Deriving safety requirements according to ISO 26262 for complex systems: How to avoid getting lost?

Thomas Frese, Ford-Werke GmbH, Köln;
Denis Hatebur, ITESYS GmbH, Dortmund;
Hans-Jörg Aryus, SystemA GmbH, Immenstaad

Abstract

This paper shows, how the new Functional Safety standard ISO 26262 can be applied to identify and classify potential hazards and to derive a safety concept and the associated safety requirements related to the prevention or mitigation of these hazards. Especially, it includes proposals 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 derivation of Safety Requirements is presented which supports the system development and ensures that no relevant requirement (or attribute) is omitted. This procedure includes the requirements allocation and the description of an appropriate OEM - Supplier interface.

1. Introduction

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

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

- Find right level of detail in Hazard Analysis (to enable an efficient review)
- Define Safety Goals such that they drive the implementation (to support the development of the System)
- Document Assumptions (to have a clear item scope)
- Justify Safety Concepts (to support the safety case)
- Don’t forget relevant requirements or attributes (to ensure completeness)
- Support OEM - Supplier interface (to avoid inconsistencies)

This paper shows how these challenges can be addressed by providing proposals for the realization of some key work products required by ISO 26262.

In section 2, the purpose and content of the ISO 26262 work product “Item Definition” is described. Section 3 describes the realization of the Preliminary Hazard Analysis. Section 4 includes a proposal how the Functional Safety Concept work product could address the justification of the Safety Concept and the completeness of the requirements. Section 5 addresses the derivation of Technical Safety Requirements, and section 6 shows how the requirements on all levels can be validated or verified. Section 7 provides a conclusion and gives directions for future work.

2. 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 Preliminary Hazard Analysis 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.

The item definition shall contain:

- the purpose of the item,
- functional and non-functional requirements,
- operating scenarios of the item if they impact the functionality of the item,
- the physical and functional boundary of the item,
- the ways the driver, co-driver and other persons interact with the system, and
- already known/given architectural constraints.

3. Preliminary Hazard Analysis

3.1 Preparation of Hazard Analysis

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

To support a systematic approach to identify malfunctions, it has been proven to be helpful that a set of guide words for failure mode consideration is prepared before performing the Hazard Analysis & Risk Assessment. The guide words help the developer to consider all relevant failures. Typical guide words are “no”, “unintended”, “early”, “late”, “more”, “less”, “Inverted” and “intermittent”. For each guide word, the meaning of the guide word should be

described in context of the main functions of the system to be considered. For example, for an Electrical Steering Column Lock function, "unintended" means that the system locks in situations where steering is necessary.
It is important to ensure that this step is done on the right level of detail. It shall be avoided to have a too detailed level with too many functions / sub-functions to make the Hazard Analysis assessable.
Usually, it is helpful to start the failure mode consideration from the actuators point of view and not from the sensors, since the task of the failure mode consideration is not a verification of an existing design – this will be done with appropriate safety analyses (FMEA, FTA…) in later steps of the Functional Safety process.

3.2 Procedure: Situation Analysis and Hazard Identification

For all combinations of function and fault determined in the previous step, it should be described how the system behaves in presence of the malfunction. For example, for the previously described fault, the effect on system level is that Electrical Steering Column Lock locks the steering column.

For each Failure Mode, all operational situations, system/operating modes, use cases and environmental conditions (solemnly or in combination) that could lead to a potential Hazard shall be

- identified (supported by a Situation Database), and
- referenced in the Hazard Analysis.

The situation database encloses operational situations, operating modes and environmental conditions. It is updated if new aspects are identified in projects in order to reduce the risk of forgetting hazardous situations.

The effect on vehicle level which could occur in case of a potential item's malfunction should be described. For example, the effect on vehicle level for the previously described fault is that steering is locked and the vehicle not steerable. Based on the effect on vehicle level, the hazards and possible consequences are described. Hazards shall be defined in terms of the conditions or events that can be observed at the vehicle level. A verbal description of consequence without ranking shall be given.

