Deriving Safety Requirements according to ISO 26262 for complex systems: A method applied in the automotive industry

Thomas Frese, Ford-Werke GmbH, Henry-Ford-Straße 1, 50735 Köln, tfrese@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-de.de;
Isabelle Côté, ITESYS Inst. f. tech. Sys. GmbH, Emil-Figge-Str. 78, 44227 Dortmund, i.cote@itesys.de,
Hans-Jörg Aryus, SystemA Engineering Gesellschaft für Systemanalyse mbH, Bürglen 11, 88090 Immenstaad am Bodensee, hans-joerg.aryus@systema-gmbh.de;
Maritta Heisel, Universität Duisburg-Essen, Fakultät für Ing.-wissenschaften, Abteilung INKO, Fachgebiet Software Engineering, 47048 Duisburg, *maritta.heisel@uni-due.de*
Keywords: Functional Safety, ISO 26262, System Development, OEM - Supplier interface, Safety Analysis

Abstract

This paper shows how the Functional Safety standard ISO 26262 can be applied to identify and classify potential hazardous events and to derive a safety concept and the associated Safety Requirements related to the prevention or mitigation of these hazardous events. Especially, it addresses the problem how the right level of detail can be found for the Safety Requirements, how Safety Goals can be defined such that the development of the system is supported, and how assumptions can be handled. A procedure for deriving Safety Requirements is presented which supports system development and ensures that no relevant requirement (or attribute) is omitted. This procedure includes requirements allocation, the Safety Analysis and the description of an appropriate OEM - Supplier interface.

1. Introduction

The purpose of ISO 26262 [1] is to identify and classify the potential hazardous events of vehicle systems and to derive a safety concept and the associated Safety Requirements related to the prevention or mitigation of these hazardous events.

For complex and distributed systems, the derivation of Safety Requirements includes several challenges, for example:

- Justify Safety Concepts
- Don't forget relevant requirements or attributes
- Cascade hardware (HW) metric requirements[1] to components
- Support Original Equipment Manufacturer (OEM) - Supplier interfaces

This paper shows how these challenges can be addressed by providing proposals for the realization of some key work products required by ISO 26262. It focusses on the derivation of Technical Safety Requirements and the HW metrics.

2. Item Definition

The purpose of the Item Definition is to define and describe the item, i.e., the functionality in the vehicle, and to develop an adequate understanding of it with the goal that each activity defined in the safety lifecycle can be performed as a basis for the Hazard Analysis and Risk Assessment. Details are described in [2].

3. Hazard Analysis and Risk Assessment

The Hazard Analysis and Risk Assessment is a "thought experiment" based upon the assumption that a fault has occurred in the item. The outcome is a list of possible hazardous events, including an assigned Automotive Safety Integrity Level (ASIL), reflecting the criticality of the hazardous event. The detailed procedure to systematically identify malfunctions using the Hazard and Operability Study (HAZOP) [3] guide words and starting at the actuators is described in [2]. This paper also describes an appropriate way of identifying relevant operational situations, the handling of assumptions, the classification of the hazardous events and rules for the definition of Safety Goals.

---

[1] Hardware metrics are used to compare the hardware design of different systems. The hardware metrics have been derived from well-known architectures that were successfully used in vehicles (e.g. ABS).

4. Functional Safety Concept

To comply with the Safety Goals of the Hazard Analysis and Risk Assessment, the Functional Safety Concept specifies basic safety mechanisms and safety measures in form of Functional Safety Requirements. The Functional Safety Requirements are allocated to elements in the system architecture. The procedure, types of Functional Safety Requirements and necessary attributes, and the Goal Structuring Notation [4], [5] to provide good argumentation for Safety Goal achievement using patterns are described in detail in [6].

