Systematic Application of ISO 26262 on a SEooC

Support by applying a systematic reuse approach

Alejandra Ruiz
ICT–European Software Institute Division
Tecnalia
Derio, Spain
alejandra.ruiz@tecnalia.com

Alberto Melzi
Vehicle Research & Innovation
Centro Ricerche FIAT
Turin, Italy
alberto.melzi@crf.it

Tim Kelly
Department of Computer Science
University of York
York, U.K
tim.kelly@york.ac.uk

***Abstract*—The automotive domain is undergoing significant transformation. The fully electric vehicle is playing a role in updating the electronic systems on the car. Systems such as electric parking are emerging. The entrance of ISO 26262 [1] functional safety standard has impacted automotive design and assurance practice. ISO 26262 includes the concept of a Safety Element out of Context (SEooC). However, it lacks a systematic process regarding the implementation of the SEooC concept. In this paper we present our experience of the application of the SEooC concept from ISO 26262 to an electric parking system. We describe a systematic approach that takes into account the needs for a safe reuse of system elements into the whole vehicle context.**

Keywords—ISO 26262, SEooC, reuse, composition, safety

I. INTRODUCTION

The arrival of ISO 26262 standard into the automotive domain addresses how to manage functional safety issues. This standard defines the best practices from the domain in order to support safety management. However, as Ruiz et al. mentioned in [2], the application of the SEooC can be difficult – especially concerning the management of assumptions. ISO 26262 can be identified as an objective-based standard in that it does not prescribe any specific process to follow as long as you achieve the objectives. In this paper we describe our experience on applying the SEooC concept to an electric parking system following the systematic approach defined by the OPENCOSS project [3].

II. ISO 26262

A. ISO 26262

The need to adopt a specific standard for vehicle E/E systems, where the "normal" functions cannot be separated from safety functions, led to the standard for functional safety named ISO 26262 [1]. ISO 26262 imposes a new structured lifecycle for all systems involving safety-critical features in the vehicle. ISO 26262 also supports a modular certification strategy [4].

The SEooC is a key concept for the automotive industry, because of the multi-tier supplier structure and variants (both, at design and exploitation stages) and promises a massive reduction in certification cost through modularization and reuse of certification evidence.

To enable the safe reuse of system elements, the element must already be developed as a SEooC even from the conceptual phase of component design. Thereby, the assumed reuse may however still diverge from the final context in which the component is reused.

As the possible contexts and systems in which the component will be use are assumed, the component might be used for a purpose different from the ones defined at design time, as long as the initial assumptions still hold true. Informal, ambiguous, and incomplete SEooC assumptions are considered to hamper the establishment of a SEooC conformant development process and ultimately could lead to larger efforts and higher costs than developing components from scratch [2].

III. ELECTRIC PARKING SYSTEM

The Electric Parking System is in charge of the management of the park pawl actuation (mechanical engagement/ disengagement). It provides mechanical locking or unlocking of the transmission when the parking mode is selected, avoiding unwanted movement of the vehicle when stopped. In this use case we have assumed that the selection can be done by the driver or automatically. The selection of the parking mode is actuated by a gear selector equipped with switches dedicated to the modes of operation of the vehicle.

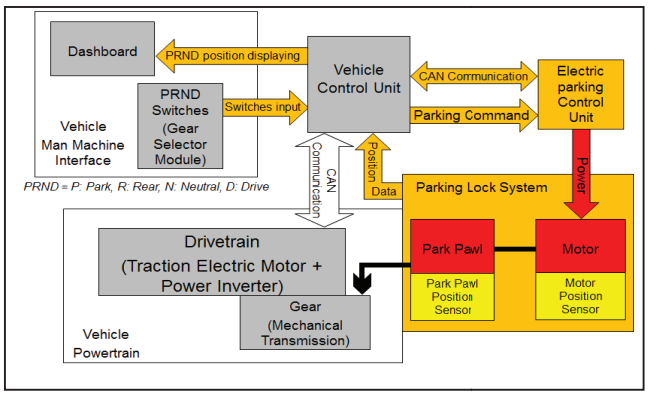


Fig. 1. Electric parking system function blocks

A. Challenges on the use case

The use case is based on the example of a system representing a potential SEooC: the functionality of it is not related to a specific vehicle, but to general assumptions related to the possible application of the system to cars with electric traction powertrain. The objective is to derive from the general assumptions the criteria for establishing safe reuse of a SEooC in the case of a specific integration in a real vehicle development.

