CHALMERS | UNIVERSITY OF GOTHENBURG

Department of Computer Science and Engineering, Agneta Nilsson
Software Engineering Master Thesis Proposal, 30hec

Continuous maintenance of an ISO 26262 Safety Case

Yulla Ibrahim: *Completed courses relevant for thesis work: DIT276, DIT847, DIT278, DIT844, DIT191 & DIT598*

Mikaela Törnlund: *Completed courses relevant for thesis work: DIT276, DIT847, DIT278, DIT844, DIT191 & DIT598*

1 Introduction

In safety critical systems, it is important to provide extensive evidence that the product is up to safety standards. In most cases, this is expressed in a Safety Assurance Case (SaAC)(Hawkins, 2013). A top level approach is taken by decomposing safety requirements in order to prove and argue that a certain part of the system is safe. A SaAC includes and organizes claims, arguments and evidence (Bloomfield, 2010). A claim refers to a safety requirement that needs to be achieved in order to prove attained safety in that particular part of the system. Arguments express how the evidence provided satisfies those claims. Evidence usually consists of information in various shapes and formats. These formats can be, but are not limited to: test cases, reviews and safety concepts.

For automotive functional safety, in order to comply with appropriate safety standards, the ISO 26262 series of standards (ISO, 2018) are required to be met. The ISO 26262 is an instrument to secure that developed electrical and/or electronic (E/E) systems are safe. This means arguing that the system does NOT malfunction, causing unreasonable risk (Schildbach, 2018). SaACs in this environment are required to provide argumentation and evidence for the achievement of functional safety. In order to achieve this, the SaAC needs to progressively contain the ISO 26262 work products (e.g. functional safety concept, software verification reports) that are generated during the safety lifecycle (Luo et. al, 2019). A complete argumentation based on those work products must then be created in order to fully comply with the safety standards.

Even though the ISO 26262 on automotive functional safety requires full compliance, it does not include guidelines on how to create and develop the safety argumentation, nor how to evaluate the quality and completeness of a SaAC (Birch et. al, 2013).
SaACs have the potential to aid in the maintenance, consistency and support evolution of safety critical products. Therefore, it is vital to the success of a product from a safety perspective to be consistent with the changes in development but also to reflect the reality

of the product.

Attempts have been made in order to automate the creation of SaACs and to introduce traceability to the documents by keeping version control up to date over multiple sources (Agrawal et. al, 2019). While experiencing positive results in research, the adoption of these tools and practises in industry has not yet seen any promising results.

The goal of this study is to improve upon the consistency and traceability of SaACs in a practical, industrial setting. Consistency and traceability are two key attributes that are difficult to achieve using currently utilized workflows and methodologies in industry. By proposing a new model for creating and maintaining SaACs which benefits the two former attributes, a more streamlined and risk-averse workflow will be created for use in industry. Furthermore, a secondary goal of this study is to provide practitioners with more practical research that can be applied in industry.

2 Statement of the problem

Creating a Safety Assurance Case within an industrial setting is not a trivial process, as evidenced by the number of challenges identified in this area (Chen et. al, 2018). This study will focus on the industrial problems faced by Volvo Group Trucks Technology (GTT) as the main source of challenges faced in a real world environment.

Five key challenges will be addressed:

1) The first challenge directly involves the creation of the SaACs. As all the evidence artefacts connected to the safety claims and arguments are not found in one framework, practitioners face a considerable overhead when having to integrate with information sources that exist in a variety of formats and are spread over a number of tools, e.g. System Engineering Tools, SW/HW Development Tools, verification tools and release tools. Currently, practitioners at GTT are manually building their SaACs with a document-based approach in order to represent the safety case argumentation trees. This process has been deemed unsustainable and time consúming. Additionally, it is critical but complex to keep this document up to date as tracing changes in any artifact that affect the state of the SaAC is also achieved manually. This hinders the continuous validity of the SaACs. Nair et. al (Nair et. al, 2014a) have identified a multitude of evidence types in SaACs, 49 of which they call ‘basic evidence types’. This pose a great obstacle for any researcher or practitioner who wants to or has made attempts to facilitate and generalize the creation of SaACs.