5. Safety Requirements Specification

In the Safety Requirements Specification, the Functional Safety Requirements are broken down to Technical Safety Requirements that are allocated to a single component or 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 Safety Requirements Specification, 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 components and subsystems, internal interfaces, and a description of the system layer architecture including the redundancy concepts on system level. This input is necessary to ensure the consistency of the System Design to the Technical Safety Requirements.
- Technical Safety Requirements including the attributes Fault Tolerant Time, Emergency Operation, and Verification & Validation. Categories for Technical Safety Requirements are e.g. “Safety Related Function”, “Internal Fault Handling”, and “Metric”. Completeness is ensured by using tables with predefined cells for the Safety Requirements, their categories and attributes.
- Additionally, in the Safety Requirements Specification, ASIL decomposition may be performed and safety-related parameters are defined. ASIL decomposition is a design measure. It can be applied during the design of the system, hardware or software architecture. The goal is to assign

adequate ASILs to similar or redundant safety requirements, which have been allocated to independent elements in the respective architecture. This is done to potentially lower the ASIL for the decomposed safety requirements. However, ASIL decomposition can only be applied if sufficient independency between the elements can be demonstrated. If this is not possible, the initial ASIL has to be assigned to each requirement and element.

- The derived Technical Safety Requirements are cascaded to the component/ subsystem suppliers.

The Technical Safety Requirements as defined by ISO 26262 cover the system level (including requirements on the subsystems/components) which is usually defined by the OEM, but also component/subsystem-internal requirements. In many cases, the OEM buys these components or subsystems from suppliers.

ISO defines two kinds of HW metrics. The Probabilistic Metric for random Hardware Failures (PMHF) describes the maximum probability of Safety Goal violation due to random Hardware Failures per hour. For faults that directly lead to the violation of the Safety Goal (SPF), a percentage of faults to be detected and handled by the system is defined by the “Single Point Fault Metric” (SPF metric). For faults that, in combination with other independent faults, lead to the violation of the Safety Goal (Latent Faults), a percentage of faults to be detected and handled by the system is defined by the “Latent Fault Metric” (LFM).

To support a clear OEM-supplier interface, the following tailoring is helpful in many cases:

- Within the Technical Safety Requirements, component/subsystem internal aspects, such as:
  - measures related to the detection and indication of faults within the component,
  - details on internal fault reaction,
  - avoidance of latent faults,
  - multiple point fault detection interval[2], and

[2] A single fault does not directly violate a safety goal. If the first fault occurs, it may not be directly visible. Then a second fault occurs which violates the safety goal while the first fault is still present. If it is necessary to detect these faults within a certain time, we talk about the “multiple point fault detection interval“.

- a description of the architecture / redundancy concept of the component including a description of measures for handling potential dependent failures.

Usually, these aspects are not described in detail by the OEM, because they depend on the supplier-specific implementation within the component/subsystems.

- For the breakdown of the HW Metrics, the following should be considered:
  - The PMHF has to be achieved by the overall system, including contributions from all components needed to fulfil the Safety Goal.
  - If redundancy concepts are applied and the fault detection is not limited to a single component, target values for SPF and the LFM have to be derived for each component. This calculation is based on the target values of the Safety Goal as given by ISO 26262. Otherwise, SPF and LFM of the Safety Goal can be directly cascaded to all components that realize requirements derived from that Safety Goal.

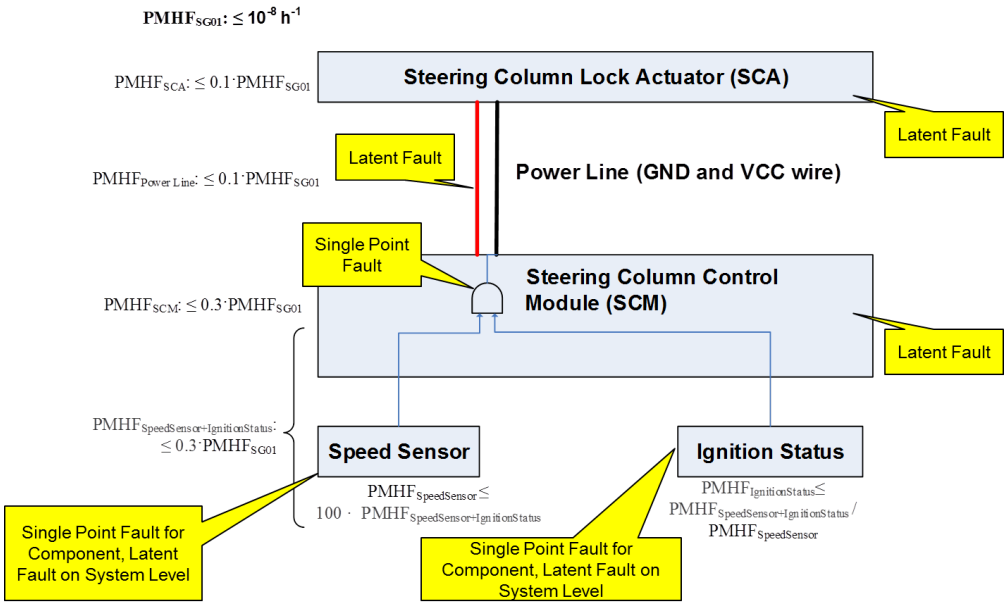

Figure 1 – System Block Diagram and PMHF Requirements

We consider a fictitious example that is based on an electronic steering column lock function, and show the contribution of the involved components (see Figure 1) to the Safety Goal “Avoid unintended locking”.