Assumptions (e.g., on driver actions to ensure controllability) shall be also described. These assumptions strengthen the scope of the Hazard Analysis. Requirements are derived and

these requirements are verified by appropriate methods in later steps (see section 6). A unique risk ID helps to refer to a certain hazard.

3.3 Procedure: 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 need to be performed:

1. Estimation of the potential severity (including rationale)
2. Estimation of the probability of exposure (including rationale)
3. Estimation of the controllability (including rationale)

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

3.4 Procedure: 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 following rules help to ensure that the derived safety goals support the system development:

- The safety goals shall be clear and precise.
- The safety goals shall not contain technical details.
- The safety goals shall be such that they can be implemented by technical means (e.g. avoid referring to non-measurable data).
- Each safety goal shall have a unique identifier.
- At least one safety goal shall be assigned to each hazard rated as ASIL A, B, C or D.
- One safety goal can be assigned to several hazards.
- A hazard could have more than one safety goal.
- If a safety goal can be achieved by transitioning to or by maintaining one or more safe states, then the corresponding safe state(s) shall be specified.

4. Functional Safety Concept

To comply with the safety goals of the Preliminary Hazard Analysis, the Functional Safety Concept specifies the basic safety mechanisms and safety measures in the form of Functional Safety Requirements. The Functional Safety Requirements are allocated to elements in the system architecture.

The consideration of following aspects is helpful for the creation of the Functional Safety Concept:

- For each Safety Goal, at least one Functional Safety Requirement is derived.
- Additionally, assumptions from the Preliminary Hazard Analysis are transformed into Functional Safety Requirements to ensure that they are handled in the Validation and Verification processes.
- The Functional Safety Requirements are structured with the categories “General Requirements”, “Safety Related Functions”, “Reduced Functionality”, “User information”, “Maintain Safe State / Recovery” and “Decomposition Requirements” and corresponding attributes (e.g, Operating modes, ASIL, Safe State). Template tables and Checklists ensure that all relevant attributes are defined. The categories and attributes help the engineers in generating an appropriate description of the requirements.
- The usage of parameters in the Functional Safety Requirements supports the developer to decide on some aspects later in the development life cycle. It also avoids redundancies in the requirements description.
- The ASIL decomposition is an ISO 26262 means to reduce the Safety Integrity Level of for single requirements if redundancy concepts are applied. Such decomposition usually leads to additional requirements.
- The Functional Safety Requirements are allocated to elements of a preliminary architecture. In general, the Functional Safety Requirements are allocated to logical blocks, not to technical/physical components. Usually, several alternatives exist to allocate the Functional Safety Requirements, resulting in different technical implementations.
- A Safety Analysis shall be performed to show compliance and consistency between the Functional Safety Concept and the Preliminary Hazard Analysis.

Attribute	General Requirements	Safety Related Functions	Reduced Functionality	User information)	Maintain Safe State / Recovery	ASIL Decompo-sition
Safety Req-ID	X	X	X	X	X	X
Safety Goal Reference	X	X	X	X	X	X
Operating modes	X	X	X	X	X	X
ASIL Classification	(X)	X	X	(X)	(X)	(X)
Safe State	(X)	X	X	(X)	X	(X)
Functional Safety Requirement	X	X	X	X	X	X
Purpose	X	X	X	X	X	X
Fault tolerant interval	(X)	X	(X)	(X)	-	(X)
Reduced Functionality interval	(X)	(X)	-	-	-	-
Functional redundancies (e.g. fault tolerance)	(X)	(X)	-	-	-	-
Description of actions of the driver or other endangered persons	-	(X)	(X)	X	-	-
Validation Criteria for these actions	-	(X)	(X)	(X)	-	-
V&V method	X	X	X	X	X	X
V&V acceptance criteria	X	X	X	X	X	X

Legend:
X required
(X) if applicable (for details see in next sections)
- not required

Figure 1 – Requirement categories and their attributes

The derivation of Functional Safety Requirements includes an argumentation for Safety Goal achievement using the Goal Structuring Notation (GSN), an overview of Safe State 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.

