Process- and Product-based Lines of Argument for Automotive Safety Cases

Helmut Martin, Martin Krammer, Robert Bramberger
VIRTUAL VEHICLE Research Center
Graz, Austria
{helmut.martin, martin.krammer,
robert.bramberger}@v2c2.at

Eric Armengaud
AVL List GmbH
Graz, Austria
eric.armengaud@avl.com

***Abstract*—The complexity of functions in today's vehicles demands a methodical procedure to ensure functional safety. Process audits and functional safety assessments confirm compliance to standards and safety of a product. One outcome of the safety life cycle is the safety case, which should "communicate a clear, comprehensive and defensible argument that a system is acceptably safe". In this paper, we propose a workflow to introduce a joint approach for process- and product- based argumentation compliant to ASPICE and ISO 26262. The approach is supported by argument patterns that cover the main lines of argument with respect to relevant standards. These patterns are elaborated in parallel to the development process and deal with visualization of the line of safety argumentation as well as the linking of evidences. They have a generic specification, provide templates and cover two argumentation aspects. Process-based argumentation deals with the engineering process and supports process audits whereas product-based argumentation deals with project specific outcomes, i.e. content of work products, and supports the functional safety assessment. The applicability of the approach is demonstrated on an automotive use case of a high voltage battery system for a hybrid electric vehicle powertrain.**

***Keywords* — ISO 26262, Automotive SPICE, Safety Case, Safety Argumentation, Safety Audit, Safety Assessment**

I. Introduction

The number of networked functions implemented on numerous control units in today's vehicles is increasing. The interaction of these heterogeneous functions causes a high degree of complexity which requires particular attention before, during and after development. From a safety point of view these functions must operate without any malfunctions, which could lead to hazards with catastrophic effects (e.g. harm people or lead to damage to the environment). The automotive safety standard ISO 26262 [1] defines an item as a system or array of systems, e.g. automotive Electric/Electronic (E/E) system, that implements a specific function. ISO 26262 provides requirements and recommendations concerning functional safety to handle required safety activities over the entire life cycle of an item, e.g. traceability over the elaborated work products. The standard compliance of the development process must be proven and the implemented product has to be safe according to recommended methods of the standard. The outcome of safety activities has to be documented in a multitude of work products. A work product is defined as a result, being associated with one or more requirements of ISO 26262. Furthermore, ISO 26262 demands conformation measures for relevant work products to check their correctness with respect to formality, content adequacy and completeness by an independent body or organization. In most cases, results are documents such as "Safety analysis", "Safety integrity determination" or "Reliability calculation". All documents as a whole provide evidence to compile the safety case.

To argue that all requirements concerning the process are fulfilled, adequate evidence is needed. However, evidence must clearly be distinguishable from the information, which led to it. From this point of view it is beneficial to find an improved methodology to indicate required evidence. The relationship between safety requirements and evidences has to be communicated by clear, comprehensive and defensible argumentation, to emphasize traceability.

All stakeholders, including engineers, reviewers and auditors, may not be in-depth familiar with the engineering process and the content of all resulting work products. Stakeholders will be able to comprehend the argumentation faster, resulting in shorter review cycles, concise feedback and a better understanding of the entire product development.

In section II the problem statement is formulated. Section III provides related work and the most important background information. Section IV describes the proposed methodology to use process- and product-based argumentation. Section V shows the application of the methodology in an automotive use case. Finally conclusions and future work are presented in section VI.

II. Problem Statement

Companies, which deal with safety critical products, engage external authorization bodies to certify their abilities concerning functional safety development (e.g. functional safety audit and functional safety assessment). Safety certification ensures that a certain product fulfills specific safety requirements in a specific environment. It requires a complete and structured collection of evidence to show that the developed system is acceptably safe.

The role of safety arguments is often neglected, thus stakeholders who are not directly involved in the creation of work products (e.g. reviewers) may have troubles to reconstruct the train of thought concerning decisions taken. Documentation of

decisions in a comprehensible manner avoids loss of crucial information. A systematic approach is required to handle the development process that deals with dependency issues of the elaborated work products because the complex relationship between them may be not obvious. Artifacts cover outcomes of a specific engineering task, which include standard compliant work products. An argumentation method is needed that accompanies the process and is able to deal with the complex linkage between these individual artifacts. In order to come up with a versatile approach, being capable of dealing with a broad range of complex systems and processes, this method must be structured, modular and scalable.

