Industrial Experiences of Building a Safety Case in Compliance with ISO 26262

Raghad Dardar, Barbara Gallina, Andreas Johnsen, Kristina Lundqvist
IDT, MRTC, Mälardalen University,
Västerås, Sweden
name.surname@mdh.se

Mattias Nyberg
Scania AB
Södertälje, Sweden
mattias.nyberg@scania.com

Abstract— The ISO 26262 functional safety standard provides appropriate development processes, requirements and safety integrity levels specific for the automotive domain. One crucial requirement consists of the creation of a safety case, a structured argument, which inter-relates evidence and claims, needed to show that safety-critical systems are acceptably safe.
The standard is currently not mandatory to be applied to safety critical systems installed in heavy trucks; however, this is likely to be changed by 2016. This paper describes the experience gathered by applying the standard to the Fuel Level Estimation and Display System, a subsystem that together with other subsystems plays a significant role in terms of global system safety for heavy trucks manufactured by Scania. More specifically, exploratory and laborious work related to the creation of a safety case in compliance with ISO 26262 in an inexperienced industrial setting is described, and the paper ends with presenting some lessons learned together with guidelines to facilitate the adoption of ISO 26262.

Keywords- Safety-critical systems, ISO 26262, safety case, GSN.

I. INTRODUCTION

Nowadays, road vehicles, including heavy trucks, are characterized by an increased complexity due to a greater variety of functionalities implemented using software solutions, and a greater number of sensors and actuators. As a consequence, there is an increased risk in terms of software or hardware failures that could lead to non acceptable hazards. Thus safety, more precisely functional safety, is a crucial property that must be ensured to avoid or mitigate these potential unacceptable hazards. In the automotive domain, recently, the ISO 26262 functional safety standard has been introduced to provide specific development processes, automotive safety integrity levels (called ASILs), and additional requirements (e.g. on work-products). To be compliant with the standard, manufactures have to: 1) adopt the development processes, 2) determine ASILs for their safety-critical systems, and 3) satisfy the additional requirements (e.g. those on work-products, and those on validation and confirmation measures).

One crucial requirement that must be satisfied by the manufacturers is the creation of a safety case [4]: a contextualized structured argument that links evidence to claims to show that the system is acceptably safe (i.e. safe enough since absolutely safety is an unobtainable goal). According to best practices in safety argumentation [5], this argument should include two types of (sub)arguments: process and product-based (sub)arguments. Process-based arguments show that the life-cycle defined in ISO 26262 has been adopted. Product-based arguments show that the deliverables of the life-cycle, related to the safety-critical system under examination, constitute founded evidence that the system behaves acceptably safe.

Quoting from the standard: "ISO 26262 is intended to be applied to safety-related systems that include one or more electrical and/or electronic (E/E) systems and that are installed in series production passenger cars with a maximum gross vehicle mass up to 3 500 kg." By now, the development of heavy trucks does not have to be compliant with the standard. However, as extensively discussed in [15], it is likely that by 2016 it will have to.

In this paper, we report about the experience gathered in applying the standard to the Fuel Level Estimation and Display System, which is one of the safety-critical systems in Scania trucks. Indeed, a wrong behaviour (e.g. false fuel level) of such system could lead to hazardous events for the driver, such as engine stop and loss of power assisted steering. Our aim is not to present a complete safety case but to show how the life-cycle-related work-products can be compiled to achieve sub-arguments to be integrated in the safety case. In particular, we focus on specific parts of ISO 26262 and we explain how we have collected and provided process and product-based evidence needed to build sub-arguments for the safety case. Moreover, among the existing approaches to document safety cases, we select GSN (Goal Structuring Notation) [10] because of its advantageous features and show how these arguments can be graphically documented and structured.

The rest of the paper is organized as follows. In Section II we present essential background concerning the system to be examined for certification purposes, safety cases, approaches to document safety cases, and ISO 26262. In Section III, we explain how we have collected or provided (when missing) the evidence needed to develop illustrative process and product-based arguments. In Section IV we use GSN to document some illustrative process and product-based arguments. In Section V, we discuss lessons learned and provide general guidelines to facilitate the adoption of ISO 26262 and the provision of safety cases. Finally, in Section VI, we present some related work, and concluding remarks and future work can be found in Section VII.