The Goal Structuring Notation (GSN) [2] - a graphical argumentation notation - explicitly represents the individual elements of the safety argument (goal, strategy, assumption, justification, context, and requirements) and (perhaps more significantly) the relationships that exist between these elements (i.e. how individual requirements are supported by specific strategies, and the assumed context that is defined for the argument).

When the elements of the GSN are linked together in a network they are described as a ‘goal structure’. The principal purpose of any goal structure is to show how goals (Safety Goals) are successively broken down into sub-goals (Functional Safety Requirements).
As part of this ‘goal structure’, it is also possible to make clear the argument strategies adopted, the rationale for the approach and the context in which goals are stated (e.g. the system cope or the assumed operational role).

To support the derivation of Safety Requirements, proposals for common used strategies are provided.

An example for such a strategy is:

- If a Safety Goal refers to some information,
  → the strategy may be, to use independent sources for this information

This strategy is described in Figure 2. For the Safety Goal (SG XX) in a given context describing the vehicle state, the strategy “Use independent sources indicating that …” is used. For such a strategy the justification shall be provided why the selected information providers are sufficient. This strategy is then split into 2 sub-strategies and also these sub-strategies are justified.

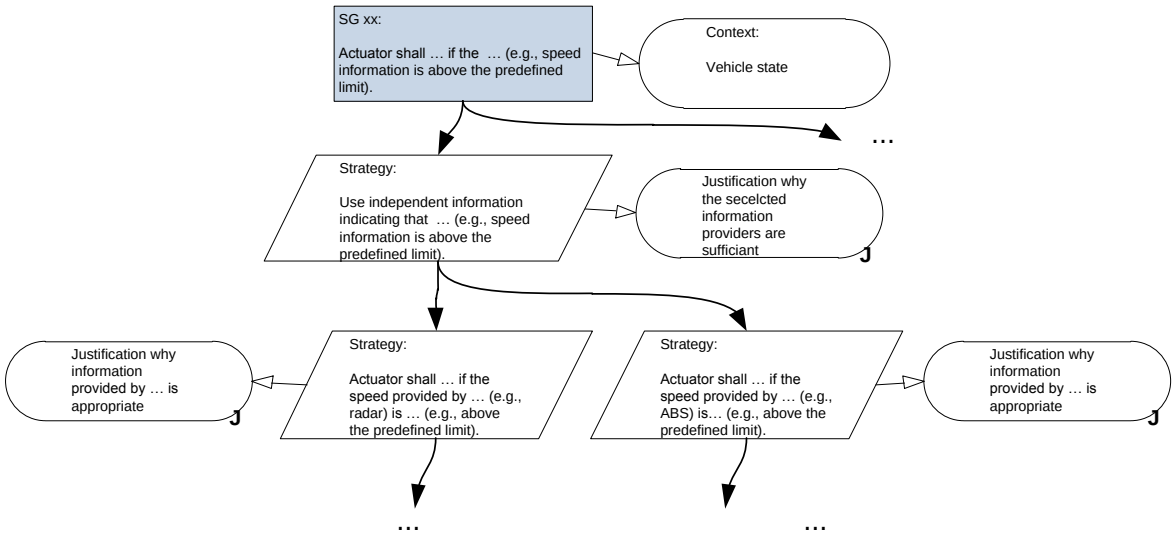

Figure 2 - Independent Sources

Further strategies are for example:

- Safety goal or strategy constrains actuator behaviour → strategy may be, to avoid faulty actuator behaviour by electrical faults or mechanical effects
- Safety goal or strategy constrains actuator behaviour → strategy may be, to detect electrical faults and perform an appropriate action in this case
- Safety goal or strategy describes the transition to a safe state → strategy may be, to inform driver and preserve this safe state until a set of conditions is satisfied or specific actions are performed

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, constrains, 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 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” and relate to the categories in the Functional Safety Concept.