For the identified problem, the following solution is proposed. Argumentation patterns and matching guidelines are defined and shall accompany the development process. They highlight the relationship between the development process and its related argumentation in an understandable way. A clear relationship between process- and product-based argumentation should be established in order to avoid systematic faults in the line of argumentation. A structured approach that offers a clear view on all present relationships will be easy to use and saves time and costs. The Goal Structuring Notation (GSN) [2] is defined for the construction of versatile arguments. In terms of ISO 26262 GSN helps to establish a valid relationship between evidence and safety requirements. Argumentation pattern should be elaborated to support corresponding artifact types. Process- and product-based argumentation is used together to compile a conclusive safety case.

III. Background and Related Work

A. Automotive Functional Safety - ISO 26262

ISO 26262 is the basis for development of safety-critical products in the automotive domain. It demands evidence to show that the established processes perform appropriately. ISO 26262 defines the "Automotive Safety Integrity Level" (ASIL) as a risk classification parameter for safety-critical hazardous situations. This is an important parameter and prescribes minimum efforts to be taken for all subsequent safety activities in the safety life cycle. The safety life cycle is defined, but ISO 26262 presupposes that special quality standards like Automotive SPICE [3] are fulfilled. An established quality level for processes is the basis for functional safety activities. Requirements in ISO 26262 expect various confirmation measures such as reviews (e.g. review of the safety analysis), audits (e.g. functional safety audit) and assessments (functional safety assessment). To pass these confirmation measures, it is beneficial if all necessary arguments are available without expenditure of time.

A very important topic in context of ISO 26262 is the elaboration of a safety case. It defines a safety case as "*the compilation of all work products that are used as evidence to show that all requirements for an item are satisfied. […] The three principal elements are requirements, arguments and evidence*". Arguments explain the relationship between evidence and requirements (objectives). ISO 26262 does not provide detailed requirements concerning safety cases, even though distributed development is omnipresent in the automotive domain. ISO 26262 defines "Development Interface Agreements" (DIA) for clarification of the relationship between OEM and different suppliers (Tier x). DIA connects safety cases, if distributed development is performed.

If we have a look to other domains, it can be seen that safety cases are regarded as important and that they obtain a lot of attention. Depending on the context different stages of safety cases can be defined. The British "Office for Nuclear Regulation" [4] defines 11 principal stages in the life cycle of a nuclear facility. Kelly [7] defines three software safety cases based on the "MoD Defence Standard 00-55" [5] from the military domain.

In context of this paper the focus is on four stages which fit for automotive safety cases. They are explained in detail in section IV.A.

B. Quality Management - Automotive SPICE

Automotive SPICE is a quality development standard which is focused on improvement of development processes for software intensive systems. Automotive SPICE provides a process reference model which covers the entire product life cycle. The three belonging process categories are "Primary Life Cycle Processes", "Organizational Life Cycle Processes" and "Supporting Life Cycle Processes". They deal with all process aspects but functional safety aspects are only covered by referring relevant standards. A metric to assess process capability is part of Automotive SPICE. The quality of the process has to achieve at least the capability level "Managed process". With help of ISO 26262 safety and automotive related requirements are added to an Automotive SPICE compliant development process.

C. Process Line for Modeling of Process Elements

Safety-oriented Process Line (SoPL) [9], [10] defines a methodology which provides the opportunity to derive reusable standard compliant processes. The aim is to increase the number of reusable process elements. A process element is a representation of a specific standard compliant activity that includes roles, tasks, work products, tools and guidance. First relevant standards become analyzed and a standard compliant process model is build consisting of reusable process elements. The SoPL is able derive an executable project specific process tailored from a company specific process. The term „company specific" indicates that a pool of tools and methods has been defined to perform quality and safety related activities within the company. We use the SoPL as a basis for our work and extend this approach with safety argumentation methodology.

D. Modeling of Argumentation using GSN

GSN [2] is a graphical notation that can be used to document arguments. In GSN, an argument is defined as a series of connected claims. Strategy-elements are used to declare reasoning behind the connection between goals and sub-goals. Context-elements provide additional information to support a correct understanding of a specific argumentation part. Solutions are elements that support goals because they document pieces

of evidence. The relationship between GSN elements is documented in a graphical way using different linkage elements (arrows). The two types of linkage elements are 'SupportedBy' and 'InContextOf'. The former, represented by lines with solid arrowheads, indicates inferential or evidential relationship, the later represented as lines with hollow arrowheads, declares contextual relationships.

