ISO/DIS 26262 in the Context of Electric and Electronic Architecture Modeling

Martin Hillenbrand[1,*], Matthias Heinz[1,*], Nico Adler[2,*], Klaus D. Müller-Glaser[1,*], Johannes Matheis[3], and Clemens Reichmann[3]

[1] Institute for Information Processing Technology, KIT, Germany
{hillenbrand,heinz,klaus.mueller-glaser}@kit.edu
[2] FZI Forschungszentrum Informatik, Germany
adler@fzi.de
[3] aquintos GmbH
{matheis,reichmann}@aquintos.com

Abstract. The draft international standard under development ISO 26262 describes a safety lifecycle for road vehicles and thereby influences all parts of development, production, operation and decommissioning. All systems affected by the standard, like anti-trap protection or advanced driver assistance systems, contain hierarchical electric and electronic parts. After publishing the final version, they all should be designed, assessed and documented to the demands of ISO 26262.

The intercommunication structure of the distributed automotive control system, consisting of electronic control units (ECU), sensors and actuators, and functions computed by this control system, are specified by the electric and electronic architecture (EEA). In the context of the ISO 26262, the EEA contributes to the intercommunication of distributed, safety related functions plus the determination of architectures.

This article discusses the impact of the standard on the EEA development and the handling of safety requirements demanded by ISO 26262 during early development phases.

Keywords: Automotive, Architecture modeling, Functional Safety, ISO 26262.

1 Introduction

The increase of number, complexity and interaction of electric and electronic systems in a vehicle, bears growing challenges for development activities in the automotive domain. Besides the decreasing development time, the increasing distribution of functions and their computing control system, the draft international standard for functional safety of road vehicles ISO/DIS 26262 (International Organization for Standardization / Draft International Standard 26262) requires attention. Automotive systems demand safety and reliability, which results in consideration of safety requirements with the same level of priority as the functional requirements of the system to develop [1].

* This research work was supported by the Ministerium für Wissenschaft, Forschung und Kunst Baden-Württemberg (AZ: 32-720.078-1/14).

H. Giese (Ed.): ISARCS 2010, LNCS 6150, pp. 179–192, 2010.

In the aerospace domain, safety considerations, methods, guidelines and certifications are applied for a long time [2] [3], establishing a safety lifecycle. State of the art processes, concerning safety in the automotive domain, base on hazard analysis, failure mode and effect analysis (FMEA) [4], fault tree analysis (FTA) [5], Markov chains and reviews. A standardized safety lifecycle is not yet applied in the automotive domain.

ISO 26262 [6] standardizes a safety lifecycle process, concurrent to the already applied development processes, which, in the automotive industry, are based on the V-Model '97 [7]. ISO 26262 is the interpretation of the DIN EN 61508 [8] [9] for road vehicles with a maximum weight of 3,5t. The draft standard has been published in July 2009, its publication as international standard is expected for 2011.

ISO 26262 enlarges the concept and design space by another dimension. This is why good processes and well applied tool support are mandatory to compete with legal requirements and in the meantime develop safe vehicles, containing forward-looking technologies.

ISO 26262 is based on the system architecture. The vehicle itself consists of different systems; their electric and electronic architecture is modeled in the according development process. The design and development of the EEA of a vehicle is based on the work products from preceding development phases like the design of a broadly defined system architecture concept. In the future it has to consider the results of analysis, considerations and classification of safety aspects, demanded by ISO 26262. The electric and electronic (EE) part of the system architecture is iteratively refined and detailed during the development process. The impact of ISO 26262 to the modeling of the EEA and the contribution of the EEA modeling towards the fulfillment of the overall safety concept is discussed in this paper.

The following chapter gives a short overview of ISO/DIS 26262. Chapter 3 presents the modeling of EE architectures with respect to safety aspects. The involvement of the EEA development in the safety lifecycle is described in chapter 4. Chapter 5 and 6 describe the flow of interpreting and formatting work products from preceding safety analysis and their handling during EEA development. The relations between classes of the EEA meta-model, depicted in a UML [10] class diagram, and safety aspects are presented in chapter 7. Chapter 8 summarizes the work and gives an outlook to further activities.

2 ISO 26262 Lifecycle

Figure 1 depicts an overview of ISO 26262. During the concept phase, the item is defined ([6] part 3, chapter 5). The item represents a system, an array of systems or a function, to which the ISO 26262 is applied ([6] part 1, chapter 1.69). Based on the item, a hazard analysis and risk assessment is performed, in which hazards are classified and assigned with an automotive safety integrity level (ASIL) [11]. Based on these hazards, safety goals (SG) are determined, and the ASIL that was determined for the hazardous event is assigned to the safety goal ([6] part 3, chapter 7). Functional safety requirements (FSR) are derived from the SGs, inheriting the ASIL from the SG, and are allocated to elements from a preliminary architectural draft of the item ([6] part 3, chapter 8).