IV. Assurance Process

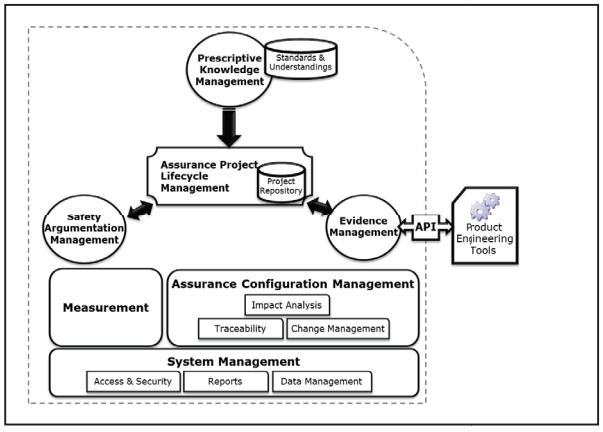
In order to cope with the challenges mentioned before we have followed a systematic approach. We can highlight five phases that should be executed: Standards modelling, Project Tailoring, Evidence management, Safety Case creation and Compliance matching.

A. OPENCOSS platform

In order to support this process, we have created a core platform [5].

Prescriptive knowledge management functionality supports the first phase where we are able to model different standards.

The Assurance Project Lifecycle Management factorizes aspects such as the creation of safety assurance projects and any "project baseline" information that may be shared by the



different functional modules.

Fig. 2. Functional decomposition for the OPENCOSS platform

The Safety Argumentation Management function supports the creation of assurance case based on the GSN graphical notation [6] and reduces the effort on creating the assurance case by applying argumentation patterns.

The Evidence Management function let us follow the evidence evolution along the lifecycle and evaluate our confidence on it.

B. Application of the assurance process

Our first step has been to create a model of ISO 26262 creating standard to establish the *reference framework*. The objective of this phase is to be able to share a non-ambiguous and formal interpretation of the standard. We have focused on the parts 3 (Safety Concept) and part 4 (Product development at system level) of ISO 26262. We have addressed two top level activities, safety concept phase and product development at system level. Those activities are decomposed into sub activities. Taking the table the following table extracted from the annexes of ISO 26262

TABLE I. Excerpt of table A.1 from ISO 26262 annexes [1]

Clause	Objectives	Prerequisites	Work products
5. Item definition	The first objective is to define and describe the item, its dependencies on and interaction with the environment and other items. The second objective is to support an adequate understanding of the item so that the activities in subsequent phases can be performed	None	5.5 Item definition

The elements of column 'Clause' can be mapped as Activity classes. The 'Objectives' column is mapped into the objective parameter of the Activity class. The columns 'Prerequisites' and 'Work products' are easily mapped as artefacts in our meta-model.

We have model the activity "Hazard analysis and risk assessment" from the clause 3.7 of the standard into sub activities such as: 'Initiation of the hazard analysis and risk assessment', 'Situation analysis and hazard identification', 'Classification of hazardous events', 'Determination of ASIL and safety goals', 'Verification (of HARA and Safety Goals)', 'Confirmation review of HARA' and 'Audit'. These activities will also be modeled with the requirements related on how they should be performed. Activities might need to fulfill requirements on how they should be done. The clause 7.4 Requirements and recommendations from ISO 26262 for example includes elements that are mapped as requirements that should be fulfilled by the activity: Hazard analysis and risk assessment.

Artefacts in our model are mapped with work products from the standard. So the activity Hazard analysis and risk assessment will produced the HARA report such at is described

on the standard ISO 26262 on clause 3-7.5.1. The work products sometimes are required to include some sections or information. In this case, we model them as requirements that constrain a specific artefact.

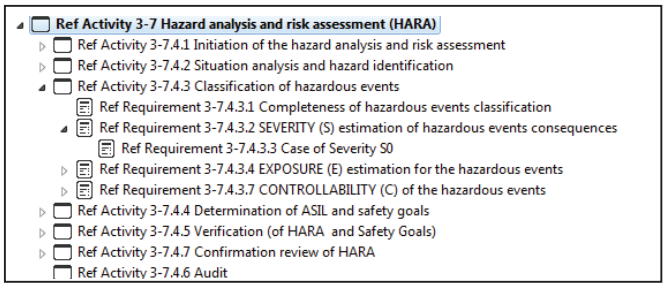


Fig. 3. Excerpt of ISO 26262 modellization

In the second phase we have tailored the reference framework created previously in order to define the actual set of activities and requirements that apply to this particular SEooC. An example of this tailoring is the inclusion of a new artefact, the preliminary architecture assumption in which the SEooC is planned to be used. This document is mentioned on Part 10 – SEooC section of the standard, which happen to be just guidelines, not prescriptive. When we define the ASIL for the project we are able to tailor the activities so we are able to produce an adapted view of the standard with just the requirements needed for the desired ASIL.

In the third phase we link the actual results of the Electric Parking System design with the different work products requested by standard and model on the previous phase. This is important especially for those work products that are refined along the lifecycle for example the safety plan. We can trace the evolution of this document and also evaluate the confidence we have on it.

In the fourth phase we address safety case generation. In this, we have worked primarily on two aspects: identified hazards have been mitigated through deriving and verifying safety requirements and then examining the confidence we have regarding the correctness and completeness of the hazard analysis and risk assessment. GSN [6] has been used as a semi-formal language in order to show the argumentation. Even more, based on the argumentation created, a pattern has been created so for further developments, the same rationale will be used and the same kind of analysis will be used as evidence.