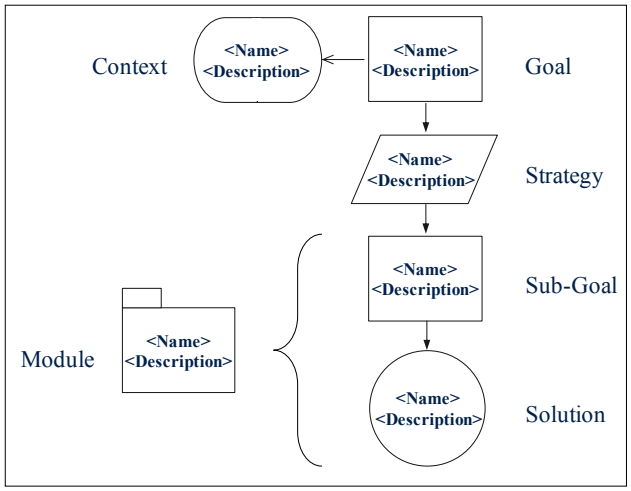

Fig. 1. Basic argumentation elements based on GSN standard

Modules are used to hide detailed structures and simplify goal structures to provide a general view. Between modules both types of linkage are possible. Furthermore, modules provide the opportunity to integrate argumentation from other sources if distributed development takes place and supports DIA of ISO 26262. Fig. 1. shows a simple goal structure for illustration. The angled brackets within elements represent metadata, in this case element <Name> and <Description>.

E. Related Argumentation Approaches

The following papers show a selection of different argumentation approaches, which investigate safety cases and argumentation topics. They emphasize the relevance to distinguish between process- and product-based argumentation in various ways.

The timely generation of well-focused safety cases is capable of bringing considerable benefit in the context of development and assessment and contributing to safety assurance of automotive E/E systems according ISO 26262. A process-based argumentation only renders the standard's implicit argumentation in a different form. Further argumentation is needed to provide a rationale argument for product-specific decisions during the development [13]. A process argumentation approach to generate process-based arguments from process models is shown in [11]. It reduces cost and time during certification process. Distinction between process- and product-based argumentation has been made in [14] but only product-based argumentation has been considered in detail. It deals with building of reusable safety cases and patterns.

The authors in [15] propose an integrated process- and product- based argumentation. Process-based arguments are backing arguments for product-based arguments to derive the safety case. The safety case development manual [17] provides guidance on the development of safety cases for the avionic domain. In this manual a clear distinction between product-based and process-based arguments is demanded since "the former is concerned with getting the right product and the latter with getting the product right."

IV. Methodology

The proposed methodology considers a company specific process which fulfills requirements from Automotive SPICE and ISO 26262. We show how to enhance the engineering process based on the SoPL approach by integration of safety argumentation modeling.

A. Definition of important Terms

To distinguish between process- and product-based argumentation, we introduce a categorization of work product as follows.

i.) Work products to prove capability and maturity of the development process (e.g. Project plan).

ii.) Work products to show compliance to ISO 26262. This type of artifact delivers proof that the defined process fulfils demanded safety aspects (e.g. confirmation review report).

iii.) Work products to ensure product safety. This type of artifact delivers product specific arguments which are needed in an assessment to show safety of the product (e.g. safety goals).

During the project life cycle, each of these work products goes through different stages of development. To ensure continuous argumentation throughout development, different states of work products must be considered. Therefore, the safety case should not be a final deliverable at the end of the project. To overcome this limitation, we introduce four stages of development based on [4] and [5] for the automotive safety case.

1. The "Preliminary Safety Case" is available after definition and review of the system requirements specification (functional safety concept is available).
2. The "Intermediate Safety Case" contains initial system design and preliminary validation activities. This type of safety case can be needed to get a permission to drive engineering prototype cars on public roads (cars are driven by professional drivers).
3. The "Pre-operational Safety Case" demonstrates that all necessary pre-operational actions have been completed, validated and implemented (basis for release for production).
4. The "Operational Safety Case" is available just prior to in-service use, including complete evidence of having satisfied the systems requirements (operational customer vehicle - field monitoring, maintenance).

Due to this variety of safety cases, it is necessary to have a systematic approach for their management. In this paper, we introduce such a systematic approach, which is applicable to all four stages. We focus on the first stage of the safety case exemplarily, the preliminary safety case.