In the product development phase on system level ([6] part 4), technical safety requirements (TSR) are formulated to describe how to implement the functional safety concept, containing the FSRs, along with the implementation of the functional concept. During this phase, the system gets more and more refined by partitioning into hierarchical sub-system structures. By the level of granularity, where a sub-system can be refined or realized in software (SW) or hardware (HW) only, the phases for product development on HW and SW level are applied ([6] part 5 and 6). TSRs must be specified ([6] part 4, chapter 6) on each level of system and sub-system granularity, followed by the system design ([6] part 4, chapter 7) on the same level of granularity.

During further development ([6] part 5 and 6), HW and SW systems are refined and TSRs are specified. After specification, implementation and integration on HW and SW level, HW and SW components are integrated step by step. This system integration is covered by [6] (part 4).

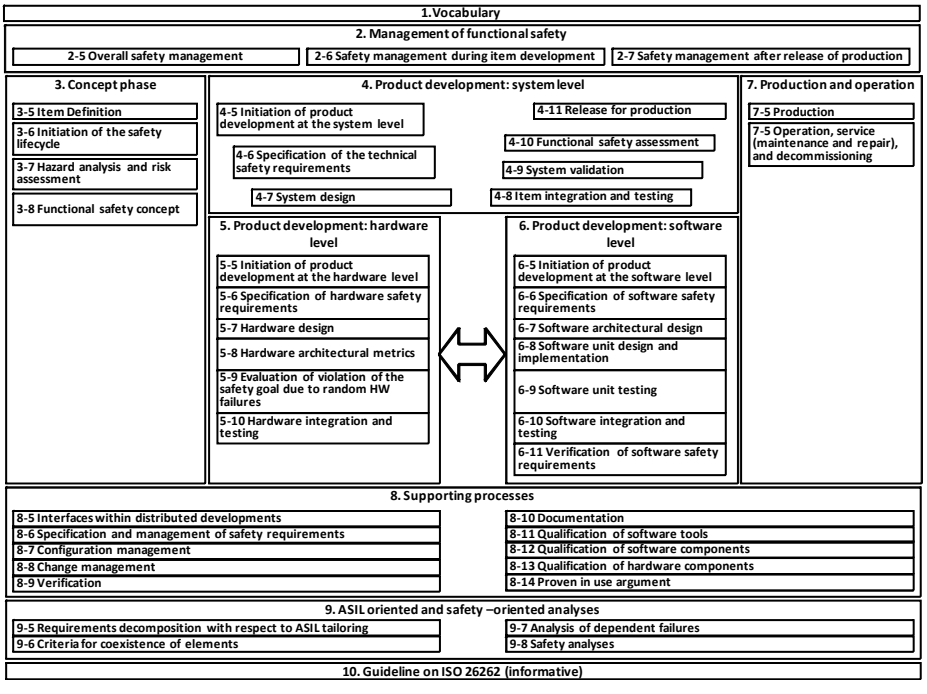

Fig. 1. Overview of ISO 26262

3 EEA Modeling

The development of modern vehicles has to consider numerous technical and functional aspects. Reliability and maintainability as well as usability, functional safety, comfort and performance influence the overall cost function for vehicle design. The demanded quality has to be established and integrated during the design phase.

The tool PREEvision [12] facilitates designing, modeling, comparing and evaluating the electric and electronic architecture of a vehicle in the system design phase [7] of a vehicle development [12] to achieve the optimal overall architectural design. For the first time, all data of the EEA design can be considered in one model. This facilitates the usage of metrics to make an assessment of the EEA. The following section gives a short overview about EEA modeling using PREEvision.

