Functional Safety Processes and Advanced Driver Assistance Systems: Evolution or Revolution?

Thomas Frese, Ford-Werke GmbH, Henry-Ford-Straße 1, 50735 Köln, tfrese@ford.com
Nils Gerber, Ford-Werke GmbH, Henry-Ford-Straße 1, 50735 Köln, ngerber1@ford.com
Denis Hatebur, ITESYS Inst. f. tech. Sys. GmbH, Emil-Figge-Str. 78, 44227 Dortmund, d.hatebur@itesys.de, and Universität Duisburg-Essen denis.hatebur@uni-due.de
Isabelle Côté, ITESYS Inst. f. tech. Sys. GmbH, Emil-Figge-Str. 78, 44227 Dortmund, i.cote@itesys.de
Maritta Heisel, Universität Duisburg-Essen, Fakultät für Ing.-wissenschaften, Abteilung INKO, Fachgebiet Software Engineering, 47048 Duisburg, maritta.heisel@uni-due.de

1. Advanced Driver Assistance Systems @ Ford

Within the last two decades, the development of electric / electronic (E/E) systems in the automotive domain was subject to a significant change: Starting with increasing E/E content in “stand-alone features” like engine control or brake system (e.g. E-Gas or ABS) realized in one single Electronic Control Unit (ECU) with directly connected sensors, networks (like the CAN-Bus) were introduced to connect the different subsystems. Later on, distributed features were developed in which the algorithms of the realized feature are spread over several ECU’s.

Key driver for this trend is the evolution of the so-called “Advanced Driver Assistance Systems (ADAS)”. These features were introduced at Ford vehicles stepwise in following generations:

This paper presents the different generations of Advanced Driver Assistance Systems brought to the market and provides an overview of the applied Functional Safety processes describes the current status and provides an outlook towards the future fully autonomous vehicles.

ADAS generation 1: it includes Adaptive Cruise Control (ACC) and a Pre Collision Assist function with driver warning in case of moving and stopping targets. The warning contains the estimation of driver reaction time. Different driver warning settings (early/normal/late) are available (Forward Collision Warning, FCW). The Brake system is pre-charged to achieve up to ~ 0.1g deceleration (Collision Mitigation by Braking, CmbB). The Emergency Brake Assist (EBA) threshold level is decreased when the radar sensor confirms the target (moving targets only).

ADAS generation 2: it adds Lane Assist, Light Feature & Driver Alert Systems. This includes features such as Lane Departure Warning (LDW), Lane Keeping Aid (LKA) with Camera, Auto High Beam Control (AHBC), Traffic Sign Recognition (TSR) with Camera and Driver Impairment Monitoring (DAS) based on driving behavior. Autonomous braking is done up to 0.5 g when the target is classified as a vehicle.

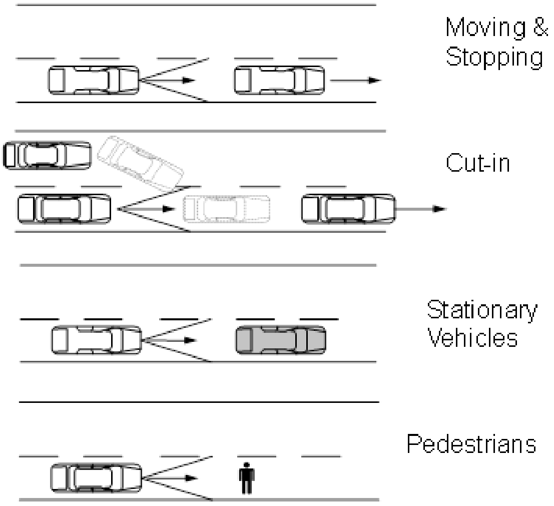

Figure 1 – ADAS @ Ford Generation 3

ADAS generation 3 (see Figure 1) enhances ACC with a Queue Assist (QA) function (ACC available 0 km/h to 200 km/h) and the next generation Pre Collision Assist, with warning for pedestrians, autonomous braking up to full braking authority when the target is classified as a vehicle or pedestrian, and braking for moving and stationary targets.

The above mentioned generations show, that the market introduction of ADAS clearly follows an evolutionary approach with a step-by-step extension of the features based on improved or new sensor technology. In the following sections, we will describe development of the accompanying Functional Safety processes.