2) The second challenge is connected to the maintenance of a SaACs, specifically the ongoing process that ensures the validity of the documents. A valid SaAC needs association links between a change and the impact of that change on the argumentations in the document. Change refers to a change in requirements, safety evidence or in design.

This implies that we need to have an ongoing maintenance of the safety arguments through-life in the SaACs (Denney et. al, 2015). This has continually been recognised by many safety standards. However, many safety engineers are experiencing difficulties with safety case maintenance. Since safety case documents contain highly interdependent elements even seemingly minor changes have the potential to have a major impact, dramatically increasing their cost. (Jaradat et. al, 2016)

3) The third challenge regards the difficulties that are faced to ensure consistency within SaACs. This study will focus on two types of consistency, internal and external. Internal consistency is achieved when all artifacts that are used to build the SaAC are up to date. This requires a version control check to keep track of the version(s) of the components that are currently in use and make updates upon a component change to ensure that the versions are compatible. External consistency ensures that a SaAC reflects the physical reality of the product, in regards to functionality and behavior. Any change should have a traceability link to the impact on the dependant safety argumentations. One major obstacle in maintaining these forms of consistency is that the information is spread out over different sources and in different formats.

4) The fourth challenge is addressing the ability to reuse safety artifacts internally within the same product and the ability to extend it to other products by generalizing some argument-fragments that include supporting evidence related to multiple SaACs. Efforts are being made in this domain in order to reduce the resources spent maintaining and updating argumentations across SaACs. Additional standards are beginning to acknowledge the need for reuse, the automotive (ISO26262) industry standards explicitly support notions that enable reuse, e.g., the notion of Safety Element out of Context (SEooC) within automotive (International Organization for Standardization (ISO), 2011). In this study we will make an attempt to find a practical application of reusability within SaACs to fit the industrial context of a real-world case.

5) The fifth and final challenge is to attempt to minimize the gap between theory and real-world practices. Issues regarding keeping SaACs consistent with products and other documents during the evolution of the product have been the focus of some initial research but have not yet been efficiently addressed (Chen et. al, 2018). Promising results have been found in research but they have not included the same number of variables as industrial projects attempting to adopt the same strategies. The conclusion of a number of experiments regarding consistency in SaACs is that there is a need for further investigation and tooling in order to deal with the different situations and variables that are present in industry (Chen et. al, 2018)(Nair et. al, 2014b)(Born et. al, 2010). As mentioned above, in industry, evidence for safety is found across multiple sources and in various formats. This is the main difference from research where work has been performed with a very limited amount of variables, especially formats. Practitioners experience the main obstacles in SaAC creation and maintenance particularly in keeping the relevant documents consistent, internally and externally, and the traceability of information across that same document. This is especially true in situations regarding changing requirements but also changes in the product under development. Consistency and traceability become

particularly difficult to attain in SaAC as they grow too large and the complexity increases (Chen et. al, 2018).

3 Purpose of the study

The purpose of this study is to improve SaAC creation and maintenance efficiency. Our aim is to propose a new solution that suggests a number of practices that could be applied in an industrial setting, especially at GTT. We will focus on ensuring internal and external consistency and providing the ability to manage change by introducing traceability in the context of continually changing artefacts.

Even though the focus of this study is on a specific industrial scenario, we aim to produce results that can be generalized in different real-world settings. Therefore, part of the study will address performance metrics that could be used in order to measure the effort of new maintenance activities applied to SaACs after implementing the new solution.

4 Review of the literature

In their paper regarding Dynamic Safety Cases (DSCs), Denney et. al (Denney et. al, 2015) discuss the issues regarding SaAC maintenance. In the many cases that have been examined, SaAC are made prior to the development of a product. Since agile development processes became widely used, development is more often than not conducted in a manner as to evolve the product and make changes after the initial planning is completed. SaACs created in this manner will rapidly be outdated and of little use in terms of assessing the safety of a system. There is a need for a new type of safety assurance that has the ability to continually assess the system and evolve the SaAC to stay consistent in light of change.