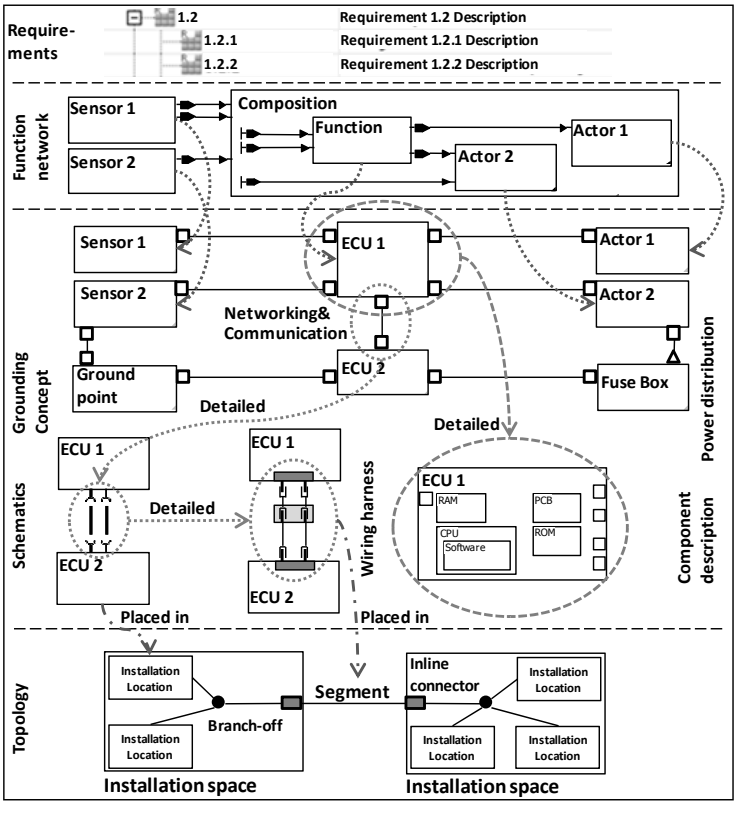

Fig. 2. EEA layered architecture

An EEA model designed in PREEvision is based on the layered architecture (Figure 2) [13]. Each layer depicts a modeling view to the EEA. The EEA model contains requirements-, software-, hardware- and networking-information, which are represented by artifacts in a model tree. Artifacts from the model tree can be visualized in one or more diagram types, each specific to a particular view. Each diagram type offers a specific view on the architecture-model, its artifacts and connections (Function Network Diagram (FN), Component Network Diagram (CMP), Schematic Diagram, Wiring Harness Diagram, etc.). Mappings model the relations between artifacts across diagram borders.

Based on underlying rule- and meta-models, model query rules can be described in PREEvision and later executed on the EEA model for evaluation and consistency checking [14]. These rules can also be used to browse the EEA model for chains of artifacts with a particular relationship.

The consideration of safety aspects and the work products from preceding safety analysis during the EEA design phase, delivers resilient input data for further development phases. Wrong architectural decisions can have devastating impact on safety, reliability and operability of the vehicle and the amount of expenses resulting from mandatory fixes during the later development. Functional safety has to be ensured top down through the development process.

Further, there are methods and strategies applicable during EEA modeling, which have the potential to reduce development and documentation effort (in the context of the safety case [15]) of HW and SW elements caused by allocation, distribution, decomposition and coexistence of safety aspects and EEA artifacts.

It is of severe importance to implement the draft international standard for functional safety ISO 26262 into the vehicle development process and therewith into the phase of EEA development. The next chapter discusses relations and influences.

4 EEA Development in the Context of ISO 26262

A brief overview of the ISO 26262 was given in chapter 2. This chapter considers the role of the EEA development during the processes specified by the draft international standard.

The derivation of safety goals in the EEA tool PREEvision is presented in [16]. The functional safety concept phase will be performed by the role of the safety expert at the original equipment manufacturer (OEM). However, the role of the safety expert at the OEM may consult the EE architect during item definition, the preliminary architectural assumption or the allocation of FSRs to elements of this architectural assumption.

The specification of TSRs during product development on system, HW and SW level, might be performed by both roles, EE architect and safety expert.

The development and refinement of the EEA lies in the responsibility of the EE architect. The compliance of the developed system to the ISO 26262 lies in the responsibility of the safety manager. Although the EEA is not a system within the meaning of the ISO 26262, the development process of the EEA strongly correlates with the ISO 26262 [6] (part 4, chapter 7). This includes the allocation of TSRs ([6], part 4, chapter 7.4.5) to the elements of the system architecture, which are artifacts of the EEA model, the accomplishment of ASIL decomposition ([6] part 4, chapter 7.4.2.5) if adaptable and the assessment for the meeting of coexistence criteria ([6] part 4, chapter 7.4.2.3). Coexistence will be detailed in chapter 6.

The development and implementation of electronic control units (ECUs), including HW and SW parts, is usually accomplished by tier one suppliers. Because of that, subdivision of sub-systems down to the HW- or SW-only level, which are covered by [6] (part 5 and 6), will be mainly performed by the tier one suppliers and their consulting counterpart at the OEM.

The role responsible for a specific electric and electronic component specifies the component HW down to its internal elements, including microcontrollers and memory, and sets up the interacting architecture of functions. This interacting architecture is comparable with AUTOSAR software components (SW-C) put onto a virtual functional bus (VFB) [17].

The EEA does not go further in subdividing the modeled systems into hardware- and software-only systems. Therefore the EE architect is not directly involved in the system development on hardware or software level. Nonetheless, advising during further development phases is possible.

5 Presentation, Import and Interpretation of Safety Requirements

At an OEM, safety requirements will be entered into a requirement tracking tool like DOORS®. At the initiation of the EEA modeling, safety requirements comprising SGs, FSRs and TSRs, if they are already formulated, are imported from the requirement tracking tool into the EEA modeling tool PREEvision as requirement artifacts. If FSRs and TSRs are available, an initial set of safety requirements to be imported to the EEA modeling tool, can be derived from the safety requirements definitions of former production series.

According to ISO 26262, safety requirements comprise several attributes, not all are relevant to be considered for the development of the EEA. SGs express a statement in textual form and have the attribute ASIL. Both should be available in the EEA model. Although the SGs are not directly allocated to artifacts of the EEA ([6] part 3, chapter 8.1), they are needed to track deriving of FSRs. Following the ISO 26262 lifecycle, FSRs are allocated to the elements of the preliminary architectural concept for the item ([6] part 3, chapter 8.2).

Due to the level of abstraction used at the specification of the preliminary architecture concept (Figure 4), the information of all aspects must be partitioned to different diagrams, obligatorily increasing the level of detail.

From the attributes of the FSRs allocated to the elements of the preliminary architectural concept, besides their ASIL, functional redundancy aspects ([6] part 3, chapter 8.4.2.3), warning concepts ([6] part 3, chapter 8.4.2.4), timing constraints ([6] part 3, chapter 8.4.2.3) and additional performance properties (bus load, wire cross-section, etc.) are important, because of their correlation with the elements to model in the EEA and their relationship.

