASIL

Requirement 03_60 (relates to ISO 26262 part 3, clause 7.4.4.2)

Safe product shall support a standardized list of operational situations to prevent the lowering of ASIL level

Status: Covered

Requirement 03_61 (relates to ISO 26262 part 3, clause 7.4.4.3)

Safe product shall allow to capture a safety goal for each hazardous event

Status: Covered

Requirement 03_62 (relates to ISO 26262 part 3, clause 7.4.4.3)

Safe process shall support determination of identical safety goal for combination

Status: Covered

Requirement 03_64 (relates to ISO 26262 part 3, clause 7.4.4.4)

Safe product shall allow to assign the ASIL of the hazardous event to the respective safety goal.

Status: Covered

Requirement 03_65 (relates to ISO 26262 part 3, clause 7.4.4.4)

Safe product shall provide the facility to represent the combination of safety goals and their associated ASILs.

Status: Covered

Requirement 03_66 (relates to ISO 26262 part 3, clause 7.4.4.6

Safe product shall support safety goal modeling in an unambiguous way (informal, semi formal or formal) according to ISO26262-8 clause 6

Status: Covered

Requirement 03_67 (relates to ISO 26262 part 3, clause 7.4.5.1)

Safe process shall allow verification of hazard analysis, risk assessment and safety goal specification and integration of results in safety plan

Status: Covered

Requirement 03_68 (relates to ISO 26262 part 3, clause 7.4.5.1 a) c) e))

Safe process shall support verification of hazard analysis and risk assessment phase according to completeness in regard to situation and hazard, consistency of the analysis and consistency of ASIL level with the hazardous event

Status: Covered

Requirement 03_69 (relates to ISO 26262 part 3, clause 7.4.5.1 b))

Safe process shall support verification of hazard analysis and risk assessment phase according to compliance and traceability of the items

Status: Covered

Requirement 03_70 (relates to ISO 26262 part 3, clause 7.4.5.1 d))

Safe process shall support verification of hazard analysis and risk assessment phase according to completeness of the coverage of hazardous event

Status: Covered

Requirement 03_71 (relates to ISO 26262 part 3, clause 7.4.5.1 c))

Safe process shall allow to perform consistency check of hazard analysis, risk assessment, and safety goals with related hazard analysis and risk assessments.

Status: Covered

Requirement 03_77 (relates to ISO 26262 part 3, clause 8.4.2.1)

Safe product shall support derivation and traceability versus safety goals and safe states

Status: Covered

Requirement 03_78 (relates to ISO 26262 part 3, clause 8.4.2.1)

Safe product shall support a preliminary architectural description with initial assumption

Status: Covered

Requirement 03_87 (relates to ISO 26262 part 3, clause 8.4.2.6)

Safe product shall allow to capture the necessary actions and adequate means to be performed by the driver or others persons, to comply to safety goal. Safe product shall also allow to include this in the functional safety concept.

Status: Partially Covered

- WT 3.1.1 addresses compliance with safety goal, inclusion in functional safety concept is a topic of WT 3.2.1.

Requirement 03_98 (relates to ISO 26262 part 3, clause 8.4.3.3 a) b) c))

Safe product shall allow to capture and identify external measures and its interface

Status: Partially Covered

- External measures are not completely in scope of WT 3.1.1.

Requirement 03_99 (relates to ISO 26262 part 3, clause 8.4.3.3 c))

Safe product shall allow derivation and trace of functional safety requirement into external measures

Status: Partially Covered

- External measures are not completely in scope of WT 3.1.1, traceability of functional safety requirements is a topic of WT 3.2.1.

Requirement 03_100 (relates to ISO 26262 part 3, clause 8.4.3.3 d))

Safe product shall allow backward traceability of external measure in system architural element (from ISO26262-4)

Status: Partially Covered

- External measures are not completely in scope of WT 3.1.1, traceability to system architectural element is a topic of WT 3.2.1.

4.1.2 Scope with regard to ISO 26262 part 4

Requirement 04_23 (relates to ISO 26262 part 4, clause 6.4.1.1 b))

The Safe product shall support the definition of system constraints, e.g. The environmental conditions or functional constraints

Status: Partially Covered

- Specification of environment conditions or functional constraints is addressed by WT 3.1.2

Requirement 04_24 (relates to ISO 26262 part 4, clause 6.4.2.1)

The Safe product shall allow to specify response time of a system to stimuli (timing requirement)

Status: Partially Covered

- Durations can be specified for values of vehicle variables in hazard specifications.

Requirement 04_24 (relates to ISO 26262 part 4, clause 6.4.2.1)

The Safe product shall allow to specify timing information in various systems or stimuli configuration (failure, operating states)

Status: Partially Covered

- Operating modes can be defined for an item.

Requirement 04_28 (relates to ISO 26262 part 4, clause 6.4.2.3)

The Safe product shall allow to specify behavioral description of safety mechanism based on safe state (to represent operating state and safe state, failure and fault tolerant time, emergency operation, measure to maintain operating states)

Status: Partially Covered

- WT 3.1.1 addresses the usage of formal methods. Hazards can be described in a way that it is possible to determine level of risk mitigation. System model (WT 3.2.1) should include safety behaviour (in functional description).

Requirement 04_87 (relates to ISO 26262 part 4, clause 7.4.8.1)

The Safe product shall be able to capture or hook the results of conducted safety verification activities

Status: Covered

Requirement 04_100 (relates to ISO 26262 part 4, clause 8.4.1.7 / 8.4.2 / 8.4.3 / 8.4.4)

The Safe product shall allow to specify verification activities. A verification activity shall define the verified system element, the assured requirements, the executed test cases, the verified system variants, the responsible person and the used test environment

Status: Partially Covered

- In context of verification hazard and risk assessment is enabled.

The Safe produce shall allow to document verification results. A verification result defines for a conducted verification activity the date of execution, the output captured during the execution and the indication of success (e.g. fail or pass)

Requirement 04_102 (relates to ISO 26262 part 4, clause 8.4.1.7 / 8.4.2 / 8.4.3 / 8.4.4)

The Safe produce shall allow to document verification results. A verification result defines for a conducted verification activity the date of execution, the output captured during the execution and the indication of success (e.g. fail or pass)

Status: Partially Covered

- Results of hazard and risk assessment can be defined.

Requirement 04_131 (relates to ISO 26262 part 4, clause 9.4.2.1)

The Safe product shall allow to describe a validation plan containing information as defined in requirement 9.4.2.1

Status: Partially Covered

- Process assessment with 6.1 is targeted

Requirement 04_133 (relates to ISO 26262 part 4, clause 9.4.3.2)

The Safe product shall allow to attach a validation strategy for each safety goal, in order to test the controllability and the effectiveness of safety measures, external measures and elements of other technologies

Status: Partially Covered

- Hazards have to be described in a way that they can be validated against safety goals.

Requirement 04_134 (relates to ISO 26262 part 4, clause 9.4.3.2)

The Safe process shall provide a method which (semi-) automatically generates validation scenarios for each safety goal to validate the functional safety of the item. A validation scenario describes operating situations and failure modes where the controllability of the vehicle and the effectiveness of safety measures, external measures and elements of other technologies shall be demonstrated. It takes for example results of the hazard and risk analysis as input, e.g. the driving situation

Status: Partially Covered

- Hazards have to be described in a way that they can be validated against safety goals.

Requirement 04_139 (relates to ISO 26262 part 4, clause 9.4.3.4)

The Safe product shall allow to track the results of the validation at the vehicle level, by specifying additional context information as proposed in requirement 9.4.3.4

Status: Partially Covered

- Hazards have to be allocated to item but described at vehicle level.

Requirement 04_140 (relates to ISO 26262 part 4, clause 9.4.3.4)

The Safe product shall support traceability for validation and sanction of test with respect to safety goals

Status: Partially Covered

- Traceability to safety goal is provided

Requirement 04_144 (relates to ISO 26262 part 4, clause 10.4.1)

The Safe model (process and product) shall support the functional safety assessment by proposing the topics to be addressed by the assessment and provide simple navigation through the required pieces of the Safe model

Status: Covered

4.1.3 Scope with regard to ISO 26262 part 5

Requirement 05_31 (relates to ISO 26262 part 5, clause 7.4.1.7 / 7.4.2.2)

The safe product artifacts shall allow to document and capture non functional cause of failure of safety related hardware component (temperature, vibration, EMC….)

Status: Partially Covered

- WT 3.1.1 only for addressing environment conditions on vehicle and item level. Documenting non-functional causes of failures for hardware-components has to be done on hardware level (WT 3.2.2)

4.1.4 Scope with regard to ISO 26262 part 8

Requirement 08_11 (relates to ISO 26262 part 8, clause 6.4.2.3 / 6.4.3.2 / 6.4.3.1)

Safe product shall support traceability by allowing for the allocation of safety requirements to elements or items, in a manner that allows for impact analyses.

Status: Partially Covered

- Traceability of safety requirements to item and hazards is supported. This requirement is addressed by other work tasks such as WT 3.6 where the relation between generated safety mechanisms and the according design element will be captured. This information can be used for impact analysis

4.1.5 Scope with regard to ISO 26262 part 9

Requirement 09_50 (relates to ISO 26262 part 9, clause 8.4.1)

Safe product shall allow to represent the results of safety analyses

Status: Partially Covered

- Results of hazard and risk assessment are supported.

Requirement 09_54 (relates to ISO 26262 part 9, clause 8.4.5)

Safe process shall allow to introduce newly identified hazards in accordance with the change management in ISO 26262-8

Status: Covered

4.1.6 Scope with regard to methods and use cases

The following requirements were identified in work task WT 2.3.

Requirement M12-003 (relates to Method M12)

SAFE process shall allow to quantify achievement of safety targets.

Status: Covered

Requirement M12-003 (relates to Method M12)

SAFE process shall allow to compare the safety characteristics of different architectures.

Status: Partially Covered

- Comparison of safety characteristics is possible on vehicle level, not for the item architecture.

Requirement M12-005 (relates to Method M12)

SAFE product shall allow to represent quantitative dependencies.

Status: Covered

4.2 Structure of the document

The document is structured as follows:

Subsequent to the introduction an overview on the parts of ISO 26262, which are relevant for the hazard and environment modeling, is given.

Within section 6, the methodology for the hazard analysis and risk assessment according to ISO 26262 is explained. To do this, in a first step a general introduction to the methodology is given. In addition to this, the formulation of hazardous events (6.4), the classification of hazardous events and determination of controllability (6.5), and the derivation of safety goals (6.6) are elaborated in corresponding subchapters.

Section 7 deals with EAST-ADL. On the one hand, the current version of EAST-ADL and in particular the dependability part is described. On the other hand, some proposed extensions to this current version are explained which enhance the possibility to perform hazard analyses and risk assessments in compliance with ISO 26262.

The contribution of WT 3.1.1 to the SAFE meta-model is described in section 8. Within this section an overview on the part of the meta-model as well as a detailed description of the classes and links used to construct the meta-model is presented. Moreover, an example for the application of the meta-model for hazard and risk analysis is presented.

In section 9 the relevant interdependencies to other work tasks of SAFE are depicted and explained.

Finally, in section 10 a conclusion and discussion is given.

5 Overview on ISO 26262

Within this section, an overview on the relevant parts of ISO 26262 with regard to hazard and environment modeling is given. The selection of the presented parts is based on the source of the SAFE requirements elicited in WT 2.1 which are allocated to WT 3.1.1.

Addressing the development process of electric / electronic components for passenger cars, the ISO 26262 “Road vehicles – Functional safety” came into effect in November 2011. This standard introduces a safety lifecycle which “encompasses the principal safety activities during the concept phase, product development, production, operation, service and decommissioning” ([1], part 2, p.3) and which can be seen as a guideline that demands a risk-based development approach with seamless traceability. In Figure 1, an overview on the different parts of ISO 26262 is given.

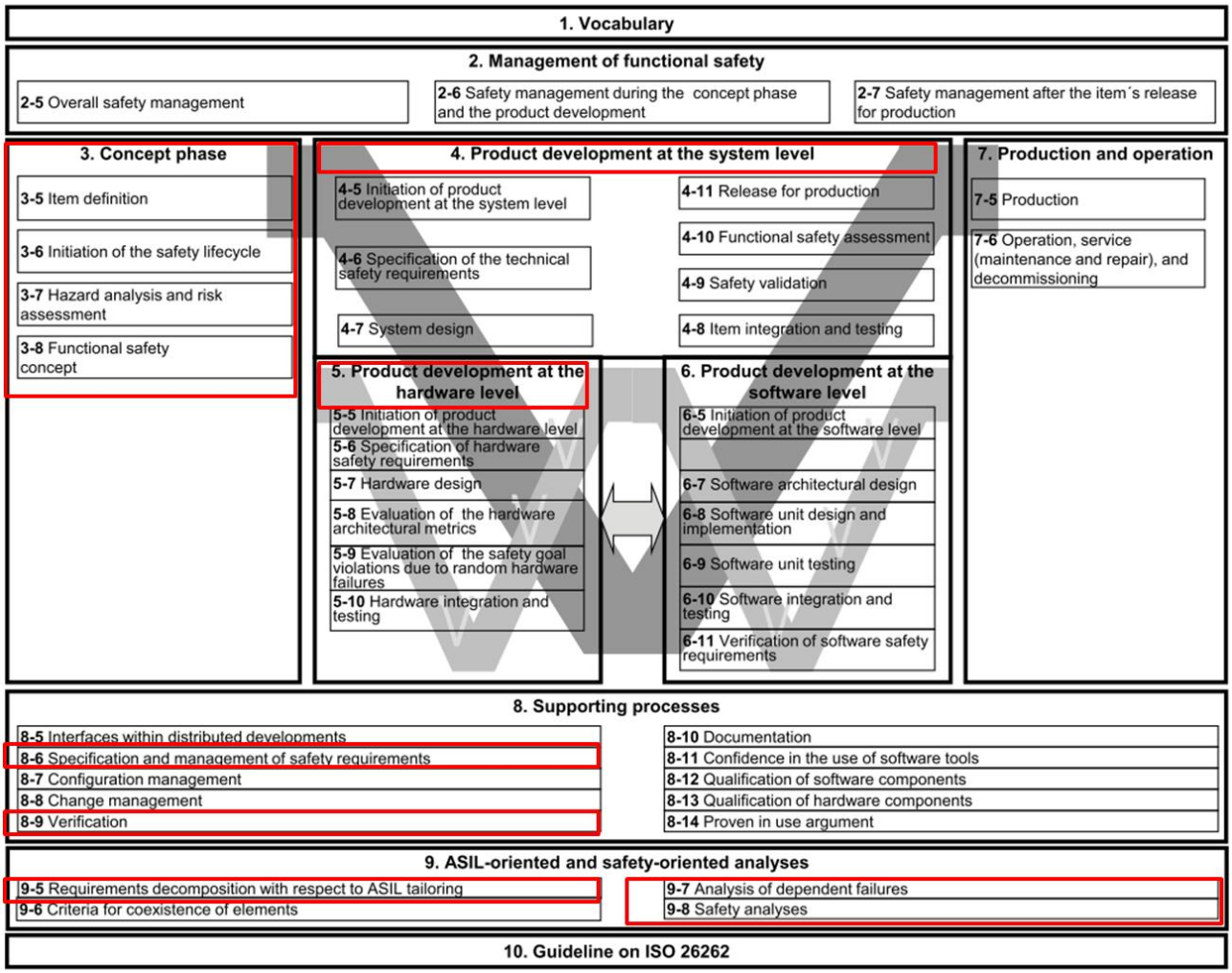

Figure 1: Overview on ISO 26262 (Relevant parts highlighted)

The requirements relevant for the hazard analysis and risk assessment as well as the derivation of safety goals are mainly provided in ISO 26262:2011, Part 3 and in particular in clause 7 which is also titled “Hazard analysis and risk assessment”. However, with regard to traceability to the safety goal and traceability to results of the hazard and risk assessment also requirements from other parts of the ISO 26262 are involved which are also addressed by other work-tasks of the SAFE project, namely requirements from Part 4 (Product development – System level), Part 5 (Product Development – Hardware level), Part 8 (Supporting processes), and Part 9 (Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analyses). In the following, an overview on the relevant aspects from the respective parts is given.

Part 3: Concept Phase

The concept phase comprises mainly four different parts, namely the item definition, the initiation of the safety lifecycle, the hazard analysis and risk assessment, and the functional safety concept. These parts are explained in the following.

Item Definition

The objective of the definition is to provide an overview on the item, the implemented functionalities and the dependencies as well as interactions of the item with the environment or other items of the vehicle. This information shall be provided in form of functional and non-functional requirements of the item. Moreover, the item definition includes a boundary description of the item as well as of elements of the item, i.e. a description of the interfaces and the expected as well as provided functionalities and interactions.