The Power Line represents a redundancy concept; it consists of two independent wires.

For the Steering Column Control Module (SCM) and the inputs, ASIL Decomposition is applied; both inputs have to fail to violate the Safety Goal.

5.1 Derivation of PMHF target values for components

The standard ISO 26262 provides target values for the PMHF on Safety Goal level, i.e. for the whole system. This target value has to be split into fractions to be fulfilled by the contributing components.

We propose to define initial values depending on the complexity of the components. For example, the contribution of the Power Line shall be equal to or less than 0.1 of the overall PMHF. For the Speed Sensor and Ignition Status, the contributions are multiplied (due to the “AND” logic in the SCM) and can be distributed as shown in Figure 1.

5.2 Derivation of SPF and LFM target values for components

SCA, Power Line and SCM do not contribute as source of Single Point Faults due to the redundancy, but as Latent Faults. Only the “AND” logic in the SCM is a source for Single Point Faults. Single Point Faults of the Speed Sensor and Ignition Status components contribute to Latent Faults in the overall system.

Safety Goal	ASIL	Safety Goal SPF	Component/ Subsystems	Component Fault Detection Coverage	T-S-Req.-IDs Category: Metric	T-S-Req.-IDs Category: Internal Fault Detection
SG01	ASIL D	99%	Speed Sensor	n/a - No Single Point Faults, see Rationale	n/a	n/a
			Ignition Status	n/a - No Single Point Faults, see Rationale	n/a	n/a
			SCM	SPF >= 99%	ESCL-T-S-Req05241	ESCL-T-S-Req12210
			Power Line	n/a - short to VCC and GND	n/a	n/a
			SCA	n/a - short to VCC and GND	n/a	n/a

Table 1: Derivation of Single Point Fault Requirements

Table 1 shows the component contributions to the SPF. The SPF requirement on Safety Goal level is only assigned to the SCM. The metric requirement, consisting of hardware metric requirement, SPF metric as well as LFM, and corresponding fault handling requirement are referenced in aforementioned table.

Safety Goal	ASIL	Safety Goal LFM	Component/ Subsystems	Component Fault Detection Coverage	T-S-Req.-IDs Category: Metric	T-S-Req.-IDs Category: Latent Fault Detection
SG01	ASIL D	90%	Speed Sensor	>= 90% (derived from System Level LFM)	ESCL-T-S-Req01041	**ESCL-T-S-Req01010**
			Ignition Status	>= 90% (derived from System Level LFM)	n/a (All Power Button Faults are perceived by the driver)	**n/a**
			SCM	LFM >= 90%	ESCL-T-S-Req05242	**ESCL-T-S-Req01210 ESCL-T-S-Req05231**
			Power Line	LFM >=90% (Fault Detection by KVM)	Covered by detailed Fault Detection requirements	**ESCL-T-S-Req05230**
			SCA	LFM >=90% (Faults are detected by KVM or perceived by the driver)	Covered by detailed Fault Detection requirements	**ESCL-T-S-Req05230**

Table 2: Derivation of Latent Fault Requirements

Table 2 shows the component contributions to LFM. The LFM requirement on Safety Goal level is assigned to all components. The metric requirement and corresponding fault handling requirement are referenced in this table. The Ignition Status does not get dedicated requirements, because all faults can be perceived by the driver.

6. Safety Analysis

Safety analyses are carried out to examine the influences of faults and failures on items regarding their architecture, functions and behaviour.

The safety analysis shall address the system including the safety/redundancy concept, measures for fault prevention, detection and mitigation in order to verify that the Safety Goals and Safety Requirements are fulfilled. For that reason, the existing functional / system specifications and the existing Safety Requirements specification build the input for the safety analysis.

