

Effective Functional Safety Concept Generation in the Context of ISO 26262

Darren Sexton, Antonio Priore, and John Botham
Ricardo UK Ltd.

ABSTRACT

The functional safety concept definition is the backbone of a project's safety process; poor choices made at this stage can have significant impact. A weak concept may result in over-engineering of systems; late re-work when missing safety requirements are eventually uncovered at advanced stages of the development process; disagreements within the supply chains regarding responsibility for safety mechanisms; or, of most concern, release of an unsafe product. Despite this importance, ISO 26262 states that the functional safety requirements are to be derived from the safety goals (top-level safety requirements) and only *notes* that safety analysis *might* be used to support this task, giving no further guidance on how this might be done.

The automotive industry's typical time pressures mean that being able rapidly to produce an initial safety concept is critical if it is to influence the system architecture and procurement decisions. At the same time, a high degree of confidence that the functional safety requirements are effective is necessary. There is therefore a balance between rapidly producing a concept versus assurance that it is complete and sufficient.

This paper discusses the role of safety analysis in rapidly and efficiently, yet systematically, deriving functional safety requirements. It considers practical issues such as selection of appropriate analysis techniques, derivation of requirements from the analysis, establishing traceability between requirements and analysis and building upon the analysis throughout the life-cycle. An industrial case study is provided in order to illustrate the suggested approach. Finally, a number of open considerations are introduced.

CITATION: Sexton, D., Priore, A., and Botham, J., "Effective Functional Safety Concept Generation in the Context of ISO 26262," *SAE Int. J. Passeng. Cars – Electron. Electr. Syst.* 7(1):2014, doi:10.4271/2014-01-0207.

INTRODUCTION

ISO 26262 has been published now for more than two years and many within the automotive industry have moved beyond gaining an initial understanding of the standard to making improvements in practical and efficient use of it, in particular with regard to the early life-cycle activities. In practice, however, we see many organizations adopting ISO 26262 for the first time struggling with how to actually implement these early activities. Practical questions such as the level of detail, style and means of generating the content of these activities are generally not directly addressed within the standard, meaning that different organizations take differing viewpoints. We have seen this particularly in the area of the life-cycle phase called the functional safety concept. As a result, problems such as re-work arise since the functional safety requirements may arrive too late to affect the initial architecture or because of a failure to allocate key requirements across the supply chain sufficiently early.

The remainder of this paper discusses the role of safety analysis in rapidly and efficiently, yet systematically, deriving functional safety requirements for the functional safety concept. The next two sections give an overview of the functional safety concept and how this compares with IEC 61508, hence supporting readers with limited knowledge of ISO 26262. We then describe the guidance that the standard provides in terms of deriving functional safety requirements; this is followed by a description of our approach and this is then set in the context of a particular project. Finally we draw conclusions and outline further challenges.

OVERVIEW OF THE FUNCTIONAL SAFETY CONCEPT IN THE CONTEXT OF ISO 26262

In the context of ISO 26262, the functional safety concept comes after the definition of the safety goals (the final step of the risk assessment process) and before the implementation of safety requirements within the technical safety concept.

therefore acts as a “bridge” between implementation detail and the more abstract safety goals that address the hazardous events; this is shown in Figure 1 (from ISO 26262).

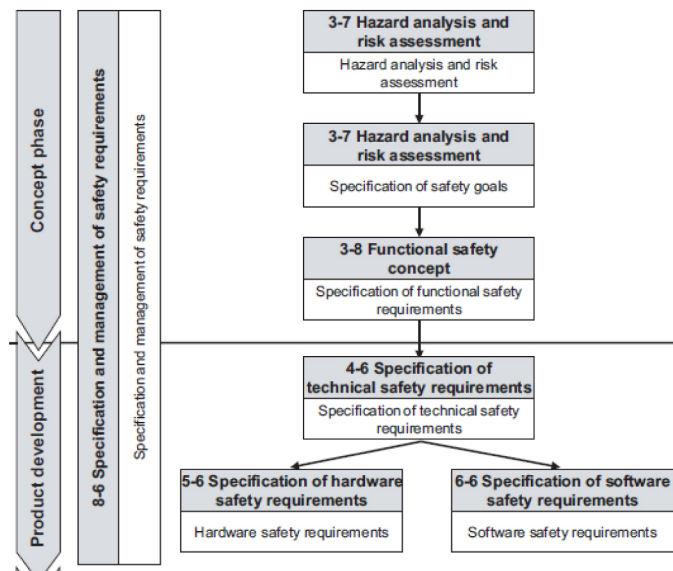


Figure 1. Life-cycle context of the Functional Safety Concept [2]