Initiation of the Safety Lifecycle

During the sub-phase of the initiation of the safety lifecycle it is distinguished between new developments and modifications of existing items. Depending on this the entire safety lifecycle or a tailored version needs to be applied. Thus, this distinction between a new or a modified item also has to be taken into account during the item definition, the hazard and risk assessment, and in subsequent steps.

Hazard Analysis and Risk Assessment

In general, the hazard analysis and risk assessment takes place based on the item definition and evaluates present risks without taking into account internal safety mechanisms of the item.

In a first step of the analysis, possible operational situations that are scenarios which might occur during the vehicles lifetime are collected. In this step it is important also to cover situations that arise through foreseeable misuse of the vehicle. Subsequent to the definition of operational situations hazards which are related to the item need to be determined. Although the hazards need to be related to the item and are associated with a malfunction of the item, the description takes place on vehicle level, i.e. the resulting behavior at vehicle level needs to be determined. After identifying the hazards, relevant combinations of both, hazards and operational situations, are captured as hazardous events. These hazardous events are subject to classification according to the three parameters controllability, probability of exposure and severity. Based on the parameters the ASIL (Automotive Safety Integrity Level) is determined and assigned to the hazardous event. In case the determination of the ASIL leads to ASIL A, B, C or D, a safety goal has to be derived from the particular hazardous event. These safety goals are the top-level safety requirements for the item and serve as a basis for the later development of the functional safety concept.

Functional Safety Concept

Subsequent to the hazard analysis and risk assessment the functional safety concept is developed. The functional safety concept consists of functional safety requirements and preliminary architectural assumptions. The functional safety requirements which are derived from the safety goals are allocated to the elements of the item.

Part 4: Product Development – System Level

During this phase the development of the item from the system level perspective takes place. The process is based on the concept of a V-model. Starting point (on the upper left side) is the specification of the technical safety requirements derived from functional safety requirements which are therefore traceable to the safety goal and results from the hazard and risk assessment. This step is followed by the development of the system architecture and the system design. The way up to the upper right point of the V-model is built by the integration, verification, validation and functional safety assessment activities.

Part 5: Product Development – Hardware Level

During this phase the development of the item from the hardware perspective is performed. The process is again based on a V-model, going down with the specification of hardware safety requirements derived from technical safety requirements which are therefore traceable to the safety goal and to results from the hazard and risk assessment. Furthermore hardware design and implementation and back upwards with hardware integration and testing are performed.

Part 8: Supporting Processes

The relevant requirements for WT 3.1.1 arise from two sections of part 8 (supporting processes), namely “Specification and management of safety requirements” and “Verification”. Therefore, only for these sections an overview is given.

Specification and Management of Safety Requirements

The objective of this section of ISO 26262 is to ensure that all safety requirements are specified correctly with respect to their attributes and characteristics and that the management of the safety requirements during the entire safety lifecycle is consistent.

Verification

Within the section “Verification” requirements are given which need to be fulfilled in order to ensure that the work products comply with their requirements.

Part 9: Automotive Safety Integrity Level (ASIL)-oriented and Safety-oriented Analyses

The relevant requirements for WT 3.1.1 arise from three sections of part 9 (automotive safety integrity level (ASIL)-oriented and safety-oriented analyses), namely “Requirements decomposition with respect to ASIL tailoring”, “Criteria for coexistence of elements” and “Safety analyses”. Therefore, only for these sections an overview is given.

Requirements Decomposition with respect to ASIL Tailoring

Within this section of part 9 of ISO 26262 requirements are given which provide “rules and guidance for the decomposition of safety requirements into redundant safety requirements” ([1], Part 9). This allows an “ASIL tailoring at the next level of detail” ([1], Part 9).

Criteria for Coexistence of Elements

Within this section of part 9 of ISO 26262 requirements are given that need to be fulfilled in case of coexisting safety-related sub-elements with and without an assigned ASIL as well as with different ASILs assigned. Mainly the goal is to avoid raising the ASIL from some sub-elements of an element to the ASIL of the element.

Safety Analyses

With the help of the safety analyses consequences of faults and failures on functions, behavior and design of items and elements shall be examined. Moreover, the analyses provide information on causes and conditions that could lead to the violations of a safety goal or safety requirement. Additionally, the analyses contribute to the identification of new hazards not discovered during the hazard analysis and risk assessment.

6 Methodology for Hazard Analysis and Risk Assessment

After presenting the relevant parts of ISO 26262 and the requirements from WP 2 allocated to WT 3.1.1 within this chapter the methodology for hazard analysis and risk assessment is described.

As already depicted in chapter 5, a key aspect of the ISO 26262 regarding the description of hazardous events is that they are not described in terms of item interface but rather in terms of the interface between the vehicle and its environment / driver. Hence other components, i.e. components that are integrated in the vehicle but do not represent the current item, may have an influence on the embodiment of the hazardous event.

Investigating the requirements given in ISO 26262 shows that it is demanded also to have a look at the roles of other components. An example for a requirement that implies this is that the hazards need to be “defined in terms of the conditions or behavior that can be observed at the vehicle level” (see ISO 26262:3-2011, requirement 7.4.2.2.2).

Although ISO 26262 requires looking at the risk emanating from the item without considering other elements of the vehicle architecture and without considering internal safety measures (cp. ISO 26262:3-2011, requirement 7.4.1.2), this risk itself is determined by the role of the item in the vehicle architecture. An example for this is that an EPS (electric power steering) system can be realized in a way that it can be overruled in any case by the driver. This would lead to a totally different classification compared to the realization of an EPS which cannot be overruled by the driver due to a too strong impact.

Therefore the model-based development process foreseen by SAFE has to take into account not only the item features but also all other elements / attributes that potentially contribute to the risk on vehicle level. The architecture suitable for the consideration of these needs has to fulfill the following aspects:

- there is a hierarchical architecture
- environmental aspects have to be distinguished
- functional / technical aspects have to be distinguished
- within technical aspects the hardware and software aspects need to be distinguished

The resulting architecture which is used is presented in Figure 2.

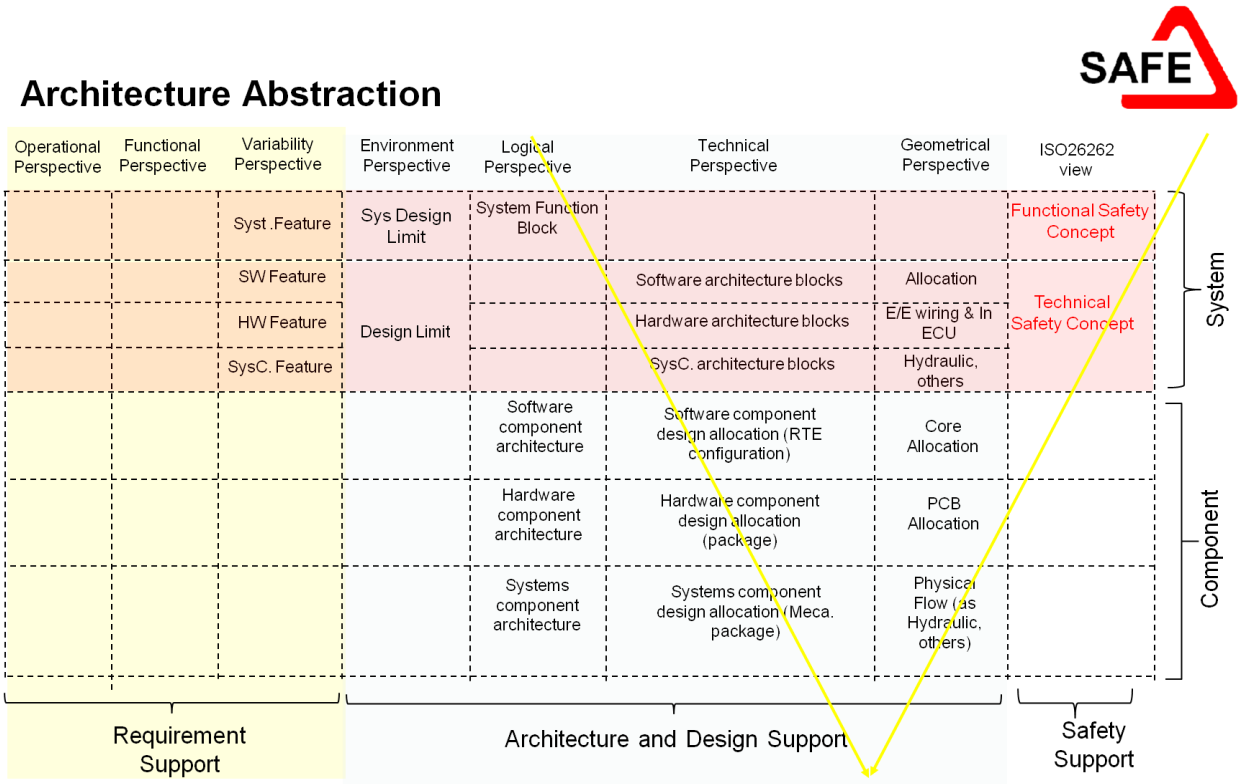

Figure 2: Overview on Structure of Architecture

Due to the structure of the architecture matrix shown in Figure 2 the ASIL allocation could be different. Moreover, ASIL decomposition could be applied on any horizontal level, which has influences to the lower horizontal levels. Analogous to this, safety requirements could be allocated to different elements within the horizontal level; this implies that a safety mechanism could be implemented into a sensor or alternatively into the controller or the actuator. By applying graceful degradation also the technical behavior in case of failure could be different and again this would lead to different inheriting of safety requirements to lower horizontal level.

Therefore, a detailed traceability to safety goals and results of the hazard and risk assessment is essential for requirements and the underlying architecture.

Key Steps of Hazard Analysis and Risk Assessment

Based on the considerations described above, the key steps of the hazard analysis and risk assessment can be formulated. A general aim is to avoid accidents. However, experience shows that product liability risks arise already in case on hazardous events which evolve from a malfunction of the respective product.

In the hazard analysis and risk assessment, the hazardous events have to be defined which are an outcome of the combination of operational situations and hazards in a given operating mode. Contributing factors to hazardous events are therefore:

- the environment (contributing to hazardous event via operational situation)
- the driver (contributing to the hazardous event via operational situation)
- other participants which might be pedestrians or other vehicles in the situation (contributing to the hazardous event via the operational situation)
- the vehicle including the way how the item is integrated into the vehicle (contributing to hazardous event via hazard)

The detailed description of the format for formal representation of hazardous events is given in section 6.4.

The hazardous events, or to be more precise the malfunctions related to dangerous situations (i.e. hazardous events), are subject to classification according to the parameters severity, probability of exposure and controllability, whereat the controllability and the probability of exposure can be seen as measures to reduce the severity. The determination of the controllability is explained in more detailed in section 6.5.1. Based on the previous named parameters the ASIL can be calculated.

In general it can be said that from the operational situations the hazardous events are derived. An example for a hazardous event may be “driving into the oncoming traffic”. The severity is then derived from the consequences of the hazardous event, for example “death in case person hits an oncoming vehicle with an impulse speed higher than 40 km/h”.

Moreover, it has to be considered that the item in its environment, which is the embedding of the item in the vehicle, could create malfunctions. At this time the first estimation is done about the probability of the malfunction for an item in its environment. In general it can be said that malfunctions can be a result of interactions of elements within one item or results of interactions of elements within the item and its environment.

Combining the worst case scenario and the possible malfunctions leads to the basis for the derivation of safety goals. The general term for the safety goal is to prevent or respectively avoid, limit, or mitigate, the malfunction and its consequences. For the detailed description of the safety goal derivation and allocation please refer to section 6.6.3 and 6.6.4.

Also within the hazard analysis and risk assessment the traceability needs to be ensured. The realization of this traceability can be seen in section 8, where the WT 3.1.1-contribution to the SAFE meta-model is described.

The application of the meta-model for the steps mentioned above is also described based on an example in section 8.3 in order to address the need of SAFE of implementing the steps based on the meta-model.

In the following sections the methodology for performing an ISO 26262 compliant hazard analysis and risk assessment in a model-based development process will be presented. In particular, it is shown how to layout the model such that hazard descriptions can be integrated in this process and such that the following criterions are satisfied:

- The elements and structure of the hazard descriptions is compliant to the ISO 26262;
- The hazard descriptions are linked to a model of the vehicle/item that can be subsequently refined in a traditional model-based development process;
- (Formal) safety goals can be checked against the descriptions of hazards and hazardous events.

Having such methodology available allows also the application of rigid V&V methods (see [13] and [14]). In particular, virtual integration tests become possible in the (very early) design phase when the functional safety concept is established. The description of the methodology is structured as follows. First an overview about related work is proved. Second, an overview about the process and the steps of the methodology are described. Finally the steps will be illustrated by means of an example.

6.1 Related work

In this section a brief overview about related work with regard to hazard and environment modeling is provided.

Automotive Generic Hazard List

The Automotive Generic Hazard List [9] has been defined on the basis of the approach of hazard lists used in military as well as railway applications and provides a means to structurally identify hazardous events. Currently, the list is specialized for the analysis of Advanced Driver Assistance Systems (ADAS). In general the AGHL has the form of a matrix in which variables assigned to the system environment can be associated with variables of the classes operation and accident. Hazardous events, which are combinations of the three factors system environment, operation, and accident, are labeled with a number. For every number stated in this matrix, there need to be a textual description in an additional document. The usage of a generic hazard list provides a useful complementary tool for the initial identification of hazards.

Requirements Specification Language

Stating requirements and formal verification are essential tasks in developing safety related systems. Formalizing requirements towards formal verifiable specifications was a task in the CESAR project [10]. The Requirements Specification Language (RSL) [5] was a major output of this project. An overview about the RSL and a description of its purpose and usage will be provided in section 6.6.1.

EAST-ADL

EAST-ADL [6] is an architecture description language that has been developed in various projects jointly by automotive OEMs, suppliers and tool vendors. The objective thereby is to define an architecture description language tailored to the needs of the automotive industry. With the hierarchical modeling concept which develops through the different abstraction levels the complexity of systems can be controlled more easily. EAST-ADL defines dependability concepts to capture item definition, hazards and hazardous events related to features of an automotive system. The error modeling concepts allow describing the abnormal behavior of a system architecture. An overview about EAST-ADL and a description of proposed extensions with regard to hazard and environment modeling will be provided in section 7.

6.2 Process Overview

The requirements on the hazard analysis and risk assessment according to ISO 26262 are stated in part 3, clause 7. The main input needed for the analysis is the item definition, which includes also the dependencies to and the interaction with other items of the vehicle as well as with the environment of the vehicle that can also be the driver or other traffic participants.

Based on the item definition in a first step the operational situations need to be determined. These are the driving situations that might occur during the vehicles lifetime. After that, the hazards, in this context a potential source of physical injury of persons which is caused by a malfunctioning behavior of the item, need to be identified. Although this hazard identification needs to be done for the item, the hazards have to be formulated as they are visible at vehicle level. This means that not the malfunction itself is described but the resulting behavior that can be recognized by the driver and/or other traffic participants. An important consequence for the description of hazards is that they need to be formulated in terms of variables that can be observed at vehicle level. When

we look at a steering system, a possible hazard is the inability to steer the vehicle in the desired direction. A formalization of the hazard would refer to variables reflecting the steering input of the driver and variables characterizing the actual movement of the car.

In case the operational situations are specified and the hazards are identified, relevant combinations out of these two sections need to be determined and modeled. The outcome is a list of hazardous events that can occur. These hazardous events are subject to classification according to three parameters, the controllability C, the severity S, and the probability of exposure E. The controllability determines the ability of the driver and other traffic participants to avoid the identified harm. The probability of exposure is determined based on the frequency of the operational situation or the duration of the operational situation. The severity is determined by an estimation of the injuries that might evoke in case of an accident. Based on the aforementioned parameters, the applicable ASIL can be determined according to table 4 provided in ISO 26262-3:2011 [1]. The combination of both, operational situations and hazards, need to be captured and modeled as hazardous events. Within the model-based development it is expected that all identified hazardous events can be "executed" in the model.

Subsequent to the ASIL determination a safety goal has to be derived from each hazardous event which states the hazard avoidance or mitigation. Since the safety goals are top-level safety requirements for the item, they need to be specified also according to the requirements with respect to the specification and management of safety requirements which are provided in ISO 26262, part 8, clause 6. Focal aspects of these requirements are that the safety requirements need to be unambiguous and comprehensible and that the safety requirement is allocated to an item. In addition, the traceability to the upper hierarchical level (which refers to the hazardous events) and the lower hierarchical level needs to be ensured.

The result of the hazard analysis, namely the safety goals defined for the item, is used as the starting point for the functional safety concept. Within the further development process it also needs to be demonstrated that a failure of a function does not lead to a violation of the safety goal. This can also be done by using model-based techniques with, for instance, a failure mode as a model property.

