ISO 26262 concept phase safety argument for a complex item

I. Ibarra*, S. Hartley, S. Crozier, D. Ward

**MIRA Ltd, England, Watling Street, Nuneaton, Warwickshire, CV10 0TU.*
**ireri.ibarra@mira.co.uk*

Keywords: safety goals, GSN, ISO 26262, SysML.

Abstract

This paper presents a safety argument using GSN to support product development at the “concept phase”, following ISO 26262-3, with emphasis on the application of the standard to complex “items” that integrate multiple functions.

1 Introduction

The purpose of this paper is to explore how to apply the principles of ISO 26262 [1], particularly during the “concept phase”, to complex “items” that integrate multiple functions. In ISO 26262 the “item” is defined as “*a system or array of systems to implement a function at the vehicle level, to which ISO 26262 is applied*”. Additionally, it is considered how to support product development at the “concept phase”, through the principles of ISO 26262 part 3. The approach consists of arguing how safety objectives are achieved using the work products required by the standard, whilst presenting such an argument in a graphical form using the Goal Structuring Notation (GSN). This is additionally supported by documenting some of these work products, or at least their relationships, in SysML.

The questions this paper addresses are as follows:

a) What is required in terms of the processes that allow the standard to be applied to complex “items” which deliver multiple functions?

b) What is required to enable bidirectional traceability from safety goals via functional safety requirements through to the “element” level?

c) What is required in order to formulate a strategy for arbitration logic issues?

d) What tool support for functional safety management is necessary in order to achieve the points above?

2 Approach

The safety argument was captured using the Goal Structuring Notation (GSN), as an aid to deliver the ISO 26262 required work products. This paper specifically addresses Part 3 of the standard, this paper expands the work of [3] with respect of the approach taken for the hazard analysis and risk assessment; it also develops [4] further on the approach taken to model the “item definition”; additionally some fundamentals on assurance have been expanded from [5] by taken on the use of GSN to represent the argument on the safety objectives of the system.

The approach also considers a hierarchical organisation for both the system design and the argument over the safety objectives in line with ISO 26262. ISO 26262 introduces the terms “item” and “element” to form such a hierarchy. The “item” is usually the top-level system or group of systems which are integrated into a specific vehicle application, and therefore the design authority for the “item” is usually a vehicle manufacturer (OEM) or at least a system integrator. The term “element” is used to describe a system or any constituent part thereof at any level of the design hierarchy. The reason for this is that traditionally in the automotive industry, the supply chain is structured around the outsourcing of major “element” developments from the OEM to Tier 1 suppliers. Some of these “elements” may be within the OEM’s design authority, while others may lie fully or partially outside this authority.

The intention of using GSN is twofold: firstly because it allows developing a hierarchical argument, i.e. one that is valid at the “item” level and which incorporates sub-arguments at the “element” level, as shown in Figure 1. Secondly this approach is also suitable to produce arguments over different stages of the product lifecycle, in alignment to ISO 26262, as shown in Figure 2.