Birch (Birch, 2013) talks about the importance of SaAC creation as a process alongside the development process. Creating SaACs aids developers to identify issues or omissions of the safety arguments and evidence as early as possible in the development of the product. This is only possible if the SaAC is up to date and is being continuously updated in parallel to the development, keeping the SaAC consistent with the product.

Chen et. al (Chen et. al, 2018) interviewed practitioners regarding their obstacles and challenges working with SaACs. Scalability, lack of tool support, managing change and complexity were the main challenges they expressed. The automation tools available today either can not deal effectively with scalability or are too narrow, i.e. only comprise of domain specific features. There are no effective ways of dealing with changes in requirements nor in the product under development. The SaACs requires a considerable amount of skill to create, especially with complex systems. In a complex system, many parts are interconnected and hard to keep track of. This is true especially during change in the product or its requirements.

There are many sources discussing the need for automation and tooling (Maksimov,

2018)(Chen et. al, 2018)(Denney et. al, 2018). A number of tools have been developed in order to automate the creation and/or maintenance of SaACs. These tools possess different levels of accuracy and completeness in different aspects of the SaAC (Maksimov, 2018). Automation can be very useful in maintaining consistency, supporting evolution and saving time by minimizing effort in the creation of the SaACs. As creating SaACs is tedious work, it is important that this process is improved. (Denney et. al, 2018).

Nair et. al (Nair et. al, 2014b) highlights in their systematic literature review, that research has shown the need for traceability in SaACs. Some results have been produced in this area but limited attempts have been made to implement these in an industrial setting. Traceability in SaAC focuses on establishing relationships between artifacts and how they interact in light of change. This becomes more and more important as a system grows in size and complexity. A big part of SaAC traceability regards versioning of the current artefacts in use and keeping those versions up to date. There are many important traces that needs to be established in a SaAC. These traces are, but not limited to, those between the artefacts, between evidence and claims, between evidence and arguments and versions of a single artefact. Nair et. al. created a "Traceability Information Model for Safety Evidence" called SafeTIM. However, this model is still in need of additional tool support in order to simplify the adoption by industrial cases. The main challenges for enabling traceability in SaACs are that artefacts and evidence can be spread over multiple sources and locations, the sheer amount of artefacts can be overwhelming. This is especially true if the information is stored in different tools.

Born et. al (Born et. al , 2010) investigates a Model-based approach as an alternative to the traditional document-based approach in order to introduce automatic traceability to the SaACs. In order to produce a complete SaAC, it is necessary to establish the relationship between the different artefacts. In most cases, traceability is established with IDs that are added manually or semi-automatically which impose risk of errors. There are some tools available to automatically include traceability to some of the artefacts in these documents. IBM DOORS is one example of such a tool. However, these tools are not complete as traceability between all artefacts are a requirement in order to achieve sustainable traceability.

5 Research question

- RQ1: To what extent can we assure consistency of SaACs in an industrial setting?
    - RQ.1.1. To what extent can we ensure internal consistency in SaAC?
    - RQ.1.2. To what extent can we ensure external consistency in SaAC?

- RQ2: How can we implement traceability in SaAC to ensure consistency in light of change?
    - RQ.2.1: How can we identify components in a SaAC that has been affected by an occuring change?

- RQ.2.2: How can we update SaAC components that has been affected by a change in order to maintain a consistent SaAC?

In order to write concise and coherent research questions we have followed the guidelines in the paper written by Agee (Agee, 2009). Agee discusses the appropriate construction and wording of good research questions, the structure of the overarching questions and their sub-questions and how to clearly convey the purpose of the study.

6 The Design – Methods and Procedures

This thesis will be conducted in collaboration with Volvo Group Trucks Technology GTT. In particular with their Cybersecurity and Functional Safety department. Volvo Trucks is one of the largest heavy-duty truck brands in the world; with trucks sold and serviced in over 140 countries.

We will utilize the design science research (DSR) methodology (Hevner, 2004). The process of a design science research is an iterative approach that consists of a number of cycles. The name of these cycles in this particular method are called the 'regulative cycle'. Each one comprises of five phases: problem investigation, design candidate, validation, implementation and evaluation. When a cycle is complete, the generated output is used as input for the upcoming one (Wieringa, 2009).
This study is going to be distributed over two cycles, each dedicated to answer one of the two research questions.