6.3 Item Definition

As it has been already stated a required input for the hazard analysis and risk assessment is the item definition. Within the ISO 26262, the requirements applicable are stated in part 3, clause 5.

In the item definition, the general functionality provided by the item, the interfaces of the item as well as functional and non-functional (e.g. legal requirements) requirements are defined. Moreover, the interaction and dependencies with the environment, that is not only other items but also the environment of the vehicle, is specified. This includes also known failure modes and their potential consequences.

With respect to the boundary of the item and the interaction with other items or the environment also the elements of the item and the allocation of functions among involved elements need to be determined. Additionally, the functionality required by other items or elements is part of the item definition.

6.4 Identification and Formulation of Hazardous Events

Having a closer look to the parts forming a hazardous event, namely hazards and operational situations, it gets visible that there are again different contributing factors forming each of them. The hazard is formed by the contribution of the vehicle that means the influences which come up due to the embedding of the item in the car. The operational situations are formed by the contributions of the driver, the environment, and other participants. The correlation is shown in Figure 3.

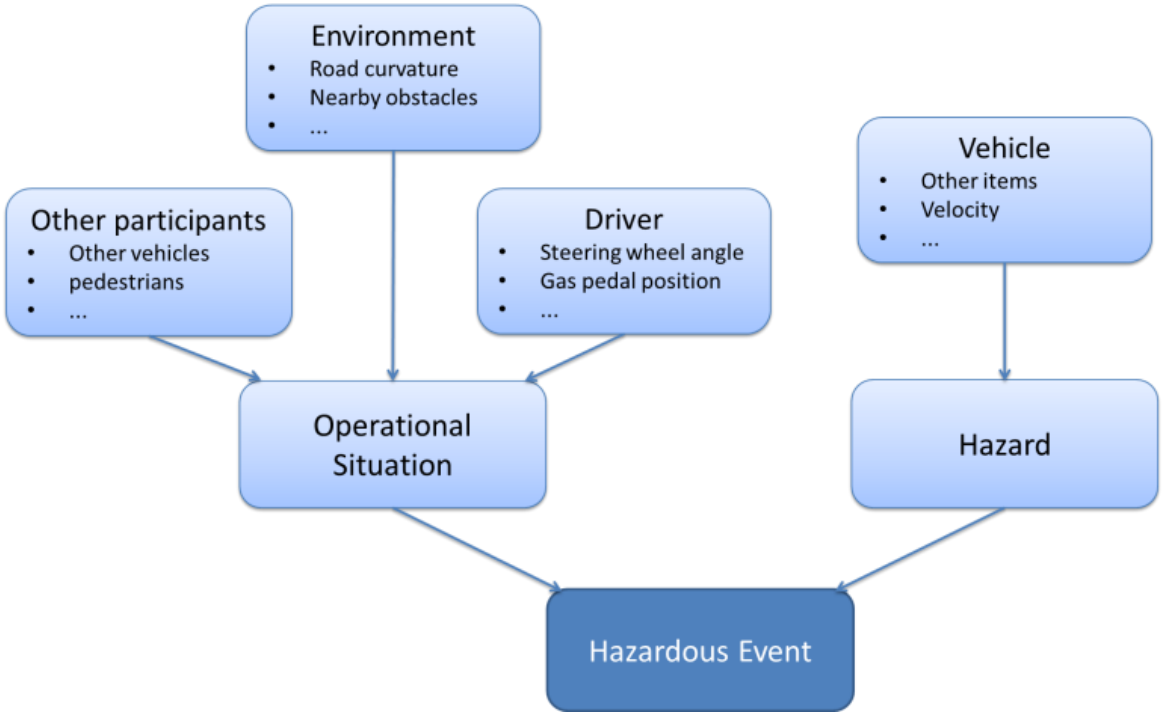

Figure 3: Contributing factors to hazardous events [7]

After determining the hazards as well as the operational situations by using adequate techniques (e.g. checklists, brainstorming, FMEA, ...) and combining them to hazardous events, the contributions of the particular factors can be extracted. Subsequent to that for each relevant contribution a variable needs to be defined which can be used to express the circumstances formally. In accordance with the informal expression a value needs to be assigned to the variables afterwards.

6.4.1 Characteristics of Hazard Descriptions

In [7] it is recommended to use the same principles as for requirements engineering for safety related systems when stating the hazards and hazardous events. These principles are given in the ISO/IEC/IEEE 29148 targeting the requirements engineering and "provides a unified treatment of the processes and products involved in engineering requirements throughout the life cycle of systems and software" [8]. Within these standard properties of a "good" requirement and the application of requirements processes in the lifecycle are described. Moreover, the general requirements engineering process as well as the management of activities related to requirements are accompanied with guidance on application. Although being dedicated to system and software, the standard provides a good overview on how requirements should be formulated in general. The characteristics of individual requirements are specified as necessary, implementation free, unambiguous, consistent, complete, singular, feasible, traceable, and verifiable. The concrete meaning of this attributes for the specification of requirements can be read in [8].

Focusing on the expression of hazardous events, all characteristics are also important, however, the reason why is slightly different. In the following the description for the aspects in the realm of stating hazardous events is presented.

- ***Necessary*:** The hazardous event defines a potential source of harm. If deleted or left out, this would lead to an unknown source of harm which is not handled.
- ***Implementation free*:** Hazardous events need to be defined subsequent to the item definition. Since at this level only the functionality as well as the limitations and boundaries are known, the formulation of a hazardous event should be independent from implementation.
- ***Unambiguous*:** The hazardous event should clearly describe the circumstances leading to an endangerment.
- ***Consistent*:** No conflicts to other hazardous events exist.
- ***Complete*:** The hazardous event contains all necessary information to identify the endangerment.
- ***Singular*:** The hazardous event is singular in the sense that no two parts of it on their own would also describe a hazardous event.
- ***Feasible*:** The hazardous event is not only caused by force majeure; it might occur due to technical reasons.
- ***Traceable***: The hazardous event is traceable to its components, namely the hazard and the operational situation, as well as to the corresponding safety goal addressing this hazardous event.
- ***Verifiable***: It is provable, that the hazardous event might occur during a vehicle's life; the hazardous event is not only far-fetched.

Besides the characteristics which are also important properties of hazardous events there are additional advantages by using the same structures for hazardous events and requirements. As it will be described later in the section hazard analysis and risk assessment the safety goals (top-level safety requirements) need to be derived from the hazardous events. Having a similar structure this process is simplified. Moreover, there are already existing safety analyses which can handle safety requirements. In case hazardous events rely on the structure of requirements, these analyses can easily be adapted to hazardous events.

6.4.2 Hazard Description Language

Starting point for the formalization of hazardous events is the informal notation. Already in this representation a differentiation of the contributing factors shown in Figure 3 can be performed. As an example, in Figure 4 an informal hazardous event is shown. The differentiation of the contributing factors is done by using different colors whereat green is used for the contribution of the driver, blue is used for the contribution of the vehicle, and orange is used for the contribution of the environment. Based on the informal description of the hazardous event the relevant variables and associated values which can be used to describe the informal expression in the formal hazardous event need to be determined.

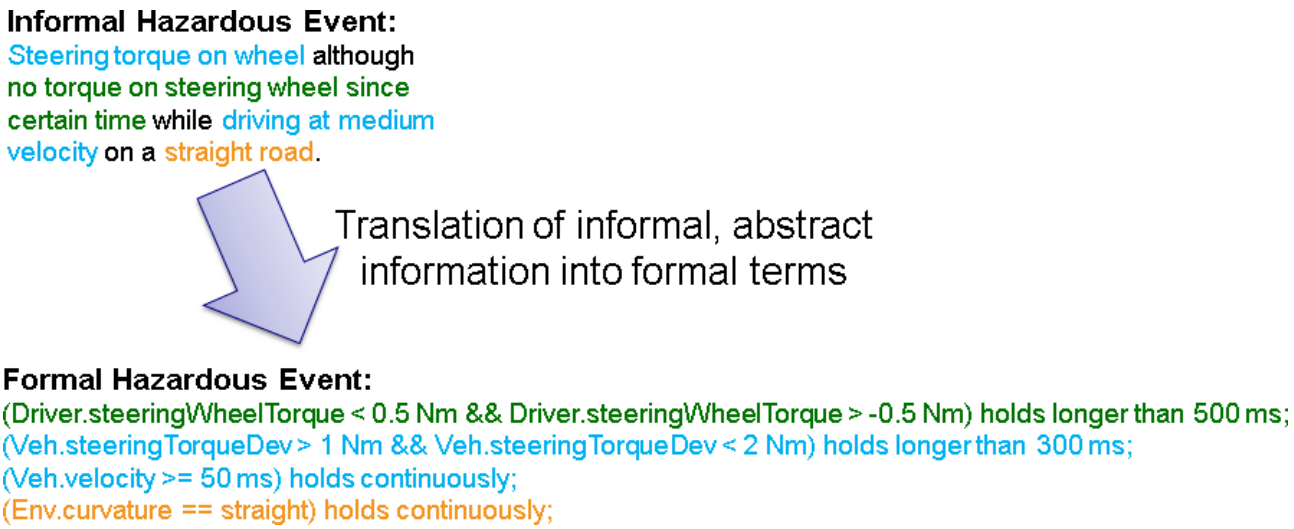

Figure 4: Example for informal and formal representation of hazardous event

The following syntax is used to describe hazardous events:

Hazard = Condition [**holds longer than** Time | **holds at least** Time | **holds at most** Time | **holds** Time | **holds continuously**] [**within interval of length** Time] | Event **less than** NUMBER **times** | Event **more than** NUMBER **times** [Interval].| Event **does not occur** Interval.

Interval = **within interval of length** Time [**after** Event].

Event = Expression **becomes true** | Expression **becomes false** | event IDENTIFIER **occurs**

Time = NUMBER **s** | NUMBER **ms** | NUMBER **ns**.

Condition = Condition **and** Condition | Condition **or** Condition | **not** Condition | Predicate.

Expression = ...

Predicate = …

Expressions denote arithmetic expression over variables that are used to characterize the vehicle behavior. Conditions denote predicates over these expressions

6.4.3 Anchoring Hazardous Events in Automotive Architecture

The hazardous event shall be assigned the architectural description of the item. The EAST-ADL meta-model can be used for the representation of the automotive architecture. Basic elements are the operational situation, the hazard, the hazardous event, the safety goal, the item and the elements of the item in order to enable a further refinement of the item in the development phases. An overview on the basic classes and relationships is in shown in Figure 5.

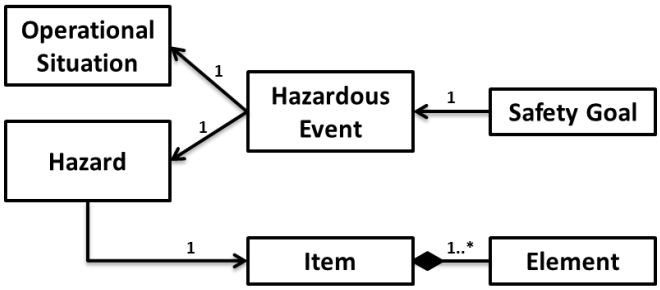

Figure 5: Key elements of model and their relationships [7]

6.5 Classification of Hazardous Events

Having determined the hazardous events the next step to perform is the assignment of the parameters. As already presented there are three different parameters, namely the probability of exposure, the severity and the controllability. Finally an ASIL is determined.

6.5.1 Determination of Controllability

One focal point within the classification of hazardous events is the determination of the controllability. In general it has to be understood that the controllability is not only influenced by the driver but also by other traffic participants that might be involved in the situation. However, in a first step only the contribution of the driver will be examined. Four classes of controllability (C0-C3) are defined in the ISO 26262 part 3. Clause 7.4.3.7, Table 3, which is depicted in

Table 3 — Classes of controllability

	Class			
	C0	C1	C2	C3
Description	Controllable in general	Simply controllable	Normally controllable	Difficult to control or uncontrollable

Figure 6: Classes of controllability from ISO 26262 part 3, clause 7.4.3.7 Table 3 [1]

Starting point for the determination of controllability is the execution of road tests in which a set of drivers assess the influences they recognize in case that failures are injected according to the three categories “recognizable”, “disturbing” and “uncontrollable”. The outcome of such road test is a diagram in which the boundaries of the system variables for recognition, disturbance and controllability can be determined. An example for such a resulting diagram is displayed in Figure 7.

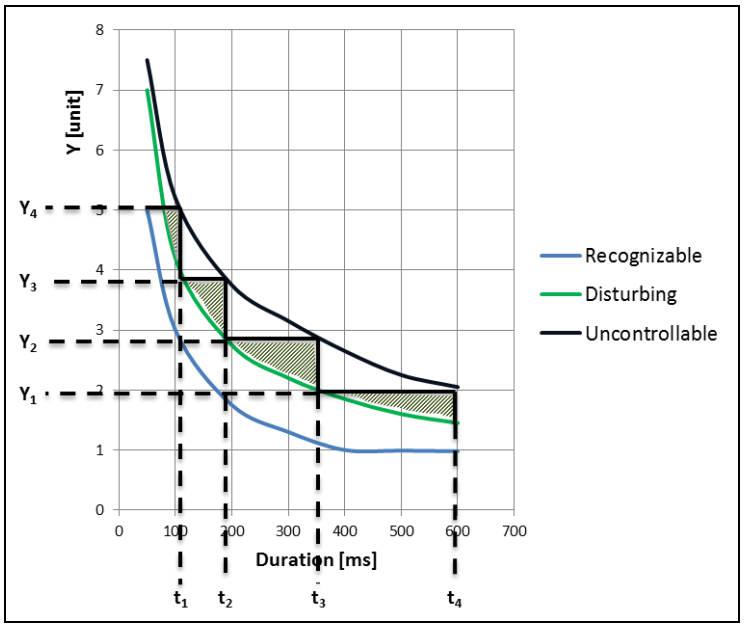

Figure 7: Resulting diagram from road test with added step function

Based on this diagram a discretization is conducted, which is always “safer” than the original curve as it is shown in Figure 7. The advantage of this new step function is that intervals with associated maximum values can be established that can be used for the later checks. In addition to these reference intervals, the timely progress of the deviation between the actual and the target value of the observed variable given in the hazardous event is needed.

For the determination of the controllability it needs to be checked whether there is no point in time for which the observed variable exceeds the given intervals of the step function. That means that the following conditions need to hold:

$$\forall t(\forall t' \in [t, t + t_1], Y_D(t') < Y_1)$$

$$\forall t(\forall t' \in [t, t + t_2], Y_D(t') < Y_2)$$

$$\dots$$

$$\forall t(\forall t' \in [t, t + t_n], Y_D(t') < Y_n)$$

In case that all those conditions are true it is demonstrated that the overall timely progress is permanently below the step function for which the test has been performed and therefore that the controllability can be assigned according to the respective value and the contribution of the driver to the controllability is determined. The expression of the deviation of the observed variable in the hazardous event in combination with the diagram which stems from road tests thus permits the unambiguous differentiation between controllable and uncontrollable events.

However, as it has been already said at the beginning of this paragraph there might also be the possibility that other involved actors in the situation (i.e. other vehicles, pedestrians etc.) contribute to the controllability. To consider the additional contribution of other involved actors one option is to extend the approach to determine the controllability describe above. For this purpose it is assumed that even if the driver classifies a situation characterized by the injection of a specific failure during the road test as disturbing, for a certain proportion of all cases the situation can be controlled by other involved actors. To represent this, the values of the curve can be jacked up and automatically represent the combined controllability of drivers and other actors. In this case the concept described above only needs to be used with the adapted curves.

With respect to the meta-model it is necessary to introduce a class for capturing the diagrams in form of functions or tables of values. Moreover, the relationship of this class with the hazardous event needs to be established.

6.5.2 Determination of Exposure

For the determination of the probability of exposure only the operational situation needs to be considered. This means for the example that it needs to be determined with which frequency or with which duration a certain the operational situation is present. Five classes of probability of exposure regarding operational situations (E0-E4) are defined in the ISO 26262 part 3, clause 7.4.3.4, Table 2, which is depicted in Figure 8.

Table 2 — Classes of probability of exposure regarding operational situations

	Class				
	E0	**E1**	**E2**	**E3**	**E4**
Description	Incredible	Very low probability	Low probability	Medium probability	High probability

Figure 8: Classes of exposure from ISO 26262 part 3, clause 7.4.3.4 Table 2 [1]

6.5.3 Determination of Severity

For the determination of the severity table B.1 of the ISO 26262, part 3, depicted in Figure 7 can be used.