B. Connect Standard Compliant Process and Argumentation

As shown in [10] a complete process takes aspects like functional safety and process quality into consideration. ISO 26262 formulates process requirements, which can be seen as a framework for tailoring. The direct derivation of a development process based on this single standard is not constructive. For the realization of an E/E system additional product specific standards have to be obeyed (e.g. EMC directive for hardware components, IEC 62660 for lithium-ion cells, etc.). Each supplier company determines its own priorities and way of engineering, and therefore defines its own specific development process. For that reason each process needs individual argumentation to prove standard compliance.

To ease the construction of an argument accompanying the development process, GSN argumentation patterns are used. A direct relation enables traceability between standards (e.g. ISO 26262, Automotive SPICE), process and argumentation (realized in GSN). This is important because traceability of arguments and requirements is a fundamental topic in current standards. If the arguments are provided in a systematic way, they are easy to comprehend and can be re-used by any stakeholder in a specific project. A good example thereof is field experience. In case of a cumulation of system failures in the field, the car manufacturer needs to take action. This likely requires engineers to comprehend design decisions which were made numerous product generations earlier.

Evidences in GSN argumentation structure are modeled as solution elements, which are directly process related. The name of a solution in development projects may differ from names used in the standard. For this reason work products designated standard compliant refer to outcomes created during process execution. The relation of product specific work products and standard compliant work products is given at any time.

C. Process- and Product-based Line of Argument

To deliver proof of functional safety for a defined development phase all requirements demanded by a standard (e.g. ISO 26262) have to be covered.

This section explains the difference between two types of argumentation, namely process-based and product-based argumentation. The proposed methodology defines each type of argumentation separately although they stay in direct relationship in the line of argument. Product development forces an established engineering process, supported by joint argumentation.

1) Process-based Argumentation

In case of process-based argumentation the arguments are directly associated with company specific processes which are derived from the Automotive SPICE process reference model as well as the ISO 26262 safety life cycle. Automotive SPICE contributes quality requirements which are presupposed by ISO 26262. During the process execution tools and methods which fit best are selected for a problem specific area of application. This selection leads to a project specific process. Process-based argumentation provides arguments to prove that the defined process fulfils demanded requirements. The argumentation is based on the existence of needed work products but not on their content. Usable work products are the types (i) and (ii) which have been defined in section IV.A. The approach in case of process-based argumentation is to document arguments, which support the process, in parallel with the process development. ISO 26262 demands functional safety audits to evaluate the implementation of the process and Automotive SPICE defines a quality assurance strategy to ensure the process quality. The process argumentation contains reasons why a particular process task has to be done in the described way. GSN elements like strategy and context are used to explain the decision why a goal splitting was done. Information about decisions is needed for process audits therefore it should always be documented. The GSN notation uses the possibility of unrestricted formulation to discriminate from the generic process and to emphasize arguments why the deviation is needed.

2) Product-based Argumentation

Within a generic formulated process a product specific decision determines a branch-off point. A decision based on a product specific requirement causes the necessity for different safety measures. For example, the development of a battery system requires different safety measures for battery packs with different capacity and different number of cells due to chemical and electrical issues. The safety measures are related to different software and hardware to manage the battery system. At that time the process becomes product-requirement-driven.

Product-based argumentation is elaborated based on content of available work products which are from type (iii) defined in section IV.A. With help of these work products it must be possible to establish an argument that the developed product is safe in terms of the relevant standards. Before project release for production a functional safety assessment has to be passed and arguments have to be prepared in a way that an external assessor can comprehend them. The focus of attention is to provide arguments why particular product related, technical decisions have been made and why specific methods or tools have been used.

D. Patterns - Development of reusable Artifacts

A pattern provides templates, guidance and formalisms to create goal structures for previously defined processes or products. The paper at hand uses definitions from [16] concerning patterns and templates and additional structural details of patterns which are defined in [6]. The most relevant attributes of patterns (based on [6]) are listed below:

- Intent of the pattern: What is the pattern for? (e.g. verification)
- Template: GSN argumentation structure used for implementation.
- Motivation: Scenario that supports the understanding (e.g. perform a complete verification)
- Applicability: Situations in which it can be applied (e.g. pattern is designed for HARA-verification in the automotive domain)

- Pitfalls: What possible pitfalls, hints or techniques should you beware of when using the pattern?
- Consequences: How does the pattern support its objectives? (e.g. pattern prevents users to make common mistakes)