2. Example for a distributed Advanced Driver Assistance System (ADAS)

An exemplary Advanced Driver Assistance System is explained in this section, describing a possible distribution of the ADAS functions to different subsystems.

Figure 1 provides an overview of a physical architecture of such a feature. The modules colored in gray are subsystems already implemented in the vehicle for their own functionality, like Engine Control Module for motor control or Brake Control Module including the Antilock Braking System (ABS) and Electronic Stability Control (ESP) functions. The light-gray modules are sensors/switches included in these functions, like Steering Angle Sensor for ESP functionalities etc.

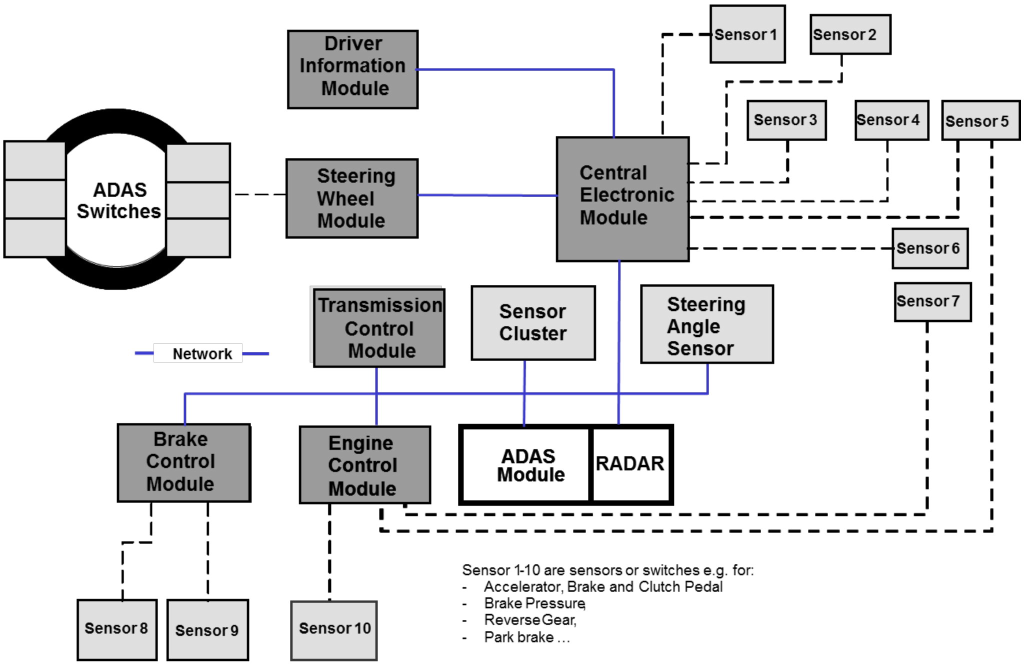

Figure 1 - Architecture example for ADAS

ADAS is now implemented by adding additional subsystems to the existing architecture. For our example, these are:

- The Radar Sensor and possible other sensors (like camera, ultrasonic sensors etc.) as the main input for environmental observation for the different ADAS functions.
- The ADAS Module to execute the algorithm for the functions, e.g. determination of the acceleration needed for distance control, transmission of acceleration limitation requests to the Engine Control Unit and brake force requests to the Brake Control Unit.

For the distributed ADAS function, the existing subsystems (gray) and sensors (light-gray) take over new, ADAS-related functionalities:

- The Engine Control Module acts as both, actuator (e.g. the speed control and the limitation of the engine torque) and sensor (determination of the ACC mode (off, standby, active, denied)) for the ADAS functions.

- The Brake Control Module is the second module which performs actuator functions (e.g. braking based on the requests from the ADAS Module) and sensor functions (e.g. determination of the actual vehicle speed).
- The Central Electronic Module provides the ADAS Module with information needed for a proper execution of the functions (e.g. driver buttons, accelerator pedal position, clutch position).
- The Driver Information Module displays ADAS-related information to the driver.
- The Steering Wheel Module reads the driver buttons and informs the ADAS about their states (on/off).