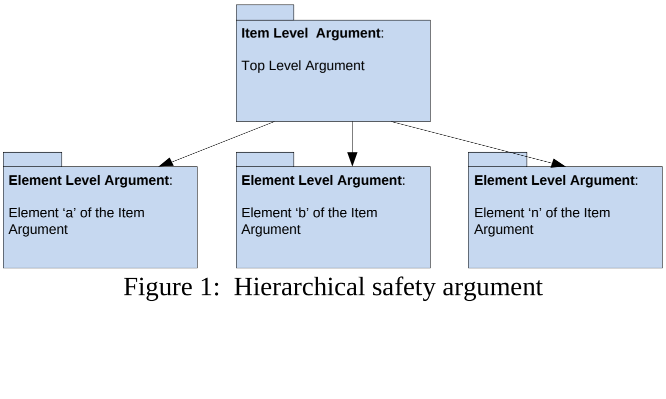


Figure 1: Hierarchical safety argument

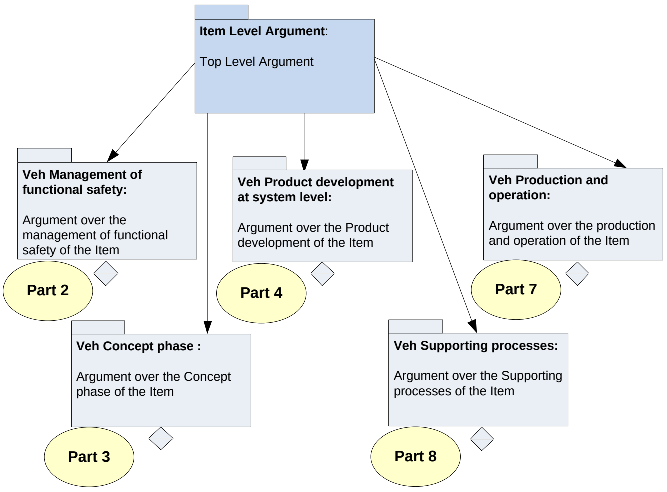

Item Level Argument:
Top Level Argument
Veh Management of functional safety:
Argument over the management of functional safety of the Item
Part 2
Veh Product development at system level:
Argument over the Product development of the Item
Part 4
Veh Production and operation:
Argument over the production and operation of the Item
Part 7
Veh Concept phase :
Argument over the Concept phase of the Item
Part 3
Veh Supporting processes:
Argument over the Supporting processes of the Item
Part 8

Figure 2: Product lifecycle argument structure

The more detailed argument over product development at system level (Part 4) is supported by arguments over the development at hardware (Part 5) and software level (Part 6), as shown in Figure 3.

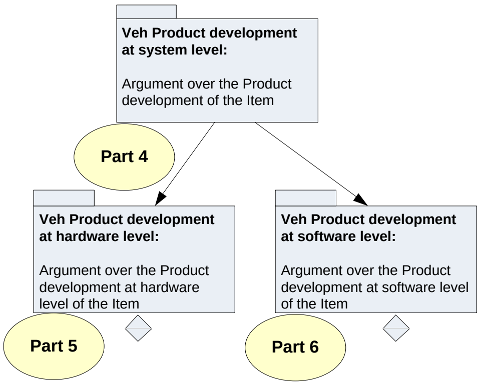

Veh Product development at system level:
Argument over the Product development of the Item
Part 4
Veh Product development at hardware level:
Argument over the Product development at hardware level of the Item
Part 5
Veh Product development at software level:
Argument over the Product development at software level of the Item
Part 6

Figure 3: Arguments over development at hardware and software level

The "item" definition argument is presented in Figure 4. Note that the definition of "item" in ISO 26262 seems to imply that the "item" delivers a single function (e.g. powertrain control, brake control). However, at present many systems under development such as hybrid vehicle control are responsible for multiple functions. Hence, if such a system is treated as an "item" that provides multiple functions, this appears to extend the assumed normal use of the standard. Another point to make here is that defining the "item" is not a trivial activity. Rather than simply naming the "item", it involves information from different sources in diverse formats, as can be seen in Figure 4. A correct and complete item definition is an essential pre-requisite to the rest of the activities required by the standard, especially most of the activities in Part 3.