Before and during the development on system level, TSRs are specified for refinement and realization purposes of the functional safety concept. The specification of the first set of TSRs is based on the preliminary architectural concept. TSRs also comprise attributes and considerations ([6] part 4, chapter 6.4.1). Detection, indication and control mechanisms of the system itself (internal architecture) or for devices interacting with the system (sensors, actuators or control mechanisms), can be depicted by high level SW functions (artifacts of the FN of the EEA) or wired connections between the item's HW artifacts and external devices (artifacts of the CMP of the EEA). More details about how this detection, interaction and control, as well as the enabling or achieving of a safe state works, is described by activities. The application of the EEA modeling, to develop a static architecture, does not cover the modeling of functional behavior.

SGs should be structured to keep the derivation structure to FSRs and TSRs traceable. During the safety concept and the system development, safety requirements are derived from each other considering additional aspects (environmental, interfacing, architectural, etc.). Similar specialized requirements derived from different abstract requirements can be combined. Therefore, the hierarchical structure with SGs as root, FSRs on the second level and TSRs on the third level is not feasible. We suggest a flat hierarchy of safety requirements with separate packages for SGs, FSRs and TSRs. The correlation between the requirements is then modeled by links, which additionally allows 1..n relations bottom up, from TSRs over FSRs to SGs. The correlation between the requirements can be tracked and visualized on demand by the execution of predefined model query rules browsing the EEA model for artifacts bearing specific relations.

Generally, the most important attributes of safety requirements are the ASIL and the type of requirement (SG, FSR or TSR). Among others, these attributes require typecasting, to enable automatable analyses on the EEA model based on ASIL and safety requirement types by the application of model query rules.

6 How to Handle Safety Requirements during EEA Development

Based on the preliminary architectural concept and assumptions, used during the development of the safety concept or EEAs from former production series, the EEA is set up. Figure 3 depicts exemplary safety requirements and their attributes ASIL and requirement type, organized and formatted according to the preceding discussion in a PREEvision requirements table. These requirements are allocated to artifacts of the EEA during further EEA development activities. Safety goals and functional safety requirements as well as the following explanations are leant on the example of a powered sliding door from [6] part 10. The technical safety requirements depicted in Figure 3 are additional examples, why their ASIL-cells are grayed out.

List of Safety Goals and Safety Requirements			ASIL	Type
Safety Goals				
	1.1	Not to open the door while the vehicle speed is higher than 15 km/h	ASIL_C	SG
Functional Safety Requirements				
	2.1	The door actuator will only open the door when powered by the PSDM	ASIL_C	FSR
	2.2	The DSC will send the accurate vehicle speed information to the PSDM	ASIL_C	FSR
	2.3	The PSDM will allow the powering of the actuator only if the vehicle speed is below 15 km/h	ASIL_C	FSR
Technical Safety Requirements				
	3.1	The information about the actual vehicle speed should be actualized with a cycle time of 100ms.		TSR
	3.2	The transmission of the information of the actual vehicle speed should be secured by a CRC		TSR
	3.3	The plausibility of successive information about the actual vehicle speed should be verified by the receiver		TSR
	3.4	The wheel rotation sensors should be diagnosed by the connected ECU		TSR
	3.5	A failure at a wheel rotation sensor should be signalized by a yellow warning light		TSR
	3.6	If a failure at a wheel rotation sensor is recognized, an according information should be stored in the ECU memory		TSR
	3.7	The wheel rotation speed should be measured with an accuaracy of at least 30 rad/min		TSR
	3.8	The status of the door lock should be monitored all 500 ms		TSR
	3.9	On a motion of the vehicle between 0,1 and 15 km/h, an ajar door should be signalized to the driver with a yellow warning light		TSR
	3.10	On a motion of the vehicle above 15 km/h, an ajar door should be signalized to the driver with a red warning light		TSR
	3.11	The button should be activated longer than 200ms to trigger an action.		TSR
	3.12	If the button is pressed more than 10 times within 30sec, the function should be blocked for 5 min.		TSR
	3.13	If a false activity of the sliding door actuator is recogniczed, the controlling and actuator should be transfered in a safe state.		TSR
	3.14	The actuator activity of the sliding door should be monitored		TSR

Fig. 3. Safety requirements in PREEvision, example powered sliding door from [6] part 10

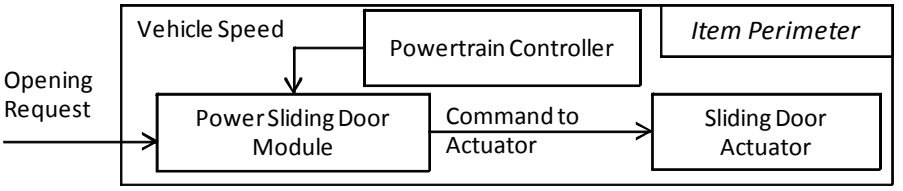

Fig. 4. Item perimeter of a powered sliding door

Figure 4 depicts a preliminary architectural concept of the system in block diagram form, used during safety considerations in the concept phase. The opening of the sliding door during driving activities, and the possibility of people getting seriously injured by accidently falling out, was identified as hazard for the item (powered sliding door) and classified with ASIL C ([6] part 10).