II. BACKGROUND

In this section we briefly present the essential background on which we base our work. In Section II.A we introduce the safety-critical system to be examined for safety argumentation purposes. In Section II.B we give an overview of ISO 26262. In Section II.C, we recall the definition of safety case. Finally, in Section II.D we present GSN, which is a widely accepted safety case documentation approach.

A. Fuel Level Estimation and Display System

The system under examination is called Fuel Level Estimation and Display System (FLEDS) and is part of a system of systems aimed at providing the controlling functionalities needed in heavy trucks and buses produced by Scania. As mentioned earlier, FLEDS plays a significant role in terms of global system safety.

The main functionality of the system consists of the estimation of the fuel level in the vehicle tank and presentation of this level on the display located in the dashboard. Additionally, the system must warn the driver if the fuel level is below a predefined level. As Figure 1 shows, the functionality is deployed onto three ECUs (Electronic Control Units): Engine Management System (EMS), Instrument Cluster (ICL), and Coordinator (COO). COO is responsible for estimating the fuel level, ICL is responsible for displaying it and EMS is responsible for calculating the fuel consumption, used in estimating the total fuel level. The ECUs are interconnected by a CAN (Controller Area Network) bus. The system has one sensor located in the fuel tank to sense the fuel volume and one actuator (fuel gauge) for displaying the fuel level to the driver. Moreover, a lamp is used to warn the driver in case a low fuel level has been reached. The correct behavior of FLEDS or at least a behavior qualifiable as acceptably safe is necessary to contribute to the safety of the global system. For instance, in the case of low level fuel, if the driver is not alerted (omission failure), it may happen that suddenly the truck stops and, in case of heavy traffic, human life can be threatened.

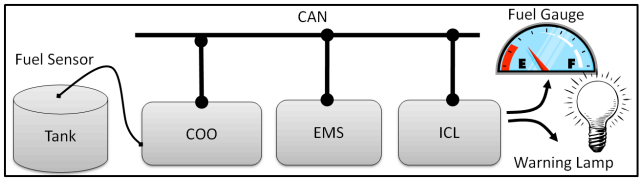

Figure 1: Fuel Level Estimation and Display System.

B. ISO 26262

The ISO 26262 standard [2] is an automotive-specific interpretation of the basic safety standard IEC 61508 [3] for functional safety of electrical/electronic (E/E) and programmable electronic safety-related systems. The standard thereby provides a safety lifecycle that complies with the needs specific to the development of safety-related E/E systems within road vehicles with a maximum gross weight of 3.5 tons. Essentially, the standard addresses potential hazards caused by malfunction of E/E safety-related systems, and provides the necessary safety measures in order to achieve an acceptable level of safety. ASILs are provided for classifying risks of hazards. ASILs specify the necessary safety requirements that must be achieved to ensure an acceptable residual risk (i.e. the risk that remains after required safety measures have been applied, where the remaining risk must not include any unreasonable risk, that is, judged to be unacceptable in a certain context according to valid societal moral concepts, and where risk is the combination of the probability of occurrence of harm and the severity of that harm). Defined confirmation measures must finally be performed to ensure an acceptable level of safety.

As a reference process model, the standard uses a V-model to represent the different phases of the system development. The reference model mainly consists of three phases: Concept phase (part 3), Product development (part 4, 5 and 6), and Production and operation (part 7).

In the Concept phase: the item – which could be a system (1.129) or array of systems to implement a function at the vehicle level, to which ISO 26262 is applied – to be developed in compliance with the standard is firstly defined. This entails in defining the functional, non-functional, legal and already known safety-requirements of the item. The purpose, primarily assumed architecture, boundary and interfaces of the item shall be defined as well. Secondly, potential hazards of the item are identified and ASIL-classified through hazard analysis and risk assessment. Concurrently, Safety Goals (SGs), which inherit the ASILs of the corresponding hazards, shall be formulated for the identified hazards. These SGs describe characteristics needed to avoid hazards or to reduce risk associated with the hazards to an acceptable level. Thirdly, Functional Safety Requirements (FSRs) shall be specified for each SG. FSRs describe basic safety mechanisms, implementation-independent safety-related behaviour, and safety measures that have to be provided by elements in the primarily assumed system architecture for complying with the SGs and their ASILs. FSRs do only consider functional aspects of the system and not how these are technically implemented in hardware or software. FSRs inherit the same ASILs as the corresponding SGs and shall be allocated to elements of the primarily assumed system architecture.