Cycle One:

The first cycle will focus on addressing the challenges of creating and maintaining the SaACs that have been identified by Chen et. al (Chen et. al, 2018). We will address issues regarding consistency (internal and external) faced by practitioners when creating and maintaining SaACs. The goal of this cycle is to answer RQ1 and provide results that have the ability to provide input in answering RQ2.

The first cycle will comprise of the following phases:

Problem investigation:
In this step we will focus on the problem of implementing theoretical solutions in an industrial setting. We will further explore the issues that are faced by practitioners and identify what tools and practises that have been attempted or utilized up until now at GTT. Targeting and assuring consistency is the main focus of this cycle, therefore the problem identification will be focused on the first research question.

Design candidates:
Based on the understanding of the problem, we will develop initial prototypes. An investigation will be conducted into the Model-based approach proposed by Born et. al (Born et. al , 2010). It is a promising alternative to the traditional document-based

approach that is utilized at GTT today which has a strong reliance on Microsoft Word. While we investigate the model-based approach, we will not be limited to this proposed solution. Further investigation into alternative solutions shall be conducted in order to generate a candidate that addresses the goals and is feasible in an industrial setting.

Validation:
The design candidates will be validated against the issues stated in the problem investigation of this phase. We will evaluate which candidate has the highest potential to solve the problems faced in industry and that also possess promising insights in how to reduce the effort and time consumption to manage a constant SaAC

Implementation:
In this phase, the validated design candidate will be further developed into an initial version of our solution. This will be performed in close collaboration with the case company in order to receive aid in what direction to pursue but also to receive rapid feedback on our progress. The solution will be comprised of a set of strategies and tool(s) in which the aim will be to enable consistency in SaAC.

Evaluation:
An expert evaluation will be conducted with practitioners of SaACs and experts in function safety at the case company. Additionally, GTT will contribute with a pilot SaAC to undergo evaluation and act as a baseline for comparing the output SaAC of the proposed methodology.

Cycle 2:

This cycle is dependent on the output from the previous cycle. Our aim is to generate an improved solution based on the evaluation and identified problems that arise from the first cycle. Additionally, we will include a number of activities focusing on providing a solution to the traceability problem in SaACs as stated in RQ2. The goal is to generate one solution connecting consistency and traceability to provide a final solution applicable within GTT. A recommendation report detailing an implementation strategy will be generated for the practitioners in GTT to apply within an industrial setting.

The second cycle will comprise of the following phases:

Problem investigation:
Alongside the problems that arise from the previous cycle in regards to consistency, we will also focus on the traceability of SaACs. By working closely with practitioners in GTT, we will identify components that are affected by change and categorize them based on the type of change that occurred. The aim is to construct a process for managing SaACs by creating live links between components that will be affected by a change.

Design candidate:
Based on the result from the previous step, we will develop design candidates for the final solution model. We will make an attempt to improve the generated solution from the first cycle. The design candidates will be generated based on feedback from participants at GTT and the current research results regarding combining consistency and traceability features in the target solution for SaAC.

Validation:
The validation of the design candidates will be conducted based on their ability to answer our research questions both RQ1 and RQ2.

Implementation:
Based on the results from the validation phase, we will generate two components in our study:

1. A prototype SaAC.
2. A recommendation report: a guide detailing an implementation strategy for future creation of SaACs at GTT.

Evaluation:
The final solution will be evaluated against the research questions of this study. Additionally, practitioners at GTT will provide their feedback of the solution's applicability in an industrial settings.

7 Limitations and Delimitation

Limitations:
The main limitation of the study is that GTT does not, as of today, have any completed SaACs to evaluate our solutions against. However, the company has started the process of creating SaACs in ongoing projects. These ongoing projects will be of benefit to the evaluation process as we can use them as a pilot for verifying our output. Further evaluation will be done using the expert evaluation method. Gathering people with extensive knowledge in SaAC creation and neighboring areas will enable us to evaluate our generated solution.