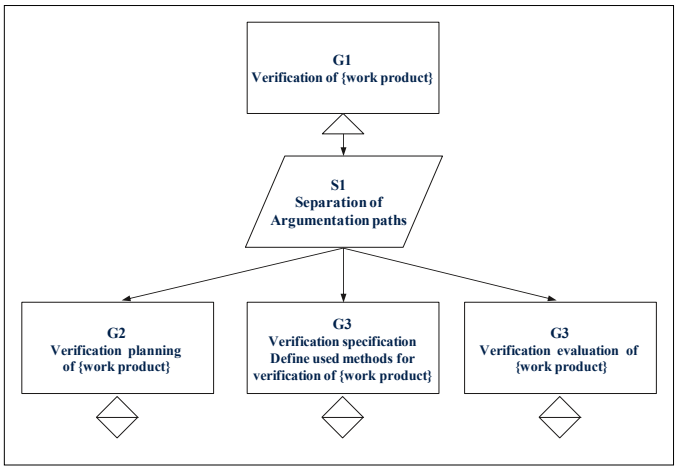

Fig. 2. Template for verification activity

The objective of patterns is to support standard compliant safety argumentation and best practices from previous projects. Additionally it should be designed to be extendable and adaptable based on lessons learned. Patterns assist users by providing predefined elements, which are adaptable for tailoring needs. The pattern is not present in the final argumentation.

The focus of considerations is mainly on the attribute "Template" which contains a chain of arguments. Templates are graphical representations, i.e. argumentation structures, which contain symbols as well as text and require instantiation. Templates are basically reusable for similar lines of arguments. The GSN community standard provides two types of abstractions that are usable in templates, "structural" and "entity". Structural abstraction supports the concept of multiplicity and optionality and entity abstraction which provides the notions "Uninstantiated (UI)" and "Uninstantiated and Undeveloped (UU)". A formal definition of these concepts is given in [8]. Graphical entities of GSN are annotated as uninstantiated, and may contain a textual expression in curly brackets to be replaced during instantiation. In templates the standard compliant name of a work product might be used as placeholder. The instantiation uses a project specific name. For illustration Fig. 2. shows a very generic template related to verification activities. Verification is split up to three activities which remain uninstantiated and undeveloped. The square at the bottom of the goals denotes that further development of the goals and instantiation of terms in curly brackets is needed.

A template is used twofold. The first aspect is related to decisions which are put into practice repeatedly whereby the line of argument is always identical. In this case instantiation is adding concrete project and evidence description. This use can often be found in connection with process argumentation (e.g. for the process to argue a HARA). The second use is when aspects of the product differ. In this case the provided templates have to be instantiated before they are applied (e.g. variation of product specific parameters).

E. Workflow for Introduction of Methodology

To introduce the proposed methodology to an engineering project, we define the following three sub-sequent phases which are shown in Fig. 3. .

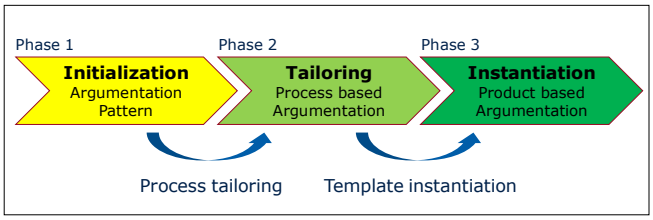

Fig. 3. Phases to create process- and product-based arguments

Phase 1 - Initialization of Development Process. The initialization phase is used to prepare all needed process elements to design a complete standard compliant development process. Activities in this phase are selection of relevant standards as well as identification of existing process and argumentation patterns which are suitable for reuse. The company specific process and the accompanying argumentation pattern are outcomes of this phase.

Phase 2 - Tailoring for process-based Argumentation. The tailoring from the company specific process to the project specific process means that process elements are selected to form the project specific development process. This selection includes the corresponding argumentation templates provided by patterns as well as methods and tools which should be used in the project. Creating a project specific process deals with decisions and judgments dependent on ASIL and needs expert knowledge. Process-based argumentation is needed for functional safety audits.

Templates are able to support process developers. They are used in two different cases. The first case provides arguments for repeatedly used generic process activities. This means, templates are available, which provide arguments that process requirements are fulfilled. In other words the template is included in the safety argumentation without changes. High level goals in a project are very similar to the company specific argumentation (e.g. the process for a HARA is quite similar in different projects). In the second case templates have to be instantiated because the project specific development process deals with activities beyond the template. This can occur if the process changes driven by a product or a customer demand. For example, one project uses HAZOP for hazard identification and in another project FMEA is required (see section V.B.) Fig. 4. shows an instantiated process template for HARA.