In the Product development phase: Technical Safety Requirements (TSRs) shall firstly be specified for each FSR. These shall detail and decompose the FSRs into requirements which describe how to implement the safety mechanisms and safety measures described by the FSRs. Secondly, a system design that meets the FSRs and TSRs shall be developed. Hence, the design must be verified against the TSRs. Thirdly, TSRs shall themselves be decomposed until they are allocated to concrete hardware and software elements in the design, i.e., down to the separation of software and hardware. Concurrently, the design must be refined and verified (e.g. model-checked) with respect to the granularity of the requirements.

The Production and operation phase: impose the necessary directives to ensure that the required functional safety is guaranteed through the production process, and

maintained during the vehicle operation. We will not elaborate on this subject in the paper.

In addition, the standard provides a vocabulary (part 1), requirements of the institution responsible for the complete safety lifecycle and its individual activities (part 2), supporting processes (part 8), and ASIL-oriented and safety-oriented analyses directives (part 9).

C. Safety Cases

In the case a safety critical system must be certified, it has to be shown to be acceptably safe to achieve the certificate. The proof is provided through a contextualized structured argument that links evidence to claims. This structured argument is known as a safety case [4]. The main conceptual elements of a safety case are:

- *Requirements (claims)*: represent the safety requirements (goals) that must be satisfied (achieved) in order to ensure the safety of the system.
- *Evidence*: represents the proof that a goal is achieved. It is based on the development process, on product-based deliverables (testing, verification, simulation results), and on safety management.
- *Argument*: represents the relationship between safety requirements and their evidence.
- *Context*: Identifies the domain or scope within which the safety is to be argued.

It must be recalled that a safety case without evidence is unfounded and a safety case without an argument is unexplained [11]. A safety case is expected to include two types of arguments: process and product-based arguments. The first type is devoted to show that a product has been developed in compliance with the process defined in the domain-specific standard. The second type is devoted to show that the product satisfies the safety requirements derived during the hazard analysis.

D. Documentation of safety cases

As extensively discussed in [7], several documenting approaches (textual and/or graphical) exist to structure a safety case. A review of these approaches is outside the scope of this paper. By building on existing reviews, among the existing approaches, we select the Goal Structuring Notation (GSN) [10] since, with respect to our needs, it is an adequate means to structure parts of the safety case for FLEDS. From a user perspective, the main interesting features of GSN are: an easy to grasp syntax (direct experience), support for modularity [12] and product lines [13] enabling reuse possibilities, availability of patterns [14], active research community aiming at enhancing its formality and thus increasing its acceptance, and tool support (commercial/open-source).

GSN permits users to structure their argumentation into flat or hierarchically nested graphs (constituted of a set of nodes and a set of edges), called goal structures. To make the paper self-contained, in Figure 2, we recall the concrete syntax of the GSN core modeling elements used in Section IV, and the following list describes their informal semantics.

- *Goal:* represents a claim about the system.
- *Strategy*: represents a method that is used to decompose a goal into sub goals.
- *Solution*: represents the evidence that a particular goal has been achieved.
- *Context*: represents the domain or scope in which a goal, evidence or strategy is given.
- *Supported by*: represents an inferential or evidential relationship. Inferential relationships declare that there is an inference between goals in the argument. Evidential relationships declare the link between a goal and the evidence used to substantiate it.
- *In context of*: represents a contextual relationship.