3. Requirements on a safety design process for distributed functions

Safety related functions distributed over several embedded subsystems lead to various challenges for vehicle manufacturers (OEM's). This concerns both, systems engineering and functional safety. The example shows how distributed features are spread over several subsystems. The distributed functions are realized by adding new modules (e.g. several sensors like radar or camera) and by using several existing subsystems acting as sensors, actuators, for plausibility checks, crosschecks, redundancy etc. The allocation and tracking of safety requirements for such distributed functions is thus an essential claim OEMs have to meet [1].

For requirements engineering, it has to be determined who has to provide which content at which level of detail. Usually, the OEM division responsible for the development of the overall function creates the logical architecture and then distributes requirements to different divisions within the OEM responsible for the subsystems. These divisions receive all requirements from systems in which their subsystem is involved in, integrate the requirements and cascade the requirements to the suppliers.

For verification and validation (V&V), the OEM division responsible for the overall function has to ensure that the V&V tasks are defined and cascaded to the other divisions and the suppliers. Some aspects can only be validated on vehicle level by the OEM division responsible for the system (e.g. the overall behavior of the system), some aspects can be validated on subsystem level by the divisions responsible for the subsystems (e.g. the behavior of the subsystem), and other aspects affecting internal interfaces within the subsystems can only be validated by the suppliers.

When the V&V is performed, the results of the V&V activities at the supplier side and within the different OEM divisions need to be fed back and collected by the division responsible for the system.

4. History: Safety Analysis as Backbone for the Functional Safety process

Functional requirements and safety requirements for the subsystems are developed under the scope of their conventional usage (example: plausibility checks of the steering angle and yaw rate were developed for the ESP functions) and must be adopted to the requirements of the new distributed functions in which they are embedded.

For the safety validation, all this engineering information has to be tracked and documented, and especially the safety-related aspects need to be traced.

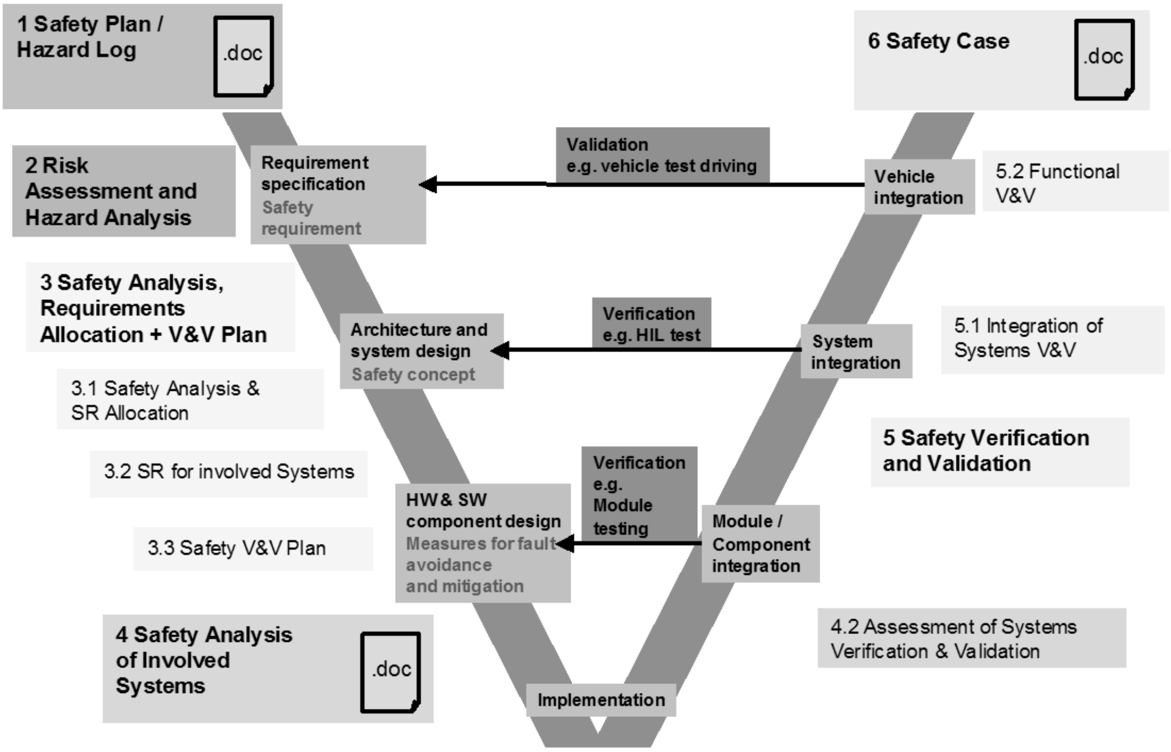
1 Safety Plan / Hazard Log
.doc
6 Safety Case
.doc
2 Risk Assessment and Hazard Analysis
Requirement specification
Safety requirement
Validation e.g. vehicle test driving
Vehicle integration
5.2 Functional V&V
3 Safety Analysis, Requirements Allocation + V&V Plan
Architecture and system design
Safety concept
Verification e.g. HIL test
System integration
5.1 Integration of Systems V&V
3.1 Safety Analysis & SR Allocation
3.2 SR for involved Systems
5 Safety Verification and Validation
HW & SW component design
Measures for fault avoidance and mitigation
Verification e.g. Module testing
Module / Component integration
3.3 Safety V&V Plan
4 Safety Analysis of Involved Systems
.doc
4.2 Assessment of Systems Verification & Validation
Implementation