This simplified architecture, presenting static as well as functional and communication aspects, will in the next steps be refined to a detailed EEA model, presented by PREEvision FN and CMP diagrams.

A FN is set up to realize the demanded functionality. ISO 26262 contains aspects towards safety considerations of hardware-software-interfaces ([6] part 4, chapter 7.4.6) like interrupts, timing consistency, data integrity, memory management, etc. ([6] part 4, Annex B). Regarding the AUTOSAR layered architecture, these are services of the AUTOSAR Basic Software (operating system, communication, microcontroller abstraction, etc.) [17]. These functions and services are not subject of the EEA model. FSRs and TSRs are allocated / mapped to function blocks realizing the functionality and considered under safety aspects ([6] part 4, chapter 7.4.5). Figure 5 depicts the function network including the mapped safety requirements displayed in external boxes.

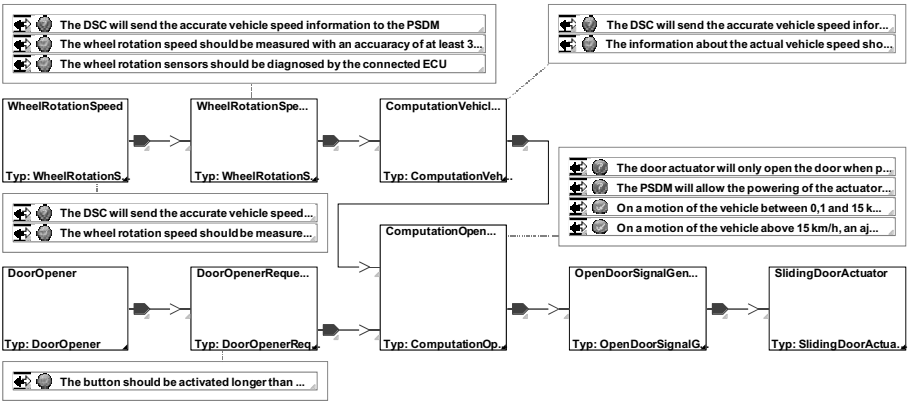

Fig. 5. Function network (FN)

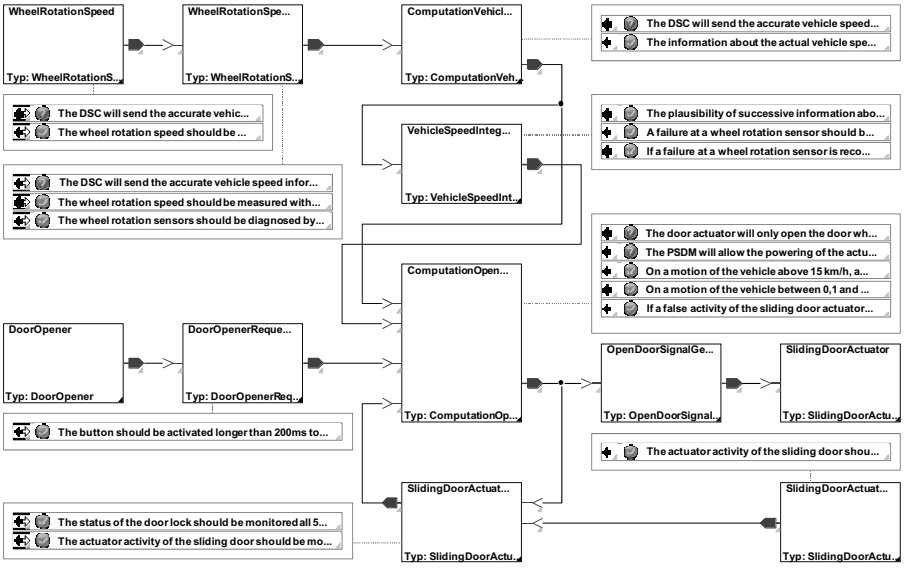

Fig. 6. Refined function network

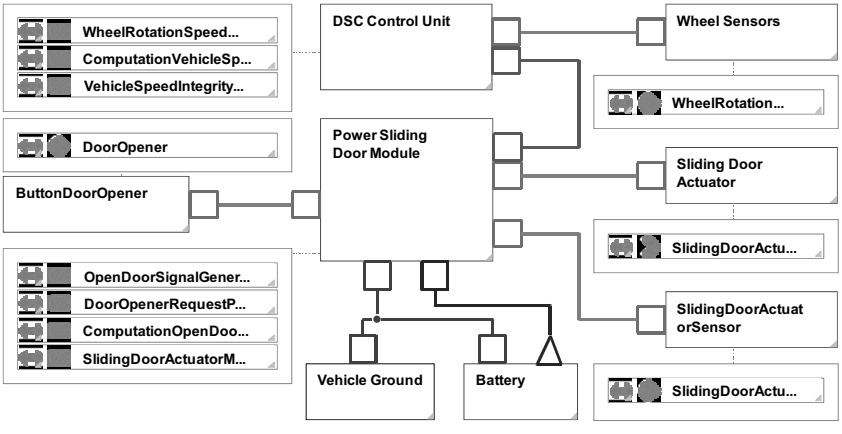

Fig. 7. Component network

If some safety requirements, like plausibility checking or actuator monitoring were not mapped, because no function blocks were available, contributing to the fulfillment of these particular safety requirements, the FN needs additional refinement.