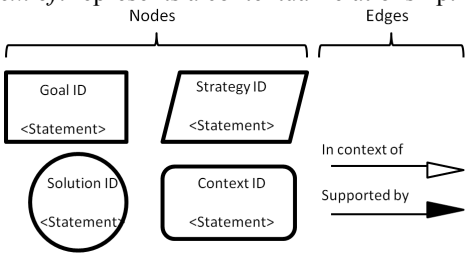

Figure 2 Partial concrete syntax of GSN.

As Figure 2 shows, all the nodes are characterized by an identifier (ID) and a statement, which is supposed to be written in natural language and thus can contain fallacious information [6]. GSN is not a formal language and thus ambiguities and fallacies can be introduced. However, its user-friendly characteristics are convincing enough to select it as a means for structuring argumentations in contexts previously used to natural language.

III. COLLECTION AND PROVISION OF EVIDENCE

To build a safety case, first of all, the claims to be supported must be clear and the evidence to support them must be identified. Usually, the top-level claim is that the system is acceptably safe with respect to the definition of acceptably safe. This top-level claim is shown to be founded by providing evidence that all the hazards that lead to intolerable risk are mitigated. This top-level claim stems from the objective of ISO 26262, which states that the product should ensure a sufficient and acceptable level of safety. Our work has not consisted in making a cost and benefit analysis to achieve a definition of acceptably safe for which the risk is as low as reasonably practical. Instead, we have proceeded as if a definition was present or at least could be provided in further developments of this work. Our main focus has been in finding a clear mapping between the evidence required by the standard and the evidence available in the company. This mapping was needed to understand which evidence could be collected to build the safety case and which evidence was missing and needed to be provided. To do such mapping, we thoroughly studied FLEDS, ISO 26262 and the safety life-cycle adopted by the company. Moreover, interviews have been conducted with the

employees who were involved in the development of the system. The interviews and the study have allowed us to identify the product and process-based evidence. The following list shows the evidence that was available.

- Requirement definitions have been found. The requirements were specified at different levels of abstraction.
- Item definition has been found. Available documents described the system, its dependencies, as well as interactions with other systems and the environment, as required in clause 5 of the concept phase.
- Hazard analysis using FMEA has been found. The inputs and the outputs of system's functions with respect to different failure modes (e.g. early/late) have been analyzed. The analysis is in compliance with the requirements 7.4.4.2.1-2 (part 4 of ISO 262626).
- System design specification in the form of Block diagrams in Matlab/Simulink has been found.
- Verification of the function's robustness using simulation has been found. Different scenarios that were significant for the function's correctness (e.g. up hills and down hills) have been considered.
- Coverage of the requirements during testing at different levels of abstraction (ECUs system testing and integration testing) has been found.
- Traceability between requirements and testing has been found in the testing reports. The traceability has been maintained by using tables where, for each test case, the corresponding requirement is documented as well as the corresponding result of the test case execution.
- Evidence about model checking of the system has been found. Model checking covers a particular set of requirements of the fuel level estimation and low fuel level warning functionalities.
- Evidence about testing in different environments has been found. The ECUs of the system have been mounted on test plates and tested together (integration test).

With respect to process-based evidence, we noticed that some process tasks were not part of the life-cycle of the company and thus no evidence was obviously available. The above listed evidence was not enough to be compliant with the standard and thus we have contributed in providing additional evidence. More precisely:

- ASIL classification of hazards has been provided by following clause 7 of the first phase.
- Hazard identification and analysis using an adapted version of HAZOP (HAZard and Operability analysis) technique has been provided by following clause 7 of the first phase. The analysis didn't introduce any new/changed hazards.
- Identification of SGs, FSRs, and TSRs has been provided by following: clause 7 of the first phase (regarding SGs), clause 8 of the concept phase (regarding FSRs), and clause 6 of the second phase at the system level (regarding TSRs).
- Traceability between hazards, SGs, FSRs, and TSRs and system design has been provided through tables by using cross reference identifiers.
- System design specification using the SysML modeling language has been provided (according to clause 7 of the second phase at the system level).
- Analysis of the design with respect to the systematic causes of failures using FTA has been provided according to clause 7 of the second phase at the system level.
- Safety mechanisms (e.g. detection and handling of faulty input signals) have been provided in the system design.