Figure 1 - Historical Safety Design and Documentation Process

In absence of a dedicated Functional Safety Standard for the automotive domain when ADAS generation 1 was brought into the market, a process was developed within Ford with focus on Safety Analyses [3]. The different steps of this process are shown in Figure 1 and are explained in the following.

4.1. Safety Plan

The primary purpose of the “Safety Plan” is to establish the organizational framework and to define the responsibilities for the safety process, including the tailoring of the safety processes between the OEM and the suppliers.

4.2. Risk Assessment & Hazard Analysis

This step is common for all Functional Safety processes. Before a dedicated automotive approach for performing a Hazard Analysis and Risk Assessment was provided by ISO 26262, several methodologies described in standards and publications, e.g. the risk graph given in IEC (DIN EN) 61508 [2] or in MISRA (Motor Industry Software Reliability Association, https://www.misra.org.uk/), were adopted by different OEMs.

4.3. Safety Requirements Allocation and V&V Plan

General safety requirements, derived from Risk Assessment & Hazard Analysis have to be fulfilled by the particular subsystems.

The allocation of the safety requirements to the elements of the architecture is done on the basis of a safety analysis. The safety requirements are collected in a Safety V&V plan, representing the central documentation for the traceability of safety V&V activities.

As a focal element used for this procedure a Fault Tree Analysis (FTA) was chosen, because it allows for the tool-supported generation of a central database which directly links the system analysis with safety requirements.

The FTA logic represents the complete system in a hierarchical structure of all levels:

- overall functional safety concept
- system architecture with the contribution of the involved subsystems
- system integration in the multiplex network, including monitoring functions
- safety functions allocated at subsystem level for both, Hardware and Software

Intermediate evaluation of the results is possible at any stage of the project. Finally, relational databases based on the FTA provide essential information for further safety activities.

4.4. Safety Verification & Validation Plan

By extending the safety requirements with corresponding verification methods for each requirement, the set of safety requirements provides the integral input for both, systems engineering as well as for verification and validation (V&V).

This facilitates the follow-up of the safety-related V&V measures to be carried out by the responsible organizations (suppliers and/or OEM development departments).

4.5. Safety Analysis of involved Subsystems

The objective of this step is to investigate and to assess the functional safety achieved by the individual subsystems in the context of distributed functions.

Also the capability of the safety processes installed at the subsystems' suppliers is evaluated. This is accomplished by performing safety assessments for each subsystem.

The preparation of a schedule for the safety assessments is supported by the V&V plan where functional safety requirements to Hardware and Software of the subsystems are allocated. In this way, also V&V activities (e.g. test or analysis results) carried out by the suppliers can be tracked and integrated into the V&V plan.

4.6. Safety Verification & Validation:

The overall safety verification & validation -

- integrates the suppliers' V&V results
- considers the V&V results from functional integration into the vehicle
- supports an overall statement whether the safety requirements derived by HARA and FTA are met

The V&V plan is used as central database and checklist for the overall safety validation. It refers to all safety related information which provides the evidence for compliance with the safety requirements.

4.7. Safety Case

The “Safety Case” shall demonstrate that an adequate level of safety is achieved, ensure that safety is maintained throughout the lifetime of the system and therefore minimize the project risk.