Table B.1 — Examples of severity classification

	Class of severity (see Table 1)			
	S0	**S1**	**S2**	**S3**
Reference for single injuries (from AIS scale)	— AIS 0 and less than 10 % probability of AIS 1-6 — Damage that cannot be classified safety-related	More than 10 % probability of AIS 1-6 (and not S2 or S3)	More than 10 % probability of AIS 3-6 (and not S3)	More than 10 % probability of AIS 5-6
Examples	— Bumps with roadside infrastructure — Pushing over roadside post, fence, etc. — Light collision — Light grazing damage — Damage entering/ exiting parking space — Leaving the road without collision or rollover	— Side impact with a narrow stationary object, e.g. crashing into a tree (impact to passenger cell) with very low speed — Side collision with a passenger car (e.g. intrudes upon passenger compartment) with very low speed — Rear/front collision with another passenger car with very low speed — Collision with minimal vehicle overlap (10 % to 20 %) — Front collision (e.g. rear-ending another vehicle, semi-truck, etc.) without passenger compartment deformation	— Side impact with a narrow stationary object, e.g. crashing into a tree (impact to passenger cell) with low speed — Side collision with a passenger car (e.g. intrudes upon passenger compartment) with low speed — Rear/front collision with another passenger car with low speed — Pedestrian/bicycle accident while turning (city intersection and streets)	— Side impact with a narrow stationary object, e.g. crashing into a tree (impact to passenger cell) with medium speed — Side collision with a passenger car (e.g. intrudes upon passenger compartment) with medium speed — Rear/front collision with another passenger car with medium speed — Pedestrian/bicycle accident (e.g. 2-lane road) — Front collision (e.g. rear-ending another vehicle, semi-truck, etc.) with passenger compartment deformation

Figure 9: Table B.1 - Examples of severity classification from ISO 26262 part 3 [1]

The four classes of severity (S0-S3) are defined in the ISO 26262 part 3, clause 7.4.3.2, Table 1, which is depicted in Figure 10.

Table 1 — Classes of severity

	Class			
	S0	S1	S2	S3
Description	No injuries	Light and moderate injuries	Severe and life-threatening injuries (survival probable)	Life-threatening injuries (survival uncertain), fatal injuries

Figure 10: Classes of severity from ISO 26262 part 3, clause 7.4.3.2 Table 1 [1]

6.5.4 Determination of ASIL

Having all parameters assigned to the hazardous event, the ASIL can be determined. To do so, the table shown in Figure 11 from ISO 26262:2011-3 can be used.

Table 4 ASIL determination

Severity class	Probability class	Controllability class		
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

Figure 11: ASIL determination provided in the ISO 26262 part 3, clause 7.4.4.1 [1]

6.6 Safety Goals

Within this section the description of safety goals is addressed.

Safety goals are top-level safety requirements and should therefore be formulated as requirements. To do so, the requirement specification language described in section 6.6.1 can be used.

Since it shall be possible to check if the safety goals adequately address the corresponding hazardous events additional constraints for the formulation of safety goals arise. This topic is elaborated in section 6.6.2.

Finally, in section 6.6.3 it is explained how safety goals can be derived based on the hazardous events as well as the determined controllability and in section 6.6.4 the allocation of safety goals is described.

6.6.1 Requirement Specification Language

Stating requirements is one of the essential tasks in developing safety related systems. These requirements constitute an interface between different groups of people, i.e. customers, engineers, project managers and many more. Typically requirements are stored as natural language text which has the disadvantage that ambiguities of the sentences can cause a huge amount of requirement changes in early as well as in later development phases. To reduce the costs incurred by these ambiguities formal languages are used to ensure that requirements have a well-defined semantic interpretation. However, it does not only require some training to write requirements in these formal languages, it can also be a challenge to read them.

Pattern-based requirement specification languages fill this gap by providing an easy to learn formal language with a fixed semantic that is still readable like natural language.

Patterns consist of static text elements and attributes being filled in by the requirements engineer. Each pattern has a well-defined semantic in order to ensure a consistent interpretation of the written system specification across all project participants. On the one hand this limits the possibilities of writing a requirement; on the other hand it prevents misunderstandings regarding the interpretation of the sentences. To gain a set of unambiguous requirements this limitation is necessary. However, writing requirements shall still be possible in an intuitive way.

To gain a high degree of intuitivism the language shall consist of only a few constructs that can be easily remembered to give the requirement engineer the possibility to fully understand the requirement specification language (RSL) [5], which has been developed within the CESAR project [10], and choose the right pattern that fits the properties he wants to demand on the system.

There are patterns for each of the following categories available [5]:

- *Functional Patterns*: These Patterns express functional requirements of the system. This includes the relationship between events, handling of conditions and invariants and the possibility to define intervals in which the requirements or parts of them are valid.
- *Probability Patterns*: In nearly all safety relevant systems it is necessary to express failure or hazard probabilities. Since there are various partly redundant forms of expressing probabilities that are used quite ambiguous in common speech, these patterns guide the requirements engineer to express his needs.
- *Safety Related Patterns*: Only a small part of safety related requirements can be covered with probability patterns. The major part of the requirements outlines relationships between system components. These patterns enable the specification of single point of failures or other failure and hazard dependencies between different components.
- *Timing Patterns*: These patterns can be used to describe real-time behavior of systems. This includes periodic and aperiodic activations, jitter or delay.
- *Architecture Patterns*: These patterns specify the existence of architecture elements like components, events or connections between components.
- *Mapping Patterns*: These patterns can be used to express requirements on the mapping from the functional design perspective to the physical design perspective.

Patterns are noted in a form with optional parts that are not necessarily instantiated. A functional pattern describing the causality between two events looks like this:

> **whenever** *request* **occurs** *response* **occurs** [**during** *interval*].

Phrases in square brackets are considered optional, bold elements are static keywords of the pattern and italic printed elements represent attributes that have to be filled out by the requirements engineer. When filling the attributes there are no general restrictions on the names. [5]

In general, it should be possible to express requirements using the requirement specification language in the meta-model.

6.6.2 Semantics of Hazard Description

After depicting the formalization of hazardous events (see section6.4.2) as well as describing how the controllability of a hazardous event can be determined (see section6.5.1), within this section it will be shown how this can be integrated into the concept of contract-based design which has been introduced by [2].

In general, the hazardous events for a system under development can be seen as a set of formulas with free variables among the set of all system variables ($\mathbb{X}$). These formulas define traces which will eventually reach the hazardous event, thus they are a characterization of the undesired system behavior. Similarly, safety goals can be formalized using contracts. They define another set of possible system evolutions which are an over approximation of the set of paths that a system implementing the safety goal can take. If we can show that these two sets are disjoint then this is a formal proof that the safety goal adequately addresses the hazardous event.

In order to fulfill this analysis objective the concept of contract-based design is used [see 3]. This concept provides, amongst others, the possibility to perform dominance checks which can demonstrate that the set of traces accepted by one contract are a subset of the traces accepted by another contract.

Basically, for the dominance check the safety goals (SG) and the hazardous events (HE) have to be formulated as contracts C which are composed of assumptions A and promises G and which are both element of the set of formulas $F(\mathbb{X})$.

$$C_{SG} = (A,G);\ \ A,G \in \mathcal{F}(\mathbb{X})$$

$$C'_{HE} = (A',G');\ \ A',G' \in \mathcal{F}(\mathbb{X})$$

To generate contracts from the current representation of hazardous events, the assumption is specified by a set of formulas describing the values of the environment and velocity variables. The promise of the contract originating in the hazardous event is defined as the negation of the formula that describes the paths of the system in which the observed variable leads to uncontrollable situations. Informally this describes all valid system paths that will specifically not lead to the hazardous event. The question how the safety goals are formulated as contracts is answered in section 6.6.3.

For the dominance check it has to be checked whether $A \supseteq A'$ and $G \subseteq G'$. In case these conditions hold it can be said that the set of traces characterized by the safety goal is entirely included in the set of traces in which the hazardous event does not occur. This means that there is no trace allowed in which the hazardous event is reached and dominance is given. From this also follows that the safety goal adequately addresses the hazardous event.

The impact on the meta-model to enable the described formulation is that it needs to be possible to express hazardous events as well as safety goals as contracts which contain assumptions and promises.

6.6.3 Derivation of Safety Goals

Within this section the derivation of safety goals is addressed. For this we assume that all parameters, namely the controllability, the severity and the probability of exposure are determined and the ASIL classification of the hazardous event is performed.

Safety goals should be formulated as contracts. As it has been already described contracts are composed of an assumption and a guarantee. Based on the formalized hazardous events and the diagrams which show the boundaries for controllability the safety goals can be derived as follows:

1. For the assumption the operational situation and the velocity are taken as conditions. This leads to the following form:

$$Env.v1(t) == X \wedge Env.v2(t) == Y \wedge \ldots \wedge Env.vN(t) == Z \wedge Veh.velocity(t) >= A$$

2. The promise is then given by the conditions of the lowest curve in the diagram for the determination of controllability which shall never be violated. This leads to the form:

$\{\forall t(\forall t' \in [t, t+t_1], Y_D(t') < Y_1)\}$ does not occur $\wedge$

$\{\forall t(\forall t' \in [t, t+t_2], Y_D(t') < Y_2)\}$ does not occur $\wedge$

$\ldots \wedge$

$\{\forall t(\forall t' \in [t, t+t_N], Y_D(t') < Y_N)\}$ does not occur

In case the safety goals are captured in this way, the dominance check can be used to show that the safety goal adequately addresses the hazardous event. Moreover, other model-based safety analysis methods like Fault Tree Analysis (FTA) and Failure Mode and Effect Analysis (FMEA) are applicable in order to verify safety characteristics. How these methods can be applied is explained in [4] and [3].

As it has been already said in the previous section this means for the meta-model that an expression of safety goals as contracts consisting of assumptions and promises needs to be possible.

6.6.4 Allocation of Safety Goals

As safety goals are also safety requirements the same methodology as for the allocation of safety requirements is used. The representation of the possibility to allocate safety goals /safety requirements is shown in the meta-model part of WT 3.1.2 (Safety requirements expression).

6.7 Description based on example

In order to illustrate the methodology for hazard analysis and risk assessment according to the ISO 26262 the example of an electrical power steering (EPS) is used. The example is extracted from [7] and shows the following steps for the EPS: Item definition, identification and formulation of hazardous events, classification of hazardous events, and safety goals.

6.7.1 Item Definition

In this step the item definition is performed for the EPS. As described, for instance, in [12], the steering system of a car provides the functionality of moving the car in the direction the driver desires by converting the applied rotational movement into a modification of the steering angle. Moreover, the driver gets feedback about the road surface and the current situation. In general, the following requirements and interactions with the environment hold for steering systems (see also [12]: the required operating force should be as low as possible and adapted to the current driving conditions, the number of rotations from one mechanical stop to the opposite mechanical stop shall be as small as possible, the conversion of the rotational movement to the steering angle needs to be precise and free from float, in case the vehicle is moving and the steering wheel is not touched by the driver, the steering wheel shall go back in the position of driving straight ahead automatically, the feedback from the road condition needs to be recognizable but shall not be disturbing, the legal regulations concerning the maximum operating force as well as the operating time shall be considered.

In particular the requirements concerning the operating force lead to the fact that in modern cars the steering action of the driver is usually supported by adding torque to the steering link and therefore reducing the effort the driver has to spend for steering the car [12]. An overview on such an electrical power steering (EPS) system, one particular form of those auxiliary systems, is given in Figure 12.

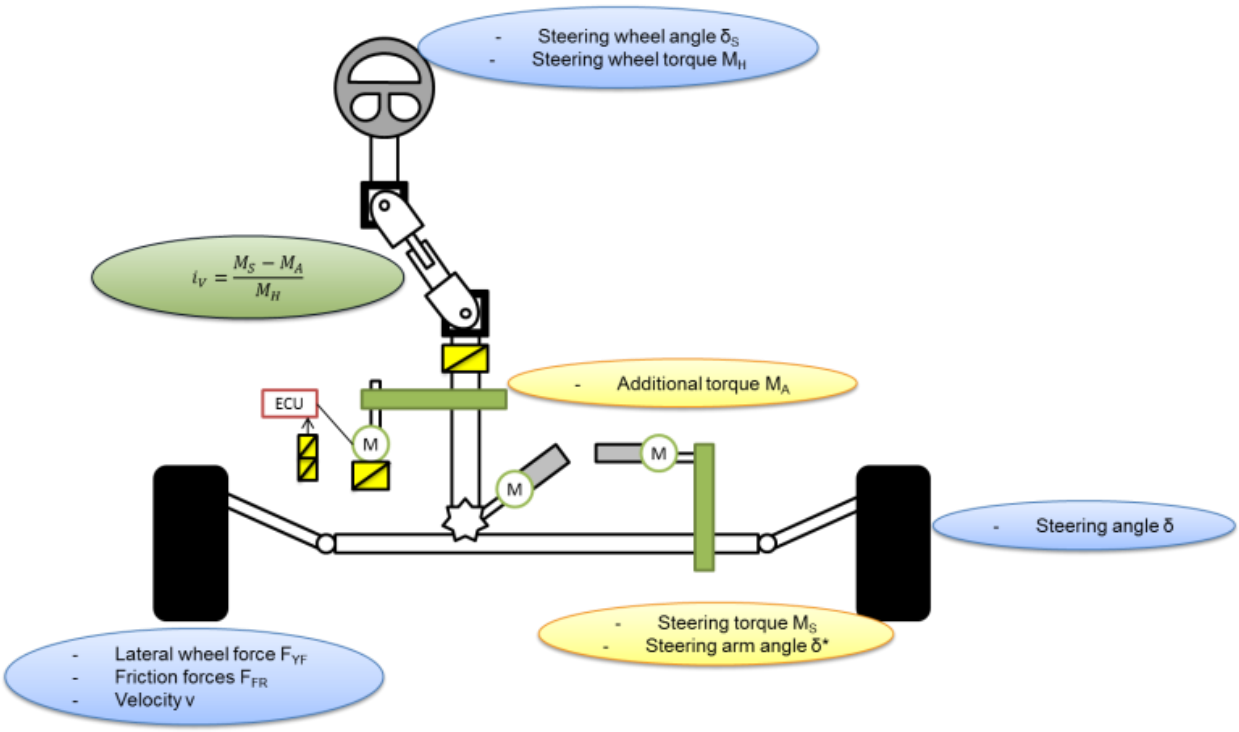

Figure 12: EPS: Overview on Electric Power Steering System [7]

In general, electric power steering systems work according to the following functional principle: The rotational movement of the steering wheel is detected by a torque sensor which passes the value to an electronic control unit (ECU). Within the ECU, the needed supporting torque which needs to be provided by an electric motor is calculated based on the received data and under consideration of other values, like, for instance, the current velocity. The electric motor is actuated by a power amplifier and passes the torque to the steering system via gears.

As a result of the item definition we obtain an architecture – which can be represented by an EAST-ADL model – that shows the item, its boundaries, and how it is embedded in the overall system consisting of the vehicle including other items and elements, the environment, and the driver and other traffic participants. The main structure of this model is depicted in Figure 13.

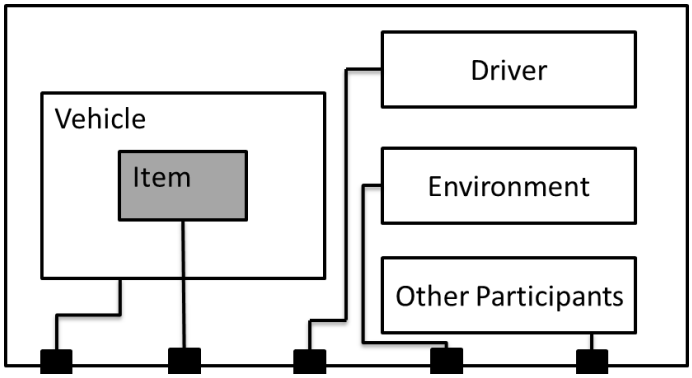

Figure 13: EPS: Structure of model resulting from item definition [7]

Note that the description of hazardous events (that will be introduced in the next section) typically needs to refer to variables of all four subcomponents (vehicle, driver, environment, other participants), since it is often the interaction of these components that make an event hazardous.

6.7.2 Identification and Formulation of Hazardous Events

An example for a hazardous event possible for the power steering system is that a torque is added to the steering link although the driver has not moved the steering wheel in combination with the operational situation of driving with medium velocity (assumed as higher than 50 km/h) on a straight road. To express this hazardous event a pattern like

Context: V*elocity larger than 50km/h* and *curvature equal to straight*
Hazard: The *torque* exceeds *MaxTorque*.

can be used (where MaxTorque would be a constant defined in the introductory part of the hazard definitions). Note that the actual pattern consists only of the words written in normal letters. Words written in *italics* actually constitute the actual parameters of the patterns (and these parameters may vary between the different applications of pattern).