The above-listed (pre-existing or newly introduced) evidence often plays a double role in the safety case: its existence witnesses that a process activity has been performed (process-based argument) and its content may be relevant to show that risk has been reduced (product-based evidence).

IV. Towards a Safety Case

After having collected and/or provided the evidence, we have exploited it for the creation of process and product-based arguments to be used for the creation of the safety case for FLEDS. For space reasons, all the arguments provided cannot be presented in this paper. The interested reader may refer to the thesis report [9] for further details. We thus decide to focus our attention on a specific process activity within the Concept phase, namely *Hazard analysis and risk assessment* and show the corresponding process-based and product-based arguments.

Figure 3 shows the partial goal structure related to the activity under examination. In this structure, the top goal G1 is directly broken down into two sub-goals (G2 and G6) pertaining to the process and product respectively.

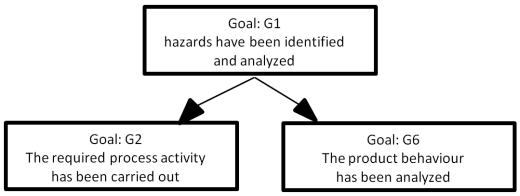

Figure 3 Partial goals structure.

As Figure 4 shows, the goal G2 is then indirectly broken down into 3 sub-goals, namely G3, G4, and G5 by using two strategies: one over the roles (S1) and the other over the activity's steps (S2). The goals G3, G4, and G5 are all supported by direct evidence.

As Figure 5 shows, the goal G6 is directly broken down into 2 sub-goals, namely G7 and G8 which are supported by direct evidence, namely E2, E3 and E4.

As mentioned in Section III, evidence can play a double role in the safety case and this is why evidence E2, E3 and E4 appears in both figures.

V. Lessons Learned

In this subsection, we discuss our experience regarding applying ISO 26262 and creating the safety case in industrial

settings not familiar with ISO 26262. By comparing the life-cycle defined in ISO 26262 and the life-cycle used by the company, we have realized that:

- Some work-products considered mandatory by the standard were not contemplated by the life-cycle used in the company and thus the life-cycle must be adapted.
- Traceability between the life-cycle work-products (e.g. SG, FSR, and TSR) is fundamental and thus it must be pursued and maintained. The company, currently, does not have a systematic approach to support traceability. A good approach would be a model-based approach.
- Studying ISO 26262 and discussing it with the company's employees has permitted us to achieve an operational interpretation allowing us to map available and supposed evidence with required evidence. Moreover, the company has developed a deeper interest in the standard.
- The application of FTA, as recommended by ISO 26262, has resulted to be useful to achieve a complementary examination of the system. Thus the company developed an interest in using the technique in the future.

By building the safety case, we have realized that:

- Product-based evidence should show that the system has the required safe behavior. For instance, when something wrong happens, the system should be able to fail in a safe way. This evidence should stem from activities such as verification (e.g. testing, model-checking), and simulation. From an end-user perspective, the product behavior is more important than the process adopted to develop the product. Thus, at a first glance, product-based arguments (showing that the risk has been mitigated), may appear more important than process-based arguments. However, there is a need for confidence in the evidence provided in the product-based arguments and thus process-based arguments play a significant role as well. Thus to have a good and more convincing safety case for the system, both of the arguments (process-based and product-based) should be provided in the safety case since they complement each other. Moreover, process-based arguments should be clearly separated from product-based arguments to enable reusability as well as ease of check by regulators. However, it is not trivial to avoid evidence repetition, in the case the evidence needed to show that a process task has been fulfilled overlaps with the evidence needed to show that the product behaves as required.
- Even though we have limited our attention to a rather simple sub-system, this experience has allowed us to realize that in the case of full compliance with the standard; even rather simple systems entail complex safety cases as the standard requires almost 100 work products that result from meeting all the requirements through different phases of the life-cycle. Thus mastering the complexity of the safety cases is challenging. Modularity and usage of patterns can help but it is only through a significantly long experience that safety case writers can acquire the needed expertise to achieve well-structured safety case.
- It is not always obvious to understand how to provide evidence and the risk of unfounded safety cases is concrete.
- Evidence may be hidden either because it is not documented or because awareness about it is lacking. Thus it is highly recommended to train the staff with respect to ISO 26262 to increase awareness about the required evidence so that it can be provided quickly in case safety experts need it to build safety cases.