Using the safety V&V plan as a checklist and the safety plan to schedule and follow-up the related activities, the Safety Case is supported both from technical and from organizational point of view.

4.8. Conclusion

The presented historical process was based on a few central documents (Safety Plan, Risk Assessment and Hazard Analysis, FTA and V&V plan). This was essential to manage both the complexity of distributed functions and the various references to detailed engineering documentation. In this way, the process was able to provide evidence that the overall safety requirements are met by the integration of many single contributions.

One of the key elements of the proposed process was the FTA. It is worthwhile to mention that FTA often is only used for probabilistic reasons and rather in late project phases for the purpose of verification. It has is to be emphasized, that the FTA in the chosen context supports a systematic approach for both, specification *and* verification. Already in early project phases it can be used for the evaluation of design alternatives. Using the database functionality of related Software-tools, FTA can be considered as a very stringent support for safety engineering.

Anyhow, the historical process described above was more based on validation/verification and lacks a consistent safety lifecycle, fitting to the needs of the automotive industry. Such a lifecycle, and a “top-down approach” for requirements engineering, was presented for the first time with the release of ISO 26262 in 2011. An implementation of such an ISO 26262 safety process is described in the next section.

5. Current State: System Engineering as Backbone for the Functional Safety process

The automotive Functional Safety standard ISO 26262 [4] was released in 2011. Key achievements are a complete Functional Safety lifecycle (see Figure 1), fitting to the best practices of the automotive industry, a standardized approach for the Hazard Analysis and Risk Assessment, and a structured proposal for safety requirements engineering.

This section describes the chosen implementation of ISO 26262 [5] based on systems engineering. Details of Hardware and Software development, production and operation are not subject of this paper.

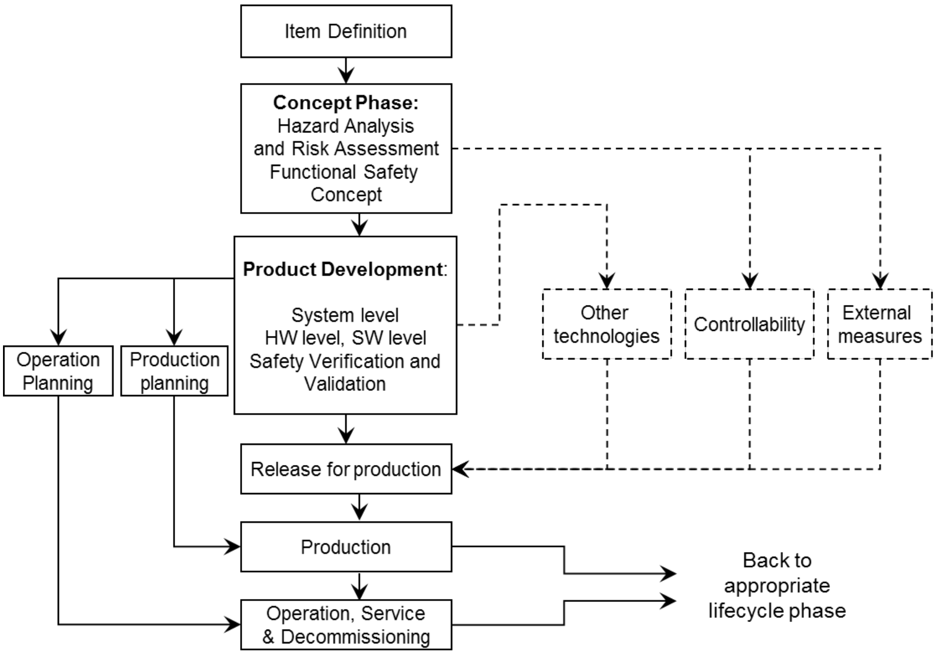
Item Definition
Concept Phase: Hazard Analysis and Risk Assessment Functional Safety Concept
Product Development: System level HW level, SW level Safety Verification and Validation
Operation Planning
Production planning
Other technologies
Controllability
External measures
Release for production
Production
Operation, Service & Decommissioning
Back to appropriate lifecycle phase

Figure 1 - ISO 26262 Functional Safety Lifecycle

5.1. Item Definition

The purpose of the Item Definition is to define and describe the item and to develop an adequate understanding of it with the goal that each activity defined in the safety lifecycle can be performed adequately. The Hazard Analysis and Risk Assessment is carried out on the basis of the Item Definition, and the Safety Concept is derived on the basis of this information. The Item Definition is a "snapshot" at the beginning of a safety project, and shall not be updated with safety requirements derived later during the safety process or in case of other technical changes. It shall be updated when functions are modified, added or deleted.