When working with the above description of the hazardous event it might turn out that it is too strong in the sense that it subsumes situations of different controllability (by the driver). For instance, depending on the duration of the additional torque the driver has different reaction possibilities. This controllability is rather dependent on the duration and deviation of this additional torque compared to the setpoint value. An example for a hazardous situation of this kind is shown in figure 5. In this case the maximum torque of M_1 can be exceeded for duration of D_{acc1}. However, the actual exceeding is of duration D_1 where D_1 is greater than D_{acc1}. In order to be able to capture this in the formal description of hazardous events the previously presented pattern needs to be adapted in the following way:

Context: V*elocity larger than 50km/h* and *curvature equal to straight*
Hazard: The *torque* exceeds *MaxTorque(x)* for an interval greater than or equal to *x*.

At a first glance it seems that the figure precisely characterizes the hazardous event. In Figure 14, for instance, a possible time progress of the variable is shown which should be expressible with the hazard description language. In this exemplary time progress the additional torque exceeds the maximum value marked as M_1 for the duration of D_1 without discontinuations. However, if we consider various evolutions of the additional torque we see, that the hazardous event is not yet precisely specified since the maximum value is not continuously exceeded in all cases of time progresses.

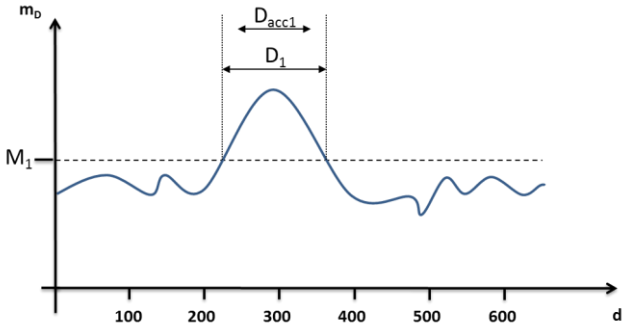

Figure 14: EPS: Possible time progress of additional torque 1 [7]

In Figure 15 and Figure 16, two other possible time progresses are shown. In Figure 15, the time progress changed in the form that the overstepping of the maximal accepted deviation is interrupted by a short negative peak. This short time of acceptable deviation does not lead to a controllable situation and the durations of overstepping marked with D_{11} and D_{12} would together also exceed the maximum allowed duration D_{acc1}; therefore this progress should also be identified as hazardous.

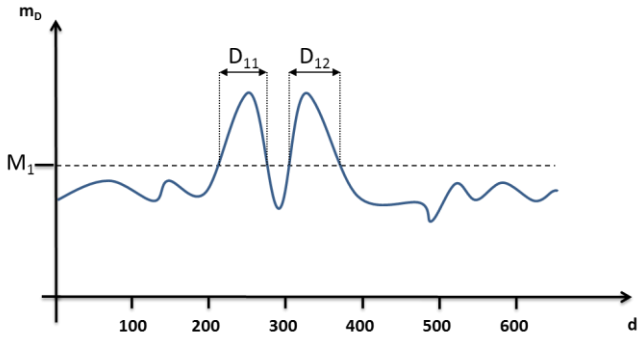

Figure 15: EPS: Possible time progress of additional torque 2 [7]

For the hazard description language this means that also this kind of progresses of variables should be expressible.

Context: V*elocity larger than 50km/h* and *curvature equal to straight*
Hazard: The *torque* exceeds *MaxTorque(x)* for duration greater than or equal to *x*.

Note that “interval” has been replaced by a “duration” here, making the hazard description more general. In Figure 16 also an interrupted overstepping of the maximal accepted deviation is shown. The durations D_{11} and D_{12} are the same as in figure 6 and together exceeding the maximum al-

lowed duration, but in contrast to the previous example there is a greater timespan in between which causes that this progress should not be identified as hazardous.

For the hazard description this means that a progress like displayed in Figure 16 should be differentiable from the progress shown in figure 6. The two considerations with respect to Figure 15 and Figure 16 lead to an additional adaptation of the proposed pattern in the following way:

Context: V*elocity larger than 50km/h* and *curvature equal straight*
Hazard: Within time interval of length *100ms* the *torque* exceeds *MaxTorque(x)* for duration greater than or equal to *x*.

Here we have strengthened the hazard description: the hazard occurs only if the peaks are sufficiently close to each other. Although being formulated textually the pattern presented has a precise semantic through using duration calculus. The basic concepts concerning duration calculus can be read in [11]. In our case the state predicate representing the acceptable torque values is defined by the formula

$$acceptable_{MaxTorque}(\tau, x) \equiv \int (\tau > MaxTorque(x)) < x \quad (1)$$

where τ denotes the additional torque that might be experienced by the driver. In addition, for the hazardous event the following formula can be used

$$he \equiv \exists x \Diamond \left(len \leq A\ ms \wedge \neg acceptable_{MaxTorque}(\tau, x) \right) \quad (2)$$

In the end, the hazardous events identified for the EPS are formally defined. After describing how the hazardous events can be anchored in an automotive architecture, the questions of how to classify the hazardous events and in particular how to determine the controllability as well as the question of how to use the formalized hazardous events to derive the safety goals will be answered.

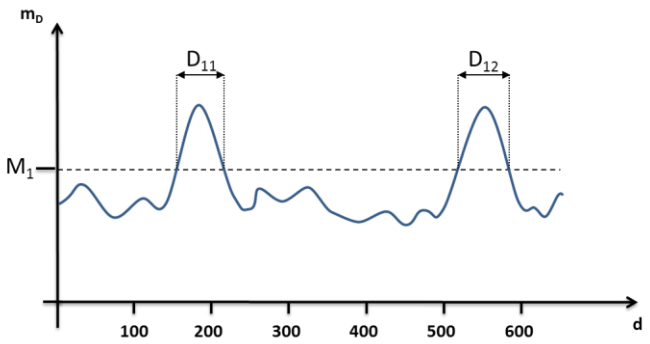

Figure 16: EPS: Possible time progress of additional torque 3 [7]

In Figure 17 it is shown how hazardous events can be described together with an item architecture within the steering system example.

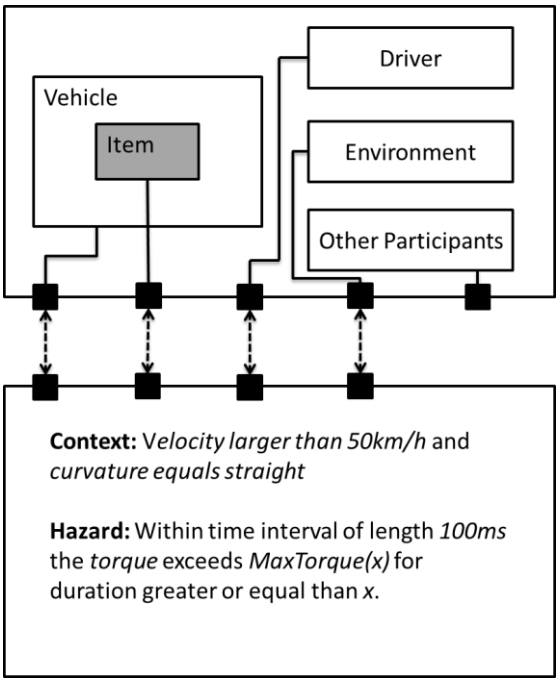

Figure 17: EPS: Representation of hazardous events with the item architecture [7]

6.7.3 Classification of Hazardous Events

In this step the hazardous event identified for the EPS is classified with regard to controllability, exposure and severity. Finally an ASL is determined.

First, the controllability is determined. Starting point is the execution of road tests in which a number of drivers assesses the influences they recognize in case failures are injected according to the three categories recognizable, disturbing and uncontrollable. The outcome of such road test is a diagram in which the boundaries of the system variables for recognition, disturbance and uncontrollability can be determined. An example for such resulting diagrams is displayed in Figure 18. Based on such diagrams a discretization is conducted, which is always "safer" than the original curve as it is shown in the figure. The advantage of this new step function is that intervals with associated maximum values can be established that can be used for the later checks. In addition to these reference intervals, the time progress of the deviation between the actual and the target value of the observed variable given in the hazardous event is needed. For the determination of the controllability it needs to be checked whether there is no interval within the progress of the observed variable which exceeds the boundaries given by the step function. How this is done is shown in the following based on the example.

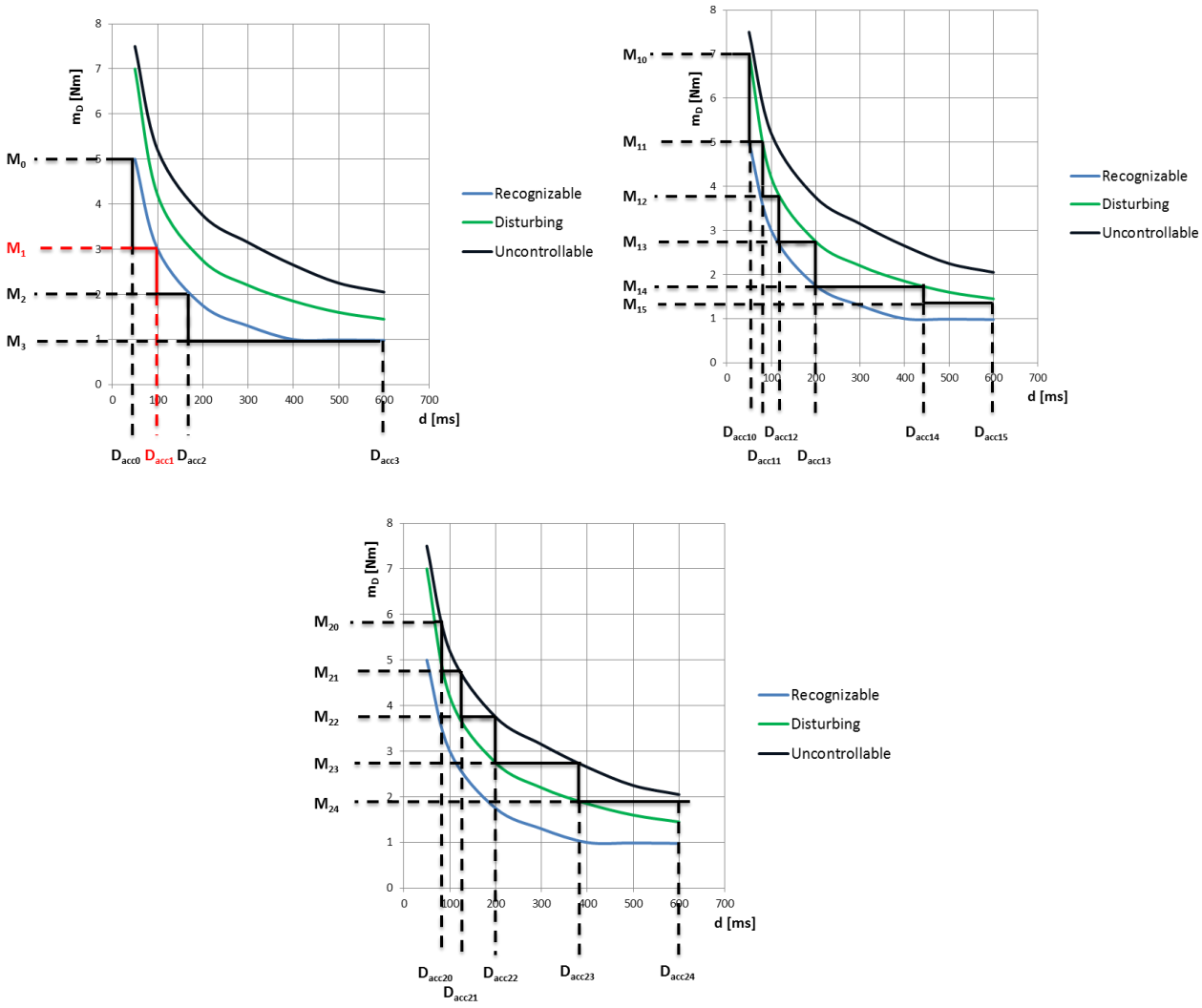

Figure 18: EPS: Controllability diagrams C0 (left), C1 (right), C2 (bottom) [7]

To determine the controllability in this example time progress of the additional torque is relevant. This time progress might look like that shown in Figure 19. As it can be seen in the figure, the additional torque is higher than 3 Nm for 120 ms. Within this interval the additional torque goes up to the maximum value of 3.6 Nm. In order to determine the controllability it is assumed that within this interval the additional torque has the constant value of 3.6 Nm. The first step function which would lead to a C0 classification if the boundary is not overstepped is shown in the left picture of Figure 18. Based on the diagram for the duration of 120 ms a maximum torque of 2 Nm is accepted. However, since the actual 3.6 Nm of additional torque exceed this boundary the same test needs to be performed for the second step function leading to a C1 classification shown in the right picture of Figure 18. Based on this diagram a maximum torque of 2.7 Nm is accepted for the duration of 120 ms, but this is also overstepped by the actual additional torque. Therefore, it needs to be tested if the boundaries given by the third step function which would lead to a C2 classification are also exceeded. Based on the diagram shown in the bottom picture of Figure 18 for the C2 classification for the duration of 120 ms a torque of 4.7 Nm is the boundary. In the example of an actual additional torque of 3.6 Nm the last boundary is not exceeded. Therefore, the controllability of the hazardous event can be set to C2. In case also the last boundary of the step function leading to a C2 classification would have been exceeded also no additional tests would have been necessary since the controllability can be set to C3, the highest controllability class.

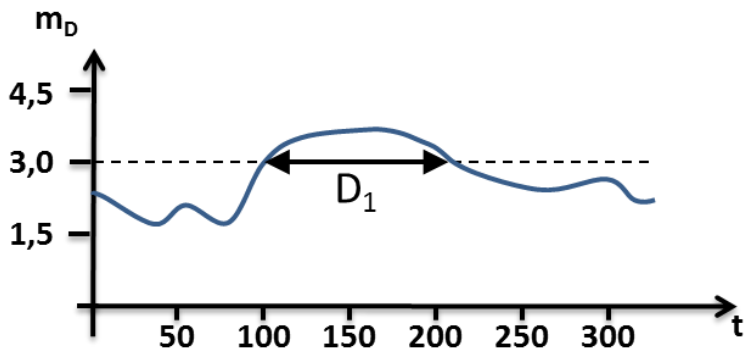

Figure 19: EPS: Exemplary time progress for the observed variable [7]

For the determination of the probability of exposure only the operational situation needs to be considered. This means for the example that it needs to be determined with which frequency or with which duration the operational situation of driving with medium velocity on a straight road is present. Since it can be said that this situation occurs in almost every driving on average the parameter is set to E4.

The last parameter, the severity, is set to S3 since in case this hazardous event occurs a side crash with a stationary object with medium speed might be the result. As stated in table B.1 of ISO 26262 [1], this would refer to the severity class S3.

Having all parameters assigned, the ASIL can be determined. To do so, the table shown in figure 14 from ISO 26262:2011-3 can be used. In our example the parameters have been assigned to C2, E4, and S3. According to the table, this would result in ASIL C.

6.7.4 Safety goals

In a final step the safety goal is derived for the hazardous event identified for the EPS example. A resulting pattern targeting that the hazardous event does not occur would be:

Context: V*elocity larger than50km/h* and *curvature equal straight*
Goal: For each time interval of length *A ms* the torque does not exceed *MaxTorque(x)* for duration larger or equal than *x*.

Like it has been already said for the patterns of the hazardous events also in this case the concepts of duration calculus [11] are taken. For the safety goal the following formula can be used:

$$sg \equiv \forall x\Big(len \leq A\ ms \rightarrow \neg acceptable_{MaxTorque}(\tau, x)\Big) \quad (4)$$

7 Performing hazard analysis and risk assessment based on EAST-ADL

Within this section the current status of the architecture description language EAST-ADL with regard to the hazard analysis and risk assessment is described. Furthermore, proposals for an extension of the EAST-ADL concepts are described which could lead to an enhancement of the possibility to perform the hazard analysis and risk assessment according to ISO 26262.

7.1 Current status of EAST-ADL

EAST-ADL is an architecture description language that has been developed in various projects in which both, automotive vendors and users are coupled together. The objective is thereby to define an architecture description language tailored to the needs of the automotive industry. [cf. 6] The current version published on the website of EAST-ADL (www.east-adl.info) is EAST-ADL V2.1.

EAST-ADL introduces different levels of abstraction, namely:

- Vehicle level,
- Analysis level,
- Design level,
- Implementation level, and
- Operational level.

With the hierarchical modeling concept which develops through the different abstraction levels the complexity of systems can be controlled more easily. [6]

Besides the different abstraction levels EAST-ADL includes several packages like, for instance, the variability package, the timing package, and the dependability package whereat the dependability package is of special interest for the hazard analysis and risk assessment. An overview on the dependability package is given in Figure 20.