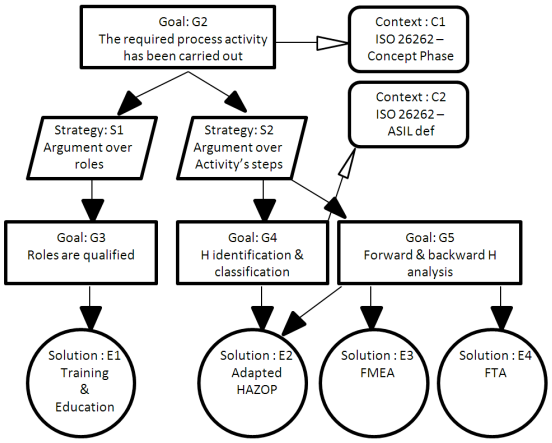

Figure 4 Goal structure for the process-based argument.

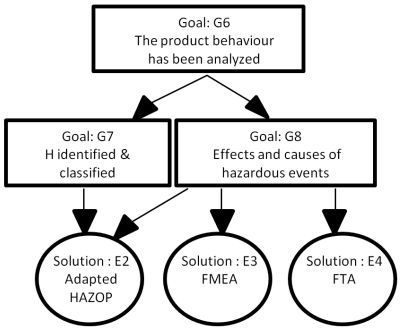

Figure 5 Goal structure for the product-based argument.

VI. RELATED WORK

To our knowledge, only a few studies present industrial experiences of certifying systems, or building safety-cases, in compliance with ISO 26262. Born et al. present in [17] their experiences from the application of ISO 26262 in various projects, most interestingly in a project executed at a German car manufacturer. Although the paper does not elaborate on the issue of building safety-cases, the experiences are significant with respect to building safety-cases in compliance with ISO 26262. Their experiences advocate three main issues of incorporating the standard to car manufacturers and suppliers.

The first issue is that organizations are in favor of the already existing internal safety processes and reluctant to quick transformations to externally imposed processes. This result is consistent with the results of an investigation carried out by Kienle et al. in [16], where an industrial questionnaire showed that internal guidelines, codes and standards are ranked as more important than externally ones.

Consequently, organizations are gradually incorporating externally imposed standards where, specifically, the provision of documentation typically is firstly incorporated. As a consequence, the actual safety process is incorporated at a later stage. This issue leads to the second issue: the effort of organizations is focused on managing the documentation and not the content that is documented. Their experiences advocate that organizations have difficulties with meeting the documentation requirements where consistency cannot be maintained among multiple documents, and their versions, containing redundant information. The third issue is the problem of having traceability among the documents. Born et al. state that traceability often is achieved through cross-referenced identifiers of requirements (e.g. ReqID), hazards (e.g. HazID), etc., which are manually or semi-automatically created. Constantly modified documents in combination with manually created identifiers generate a potential source of errors.

Törner and Öhman present in [18] an industrial exploration of a possible introduction of the concept of safety cases in the automotive industry. The study uses an approach based on interviews and workshops involving three automotive manufacturers. The study identified issues mainly in the areas of resources, information access and organizational competence. Results showed that an increase in workload was expected and that a safety case would not replace any document in their current processes. The latter issue is an issue in the sense that the vital concept of safety cases is not used. Results also showed that it might be an issue to acquire the necessary information, for building a safety case. Finally, results showed that there is a lack of competence with respect to building safety cases. As discussed in Section V, we experienced similar issues as those presented in this section.

VII. Conclusions and Future Work

In this paper, we have presented our experience of building a safety case in compliance with ISO 26262. We have discussed how we have collected and or provided evidence to be structured into product and process-based arguments. On the basis of our experience we have provided some lessons learned aimed at facilitating the adoption of ISO 26262 in industrial settings (criticality of traceability between work-products and necessity to introduce a model-based approach) as well as provision of evidence for certification purposes (clear separation between product and process-based arguments).