5.2. Hazard Analysis and Risk Assessment (HARA)

The Hazard Analysis and Risk Assessment is a “thought experiment” based upon the assumption that a failure has occurred in the system. The outcome is a list of possible hazards, including an assigned ASIL (Automotive Safety Integrity Level), reflecting the criticality of the hazardous event. It consists of following steps:

5.2.1. Step 1: Situation Analysis and Hazard Identification

For all combinations of functions and faults, it should be described how the system behaves in presence of the specific fault. For each failure mode, all operational situations, system/operating modes, use cases and environmental conditions (alone or in combination) that could lead to a potential hazard are identified (supported by a situation database), and referenced in the Hazard Analysis.

5.2.2. Step 2: Hazard Classification

The objective of the hazard classification is to assess the level of risk reduction required for the hazards. To classify the hazard, the following steps are performed:

- Estimation of the potential severity (including rationale)
- Estimation of the probability of exposure (including rationale)
- Estimation of the controllability (including rationale)

Based on these estimations, the ASIL determination is done as defined in ISO 26262.

5.2.3. Step 3: Definition of Safety Goals

A safety goal is a high level safety requirement based on the hazards identified in the Hazard Analysis & Risk Assessment. The safety goals have to be clear and precise and be written in such a way that they can be implemented by technical means (e.g. avoid referring to non-measurable data).

5.3. Functional Safety Concept

To comply with the safety goals of the HARA, the Functional Safety Concept specifies the basic safety mechanisms and safety measures in the form of Functional Safety Requirements. For each Safety Goal, at least one Functional Safety Requirement is derived. The Functional Safety Requirements are allocated to elements of a preliminary architecture.

The derivation of Functional Safety Requirements includes an argumentation for Safety Goal achievement, e.g. using the Goal Structuring Notation (GSN) [6], an overview of the different safe states and their related requirements, an operating modes overview, and the derivation of requirements on means, controls and user manual if needed to ensure controllability. These structured derivation and overview helps to derive a complete set of functional requirements.

5.4. Technical Safety Concept

As next step, the Functional Safety Requirements are broken down to Technical Safety Requirements that are allocated to a single subsystem. To specify the Technical Safety Requirements, the System Design is necessary and vice versa the derived Technical Safety Requirements have an influence on the System Design.
For the development of the Technical Safety Concept, it is important to consider:

- Input from System Design, Item Definition, and Functional Safety Concept: external interfaces, constraints, technical block diagram, functional overview of the subsystems, internal interfaces, and a description of the system architecture including the redundancy concepts on system level. This input is necessary to ensure the consistency of the System Design with the Technical Safety Requirements.
- Technical Safety Requirements derived from the Functional Safety Requirements including Fault Tolerant Times, Emergency Operations, and Verification & Validation.

Categories for Technical Safety Requirements are “Safety Related Function”, “Internal Fault Handling”, “External Fault Handling”, “Latent Fault Handling”, “Metric”, “Reduced Functionality”, “User Information”, “Maintain Safe State / Recovery”, “General Safety”, and “Decomposition.
The Technical Safety Requirements as defined by ISO 26262 cover the system level (including requirements on the subsystems) which is usually defined by the OEM, but also subsystem internal requirements. In many cases, the OEM buys these subsystems from suppliers. The derived Technical Safety Requirements are therefore cascaded to the subsystem suppliers.
The subsystem supplier derives the detailed Hardware and Software requirements from the Technical Safety Requirements.

5.5. Safety Verification and Validation

The Safety Verification and Validation includes detailed verification and validation planning and status tracking:

- Alignment between Safety Analyses and Specifications (Functional Safety Requirements, Technical Safety Requirements and detailed Hardware and Software Safety Requirements)
- Validation and Verification Status of all safety relevant parameters
- Definition, validation and status of the design verification
- Validation of Hardware metrics calculation

For the Functional Safety Requirements, the verification (e.g. test) and validation (e.g. analyses, review) is documented (including activity and acceptance criteria). The correctness and the completeness is assessed and validated.