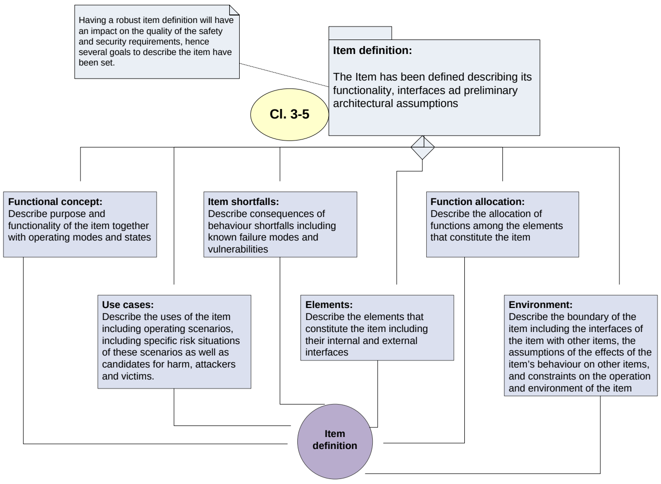

Having a robust item definition will have an impact on the quality of the safety and security requirements, hence several goals to describe the item have been set.
Item definition:
The Item has been defined describing its functionality, interfaces ad preliminary architectural assumptions
Cl. 3-5
Functional concept:
Describe purpose and functionality of the item together with operating modes and states
Item shortfalls:
Describe consequences of behaviour shortfalls including known failure modes and vulnerabilities
Function allocation:
Describe the allocation of functions among the elements that constitute the item
Use cases:
Describe the uses of the item including operating scenarios, including specific risk situations of these scenarios as well as candidates for harm, attackers and victims.
Elements:
Describe the elements that constitute the item including their internal and external interfaces
Environment:
Describe the boundary of the item including the interfaces of the item with other items, the assumptions of the effects of the item's behaviour on other items, and constraints on the operation and environment of the item
Item definition

Figure 4: "item definition" argument

Regarding the interaction of the "item" with other "items" or with the environment, the approach described in this paper handles the most complex interactions by analysing them at the highest level possible. This contrasts with a more established use of ISO 26262 where the "item" delivers just one function (e.g. steering or braking) and a simplistic approach is taken, where malfunctions as a result of failed interactions are simply eliminated by design.

Hence the main driver for the approach taken was that for the hazard analysis process, special consideration had to be given to the interactions between different systems that were involved in fulfilling the same safety goal.

In order to address "items" which deliver multiple functions, the Hazard Analysis and Risk Assessment (HARA) was carried out using the available functionality at the highest possible level, namely at the vehicle level. Although in conventional applications of ISO 26262 hazards are defined in terms of consequences at the vehicle level, and may be defined taking into account interactions between systems, it is normal to conduct the HARA on an individual electronic system defined as the "item".

The risk assessment (RA) itself was carried out using the MISRA risk graph approach [2], shown in Figure 5; rather than assessing risk directly using the ISO26262 risk parameters, with a further translation stage to convert hazard risk (*R*) values to ASIL values in order to align to ISO 26262, using the mapping in Table 1.

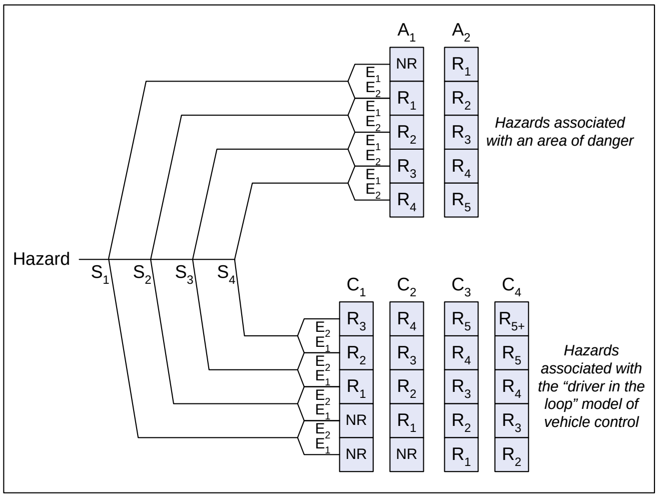


Figure 5: MISRA Risk graph

MISRA	ISO 26262
R1	ASIL A
R2	ASIL B
R3	ASIL C
R4	ASIL D
R5	No direct mapping

Table 1: R and ASIL mapping

The reason for using the MISRA approach is that ISO 26262 assumes that all necessary safety mechanisms are integrated into an individual “item”, so there is no specific means to address an “item” which only provides a risk-reduction function, or where this risk reduction is apportioned between different systems or “items”. Additionally, ISO 26262 assumes the driver is “in the loop” and therefore some risk reduction is always apportioned to controllability (the driver’s ability to influence and control) of the hazardous situation. The shortcoming here is that for some control systems within the vehicle (particularly with new and emerging technologies) the driver is not in the loop, so controllability is not appropriate. However, the “possibility to avoid” the hazard is more appropriate [2].