  The completeness is ensured by using tables with predefined cells for the safety requirements, their categories and the attributes.
- The HW Metrics as required by ISO 26262 part 5 are derived and the breakdown to components/ subsystems is justified. This breakdown of metric requirements enables a distributed development and is necessary to have a clear OEM –

supplier interface. The Maximum Probability of Safety Goal violation due to random Hardware Failures (PMHF) has to be achieved by all components contributing to the Safety Goal together. If redundancy concepts are applied and the fault detection is not limited to a single component, a target values for Single Point Fault Metric (SPFM) and the Latent Fault Metric (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, the SPFM and the LFM of the Safety Goal can be directly cascaded to all components that realize requirements derived from that Safety Goal.

- Also in the Safety Requirements Specification, ASIL decomposition may be performed and Safety related parameters are defined.
- The derived Technical Safety Requirements are cascaded to the component/ subsystem suppliers.
- A Safety Analysis shall be performed to show compliance and consistency between the Technical Safety Concept, the Functional Safety concept and the preliminary architectural assumptions and verify the system design regarding compliance and completeness with regard to the Technical Safety Requirements.

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.

To support a clear OEM/supplier interface, 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, and
  - a description of the architecture / redundancy concept of the component including a description of measures for handling potential dependent failures

  are usually 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, following should be considered:

- The Maximum Probability of Safety Goal violation due to random Hardware Failures (PMHF) has to be achieved by all components contributing to the Safety Goal together.
- If redundancy concepts are applied and the fault detection is not limited to a single component, a target values for Single Point Fault Metric (SPFM) and the Latent Fault Metric (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, the SPFM and the LFM of the Safety Goal can be directly cascaded to all components that realize requirements derived from that Safety Goal.

6. 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

It is helpful to perform following activities:

For the Safety Goals and the Functional / Technical Safety Requirements:

- Corresponding analysis elements shall be referenced, and the necessary V&V activities shall be planned in the Safety V&V Report. All activities shall be carried out as planned according to the development lifecycle and their results shall be documented to demonstrate that all safety goals are achieved and all Functional / Technical Safety Requirements have been met.

For the Safety Goals:

- The HW metrics shall be calculated on safety goal level. The result and conclusions shall be assessed and validated.

For the Functional Safety Requirements:

- The verification (e.g. test) shall be documented (including activity and acceptance criteria). The correctness and the completeness shall be assessed and validated.

- If Parameters are identified for the Functional Safety Requirement: A validation specification for the parameter values shall be generated (including activity and acceptance criteria). The correctness and the completeness shall be assessed and validated.
- The specified verification and validation (e.g. test) shall be performed and the V&V results shall be documented. The results shall fulfil the acceptance criteria.

For the Technical Safety Requirements:

- A verification specification shall be generated 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 specification are assessed and validated assessed and validated.
- The component/subsystem supplier shall generate following information to complete the Technical Safety Requirement:
  - for requirements of category “internal fault handling”, measures related to the detection and indication of faults within the component, and details on internal fault reaction
  - for requirements of category “latent fault handling”, measures related to the detection and indication of faults within the component, avoidance of latent faults, multiple point fault detection interval, and details on fault reaction
  - for requirements defining a PMHF target (because they exists once for a component with an ASIL ≥ B), a description of the architecture / redundancy concept of the component, and a description of measures for handling potential dependent failures
- The component/subsystem supplier derives the detailed HW and SW requirements from the Technical Safety Requirements (see section 5). The following aspects shall be checked:
  - the implementation process on supplier side is appropriate
  - the HW and SW safety requirements, the HW and SW interface requirements, and the Component Design are correctly derived from the Technical Safety Requirement
  - the Safety Analysis (e.g. FTA) to determine faults leading to the violation of the Technical Safety Requirement is complete (e.g. inputs) and correct (e.g. logic), and
  - the HW/SW Design (including internal and external interfaces) is appropriate and corresponds to Safety Analysis

- The component/subsystem supplier verifies the implementation of the HW and SW requirements in the component. It shall be checked that
  - the test specification to verify the effectiveness and the failure coverage of the safety mechanisms are correct and complete,
  - the stated failure rates (e.g. in FMEDA) are justified,
  - robustness testing is specified in a qualification plan for the HW components and the test results are documented, and
  - the HW metrics calculation (e.g. by FMEDA or FTA) as defined in ISO 26262 Part 5 is correct and complete

For each V&V Activity, responsibilities, references to corresponding documents are and the status and actions are tracked in the Safety V&V Report. The OEM-Supplier interface and the coverage of the ISO 26262 parts are illustrated in Figure 3.