For the Technical Safety Requirements, a verification measures are defined in order to verify the correct implementation of the Technical Safety Requirement (e.g. Fault insertion, Safety Function testing etc.). The correctness and the completeness of the verification measures assessed. The specified verification and validation is performed and all results are documented.

5.6. Conclusion

The presented ISO 26262 related process is based on a Functional Safety lifecycle, which allows a tailoring of different activities (and of the responsibility for the related artifacts) between the OEM and several subsystem suppliers.

The HARA and the derivation of Functional Safety Requirements are done on a functional level and therefore kept independent from the technical design. When the Functional Safety concept is finalized, the requirements are allocated to the elements of the (preliminary) physical architecture, i.e. the subsystems involved in the implementation of the function. The technical safety requirements are derived for these subsystems and drive the design and implementation [7]. The modular V&V approach allows the collection of contributions (e.g. test results for subsystems, the overall system and the functional level).

Anyhow, if the artifacts created by this process are based on textual information (e.g. Office-related documents and/or representations in databases or conventional requirement management tools), it is difficult to keep the content consistent, and to provide a sufficient overview.

Therefore, the authors recommend the extension of Model-Based Systems Engineering (MBSE) to cover also the requirements from ISO 26262. This approach is summarized in the next section.

6. Outlook: Model-based Systems Engineering

For complex development distributed among different locations and performed by different stakeholders, model-based engineering may be an improvement.

Our model-based development approach is based on UML (Unified Modeling Language of the OMG, Object Management Group) extended by a profile for Functional Safety. Each phase of the development is supported by stereotypes defined in the corresponding profile complemented by validation conditions using OCL (Object Constraint Language of the OMG):

- Definition of the Item (System to be developed)
- Hazard and Risk Assessment with stereotypes e.g. for situations, malfunctioning behavior, and hazardous events
- Definition of Safety Goals
- Definition of Functional Safety Requirement with all necessary attributes
- Definition of Technical Safety Requirement with all necessary attributes
- Verification and Validation of Requirements

To specify Functional Safety Requirements, the part of the profile, depicted in Figure 1, can be used.

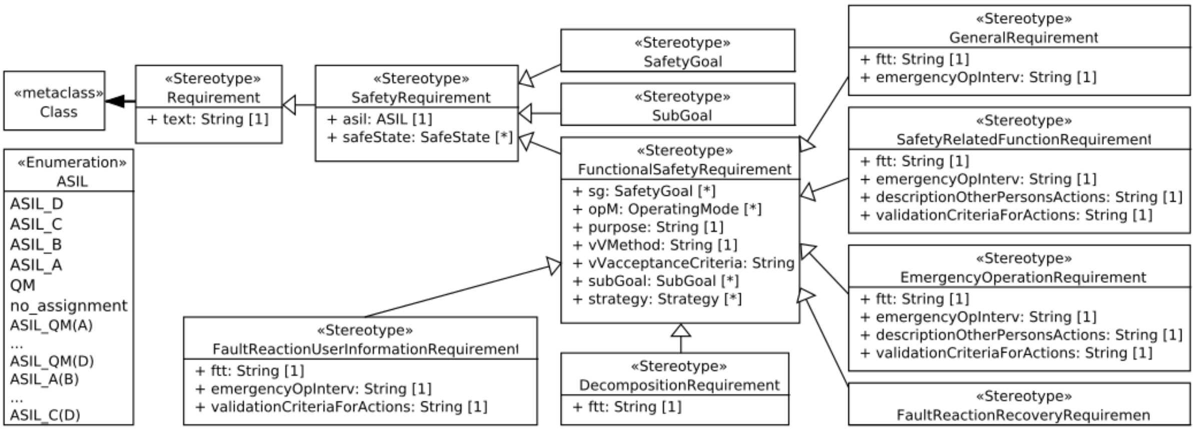

Figure 1 - Functional Safety Requirement Profile

In Figure 1, a stereotype for the ASIL of the requirement is defined. It includes “QM”, the information that no ASIL is assigned, the ASILs from “ASIL A” to “ASIL D” and the ASILs defined by a decomposition, e.g., “ASIL C(D)”. For each *Class* the stereotype *Requirement* with the requirement text as an attribute can be defined. The *Safety Requirement* is a special requirement with the attributes *ASIL* and *Safe State*. *Safety Goals*, *Sub-Goals* and *Functional Safety Requirements* are special safety requirements with additional attributes to be filled out. For the different types of Functional Safety Requirements, specialized stereotypes (e.g., *Fault* and *User Information Requirements*) with the necessary attributes are defined. The profile is presented in Beckers et. al. (2017) [8].