The RA proved to be challenging for non-functional hazards, i.e. those hazards which may be inherently associated with the technologies used, and are not necessarily caused by the malfunction of E/E systems, but nevertheless have to be accounted for when developing a vehicle. Additionally hazards that exist at the boundary between two or more safety domains (for example, functional safety and electrical safety) are rather difficult to address when using only the processes prescribed in ISO 26262 Part 3.

Following the HARA, the next step is to develop safety goals (SGs) to address the identified hazards. The SGs were written to address the hazards identified at the vehicle level.

The functional safety concept (FSC) was elaborated from the safety goals by documenting the functional safety requirements (FSRs), arbitration logic and warning and degradation concept (W&DC).

Next, the functional safety requirements (FSRs) were allocated to those architectural “elements” already known to be part of the design.

Using simple matrices to correlate information (illustrating requirements traceability) may not be enough when dealing with a large number of “elements” and safety goals. In addition ISO 26262 recommends using suitable requirements management tools, which are becoming commonly accepted as part of systems engineering practice and are acknowledged as being particularly beneficial for projects which involve distributed development.

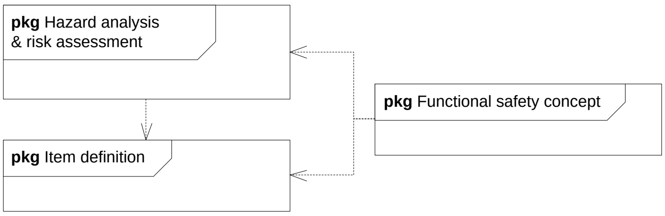
Explicit links between safety goals and the hazards are to be maintained, as well as explicit links between each safety goal and the FSRs allocated to “elements” in the “item”.

For an “item” which delivers multiple functions and where more than one “element” can influence the “item’s” ability to deliver the function, e.g. a complex braking system which includes regenerative braking; it was fundamental to establish a strategy to define which “element” takes precedence over the others, in the event that one or more faults are detected, where ability to meet a safety goal relies on a defined reaction. Such strategy for “arbitration logic” issues was also documented as part of the functional safety concept (FSC).

3 Results

The safety goals were elaborated bearing in mind the different actors involved at different stages of the product lifecycle, e.g. during maintenance, technicians are the main actor, and hence the exposure to certain hazards is higher than that of the vehicle occupants or road users. SGs also reflect the grouping of use cases; the aim was to separate out those safety goals, where much of the risk apportionment can be attributed to what ISO 26262 calls “other measures”, often procedural in nature or involving measures such as physical barriers.

For the functional safety concept; it was found that the underlying complexity of the different types of information that feed into it was critical to manage. Figure 6 shows a package diagram in SysML to emphasise the dependencies between the information contained in the HARA, “item definition” and FSC; even though this may seem obvious to the reader, it is important to acknowledge that these three components of the FSC need to be complete, consistent and correct for a successful transition to the remaining phases. If any changes are experienced in the “item definition”, the HARA or the FSC, as a result of updates in the proposed architecture or re-assessment of risks; these need to be managed accordingly by means of impact analysis, as per Part 8 Clause 8, which covers change management.



pkg Hazard analysis & risk assessment
pkg Functional safety concept
pkg Item definition

Figure 6: “concept phase” information structure

The “item definition” information can be provided in a variety of formats such as written specifications, architectural diagrams, requirements documents, etc. hence one of the first steps to be taken, is to organise such information in a format that is useful for safety analysis purposes and that will help to maintain traceability between analysis results, the actual SGs and FSRs.