Phase 3 - Instantiation for product-based Argumentation. This phase covers product development by executing the project specific process. Templates for product-based argumentation support product specific decisions for a defined product. These decisions are made once and they are put into practice for a complete product line of battery systems. The generic

template provides argumentation which is typically valid for battery systems (e.g. specific physical parameters like voltage or temperature). The complete argumentation structure is achieved by instantiation of the template to product specific context. The demand of a complete safety case is the main reason to elaborate product-based arguments for functional safety assessment. With help of results documented in work products it becomes easy to argue that product specific claims are valid. This argumentation is done bottom up starting with results of the development process. Furthermore, it is important to have quick access to related evidence that proves a product is safe.

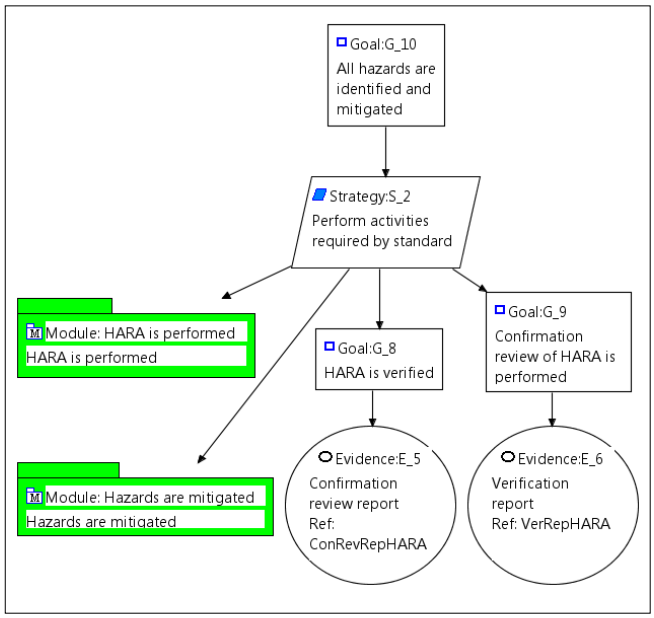

Fig. 4. Process-based argumentation for HARA (D-Case Editor)

V. Application to the Use Case

This section describes the application of the three phases (see Fig. 3.) in a concrete use case where argumentation modeling is implemented in the tool "D-Case Editor" [18].

A. Description of the Battery System Use Case

One major component of a Hybrid Electric Vehicle (HEV) powertrain is a High Voltage (HV) battery system. The current work focuses on the HV battery system for an automotive powertrain.

In the last decades, state-of-the-art technology is evolving and leading to the availability of various battery cell technologies with diverse characteristics (e.g. nickel-metal hydride, lithium-ion, and lithium polymer batteries). Some of the main targets for batteries for the HEV powertrain are low costs, high power density (e.g. >1200W/kg for HEV up to 250kW to support dynamic driving torques), very high cycle life time (e.g. >200.000 cycles of charge/discharge), high life time (e.g. >9 years), and safety. Safety becomes relevant because the power and energy density is increasing by decreasing of battery geometry, which leads to a potential increase of critical effects in the case of a critical malfunction [12].

The main functions of the battery system are providing electrical energy, storing/charging of electrical energy and electrical and thermal management. Based on these main functions potential safety-critical malfunctions can arise, e.g. overheating of battery cells, overcharging of battery cells and deep discharging of battery cells. These malfunctions could lead to following possible hazards: occurrence of high voltage, leakage of cell chemistry, toxic venting gas, fire and/or explosion.

Relevant data concerning the engineering process and safety aspects of the HV battery system was provided by the industrial project partner AVL. In the following section we show the first experimental results during the application of the proposed methodology.

B. Application of Workflow for Battery System Development

Application of the three subsequent phases defined in section IV is described in the following.

Phase 1- Initialization of Battery Development Process. The methodology is applied to develop a HV-battery system. ISO 26262 and Automotive SPICE are the standards which have to be considered in the regarded use case. The company specific process concerning the battery system is available. The argumentation patterns have been elaborated in parallel to the process. These patterns provide generic argumentation (e.g. HARA).