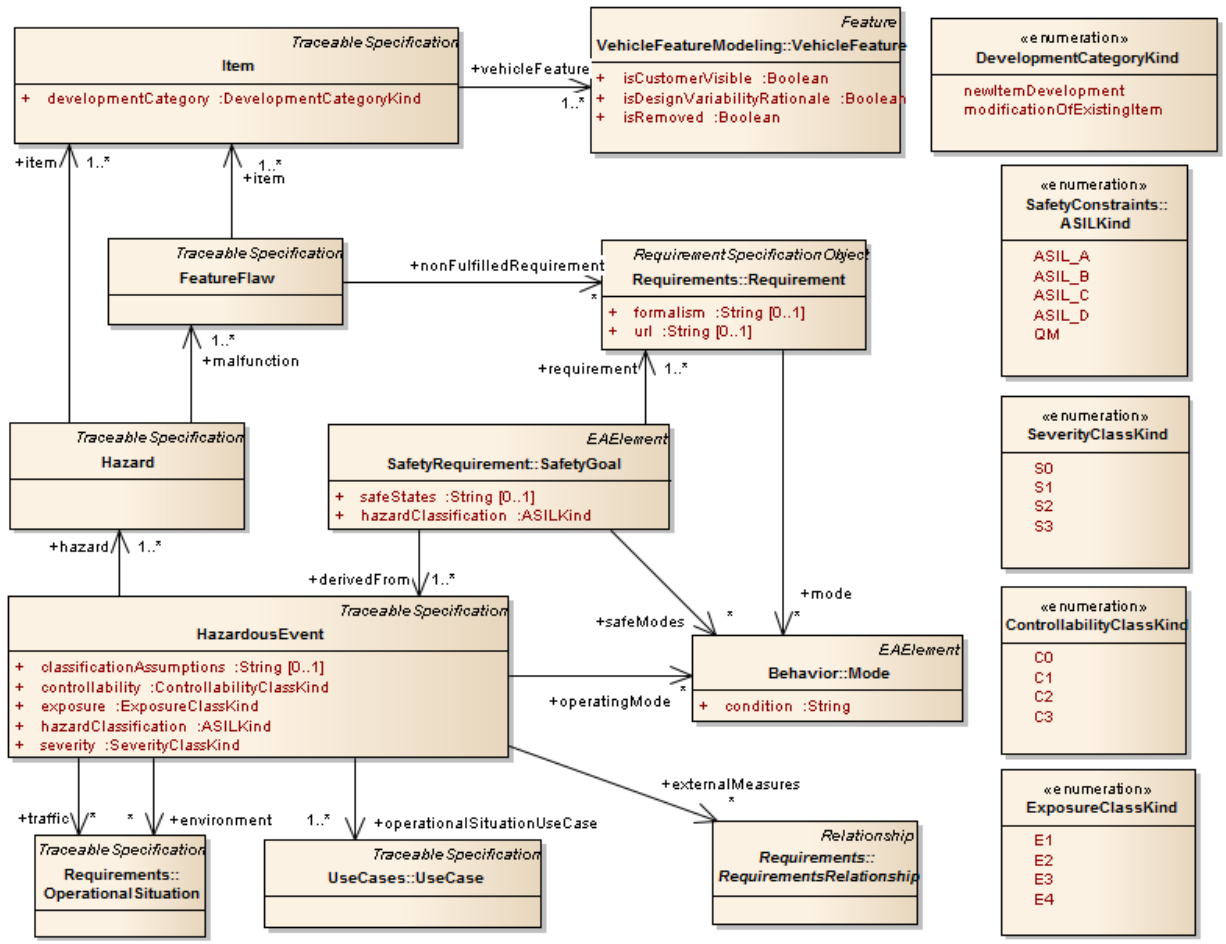

Figure 20: EAST-ADL Dependability Package

As it can be seen in the figure, the basic artifacts needed for a hazard analysis and risk assessment, like for instance hazards, hazardous events, operational situations and safety goals, are already included. For WT 3.1.1 it should be the objective to reuse as much as possible the already existing concept provided in EAST-ADL.

7.2 Proposed extensions to EAST-ADL

Investigating the possibility to perform the hazard analysis and risk assessment in EAST-ADL in more detail showed that there is a potential need for extensions. These potential extensions together with their rational are described in the following. However, as this task is still going on in future also the potential extensions will be elaborated in more detail.

Introduction of MalfunctionType and MalfunctionPrototype

Instead of using FeatureFlaw for the description of malfunctions related to a hazard it is proposed to use MalfunctionPrototype in accordance with WT 3.3.1. This new concept provides the possibility to define types of malfunctions which are associated with the item architecture which is not the case when using the FeatureFlaw.

Ensuring traceability between OperatingMode and Item

Within the current version of EAST-ADL there is no possibility to define operating modes for an item. Therefore it cannot be checked whether the operating mode which is associated with the hazardous event is also an operating mode of the item.

In order to provide the possibility of consistency checks the possibility to associate operating modes with an item should be established. However, a suitable concept how this could be realized still needs to be developed.

FunctionType to be aggregated

It is proposed to aggregate a FunctionType in the role of a function which defines the purpose and functionality of the item as a function concept.

OperationalSituation

Like it is explained in section 6 there are different factors contributing to an operational situation. Moreover, there is the need to express the operational situation informal as well as formal which is not possible in the current version of EAST-ADL. Therefore, in a first step the concept for operational situations described in section 8.1 and 8.2.4 is proposed.

8 WT 3.1.1 Contribution to SAFE Meta-Model

Within this section the contribution of WT 3.1.1 to the SAFE meta-model is described. At the beginning an overview about the model is given which is followed by the detailed description of the classes and interconnections. Moreover, in another section the meta-model is described by means of an example.

8.1 Overview

The contribution of WT 3.1.1 is mainly captured in two class diagrams within the “Hazards”-package of the SAFE meta-model created in Enterprise Architect. In the first diagram, which is shown in Figure 21, the artifacts needed for the hazard analysis and risk assessment and their interconnections are modeled. The attributes shown in this diagram are only those that are not included in the referenced classes of the current version of EAST-ADL (see also “note” in Figure 22).

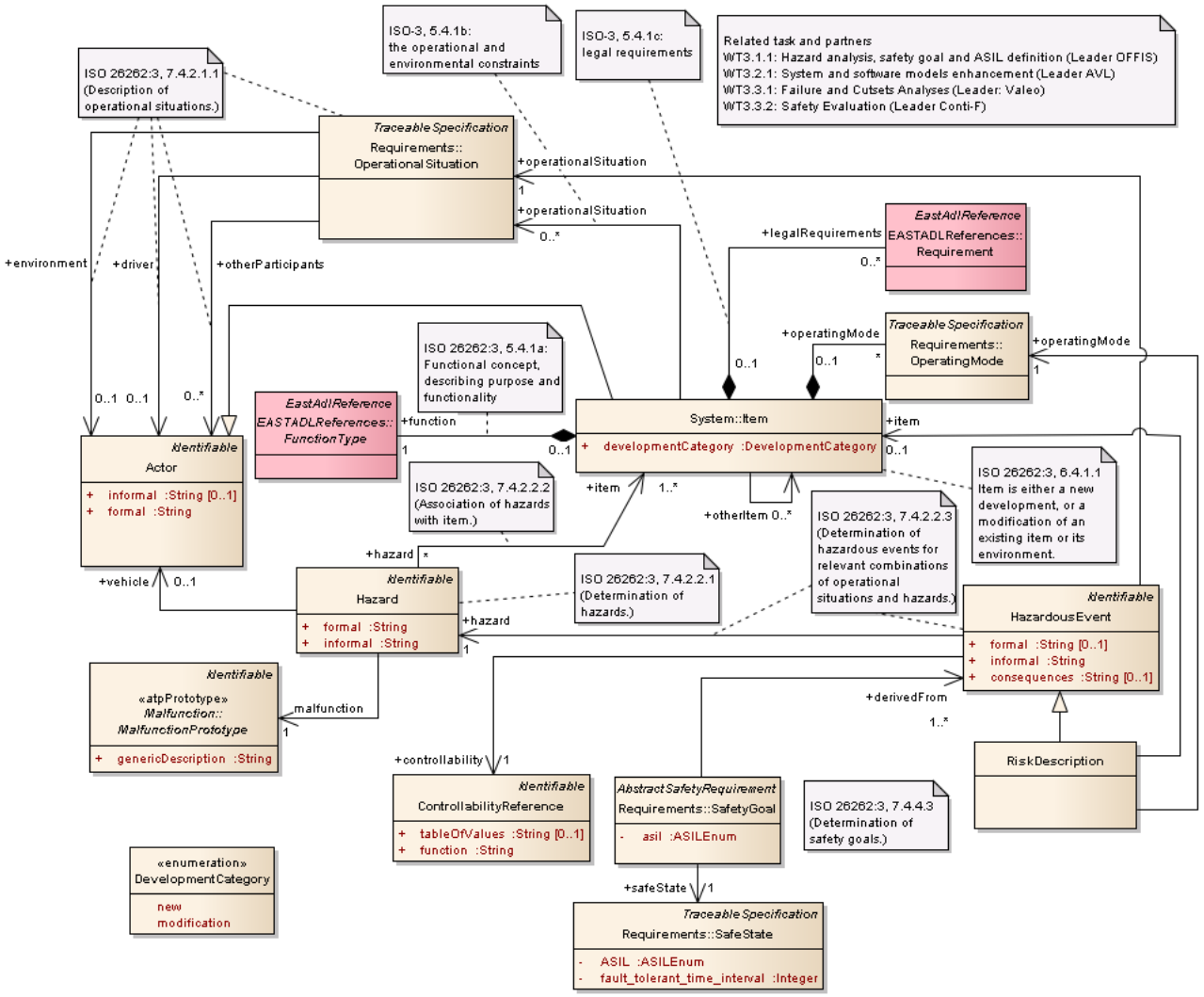

Figure 21: Overview on WT 3.1.1-contribution to SAFE meta-model

In the second class diagram, the references to EAST-ADL elements which can be reused are introduced. This diagram is also shown in Figure 22.

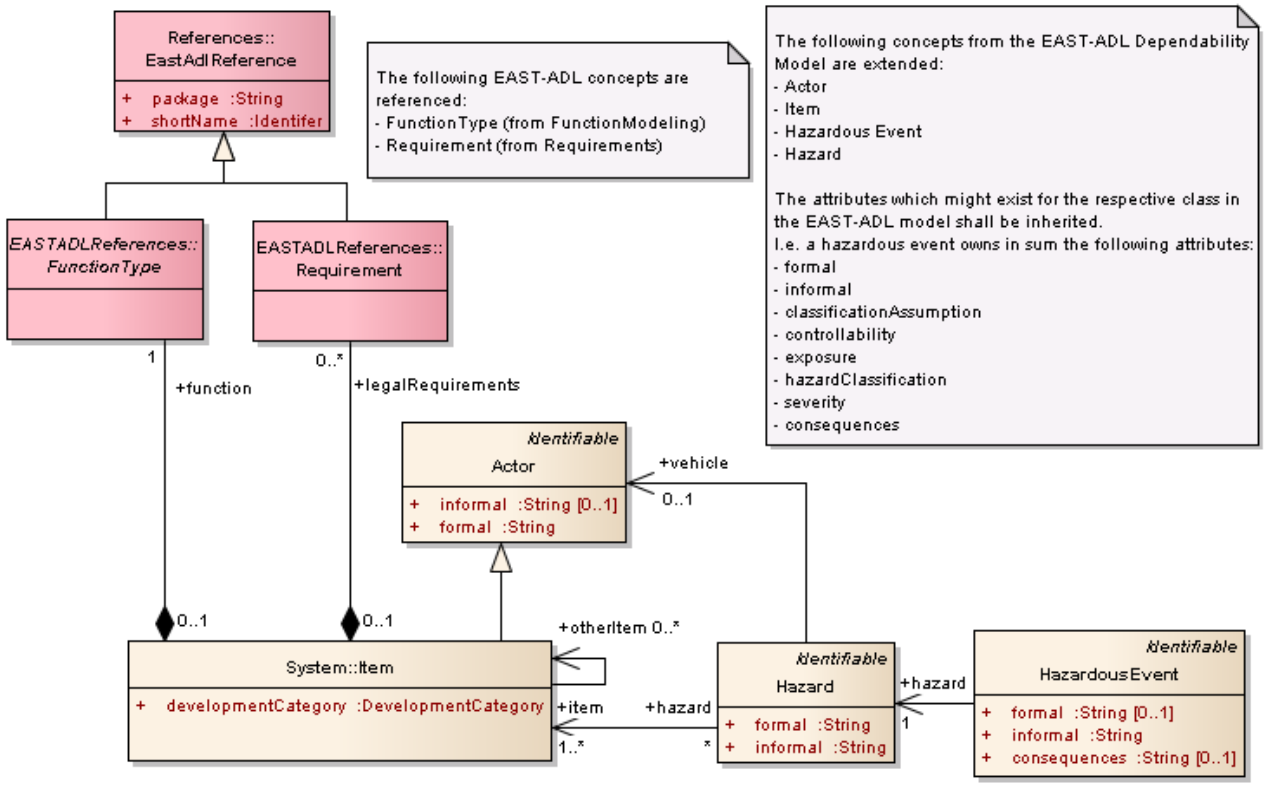

Figure 22: References to EAST-ADL elements

As it can be seen there are various elements originating in the current EAST-ADL version that can be reused or which were extended for the SAFE meta-model. In case of FunctionType (from EAST-ADL FunctionModeling package) and Requirement (from EAST-ADL Requirements package) these concepts were reused and referenced. However, the concepts “Hazard”, “Hazardous Event”, “Actor”, and “Item” these concepts were taken from EAST-ADL (Dependability package) and extended in the SAFE context.

8.2 Detailed Description of Classes and Links

In the following subsections, a detailed description of the classes and links of the WT 3.1.1 - contribution to the SAFE meta-model is given.

8.2.1 Item

Remark: The definition of this class is in the package “System”.

General Description:

The item is, according to ISO 26262, a “system or array of systems to implement a function at the vehicle level, to which ISO 26262 is applied”. Due to parallel work the item was first introduced in WT 3.1.1 and then shifted to WT 3.2.1. In accordance with WT 3.2.1 the item can be defined by different views such as a functional, design and implementation view which allows the decomposition of the item. An item can be used as an actor in the description of a hazardous event in order to distinguish it from other items which are involved in an operational situation. The item of the SAFE MM extends the item concept from EAST-ADL.

Attributes:

- developmentCategory: provides the possibility to capture the information whether it is a new development or a modification of an existing item (inherited from EAST-ADL “Item”)

Links:

- Aggregation link to “FunctionType”(in the role of function): allows the definition of the functional concept for the item, describing the purpose and functionality.
- Association with “RiskDescription” (risk description “owns” item contributions)
- Aggregation link to “OperatingMode”: allows the definition of operating modes and states of the item
- Generalization link to “Actor” (item is generalized by the actor)
- Association with “Hazard”
- Aggregation link to “Requirement” (in the role legalRequirements): allows the definition of legal requirements (especially laws and regulations)
- Aggregation link to “VehicleEnvironment” (in the role interactionsWithEnvironment)
- Association with “VehicleFeature”
- Association with “Item” (in EAST-ADL references, inherits attributes)

8.2.2 DevelopmentCategory (enumeration)

General Description:

This element is an enumeration for the development kind of an item. According to the ISO 26262 an item is either a new development, or a modification of an existing item or its environment.

Values:

- new
- modification

8.2.3 Actor

General Description:

The “Actor” class is provides the structure that is needed for the contributions of different actors to the operational situation and the hazard.

Attributes:

- Formal: provides the possibility to capture the formal description of the contribution of a particular actor
- Informal: provides the possibility to capture the informal description of the contribution of a particular actor

Links:

- Aggregation links to “OperationalSituation” (in the roles of driver, environment, other participants), “Hazard” (in the role of vehicle)
- Generalization link to item (item is generalized by an actor)

8.2.4 Operational Situation

Remark: The definition of this class is in the package “Requirements”.

General Description:

An operational situation is a scenario that may occur during a vehicles lifetime. Operational situations are formed by contributions of different actors, namely the driver (input of the driver via steering wheel, gas pedal, etc), the environment (e.g. road and lighting conditions), and other participants (pedestrians, other vehicles, etc). The definition of an operational situation may include the item as actor e.g. in order to distinguish it from other involved items.

Remark: The definition of this class is in the package “Requirements”.

Attributes:

- Formal: provides the possibility to capture the formal description of the operational situation
- Informal: provides the possibility to capture the informal description of the operational situation

Links:

- Association actor with the roles driver, environment, other participants
- Association with “HazardousEvent” (operational situation is destination)

8.2.5 Hazard

General Description:

A hazard describes a potential source of harm. Important is that it is formulated in terms of behavior that can be observed on vehicle level.