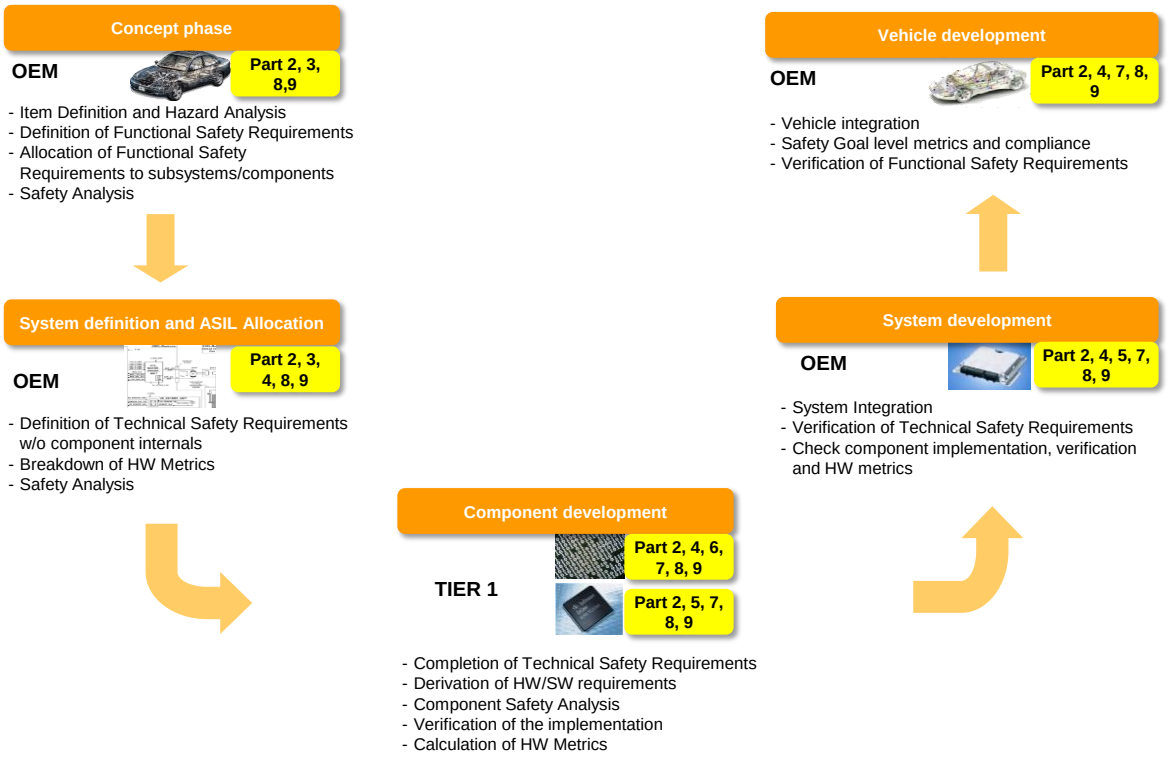

Figure 3 – OEM – Supplier Interface

7. Conclusion and Future Work

With our approach, we achieve the following goals:

- The hazard analysis with the guideword approach and with the selection of function-fault combinations beforehand, as well as the structured approach for deriving functional technical and technical safety requirements helps to find the right level of detail and allows an efficient review.
- The established rules ensure that Safety Goals are defined such that the development of the system is supported.
- Documentation of the assumptions improves re-usability of the analysis and identification of sections which need an update due to changes in scope (other target vehicle, functional changes etc.). Within the process, it is ensured that the assumptions are verified or validated.
- The “Goal Structuring Notation” to derive Functional Safety Requirements is a structured approach to derive, justify and document the Safety Concept. Proposals for strategies help to create the “Goal Structuring Notation” systematically.
- 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.
- 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.

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

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

[2] Dr Tim 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