Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

A structured and systematic model-based development method for automotive systems, considering the OEM/supplier interface

Kristian Beckers[a], Isabelle Côté[b,*], Thomas Frese[c], Denis Hatebur[b,d], Maritta Heisel[d]

[a] Technische Universität München, Germany
[b] Institut für technische Systeme GmbH, Germany
[c] Ford Werke GmbH, Germany
[d] paluno – The Ruhr Institute for Software Technology, University Duisburg-Essen, Germany

ARTICLE INFO

Keywords:
ISO 26262
Automotive
Hazard analysis
Risk assessment
Safety goal
Safety
Functional
Technical
Requirement
UML
Validation and verification

ABSTRACT

The released ISO 26262 standard for automotive systems requires to create a hazard analysis and risk assessment and to create safety goals, to break down these safety goals into functional safety requirements in the functional safety concept, to specify technical safety requirements in the safety requirements specification, and to perform several validation and verification activities. Experience shows that the definition of technical safety requirements and the planning and execution of validation and verification activities has to be done jointly by OEMs and suppliers. In this paper, we present a structured and model-based safety development approach for automotive systems. The different steps are based on Jackson's requirement engineering. The elements are represented by UML notation extended with stereotypes. The UML model enables a rigorous validation of several constraints. We make use of the results of previously published work to be able to focus on the OEM/supplier interface. We illustrate our method using a three-wheeled-tilting control system (3WTC) as running example and case study.

1. Introduction

Developing and constructing road vehicles has become a complex task due to the increase of features, such as adaptive cruise control or lane keeping assist functions. The safety aspects of these features have to be taken into account during the product development. Another fact is that most of these complex systems are developed by different organizations. This means that the overall system is broken down into several components and/or subsystems. Different divisions within the OEM are responsible for the components/subsystems, which are provided by different suppliers.

This raises the complexity for the manufacturer (OEM), who has to organize the necessary activities. With the release of ISO 26262 – Road vehiclesFunctional safety in November 2011 [1], the automotive sector benefited from a consistent functional safety process for developing and constructing electric/electronic (E/E) systems. ISO 26262 addresses all levels of development, including definition of functions/features, systems engineering as well as details of software and hardware development. The standard should be applicable to different scenarios for establishing this process, including, e.g., the OEM and any number of suppliers for the distributed systems.

Since ISO 26262 is a risk-based functional safety standard addressing malfunctions, its process starts with a hazard analysis to determine the necessary risk reduction to achieve an acceptable level ofrisk. The hazard analysis results in safety goals with an automotive safety integrity level (ASIL) that describes the necessary risk reduction. Performing such a hazard analysis is a challenging task because

- It should be comprehensible for different stakeholders, e.g., engineers, project leaders, managers.
- It should be possible to review the hazard analysis within a realistic time period.
- Hazard analyses of different projects should be comparable.
- In a hazard analysis, all relevant faults or situations need to be considered.

This hazard analysis is usually performed by the OEM division responsible for the development of the overall system.

According to ISO 26262, the next steps are to break down the safety

* Corresponding author.
E-mail addresses: beckersk@in.tum.de (K. Beckers), i.cote@itesys.de (I. Côté), tfrese@ford.com (T. Frese), d.hatebur@itesys.de (D. Hatebur), maritta.heisel@uni-due.de (M. Heisel).

http://dx.doi.org/10.1016/j.ress.2016.08.018

Available online xxxx

goals derived in the hazard analysis into functional safety requirements. It has to be justified that the derived functional safety requirements are suitable to achieve the stated safety goals. These functional safety requirements are then detailed and the technical safety requirements are derived. In addition, the verification and validation (V & V) is performed. The results of the V & V activities is fed back and collected in an appropriate way to support the creation of the safety case.

Most of these complex systems are distributed. This distribution includes several challenges: For the requirement 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 system creates the logical architecture and then distributes requirements to different divisions within the OEM responsible for the components. These divisions receive all requirements from systems in which their component is involved in, integrate the requirements and cascade the requirements to the component suppliers. They do the implementation and supply pieces of hardware and software that later have to be integrated into the vehicle. Some of the requirements engineering (RE) have to be done by the OEM and the supplementary RE has to be added by the suppliers.

For the verification and validation (V & V), the OEM division responsible for the overall system 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 component level by the divisions responsible for the components (e.g., the behavior of the component) and other aspects can only be validated using internal interfaces of the component by the suppliers. When the V & V is performed, the results of the V & V activities at supplier side and within the different OEM divisions needs to be fed back and collected by the division responsible for the overall system.