Attributes:

- Formal: provides the possibility to capture the formal description of the hazard
- Informal: provides the possibility to capture the informal description of the hazard

Links:

- Association with “Item”
- Association with “MalfunctionPrototype” (malfunction)
- Association to “Actor” (vehicle contributions to hazard)
- Association with “HazardousEvent” (hazard is destination)

8.2.6 Hazardous Event

General Description:

The hazardous event describes a relevant outcome of combinations of a hazard and an operational situation.

Attributes:

- formal: provides the possibility to capture the formal description of the hazardous event
- informal: provides the possibility to capture the informal description of the hazardous event
- controllability (from EAST-ADL): provides the possibility to assign a controllability parameter to the hazardous event
- severity (from EAST-ADL): provides the possibility to assign a severity parameter to a hazardous event
- exposure (from EAST-ADL): provides the possibility to assign a parameter for the probability of exposure to the hazardous event
- hazardClassification (from EAST-ADL): provides the possibility to assign an ASIL to the hazardous event
- classificationAssumption (from EAST-ADL): provides the possibility to capture an assumption about the classification of the hazardous event
- consequences: provides the possibility to capture the consequences of a hazardous event

Links:

- association with “Hazard”
- association with “OperationalSituation”
- association with “ControllabilityReference”

8.2.7 Risk Description

Remark: The definition of Risk Description is not final. It is intended to be used when undesired behavior cannot be described by hazardous events. It was introduced when no general concept was available to define such undesired behavior. Ongoing discussions with WT 3.3.1 can lead to a complete or partial replacement of the “Risk Description” by the malfunction concept.

General Description:

The risk description is the counterpart formulated on item level to the hazardous event which is formulated on vehicle level. It describes the endangerment in terms that can be observed at the item boundary in combination with the operational situation.

Attributes:

- formal: provides the possibility to capture the formal description of the risk description

- informal: provides the possibility to capture the informal description of the risk description
- controllability (from EAST-ADL reference): provides the possibility to assign a controllability parameter to the risk description
- severity (from EAST-ADL reference): provides the possibility to assign a severity parameter to a risk description
- exposure (from EAST-ADL reference): provides the possibility to assign a parameter for the probability of exposure to the risk description
- hazardClassification (from EAST-ADL reference): provides the possibility to assign an ASIL to the risk description
- classificationAssumption (from EAST-ADL reference): provides the possibility to capture an assumption about the classification of the risk description

Links:

- Generalization link to “HazardousEvent” (hazardous event generalizes risk description)
- Association with “OperatingMode”
- Association with “Item” (risk description “owns” item contribution)

8.2.8 Controllability Reference

General Description:

The class “ControllabilityReference” is introduced to provide the possibility to capture diagrams. These diagrams are based on road tests and enable a determination of the controllability parameter of the hazardous event.

Attributes:

- tableOfValues: provides the possibility to capture the diagrams in form of tables of values
- function: provides the possibility to capture the diagram in form of functions

Links:

- association with “HazardousEvent”

8.2.9 Safety Goal

Remark: The definition of this class is in the package “Requirements”.

General Description:

The safety goal is the top-level safety requirement for the item. It needs to be derived from the hazardous event and inherits the ASIL classification.

Attributes:

- name (inherited from TraceableSpecification): provides the possibility to name the safety goal
- stakeholder (inherited from TraceableSpecification): provides the possibility to interrelate a stakeholder with the artifact
- faultTolerantTimeInterval (inherited from AbstractSafetyRequirement): provides the possibility to capture the fault tolerant time interval

- formal (inherited from TraceableSpecification): provides the possibility to capture the formal expression of the safety goal
- informal (inherited from TraceableSpecification): provides the possibility to capture the informal expression of the safety goal
- asil: provides the possibility to capture the ASIL, which is inherited from the associated hazardous event
- asilDecomposed (inherited from AbstractSafetyRequirement): not used for safety goals
- emergencyOperationTimeInterval (inherited from AbstractSafetyRequirement): provides the possibility to capture an emergency operation time interval

Links:

- Association “derived from” to “HazardousEvent”
- Inheritance relation to “AbstractSafetyRequirement” (defined in package “Requirements”)
- Indirect inheritance relation to “TraceableSpecification” via “AbstractSafetyRequirement”
- Association with “SafeState”

8.2.10 Safe State

Remark: The definition of this class is in the package “Requirements”.

General Description:

The safe state is, according to ISO 26262, an “operating mode of an item without an unreasonable level of risk”.

Attributes:

- name (inherited from TraceableSpecification): provides the possibility to name the safe state
- stakeholder (inherited from TraceableSpecification): provides the possibility to interrelate a stakeholder with the artifact
- formal (inherited from TraceableSpecification): provides the possibility to capture the formal expression of the safe state
- informal (inherited from TraceableSpecification): provides the possibility to capture the informal expression of the safe state

Links:

- association with “SafetyGoal”

8.2.11 Operating Mode

Remark: The definition of this class is in the package “Requirements”.

General Description:

The Operating Mode is, according to ISO 26262, a “perceivable functional state of an item or element”. Therefore, it is associated with the item. Moreover, it is associated with the risk description since it describes a state of the item.

Attributes:

- name (inherited from TraceableSpecification): provides the possibility to name the operating mode
- stakeholder (inherited from TraceableSpecification): provides the possibility to interrelate a stakeholder with the artifact
- formal (inherited from TraceableSpecification): provides the possibility to capture the formal expression of the operating mode
- informal (inherited from TraceableSpecification): provides the possibility to capture the informal expression of the operating mode

Links:

- aggregation link to “Item” (item has a set of defined operating modes and states)
- association with “RiskDescription”

8.2.12 Function Type

Remark: The definition of this class is in the EAST-ADL Package “FunctionModeling”.

General Description:

Extract from EAST-ADL description: “The abstract metaclass FunctionType abstracts the function component types that are used to model the functional structure, which is distinguished from the implementation of component types using AUTOSAR.”

Attributes:

- isElementary: Boolean value that is set to true in case that the FunctionType must not have any parts (inherited from EAST-ADL element FunctionType)

Links:

- aggregation link with “Item” (in the role of the associated function)

8.2.13 Requirement

Remark: The definition of this class is in the EAST-ADL Package “Requirements”.

General Description:

Extract from EAST-ADL description: “The Requirement represents a capability or condition that must (or should) be satisfied. A Requirement can also specify an informal constraint, e.g. "The development of the component X must be according to the standard Y", or "The realization of this function as a software component must adhere to the scope and external interface as specified by this function". It will be used to unite the common properties of specific requirement types. A Requirement may either be directly associated with a Context (by inheriting from TraceableSpecification) or it may be included in a RequirementContainer, which represents a larger unit or module of specification information.”

Attributes:

- formalism : String [0..1]

  Specifies the language used for the requirement statement.

- url : String [0..1]

  Reference to possible external file containing the requirement statement.

Links:

- aggregation link with “Item” (in the role of a legal requirement)

8.2.14 Malfunction Prototype

Remark: The definition of this class is done in accordance with WT 3.3.1.

General Description:

A malfunction is a failure or unintended behavior of the item or element of the item that has the potential to propagate. A malfunction prototype refers to a condition that deviates from expectations based on requirements specifications, design documents, user documents, standards, etc., or from someone's perceptions or experiences (ISO26262). The set of available faults or failures represented by the MalfunctionPrototype is defined by its type.

Attributes:

- genericDescription : String [0..1]

  A description of the MalfunctionPrototype

Links:

- association with “MalfunctionType” (malfunction): The type of the malfunction prototype. It describes how the malfunction prototype becomes visible.
- association link with “Hazard” (malfunction):

8.3 Description Based on an Example

Within this section the concept of hazard analysis and risk assessment supported by the WT 3.1.1-contribution to the SAFE meta-model is described based on the example of a steering system.

8.3.1 Step 1: Definition of Operational Situations

- Determination of operational situations, i.e. situations that might occur during a vehicles lifetime (done by OEM) → ISO 26262:3, 7.4.2.1.1
- Operational situations can be expressed formal as well as informal
- As it can be seen in Figure 23 operational situations contain contributions of the environment and of the driver (However, if there is no contribution related to the actor, the contribution of the actor can be omitted. In this example this applies to the contribution of "otherParticipants".)

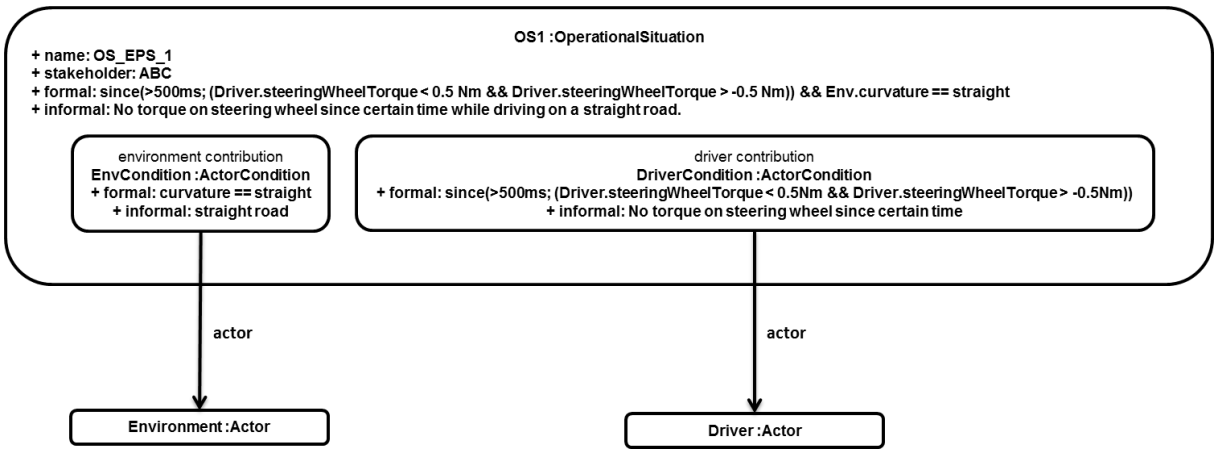

Figure 23: Operational Situation

8.3.2 Step 2: Determination of Hazards

- In a next step the hazards which are associated with the item are determined (by OEM) → ISO 26262:3, 7.4.2.2.1
- For WT 3.1.1 it is assumed that the item definition is completed and available
- Hazards are formulated on vehicle level and can also be expressed formal or informal
- Hazards contain contribution of the vehicle
- Hazards are linked to the item (→ ISO 26262:3, 7.4.2.2.2) and an associated malfunction

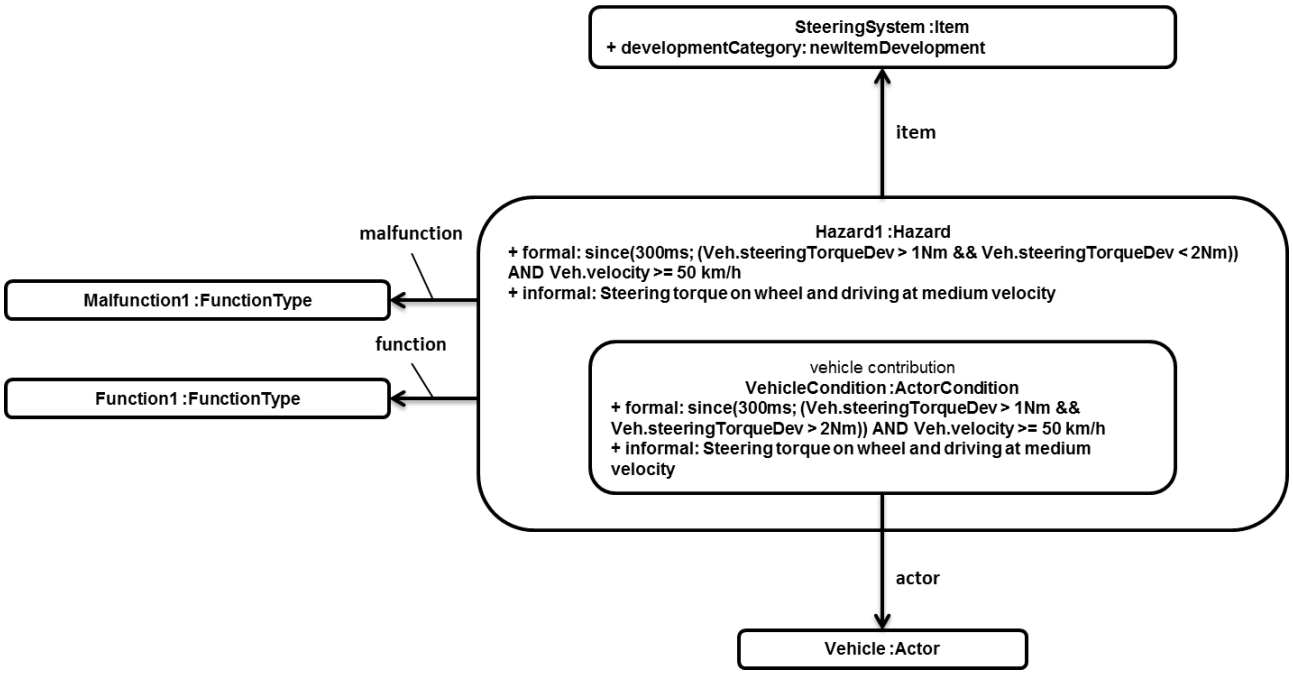

Figure 24: Hazard

8.3.3 Step 3: Capturing Hazardous Events

- Hazardous events, i.e. relevant combinations of operational situations and hazards, are determined → ISO 26262:3, 7.4.2.2.3
- Hazardous events can be expressed formal and informal
- Hazardous events contain the classification parameters as well as the assigned ASIL as attributes
- Hazardous events are linked to the respective hazard and the respective operational situation as well as to a controllability reference, which is explained in the next step

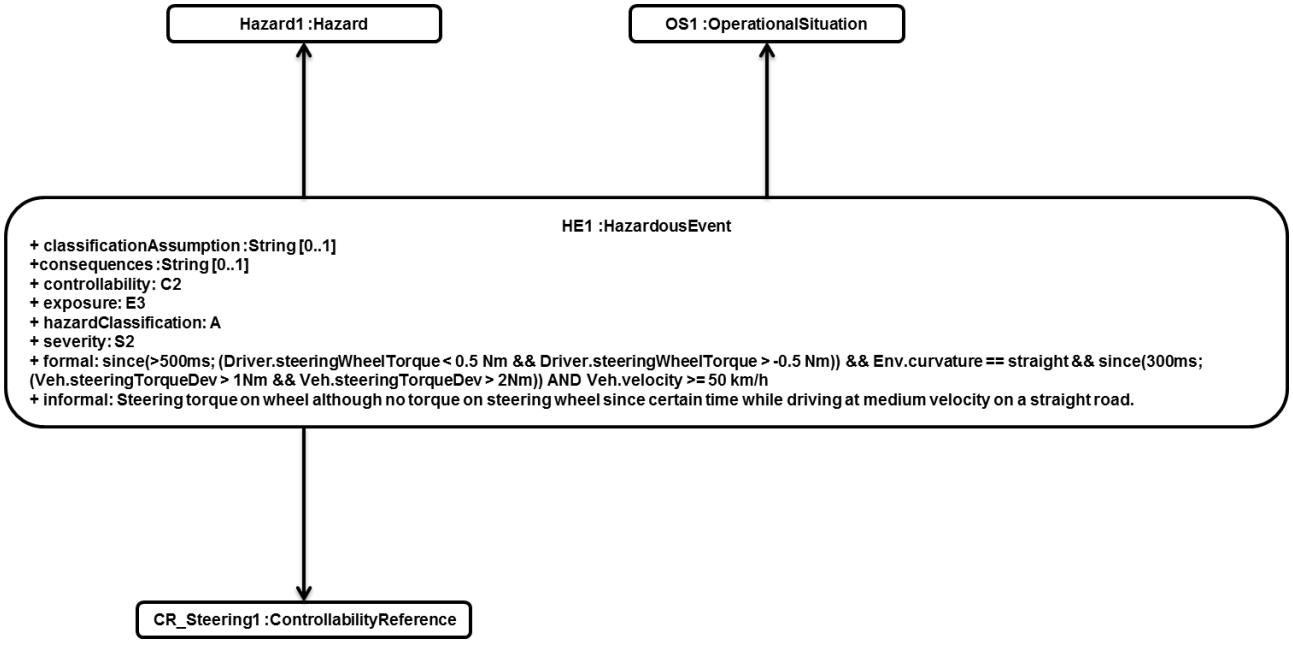

Figure 25: Hazardous Event

8.3.4 Step 4: Derivation of Risk Descriptions

- OEM defines the vehicle architecture and embedding of item in the vehicle
- Based on this, the risk descriptions can be derived from the hazardous events. Risk descriptions are similar to hazardous events, but described on item level. The risk descriptions are the basis of the work of the suppliers.
- Risk descriptions can be expressed formally and informally
- Risk descriptions contain the contribution of the item

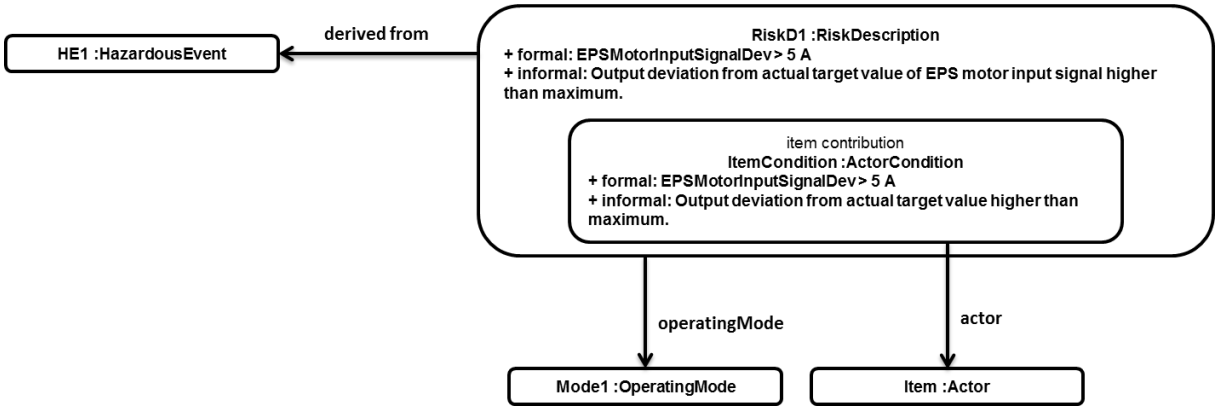

Figure 26: Risk Description

8.3.5 Step 5: Establishing a Controllability Reference

- Based on the results of road tests diagrams are created which determine the boundaries of the different controllability stages. Such a diagram may look like shown in Figure 27. The diagram is used to determine the controllability of a hazardous event.