Phase 2 - Tailoring for Battery Development Process. The tailoring step derives the battery specific process and needed argumentation. Argumentation associated with the process is related to specific methods which have been selected (e.g. HAZOP for identification of hazards). The objective is to provide argumentation why HARA supports the goal that has to be achieved. Fig. 4. shows the argumentation concerning HARA starting with the goal "Hazards are identified and mitigated". The list below shows the four argumentation paths required by ISO 26262 for a functional safety audit concerning HARA:

- HARA is performed
- Hazards are mitigated
- Verification of HARA is performed
- Confirmation review of HARA is performed

The audited engineering process is ready for execution to develop a HV battery system.

Phase 3 - Instantiation for Battery System Argumentation. Fig. 5. shows exemplary the product-based argumentation concerning overheating of a battery system for a hybrid car. In particular it deals with the argumentation related to a hazard which has been identified in a HARA. The hazard and situation analysis has been performed, hazardous events have been defined and classified by S/E/C parameters and the ASIL is determined. For the hazard "Overheating of the battery system" ASIL C has been determined for all charging situations of the battery system. The safety goal "Prevent overheating of the battery system" has been derived from this hazard. Related to this safety goal the safety measure "Temperature monitoring" has been defined.

In this example the safety measure is visualized as "Strategy" which is connected to sub-goals. The identified sub-goals lead to functional safety requirements which support the safety goal at the top. The functional safety requirements are stored in the project specific file "HV_Batt_FSR". This file is linked to the ISO 26262 compliant work product "Functional safety concept". It represents the product specific argument that implementation of derived requirements prevents the battery system of overheating. The file contains the evidence for a functional safety assessment.

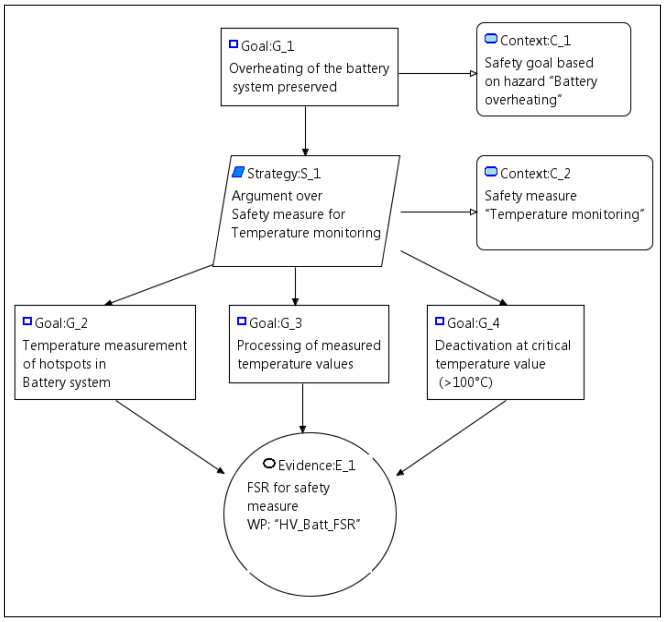

Fig. 5. Product-based argumentation for a battery system (D-Case Editor)

C. Evaluation Results

The application of the elaborated approach shows that the presented methodology is beneficial for safety case creation. Following benefits have been identified as results of evaluation.

- Argumentation patterns and the included structures accompany ISO 26262 and Automotive SPICE compliant processes.
- Traceability between argumentation goals and standard requirements is emphasized.
- Separation of process and product specific argumentation makes the methodology manageable and understandable.
- Reusable patterns and templates simplify argumentation and guarantee completeness.
- The elaborated argumentation structure reduces audit and assessment costs.
- The presented approach is usable for different stages of safety cases (see section IV.A).

VI. Conclusion and Future Work

This paper presents a methodology to create argumentation structures which are in direct relation to development processes and demanded requirements. The formalism deals with patterns and templates to make it easier to establish a complete understandable line of argumentation and prevents information loss. A workflow has been defined to introduce a methodology for process- and product-based argumentation. Project specific tailoring is used to create a standard compliant development process. Instantiation of templates provided by the engineering process leads to product specific safety argumentation. Application of the proposed workflow results in a complete and structured safety argumentation, which is needed for the safety case and supports functional safety audits and functional safety assessments. First experiences have been gained by successful application to an automotive battery use case to ensure compliance with ASPICE and ISO 26262.

As a next step, it is planned to evaluate tools that support GSN modeling. In cooperation with tool vendors of the EMC² project, existing tools will be enhanced to support the argumentation part of the presented methodology. In a long-term perspective it is intended to develop a tool which is able to support process development, process execution and process argumentation based on the proposed approach. A further aim is the extension of the methodology to cover security argumentation in a joint safety and security approach.