Figure 6 depicts the refined FN. The remaining safety requirements are allocated.

The modeled software architecture must be computed by the computation nodes of the CMP. After setting up the CMP, the functions from the FN are mapped to their computation nodes of the CMP (Figure 7). The mapped functions are depicted in external boxes.

Every electric component including sub-systems and external interfaces inherits the highest ASIL from the functions mapped to them. In addition to hardware elements inheriting an ASIL by computing a function which has an ASIL assigned, there may be TSRs only affecting hardware elements like contact safe plug connections or special wires for electromagnetic compliance.

During EEA modeling, preliminarily, simplified modeled function- or component-systems with ASIL assignment are refined, which includes specification of their internal structure by sub-systems. The criteria for coexistence ([6] part 10, chapter 6) can be applied to the refined system, if it can be proven, that only some of the sub-systems are involved in fulfilling the safety requirements and that these determined sub-systems are not influenced by the others. In that case, only the safety related sub-systems inherit the ASIL. This procedure can be applied to compositions of functions in the FN and component refinement in the CMP.

Figure 8 depicts an example for the application of the criteria for coexistence. The ECU at the left hand side contains two proven independent microcontrollers, only one of them computing a safety related function. The dashed border encircles safety related elements.

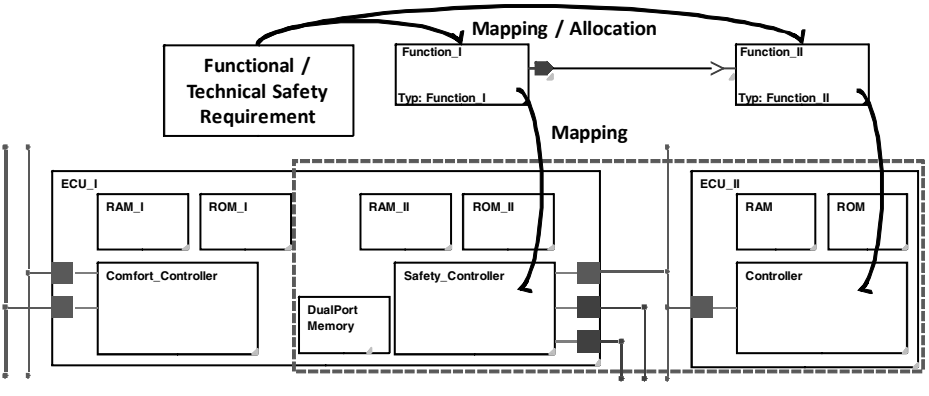

Fig. 8. Coexistence

While designing automotive systems, it will be indispensable to trace the dependencies between artifacts of the EEA, the allocated safety requirements and the ASILs according to which the architecture elements have to be developed later on. Based on the specification of model query rules, the EEA model can be browsed for chains of artifacts in a specific relationship. Based on this, for example all hardware elements involved in fulfilling a SG, all functions assigned to a specific ASIL, or all artifacts having the same safety requirement allocated, can be determined. The results of these model query rules can be displayed to support the overview of the dependencies.

Figure 9 depicts the dependency between ECU (upper right), computed function (middle) and allocated safety requirements (left) by the support of model query rules.

ISO 26262 demands the verification of the system design ([6] part 4, chapter 7.4.8). The verification of the EEA for consistency is mandatory, because work products from the EEA modeling phase are input data to following development phases. The EEA

can support to this by consistency checks executed on the model and browsing for specified inconsistency cases like not correctly inherited safety requirement, etc.

Parts 3 to 7 of the ISO 26262 contain chapters requesting development activities in the context of functional safety. Each of these chapters specifies work products as input to subsequent processes of the lifecycle or for documentation purposes used for the deployment of the safety case. Reports, documenting content and relations of the EEA model, can be automatically generated and formatted out of PREEvision and thereby support the deployment of the safety case. The content of reports is based on results of predefined model query rules.