The analysis guides the development and specification of additional safety measures wherever the analysis reveals elements with insufficient safety coverage. Therefore,

the analysis can be used as a tool for requirements engineering and provides essential input for specification updates as well as test specification improvements.
Safety analyses can also contribute to the identification of new functional or non-functional hazards not previously identified during the hazard analysis and risk assessment.
The safety analyses document includes analyses for the various development phases:

- Analysis of the Functional Safety Concept
- Analysis of Safety Requirements Specification and System Design
  This includes the final verification, metric target values and reached metric values and does not include the derivation of component target values (done in the Safety Requirements Specification)
- Analysis of components/subsystems

It is required to document which methods for quantitative (e.g. Failure Modes and Effects Analysis (FMEA), Fault Tree Analysis (FTA), HAZOP) and qualitative (e.g. quantitative and qualitative FMEA, FTA, Markov Models) Safety Analysis are applied and which tools are used.
It has to be checked that the Safety Analysis is complete, i.e. an analysis for each Safety Goal is performed, the interaction with other items or elements is considered, the fault/failure handling, and all fault/failure causes and consequences including dependent failures are considered. Additionally, it has to be checked that the analysis is represented in accordance with appropriate Standards or Guidelines and the Safety Analysis is traceable to Safety Requirements.
At least for ASIL C and ASIL D, Safety Goals are checked (according to ISO 26262) to decide whether a deductive analysis performed on the system level, a quantitative analysis for verifying target values, and an analysis of mechanisms avoiding single point faults and latent faults has to be performed.
The Safety Analysis has to provide evidence that possible dependent failures are covered appropriately.
For each component, target values for PMHF, SPF metric and LFM are derived in the Safety Requirements Specification from the respective Safety Goal target value. It is checked if all components achieve their target values by comparing the supplier value and the target value.

Additionally, the PMHF values are verified by a quantitative system level fault tree containing the supplier values. SPF and LFM are verified by a System Level Failure Modes, Effects and Diagnostic Coverage Analysis FMEDA [7].

7. Safety V&V Report

The Safety V&V Report includes detailed verification and validation planning and status tracking:

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

The detailed procedure is described in [8].

8. Conclusion and Future Work

With our approach, we achieve the following goals:

- The categories in the Functional Safety Concept and the Safety Requirements Specification and the tables including predefined cells for all required attributes reduce the risk of forgetting relevant requirements.
- By the break-down of metric requirements and the proceeding related to the content to be specified by the OEM and by the supplier(s) and the overall check within the V&V activities, a clear OEM-supplier interface is provided which allows efficient distributed development.
- The achieved metric values are crosschecked by an appropriate safety analysis to confirm the Safety Goal target values.

Currently, the Functional Safety process is supported by template documents, guidelines and example documents. For the future, a full implementation in a development tool chain is planned.

Bibliography

[1] ISO, *ISO26262:2011 Road vehicles - Functional safety,* International Organization for Standardization, 2011.

[2] K. Beckers, T. Frese, D. Hatebur und M. Heisel, „A Structured and Model-Based Hazard Analyss and Risk Assessment Method for Automotive Systems," *24th IEEE Int. Symposium on Software Reliability Engineering,* pp. 238-247, 2013.

[3] IEC, *BS IEC 61882:2001 Hazard and operability studies (HAZOP studies) - Application guide,* BS IEC, 2001.

[4] T. P. Kelly, „A Systematic Approach to Safety Case Management," *SAE 2004 World Congress,* March 2004.

[5] T. P. Kelly und R. A. Weaver, „The Goal Structuring Notation - A Safety Argument Notation," *Proceedings of the Dependable Systems and Networks, Workshop on Assurance Cases,* 2004.

[6] K. Beckers, I. Côté, T. Frese, D. Hatebur und M. Heisel, „Systematic Derivation of Functional Safety Requirements for Automotive Systems," *Proceedings of SAFECOMP,* pp. 65-80, 2014.

[7] W. M. Goble, The Use and Development of Quantitative Reliability and Safety analysis in New Product Design, Eindhoven, 1998.

[8] K. Beckers, I. Côté, T. Frese, D. Hatebur und M. Heisel, „A Structured Validation and Verification Method for Automotive Systems considering the OEM/Supplier Interface," *Proceedings of SAFECOMP,* pp. 90-107, 2015.