ISO 26262 defines the functional safety concept as the “[...] specification of the functional safety requirements [...], with associated information, their allocation [...] to architectural elements [...], and their interaction necessary to achieve the safety goals [...]” [1]. From this, it is clear that requirements about the functional safety of the item are a key part of the concept. In addition, information such as the traceability to the safety goals is necessary to establish whether the concept fulfils them. Within the standard there are no requirements mandating the use of safety analysis to *derive* functional safety requirements (as opposed to *verifying* a concept). It is our view that safety analysis should play an important role in the derivation of functional safety requirements rather than just being seen as a means of verification.

The scope of the functional safety concept is intended to be limited to addressing malfunctions of the implemented systems; this is implied by the wording in the scope of the standard - “ISO 26262 addresses possible hazards caused by malfunctioning behavior of E/E safety-related systems, including interaction of these systems. It does not address hazards related to electric shock, fire, smoke, heat, radiation, toxicity, flammability, reactivity, corrosion, release of energy and similar hazards, unless directly caused by malfunctioning behavior of E/E safety-related systems” [4]. Therefore, it is not intended that the functional safety requirements should address other concerns that might also impact safety. In practice, the vehicle owner is not concerned with why they may be put in harm's way, and thus the functional safety concept must be integrated with other means of addressing the safety concerns outside of ISO 26262's scope.

COMPARISON WITH IEC 61508

Before the publication of the ISO 26262, companies in the automotive market sector often used IEC 61508 [6] or in-house standards to address the functional safety aspects of their product development projects. IEC 61508 aims to address a generic product safety lifecycle regardless of the field of application. The advent of the new, domain-specific standard has led many automotive companies to adapt their safety engineering processes to comply with the latest “state of the art”. Although ISO 26262 is derived from IEC 61508, in practice there are a significant number of differences between the two. The functional safety concept stage represents one of the additions of ISO 26262 with respect to IEC 61508 in terms of functional safety life-cycle steps and the approach to safety critical systems. The aim of this section is to provide the basis for a comparison in order to help readers with a background in the use of the IEC 61508 to understand the new requirements of ISO 26262 with respect to the definition of the functional safety concept in the automotive domain.

Our opinion is that the ISO 26262 life-cycle is generally better suited to projects where there is a high degree of innovation and there is a lack of standardized solutions. This is valuable given the automotive industry's continual addition of new features to vehicles. Conversely, however, the functional and technical safety concept phases can appear to be a burden when the solutions are already known or understood.

Safety Functions in the Context of the IEC 61508

A visual context of the relevant parts of the comparison is provided with Figure 2. During stage 4 of the safety lifecycle within the IEC 61508, at least one overall safety requirement must be defined for each hazardous event. This part of the standard matches with the creation of safety goals in the context of ISO 26262 (safety goals are defined at the end of the Hazard Analysis and Risk Assessment stage (HARA), [2]). In fact, safety goals are top level safety requirements for each hazardous situation in the HARA. IEC 61508 makes clear that “The overall safety functions to be performed will not, at this stage, be specified in technology-specific terms since the method and technology of implementation of the overall safety functions will not be known until later” [6]. This fits with the definition of the safety goals where “Safety goals are not expressed in terms of technological solutions, but in terms of functional objectives” [1].

As shown in Figure 2, the next phase according to IEC 61508 is the allocation of the overall safety requirements to the Electrical / Electronic / Programmable Electronic (E/E/PE) systems. IEC 61508 describes this allocation activity as “[...] iterative, and if it is found that the tolerable risk cannot be achieved, then the specifications for the EUC [Equipment Under Control] control system, the designated E/E/PE safety related systems and the other risk reduction measures shall be modified and the allocation repeated” [6]. This approach slightly differs between

the two standards in the sense that, in ISO 26262, the focus is driven towards the generation of a new “layer” of requirements before any allocation to the safety-related systems. This new step is described as the functional safety concept. Functional safety requirements are derived from the safety goals (top level requirements) and they define, in functional terms, the satisfaction of the safety goals by the “concept” of the item. In other words, the safety goals describe “what” the concept must avoid or achieve to mitigate the hazardous situations whilst the functional safety concept defines “how” (from a functional viewpoint) it will be achieved. Both of these phases are still independent from any specific technological implementation (besides a preliminary architecture, if available).