In addition, heterogeneous and concurrent engineering processes, methods and tools exist within the affected parties which need to be harmonized. Communication between OEM and divisions/suppliers has to be organized via requirements as well as verification and validation documents.

In this paper, we propose a structured method based on UML models supported by a tool for the hazard analysis, the requirement engineering, and the V & V activities.

The advantage of a UML model-based approach is that the different artifacts are explicitly connected instead of having loosely coupled documents. On this overall model, consistency checks can be performed. These consistency checks can be specified with the Object Constraint Language (OCL) from the Object Management Group (OMG) [2].

Our paper is organized as follows: In Section 2, we introduce some background knowledge as well as previous work to establish a common understanding. Section 2.1 briefly introduces the underlying standard used throughout our method followed by a short description of the requirements analysis method in Section 2.2. The framework, in which the method is embedded, is outlined in Section 2.3 and the model is introduced in Section 2.4.

Section 3 introduces the case study we use to illustrate our method. Section 3.2 describes the hazard analysis and risk assessment artifacts [1]. In Section 3.3, the artifacts created in the functional safety concept are given [2].

In Section 4, the technical safety requirement specification method illustrated with the example is presented.

Section 6 introduces the applied support tool and Section 7 discusses related work. Finally, in Section 8, we provide a conclusion and an outlook on future work.

Remark: The parts of the method that have already been published will only be briefly discussed. The interested reader can find more details in the provided citations.

2. Background

2.1. ISO 26262

In 2011, the functional safety standard, ISO 26262 [3], was published. It is derived from the generic functional safety standard IEC 61508 [4] and aligns with the automotive safety life-cycle including specification, design, implementation, integration, verification, validation, configuration, production, operation, service, decommissioning, and safety management. ISO 26262 provides an automotive-specific risk-based approach for determining risk classes that describe the necessary risk reduction for achieving an acceptable residual risk, called *automotive safety integrity level (ASIL)*. The possible ASILs are *QM*, *ASIL A*, *ASIL B*, *ASIL C*, and *ASIL D*. The ASIL requiring the highest risk reduction is called ASIL D. In case of a QM rating, the normal quality measures (e.g., ISO/TS 16949 [5]) applied in the automotive industry are sufficient. The standard also addresses the OEM–supplier interface to some extent. ISO 26262 Part 8 requires an appropriate definition (e.g., by using a development interface agreement) of the interface between OEM and supplier, but as the application of the standard should be possible in different project scenarios, the standard does not provide a predefined and dedicated method to split technical responsibilities amongst the different participating parties.

2.2. Requirements analysis

Our requirements engineering method is inspired by and based on the approach proposed by Jackson [6]. In this approach, requirements can only be guaranteed for a certain context. Therefore, it is important to describe the *environment* in which the system to be built (called *item* in the automotive domain) will operate. This is achieved by a *context diagram*. Fig. 1) shows an example of such a diagram. The context diagram consists of boxes representing different elements, also called *domains* (e.g., SteeringWheel in Fig. 1[1]), in the application environment that already exist.

A special domain is the system to be built, i.e., the item. The different domains are connected by interfaces consisting of shared phenomena. Shared phenomena may be events, operation calls, messages, and the like. They are observable by at least two domains, but controlled by only one domain. The phenomenon *steering_angle* is an example for such a shared phenomenon. It is observable by the domains 3WTC (3-Wheeler-Tilt-Control system) and *SteeringWheel* (SW). However, only SteeringWheel controls that phenomenon. This is indicated by the exclamation mark after the abbreviated name of the domain (see 'SW!{steering_angle}' in Fig. 1).

2.3. Functional safety framework

The Ford Integrated process for Functional Safety (FIFS) consists of templates, examples and guidelines in Microsoft Word and Microsoft Excel. These templates, examples and guidelines were developed and improved (using project feedback) since 2009. They were applied in more than 30 projects and cover all parts of ISO 26262 being relevant for an OEM who does not develop software and hardware. Currently, the first pilot projects are aiming to use a model-based approach for functional safety. If the templates are applied according to the guidelines, ISO 26262 compliant (work) products are developed. The method is based on practical experience in the automotive domain.

Within the V-model applied in ISO 26262, the first step of requirements engineering is to perform a hazard analysis and risk assessment for the system under consideration. Output of this step is

[1] As a simplification, we assume that the domain SteeringWheel consists of the actual physical steering wheel as well as a steering wheel provider module.