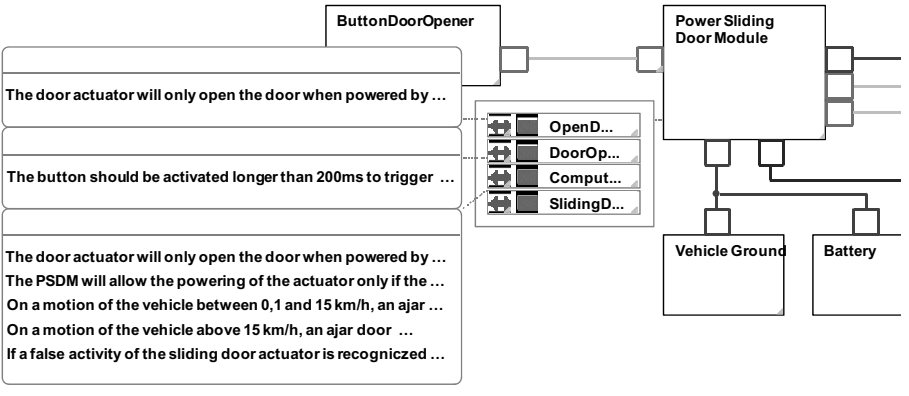

Fig. 9. Dependencies between HW elements, functions and safety requirements

7 Relations between Safety Requirements and PREEvision EEA Artifacts

The assignment of safety requirements and ASILs to artifacts of the EEA is an important step during the EEA development. Especially the determination to which artifacts of the EEA safety requirements have to be assigned and to which not, does not represent an easy task.

EAST-ADL supports determination and modeling of FSRs by safety cases. The derivation of FSRs is not supported [16]. In EAST-ADL-2.0, the relation between an item and its containing elements or systems is depicted by a composition between the class *item definition*, which is interpreted as a collection of entities defining the item that the safety case is valid for (i.e. a "system"), and the abstract class *ADLEntity* [18]. More precise statements about specializations of *ADLEntity* are not provided.

Therefore, the following chapter discusses and specializes the connection between EEA artifacts modeled in PREEvision and safety requirements. A simplified excerpt of the PREEvision meta-model, extended by safety aspects encircling the super class *Safety Related Element*, is applied for this discussion. The class diagram of the applied meta-model is depicted in Figure 10.

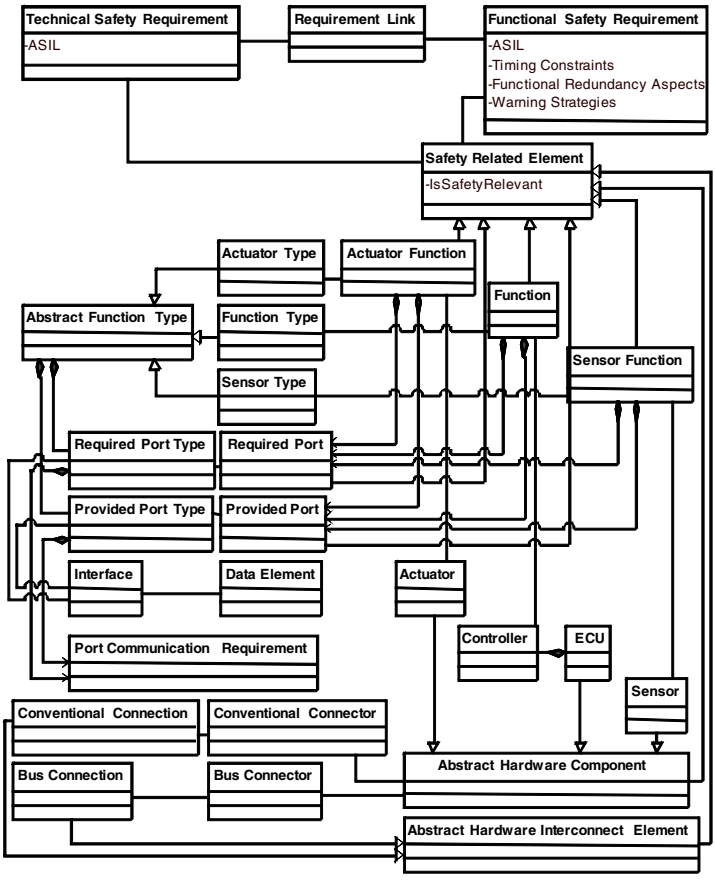

Fig. 10. Simplified EEA meta-model

The super class *Safety Related Element* adds a boolean value for safety relevance to the inheriting instance. The dependence and derivation between the safety requirements can be tracked by the associated *requirement link*.

Abstract Function Type is a typecast for a function (*Actuator Type*, *Function Type* and *Sensor Type*). It is instantiated to fulfill functional safety or non-safety requirements in the FN. The purpose of the usage of an *Abstract Function Type* cannot be foreseen. The instantiation becomes a safety related element by the context of application, but not the type. Therefore the *Abstract Function Type* is not a *Safety Related Element*.

The class *Interface* specifies the communicated data between function objects. Based on their characteristic as types, for most of them, safety relevance can't be determined, caused by the unknown application of their instances. During further modeling, signals are instantiated based on the specification of *Interfaces*. If a signal is a unique communication unit, used to transfer safety related information between hardware elements, it must be regarded as safety relevant.

Like *Abstract Function Types*, *Port Types* are not safety relevant, but their instances can be.

Port Communication Requirement specifies the communication properties of ports (cycle time, etc.). This information has to be considered independently from the fact, if the instance of the specified port belongs to a safety relevant function or not.

Attributes of *Required Port* and *Provided Port* realize the interface of a function. The ASIL is inherited from the function to the ports, realizing the communication of safety relevant information. If a function fulfills safety requirements with different ASILs, all ports of the function get the highest ASIL unless criteria the for coexistence is applicable. Regarding the development of the FN in the phases of EEA modeling, this concerns more compositions (systems of functions) than functions. Functions are atomic elements from the EEA point of view. Compositions outline the demanded functionalities and can be detailed during the EEA modeling, which is strongly correlated to the explained scenario.