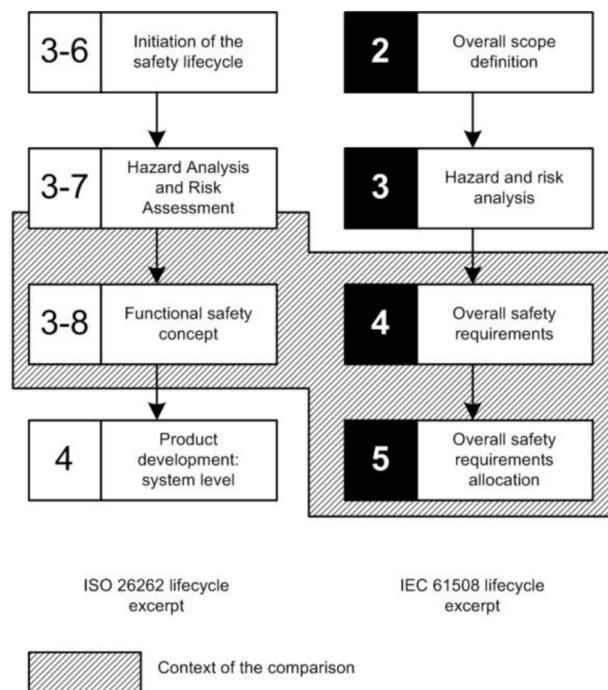


Figure 2. Boundaries of the comparison between the two standards

With respect to the approach to safety analysis proposed in this paper, IEC 61508 suggests the use of unspecified “appropriate techniques” for the combination of probabilities in order to allocate the requirements among the different systems. ISO 26262 encourages, explicitly but vaguely, the use of safety analysis such as FTA, FMEA, both for the derivation and the allocation of the functional safety requirements. Thus, even though neither standard explicitly requires safety analysis for the derivation and allocation of safety requirements, they both hint at the approach. The choice is left to the user implementing the process. In our opinion, this analysis-driven approach is very useful when major design choices are still open and there is a range of different suitable concepts that will need to be analyzed before being detailed in the form of functional requirements.

At the end of stages 4 and 5, IEC 61508 moves to the system design stage where the technological solution is defined and implemented in a similar manner to the technical safety concept from ISO 26262 (system design stages have not been included in the excerpts of the lifecycles within Figure 2).

DERIVING THE FUNCTIONAL SAFETY CONCEPT

Despite the importance of the safety analysis in driving the contents of the functional safety concept, ISO 26262 provides little guidance on how to do this in an efficient and sufficient manner. The primary requirement related to derivation of the functional safety requirements states that they flow principally from the safety goals and safe states - “*The functional safety requirements shall be derived from the safety goals and safe states, taking into account the preliminary architectural assumptions*” [2]. A related requirement gives guidance on what must be specified for each functional safety requirement, such as the fault tolerant time interval. An informative note to this requirement states that “*This activity can be supported by safety analyses (e.g. FMEA, FTA, HAZOP) in order to develop a complete set of effective functional safety requirements*”. Thus, it is not *mandated* that functional safety requirements are generated through the systematic application of safety analysis techniques. Further guidance on the management and specification of safety requirements (in all life-cycle phases) is given in the supporting processes part of the standard [3]; although this places requirements on the verification, traceability and management of those requirements, it does not provide any guidance on their derivation. Similarly, guidance is provided on the use of safety analysis techniques for verification, but not on other uses beyond stating that any “[...] measures derived from the safety analysis shall be implemented [...]” [9].

Overall, whilst ISO 26262 provides guidance on the content of the functional safety requirements, it provides little assistance on how they should actually be generated in practice. This observation is not a criticism of the standard, as its primary objective is to set out the requirements on the development process, not to provide guidance on the most effective way to meet those requirements. The remainder of this paper attempts to provide guidance in this area, based on industrial experience.

RICARDO APPROACH

Timing of Activities

The first issue we consider is the timing of the activities used to generate a functional safety concept. At the concept stage we need to ensure that system safety considerations are among the drivers for the system architecture (alongside typical factors such as packaging, cost, re-use of existing architectural patterns, etc.). Decisions made at this stage are often the most expensive or difficult to change later. For example, if a decision is not made to use an independent monitoring approach at this