In the future, by benefiting from our lessons learned, we aim at providing patterns to ease the argumentation and plan to focus on process-based patterns targeting not only ISO 26262, but also the set of safety standards that present evident commonalities. To conceive such patterns we plan to exploit the findings presented in [8], in which a process line of safety standards was discussed.

Acknowledgment

This work has been partially supported by the SYNOPSIS project [1] and VINNOVA Espresso project (see http://www.vinnova.se/sv/Resultat/Projekt/Effekta/ESPRESSO).

References

[1] SYNOPSIS- SSF- RIT10-0070. Safety Analysis for Predictable Software Intensive Systems. Swedish Foundation for Strategic Research.

[2] ISO26262. Road vehicles – Functional safety. International Standard, November 2011.

[3] IEC 61508:2010. Functional safety of E/E programmable electronic safety-related systems.

[4] N. Leveson. White Paper on The Use of Safety Cases in Certification and Regulation, updated May 6, 2012.

[5] I. Habli, T. P. Kelly. Process and Product Certification Arguments - Getting the Balance Right Workshop on Innovative Techniques for Certification of Embedded Systems. Proc. of 12th IEEE Real-Time and Embedded Technology and Applications Symposium, San Jose, California, United States, 2006.

[6] W.S. Greenwell, J. C. Knight, C.M. Holloway, J.J. Pease. ATaxonomy of Fallacies in System Safety Arguments. Proc. of the 24th International System Safety Conference, Albuquerque, New Mexico, 2006.

[7] C.M. Holloway. Safety Case Notations: Alternatives for the Non-Graphically Inclined? In C.W. Johnson and P. Casely (eds.), Proc. of the IET 3rd International Conference on System Safety, IET Press, Savoy Place, London, 2008.

[8] B. Gallina, I. Sljivo, and O. Jaradat. Towards a Safety-oriented Process Line for Enabling Reuse in Safety Critical Systems Development and Certification. Post-proc. of the 35th IEEE Software Engineering Workshop (SEW-35), Heraclion, Crete (Greece), (to appear in 2013).

[9] R. Dardar. Building a safety case in compliance with ISO-26262. Master thesis, Mälardalen University, School of Innovation, Design and Engineering, to appear in 2013.

[10] GSN Community Standard Version 1. November, 2011, http://www.goalstructuringnotation.info/documents/GSN_Standard.pdf

[11] T. Kelly and R. Weaver. The Goal Structuring Notation – A Safety Argument Notation. Proc. of the Dependable Systems and Networks 2004 Workshop on Assurance Cases, 2004.

[12] I.Bate, T.Kelly. Architecture Consideration in the Certification of Modular Systems. Reliability Engineering and System Safety, vol. 81, Issue 3, pp 303-324, 2003.

[13] R. Alexander, Tim Kelly, Zeshan Kurd, John McDermid. Safety Cases for Advanced Control Software: Safety Case Patterns. Department of Computer Science University of York, 2007.

[14] I. Habli, T. Kelly A Safety Case Approach to Assuring Configurable Architectures of Safety-Critical Product Lines in Proc. of the International Symposium on Architecting Critical Systems (ISARCS), Prague, Czech Republic, 2010.

[15] Linkedin Group: http://www.linkedin.com/groups/ISO-26262-Functional-Safety-2308567

[16] H. Kienle, D. Sundmark, K. Lundqvist, A. Johnsen, Liability for Software in Safety-Critical Mechatronic Systems: An Industrial Questionnaire. Proc. of the 2nd International Workshop on Software Engineering for Embedded Systems, 2012.

[17] M. Born, J. Favaro, O. Kath, Application of ISO DIS 26262 in practice, Proc. of the 1st Workshop on Critical Automotive applications: Robustness & Safety, 2010.

[18] F. Törner, P. Öhman, Automotive Safety Case A Qualitative Case Study of Drivers, Usages, and Issues. Proc. of the 11th IEEE High Assurance Systems Engineering Symposium, 2008.