Acknowledgment

This work is supported by the EMC² project. Research leading to these results has received funding from the EU ARTEMIS Joint Undertaking under grant agreement n° 621429 (project EMC2) and from the COMET K2 - Competence Centres for Excellent Technologies Programme of the Austrian Federal Ministry for Transport, Innovation and Technology (bmvit), the Austrian Federal Ministry of Science, Research and Economy (bmwfw), the Austrian Research Promotion Agency (FFG), the Province of Styria and the Styrian Business Promotion Agency (SFG).

References

[1] International Organization for Standardization. "ISO 26262 - Road vehicles– Functional safety, Part 1–10." ISO/TC 22/SC 32 Electrical and electronic components and general system aspects, Nov. 15, 2011.

[2] Goal Structuring Notation Working Group, GSN Community Standard Version 1, Nov. 16, 2011, www.goalstructuringnotation.info [Feb. 05, 2016]

[3] VDA QMC Working Group 13 / Automotive SIG, Automotive SPICE, Process Reference and Assessment Model, Version 3.0, 2015, www.automotivespice.com [Feb. 05, 2016]

[4] Office for Nuclear Regulation, An agency of HSE, The purpose, scope, and content of safety cases, NS-TAST-GD-051 Revision 3, 2013, Available: http://www.onr.org.uk/operational/tech asst_ guides/ns-tast-gd-051.pdf, [Feb. 05, 2016]

[5] U.K. Ministry of Defence, Defence Standard 00-55, Requirements for safety related software in defence equipment, 1997.

[6] T. Kelly, J. McDermid, Safety case construction and reuse using patterns, In: Daniel, P. (ed.) Safe Comp 1997, 1997, pp. 55–69.

[7] T. Kelly, I. Bate, J. McDermid, A. Burns, Building a preliminary safety case: an example from aerospace, Australian Workshop of

Industrial Experience with Safety Critical Systems, Sydney, Australia, 1997.

[8] E. W. Denney, G. J. Pai, A formal basis for safety case patterns, 32nd International Conference on Computer Safety, Reliability and Security (SAFECOMP 2013), LNCS 8153, Sep. 2013, pp. 21-32.

[9] B. Gallina, I. Sljivo, O. Jaradat, Towards a safety-oriented process line for enabling reuse in safety critical systems development and certification, In Post-proceedings of the 35th Software Engineering Workshop (SEW-35), Oct. 2012.

[10] B. Gallina, S. Kashiyarandi, H. Martin, R. Bramberger, Modeling a safety- and automotive-oriented process line to enable reuse and flexible process derivation, 8th IEEE International Workshop Quality-Oriented Reuse of Software, July 2014.

[11] B. Gallina, A model-driven safety certification method for process compliance, 2nd International Workshop on Assurance Cases for Software-intensive Systems, 2014.

[12] H. Martin, A. Leitner, B. Winkler, Holistic Safety Considerations for Automotive Battery Systems, *Automotive Battery Technology,* Springer International Publishing, 2014, pp. 1-17.

[13] Birch, John, et al., Safety cases and their role in ISO 26262 functional safety assessment, *Computer Safety, Reliability, and Security*. Springer Berlin Heidelberg, 2013, pp. 154-165.

[14] S. Wagner, B. Schätz, S. Puchner, P. Kock, A case study on safety cases in the automotive domain: Modules, patterns, and models, In Software Reliability Engineering (ISSRE), 2010 IEEE 21st International Symposium on 2010, pp. 269-278.

[15] I. Habli, I. Ibarra, R. Rivett, T. Kelly, Model-based assurance for justifying automotive functional safety, In Proc. SAE World Congress 2010, 2010.

[16] Agusta Westland Limited, BAE SYSTEMS, GE Aviation, General Dynamics United Kingdom Limited and SELEX Galileo Ltd., 2012, Available: https://www.amsderisc.com/wp-content/uploads/2013/01/MSSC_203_Issue_01_PD_2012_11_17.pdf, [Feb. 05, 2016]

[17] European Organisation for the Safety of Air Navigation, Safety case development manual, Edition 2.2, 2006.

[18] Y. Matsuno, D-Case Editor: A typed assurance case editor, In Proceedings of the 13th Real Time Linux Workshop, Prague, Czech Republic, 2011.