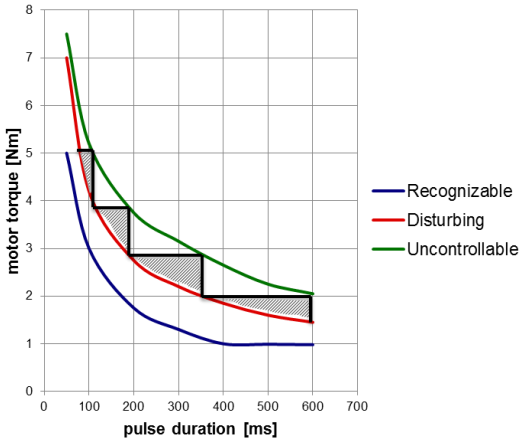

Figure 27: Resulting diagram from road test with added step function

- Within the ControllabilityReference these diagrams can be integrated in the model in form of functions or table of values
- In Figure 28 an example is shown how it is expressed in case step functions are used to describe the three curves of the diagram

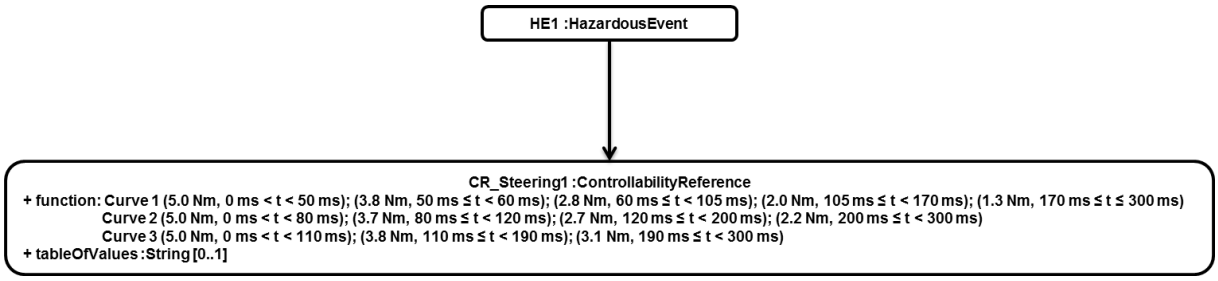

Figure 28: Controllability Reference

8.3.6 Step 6: Derivation of Safety Goals

- After all classification parameters of the hazardous event and the ASIL have been determined safety goals need to be derived from the hazardous event. → ISO 26262:3, 7.4.4.3
- Safety goals are top-level safety requirements for the item
- the safety goal inherits the ASIL of the hazardous event from which it is derived
- Safety goals can be expressed formal and informal
- Safe states and fault tolerant time intervals can be defined in the respective attributes
- The safety goal is linked to the hazardous event. Additional links (e.g. to a functional safety requirement) are expected to be continued...

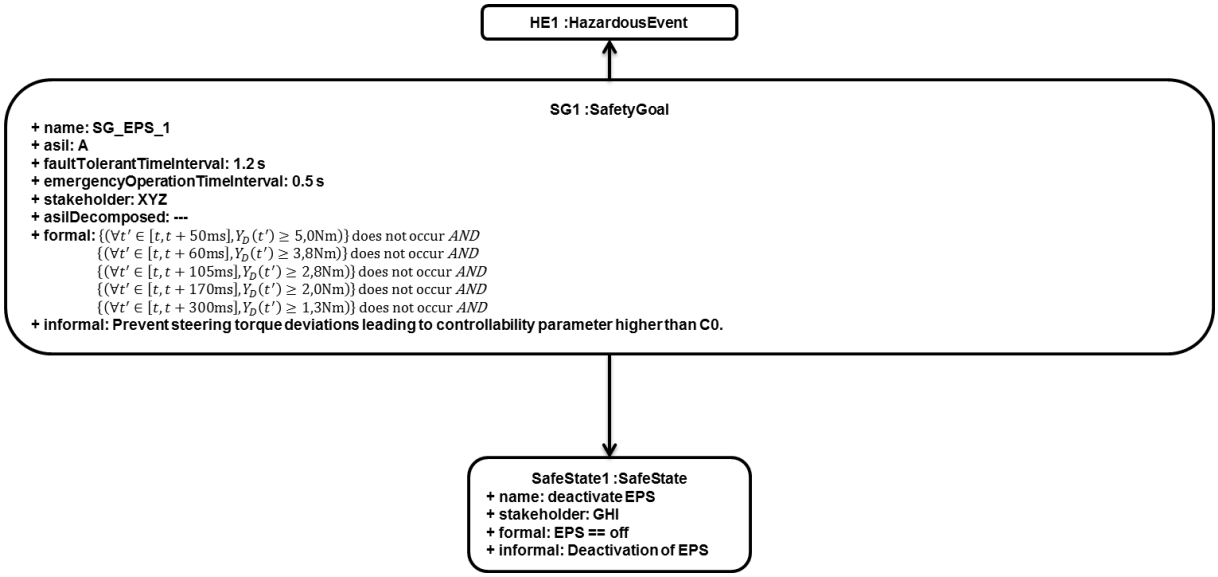

Figure 29: Safety Goal

9 Interdependencies with other work tasks / packages

The relationships between WT 3.1.1 and other work task are shown in the following Figure 30.

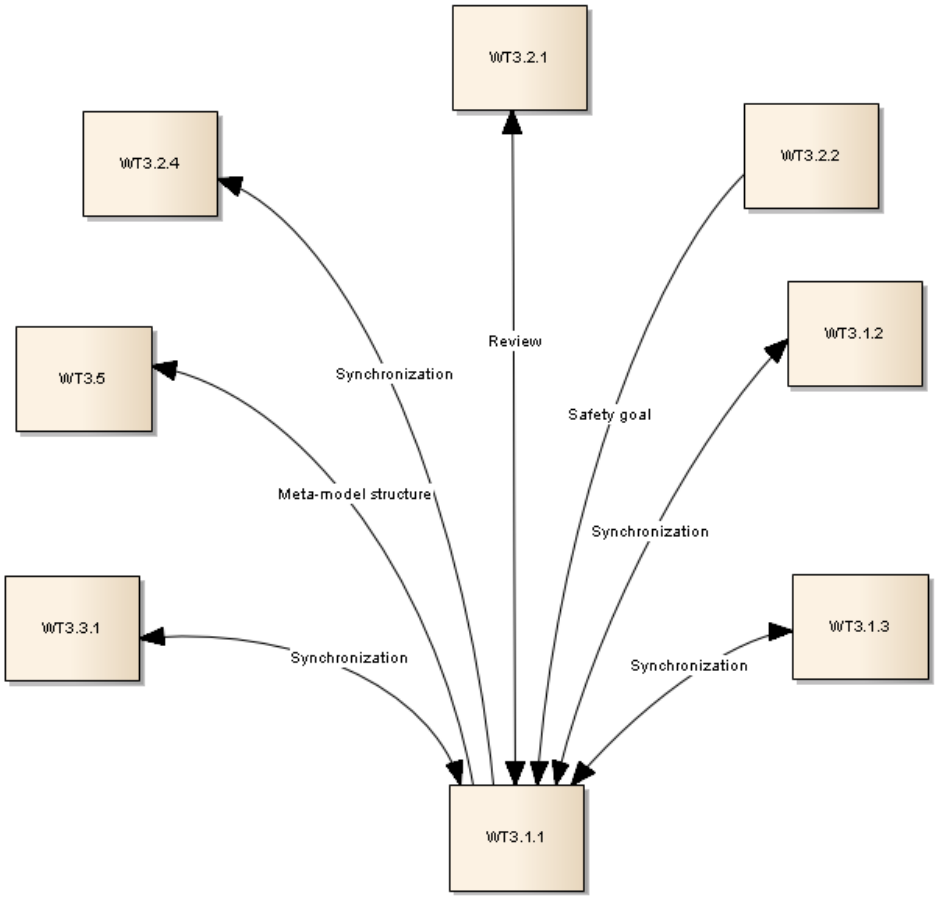

Figure 30: Relationships between WT 3.1.1 and other WTs

As it can be seen in the figure, there are various dependencies between WT 3.1.1 and other work tasks. In the following these interdependencies are described in more detail.

Like displayed in the figure there is a relationship between WT 3.1.1 and WT 3.5 concerning the meta-model structure. In particular this means that WT 3.1.1 has to contribute a respective meta-model part for the integration in the SAFE meta-model which is developed within WT 3.5. In order to ensure correctness of structure and settings as well as easy integration of the meta-model parts into the combined SAFE model WT 3.5 set up a guideline document and a master document for the model so that each work task can work with replicas. By doing this, the consistency can be ensured.

Interdependency exists with the work task 3.2.1. Within this work task the meta-model principles for the item definition and for the functional safety concept will be developed. The concepts for the item definition will be developed together with WT 3.2.1 allowing decomposition of the item as required by the ISO 26262. Since the functional safety concept includes the functional safety requirements which are derived from the safety goals which are part of the WT 3.1.1 – contribution a strong communication is necessary to ensure that all artifacts needed for the derivation are present. Moreover, seamless traceability from the artifacts of the hazard analysis and risk assessment to the functional safety requirements needs to be established.

Due to the fact that not only a seamless traceability from safety goals to functional safety requirements has to be established but also that safety goals are top-level safety requirements and need to fulfill the same requirements on safety requirement expression given in the ISO 26262 as functional or technical safety requirements there is the need for synchronization between the work packages 3.1.1 and 3.1.2.

An additional synchronization link is established between WT 3.1.1 and WT 3.1.3. Within WT 3.1.3, the fundaments for a proper safety case documentation shall be developed. An important aspect for this documentation is the tracing from hazards to their solutions; therefore an exchange with respect to the representation of all included artifacts has to take place.

With respect to WT 3.2.4 dealing with the handling of COTS there is as well the need for synchronization. By using a COTS component there might arise hazards that are already known. These hazards have to be integrated in the hazard analysis and risk assessment. With this linkage it shall be ensured that a proper integration of such known hazards and a highlighting of such known hazards is possible.

Another bi-directional relationship exists between WT 3.1.1 and WT 3.3.1 (Failure and cut-sets analysis) due to the fact that a common understanding about safety goals and their representation as well as violation needs to be present. In WT 3.3.1 concepts for error modeling and malfunctions will be elaborated which need to be related to hazard definitions from WT 3.1.1.

Besides the relationships already mentioned there is the need for communication between WT 3.1.1 and WT 3.2.2 concerning safety goals. There is the need for relating hardware failure information to safety goals in order to determine the role of violation of safety goals which then allows calculating hardware metrics.

10 Conclusions and Discussion

This document is intended to provide information about the initial proposal for a methodology for the hazard analysis and risk assessment as well as for an extension of the SAFE meta-model for hazard and environment modeling.

Besides giving an overview on the relevant parts of ISO 26262 the requirements arising from WT 2.1 (ISO 26262 Analysis) and WT 2.3 (Use Case Scenario) are presented. In an additional section, the current achievements on the requirements are illustrated.

A focal part of this deliverable is the presentation of the methodology for hazard analysis and risk assessment. This methodology is compliant to the requirements given in ISO 26262 and in addition comprises aspects arising from experiences in the development of automotive systems. However, since the topic of proper hazard analysis and risk assessment is not only very important for ensuring safety but also very complex, the methodology presented needs to be further elaborated. This is also the case for the concepts of the hazard description language, the guided determination of the parameters controllability, severity, and probability of exposure as well as the resulting ASIL, and the derivation of safety goals. Therefore, the initial concepts presented in this paper can be seen as a basis for the further development.

The initial contribution to the SAFE meta-model presented in this deliverable provides the possibility to perform an ISO 26262 compliant hazard analysis and risk assessment. At the same time the requirements coming from the methodology are considered. In case the methodology is extended there might also arise the need to adapt the corresponding part of the SAFE meta-model.

Since it is an objective to reuse EAST-ADL as much as possible the current version of EAST-ADL is presented and initial proposals for extensions are formulated. However, these proposals need to be further elaborated in future. For the proposed extension of the SAFE meta-model EAST-ADL references are used whenever possible.

Besides the already mentioned tasks which will be elaborated in further activities the methodology for first analyses and consistency checks will be developed. This can include, for instance, checking whether safety goals adequately address the corresponding hazardous event and consistency checks concerning the ASILs.

11 References

[1] International Organization for Standardization: ISO 26262 Road vehicles - Functional safety. (2011)

[2] SPEEDS Consortium: SPEEDS Meta-model Syntax and Draft Semantics, D2.1c. (2007)

[3] Damm, W., Josko, B., Peikenkamp, T.: Contract based ISO CD 26262 safety analysis. SAE Technical Paper 2009-01-0754, 2009, doi:10.4271/2009-01-0754 (2009)

[4] Peikenkamp, T., Cavallo, A., Valacca, L., Böde, E., Pretzer, M., Hahn, E.M.: Towards a Unified Model-Based Safety Assessment. In: Proceedings of SAFECOMP. (2006) 275–288

[5] Project CESAR: CESAR Partners. RE Language Definitions to formalize multi-criteria requirements V2, D_SP2_R2.2_M2, http://www.cesarproject.eu/fileadmin/user_upload/CESAR_D_SP2_R2.2_M2_v1.000_PU.pdf

[6] Chen, D., Johansson, R., Lönn, H., Papadopoulos, Y., Sandberg, A., Törner, F., Törngren, M.: Modelling Support for Design of Safety-Critical Automotive Embedded Systems. In: Proceedings of SAFECOMP (2008)

[7] Suerken, M., Peikenkamp, T., “Model-based Application of ISO 26262: The Hazard and Risk Assessment”, SAE Technical Paper 2013-01-0184, April 2013

[8] International Organization for Standardization: ISO/IEC/IEEE 29148:2011 Systems and software engineering - Life cycle processes - Requirements engineering. (2011)

[9] Beisel, D., Reuß, C., Schnieder, E.: Approach of an automotive generic hazard list. In: Proceedings of European Safety and Reliability, ESREL. (2010)

[10] Project CESAR, “Cost-efficient methods and processes for safety relevant embedded systems”, 2009-2012, http://www.cesarproject.eu/

[11] Chaochen, Z, Hoare, C.A.R., Ravn, A.P.:A calculus of durations. Inf. Process. Lett., 40(5): 269-276 (1991)

[12] Reimann, G., Brenner, P., Büring, H.: Lenkstellsysteme. In: Handbuch Fahrerassistenzsysteme. Vieweg + Teubner Verlag || Springer Fachmedien Wiesbaden GmbH (2012)

[13] Damm, W., Josko, B., Peikenkamp, T.: Contract based ISO CD 26262 safety analysis. In: SAE Technical Paper 2009-01-0754. (2009)

[14] Abid, N., Dal Zilio, S., Le Botlan, D.: Real-Time Specification Patterns and Tools. In: Proceedings of FMICS (2012)

12 Acknowledgments

This document is based on the SAFE project in the framework of the ITEA2, EUREKA cluster programme 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.