Ultimately the goal of the “item definition” is providing sufficient documentation in order to capture both architecture and functionality.

Figure 7 shows the different paths that are key to the traceability of the FSRs and the information contained in the “item definition”; this is done using <<trace>> and <<allocated>> stereotypes in SysML. Additionally, details of the warning and degradation concept are also captured in relation to the FSRs, as a refinement of them. Fault tolerant time intervals trace to the safety goals; also the safety goals trace to the use cases. Keeping the requirements structure simple proved to be challenging due to the fact that the “item” is quite large, providing many functions that rely on complex interactions. Indeed, “elements” can be considered as items in their own right as the design matures and as “elements” with their corresponding functional safety requirements are given to sub-suppliers for development within their own lifecycle.

The use of a dedicated requirements management tool made possible to better handle the large number of requirements produced at the “concept phase”. This was especially beneficial when demonstrating requirements completeness as the “item” was delivering multiple functions, certain requirements could be flowed down equally to different “elements” without modifying the overall functionality.

It was fundamental to understand not only how the functionality is achieved by one or more “elements” but also what hazards can be generated at vehicle level if different “elements” in combination are unable to achieve their required functionality.

In generating the strategies for the degraded states, other information needs to be considered such as expected driver behaviour, what other systems remain available to the driver to be able to finish the journey if at all possible, whether there is a possibility for the systems to go back to normal operation if the fault clears, amongst others.

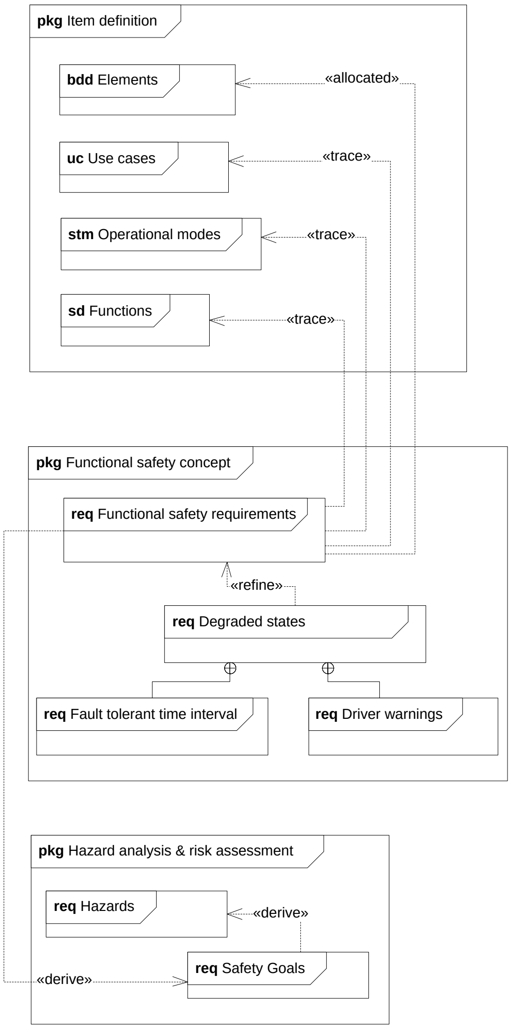


Figure 7: Detail relationship between “item definition”, hazards, safety goals and the Functional safety concept

4 Conclusions and outlook

The authors believe that the most challenging issue was dealing with managing the functional safety concept in a way that was directly traceable to the solutions in the GSN. The relationship between the different components of the functional safety concept needs to be captured in order to support the rationale for writing the requirements.

The functional safety concept required a sound structure just like the argument itself, for this it was essential to use a requirements management tool or similar to be able to organise the components of the functional safety concept in a modular way that can be easily linked to the GSN network itself.

In order to reap even more benefits from using GSN, the modular extension to GSN can be used to more formally define the safety argument; thus enabling the possibilities for reuse on similar projects, with the appropriate updates of the HARA or for benchmarking of particular concerns, which are related to novel technologies used in hybrid vehicles.