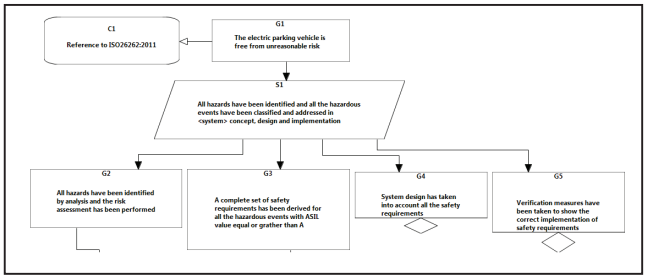


Fig. 4. Excerpt of argumentation

One of the interesting things of the argumentation is that it includes the concepts of assumptions and public claims. We have used the assumption concept to declare the assumptions made on the SEooC developments and the public claims to declare the guarantees provided to future items that will be integrated with the SEooC. The preliminary architecture of the vehicle that we have mentioned before and which is included in our tailored baseline is also mentioned here on the argumentation. This architecture is considered an assumption and the functional safety requirements allocation will be done with this assumption.

Finally in the fifth phase we have highlighted how each of the elements modeled in the earlier phases comply with the requirements of the standard. As a result of this compliance match we produce a report evaluating the extent of compliance to the standard. This enables us to evaluate the efforts still required to complete the assessment.

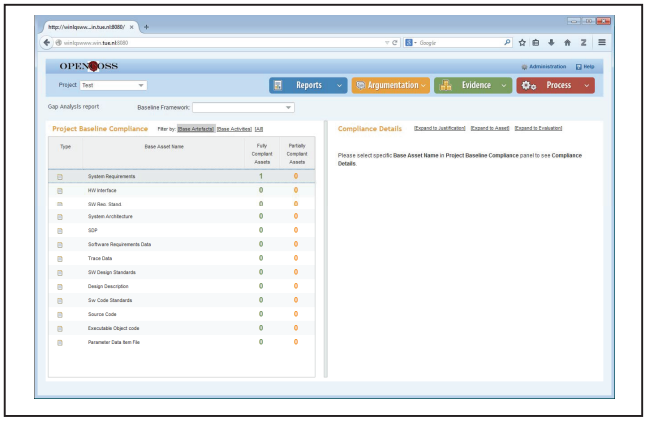


Fig. 5. Summary of the compliance elements with the ISO 26262

V. RESULTS

As the application of ISO 26262 it is something relatively new, it is hard to find projects to compare the application of these approach in relation with others.

One benefit we have discovered when we were applying this systematic approach is the use of a semi-formal language as in the structured environment. This can improve the understanding of the functional safety process description for the users and supports the assessment of the related projects. The standard has been modelled into concepts easy to understand such as activities, requirements or artefacts.

The use of graphical argumentation can support to understand the rationale behind some design decisions.

We have defined two main indicators to evaluate the benefits of this approach:

- Automation on Safety Assurance Process
- Safety Assurance Reuse across Systems

Before the application of this approach the automation was currently non-existent. Within this use case scope, we can find a solution for the standardization and management of the data flux, mainly at the level of the functional and technical safety requirements and, where possible, for the production of standardized reports. The result of the standardized compliance report that we can obtain at the end of the firth phase is a good example of this.

The reuse across systems is a baseline for the SEooC development. This example has confirmed the feasibility for reusing previous developments.

The GSN patterns will be used as on future developments. As the rationale will be reused, the best practices will be easily spread along the company with each new development.

VI. Conclusions and future work.

We have been able to apply a systematic approach for the SEooC compliance process with the support of an assurance framework. By following this approach we can demonstrate compliance with best practice and define a common approach to be adopted between the projects.

We still need to work on the integration aspects of the SEooC which will require validation of all the assumptions that we have identify on the SEooC.

Acknowledgment

The research leading to these results has received funding from the FP7 programme under grant agreement n° 289011 (OPENCOSS).

References

[1] International Organization for Standardization (ISO), ISO26262 Road vehicles – Functional safety, ISO, Nov 2011

[2] A. Ruiz, H. Espinoza, F. Tagliabò, S. Torchiaro, A. Melzi, "A Preliminary Study towards a Quantitative Approach for Compositional Safety Assurance" Proceedings of 21st Safety Critical Systems Symposium, February 2013

[3] Opencoss project. URL: http://www.opencoss-project.eu/; Last visit: 2014-09-08.

[4] John Rushby. Modular Certification. CSL Technical Report, September 2001

[5] D2.3 OPENCOSS platform architecture (report) Opencoss Project. Deliverable. http://www.opencoss-project.eu/sites/default/files/D2_3_OPENCOSS_Platform_Architecture_final.pdf; PDF-Document; Last visit; 2014-09-12

[6] Goal Structuring Notation Working Group, "GSN Community Standard" Retrieved from http://www.goalstructuringnotation.info, Nov 2011.