The UML profile establishes the basis for including the safety development according to ISO 26262 in the overall “Model-based Systems Engineering” (MBSE). The advantage of a model-based approach is that the different artifacts are explicitly connected instead of having loosely coupled documents. On the overall model, consistency checks can be performed. These consistency checks can be specified with the Object Constraint Language. Thus, the approach provides a computer-aided technique to discover errors in the complete safety development process caused by inconsistencies or errors in one or more (UML) diagrams. In addition, the model-based approach enables us to re-use the models, or parts hereof, for similar projects assuming that the same tool base is used.

Changing the development process to a model-based approach is a necessary step the cope with the increasing technical complexity of the future ADAS systems, and the growing complexity of interactions and interfaces between the multiple organizations involved in the development of such features. However, the change from using spreadsheet-processing tools for development to creating models is a challenging task for the involved engineers and requires good tool support and a sufficient amount of training and support by MBSE experts.

7. Summary

The historical development of Advanced Driver Assistance Features was clearly a kind of evolution, starting from simple and limited functions to more powerful functions. Also the accompanying Functional Safety Process was improved in an evolutionary way, based on “discrete” Safety Analyses, followed by an integrated Safety Process which is aligned to the system engineering V-Modell. The international automotive Functional Safety Standard ISO 26262 introduces a Functional Safety lifecycle, fitting to the needs of the automotive industry and suitable for development of distributed features by distributed organizations.

The roll-out of model-based Systems Engineering, including development of the Functional Safety artifacts needed for ISO 26262 compliance, appears more as a kind of revolution, but are key enablers for the future development of more complex systems pointing towards autonomous driving.

The UML profile developed contains all relevant elements for a hazard analysis, functional safety concept, technical safety requirements specification and safety V&V. Pilot projects are already started to extend the approach to Safety Analysis and Safety Management. Currently, Ford is implementing tool support in NoMagics MagicDraw. Ford is also creating import and export functionality for their current templates and is developing an interface to requirements management tools.

8. References

[1] C. Jung, M. Woltereck, Proposal of a Functional Safety Process for Distributed Development of Safety-related Systems, VDI-Berichte Nr. 1789, 2003

[2] IEC / EN 61508 Functional safety of electrical/electronic/programmable electronic safetyrelated systems

[3] F. Edler, T. Frese, Systematic Safety Design Process for Distributed Vehicle Systems. Im Tagungsband des 12. Internationalen Kongresses Elektronik im Kraftfahrzeug, CDI Berichte, 1907, 225-235, Düsseldorf 2005

[4] ISO 26262, Road vehicles - Functional safety, First edition, 2011-11-15

[5] T. Frese, H.-J. Aryus, D. Hatebur, Deriving safety requirements according to ISO 26262 for complex systems: How to avoid getting lost? In: Elektronik im Kraftfahrzeug / 5. VDI-Tagung Baden-Baden Spezial 2012 / 2012, S. 67 – 80, ISBN: 978-3-18-092172-3

[6] Dr T. Kelly, University of York, UK, GSN: A Systematic Approach to Safety Case Management, 2003, available at http://www-users.cs.york.ac.uk/~tpk/04AE-149.pdf

[7] H.-J. Aryus, T. Frese, D. Hatebur, I. Côté, M. Heisel: Deriving Safety Requirements according to ISO 26262 for complex systems: A method applied in the automotive industry
6. Wissenschaftsforum Mobilität, 2016

[8] K. Beckers, I. Côté, T. Frese, D. Hatebur, M. Heisel: A structured and systematic model-based development method for automotive systems, considering the OEM/supplier interface. Rel. Eng. & Sys. Safety 158: 172-184 (2017)