A way to formalise the approach would be to encapsulate the work products and workflow into a GSN pattern, which can then be used as a template for future "item" or vehicle developments.

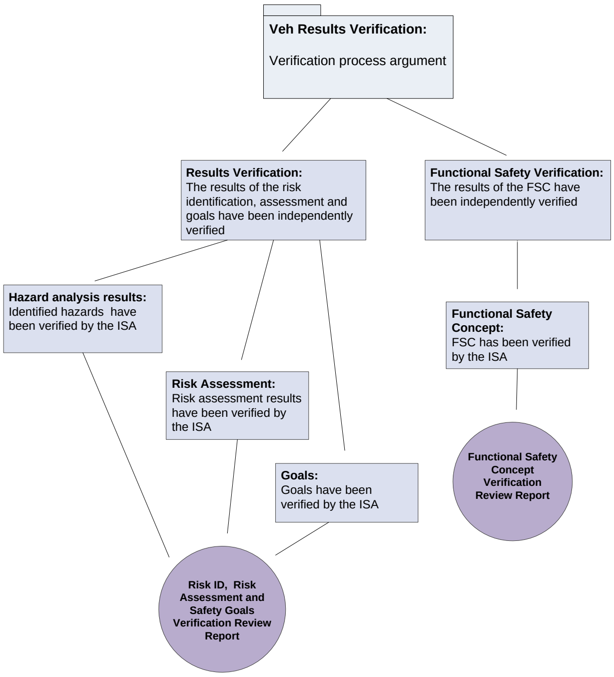

Veh Results Verification:
Verification process argument
Results Verification:
The results of the risk identification, assessment and goals have been independently verified
Functional Safety Verification:
The results of the FSC have been independently verified
Hazard analysis results:
Identified hazards have been verified by the ISA
Functional Safety Concept:
FSC has been verified by the ISA
Risk Assessment:
Risk assessment results have been verified by the ISA
Goals:
Goals have been verified by the ISA
Functional Safety Concept Verification Review Report
Risk ID, Risk Assessment and Safety Goals Verification Review Report

Figure 8: Independent safety assessment

The work products included in "concept phase" are required to be independently verified by an independent safety assessor (ISA), this is in order to verify that the work products are complete in terms of the analysis completeness, consistency with the results from the HARA and ASILs and compliance with the "item definition". The argument to support this verification review can be seen in Figure 8.

Another area of interest is that of end-to-end safety assurance and how tool integration may have a positive impact on the management of the work products required by ISO 26262.

For example, "item" or "element" models which could then be linked to SGs and to their allocated FSRs. These could then be taken further to be refined into technical safety requirements (TSRs) and possibly linked to test plans and results, enabling bidirectional traceability links in a leaner way.

A similar approach can be taken for the remaining parts of ISO 26262, the argument however, may only be able to support the claim of whether the "item" meets its safety objectives at the high level; for more specific low level behaviour or safety objectives, techniques which involve metrics may be required; such as system simulation, tests results and analysis of the probability of violation of a safety goal against given targets.

Acknowledgements

The authors would like to thank MIRA for supporting the publication of this paper.

References

[1] ISO 26262:2011, "Road vehicles – Functional safety,(2011)

[2] MISRA, Guidelines for Safety Analysis of Vehicle Based Programmable Systems, ISBN 978-0-9524156-5-7 (2007).

[3] I. Ibarra, "Complying with ISO 26262 – A novel hybrid vehicle architecture", *IET Functional Safety Assessments*, 7 March, London, UK, (2012).

[4] I. Habli, I. Ibarra, R. S. Rivett, T. Kelly, "Model-Based Assurance for Justifying Automotive Functional Safety", SAE Technical Paper 2010-01-0209,2010.

[5] R. Palin, D. Ward, I. Habli, R. S. Rivett, "ISO 26262 Safety Cases: Compliance and Assurance", *6th IET International System Safety Conference*, Birmingham, United Kingdom, September, (2011).