Elements, realizing interconnection between HW elements (*Abstract Hardware Interconnect Element*), must be considered as being safety relevant. If two interconnected functions are necessary to fulfill a safety requirement, this also concerns the interaction between these functions. If both functions are processed on different HW elements, the HW elements and their interconnection elements inherit the ASIL of the safety requirement.

8 Summary and Outlook

This paper discussed the impact of the future standard for functional safety of road vehicles ISO 26262 to the development in the automotive domain, with special focus on the development of the electric and electronic architectures of vehicles. The additional engineering effort for design, analysis, assessment and documentation, which is demanded by the standard, can be reduced by the well-wrought application of tools. As presented by the handling of safety requirements and their mapping to the item, which comprises software and hardware systems, the decisions of the EE architect influences succeeding development phases of the vehicular systems and systems of systems. The presented methods for the allocation of safety requirements, the refinement of the design, the determination and application of the criteria for coexistence as well as the fast tracking and convincing presentation of the relations between safety information and the artifacts of the EEA model, enables for development of systems demanding functional safety (according to ISO 26262) and support succeeding development activities throughout the vehicle development lifecycle.

Further activities will among others concentrate on the seamless design flow from the development of the safety concept, based on simplified preliminary system architecture and the import and refinement of this architecture during the phase of EEA modeling.

References

[1] Benz, S.: Eine Entwicklungsmethodik für sicherheitsrelevante Elektroniksysteme im Automobil. Dissertation. Bosch (2004)

[2] SAE ARP4754. Certification Considerations for Highly-Integrated Or Complex Aircraft Systems (1996), http://www.sae.org/technical/standards/ARP4754

[3] SAE ARP4761, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment (1996), http://www.sae.org/technical/standards/ARP4761
[4] VDA Verband der Automobilindustrie e.V. Produkt- und Prozess-FMEA. Band 4. Sicherung der Qualität vor Serieneinsatz. Qualitätsmanagmenet-Center (QMC) (2009)
[5] VDA Verband der Automobilindustrie e.V. Fehlerbaumanalyse (FTA). Band 4. Sicherung der Qualität vor Serieneinsatz. Qualitätsmanagmenet-Center (QMC) (2009)
[6] ISO/DIS 26262 Road vehicles – Functional safety – Part 1-10, Standard under development (2009), http://www.iso.org
[7] iABG, V-Modell-97 (1997), http://www.v-modell.iabg.de/
[8] DIN EN 61508-1,VDE 0803-1:2009-06. Funktionale Sicherheit sicherheitsbezogener elektrischer / elektronischer / programmierbarer elektronischer Systeme; Allgemeine Anforderungen (IEC 65A/522/CDV:2008), German Version. Beuth Verlag, Berlin-Vienna-Zurich
[9] DIN EN 61508-2. VDE 0803-2:2009-06. Funktionale Sicherheit sicherheitsbezogener elektrischer / elektronischer / programmierbarer elektronischer Systeme; Anforderungen an sicherheitsbezogene elektrische / elektronische / programmierbare elektronische Systeme (IEC 65A/523/CDV:2008). German Version. Beuth Verlag, Berlin-Vienna-Zurich (2009)
[10] Rupp, C., Queins, S., Zengler, B.: UML 2 glasklar. Praxiswissen für die UML-Modellierung und Zertifizierung. Carl Hanser Verlag, Munich-Vienna (2005)
[11] Maag, B.: Functional Safety of Software Determined Systems Where is the red line? Some Snapshots (2007)
[12] aquintos GmbH. E/E-Architekturwerkzeug PREEvision (2009), http://www.aquintos.com
[13] Matheis, J., Gebauer, D., Reichmann, C., Müller-Glaser, K.D.: Ganzheitliche abstraktionsebenenübergreifende Beschreibung konsistenter Elektrik/Elektronik-Architekturen. In: Systems Engineering Infrastructure Conference Seisconf. (2008)
[14] Gebauer, D., Matheis, J., Reichmann, C., Müller-Glaser, K.D.: Ebenenübertreifende, variantengerechte Beschreibung von Elektrik/Elektronik-Architekturen. In: Diagnose in mechatronischen Fahrzeugsystemen, pp. 142–151, Haus der Technik Fachbuch. Expert-Verlag GmbH (2008)
[15] Bishop, P., Bloomfield, R.: A Methodology for Safety Case Development. Adelard (1999), http://www.adelard.com
[16] Matheis, J.: (TBP 2009). Abstraktionsebenenübergreifende Darstellung von Elektrik/Elektronik-Architekturen in Kraftfahrzeugen zur Ableitung von Sicherheitszielen nach ISO 26262. Dissertation. aquintos (2009)
[17] AUTOSAR development partnership. Technical Overview, Document V2.2.2, R3.1 Rev. 0001 (2008), http://www.autosar.org
[18] EAST ADL 2.0 Specification. ATESST (Advancing Traffic Efficiency and Safety though Software Technology) (2008), http://www.atesst.org