- **Internal validity:** Due to time constraints and the long process for each new product at GTT, we will be unable to utilize our solution on a product within the company during the time period of our study. Although our results will undergo expert evaluation in order to measure the success of our findings, the remaining work after this study is to apply our findings in an actual project to ensure that the desired outcome is achieved.
- **External validity:** We will make an attempt to generalize the results. However, since this thesis is limited to one company it may be that the results will be specific to the case. The results will be connected to the systems and structures used at the company at hand. However, we will provide information on a higher level on how

to reproduce and take part of our findings in other projects independent of setting and structure.

Delimitations/Scope:
We narrow down our study by focusing on how to ensure consistency and traceability of SaACs. Our solution will not evaluate if the SaAC is complete but rather that it is up to date with the information provided. An attempt will be made to generate a set of strategies in order to provide solutions regarding consistency and traceability when creating and maintaining SaACs. The study will focus on one specific company. This will confide us to the structure and limitations they adhere to in terms of safety case creation and maintenance.

8 Time Plan

This section provides a roadmap and initial milestones for this study:

Feb 2020 - Mar 2020 : Cycle One
Feb 2020:
Literature review. Gain an in depth understanding of the problem domain and the solutions created.
Begin conducting the first cycle at Volvo GTT.

Mar 2020
Complete the first cycle at Volvo GTT.
Evaluate the outcome at Volvo GTT and document the results.
Begin further literature review to help guide improvements in the second cycle.

Apr 2020 - Jun 2020 : Cycle Two
Apr 2020
Complete further literature review.
Conduct the second cycle.
Evaluate the outcome at Volvo GTT and document the results.

May 2020
Write a paper for publication
Feedback and polishing phase
Drafts ready and sent to supervisor, opponent and examiner
Complete, preliminary thesis

Jun 2020
Final presentation of the thesis, exam.
Final report, polishing.

9 Significance of the study

Our study aims to make an attempt to minimize the gap between the progress made in research and the difficulties of adopting those strategies in an industrial setting. There are a number of problems when translating the theoretical solutions into practical strategies which we will make an attempt to facilitate.

The main issues in SaAC creation and maintenance experienced by practitioners are related to consistency and traceability. Even though there are studies available which have generated promising results, they do not translate well into an industrial setting. When attempts have been made to implement those solutions in industry, the consensus is that the unique variables and scenarios present in real-world industrial scenarios are not considered in currently available research.

10 References

Hawkins, R., Habli, I., Kelly, T., & McDermid, J. (2013). Assurance cases and prescriptive software safety certification: A comparative study. Safety science, 59, 55-71.

International Standardization Organization (2018). https://www.iso.org/obp/ui/#iso:std:iso:26262:-2:ed-2:v1:en pp. 5–6.

Luo, Y., Saberi, A. K., & van den Brand, M. (2019). Safety-Driven Development and ISO 26262. In Automotive Systems and Software Engineering (pp. 225-254). Springer, Cham.

Schildbach, G. (2018). On the application of iso 26262 in control design for automated vehicles. arXiv preprint arXiv:1804.04349.

Bloomfield, R., & Bishop, P. (2010). Safety and assurance cases: Past, present and possible future–an Adelard perspective. In Making Systems Safer (pp. 51-67). Springer, London.

Birch, J., Rivett, R., Habli, I., Bradshaw, B., Botham, J., Higham, D., ... & Palin, R. (2013, September). Safety cases and their role in ISO 26262 functional safety assessment. In International Conference on Computer Safety, Reliability, and Security (pp. 154-165). Springer, Berlin, Heidelberg.

Denney, E., & Pai, G. (2018). Tool support for assurance case development. *Automated Software Engineering*, *25*(3), 435-499.

Denney, E., Pai, G., & Habli, I. (2015, May). Dynamic safety cases for through-life safety assurance. In *2015 IEEE/ACM 37th IEEE International Conference on Software Engineering*(Vol. 2, pp. 587-590). IEEE.

Maksimov, M., Fung, N. L., Kokaly, S., & Chechik, M. (2018, September). Two decades of assurance case tools: a survey. In International Conference on Computer Safety, Reliability, and Security (pp. 49-59). Springer, Cham.

Agrawal, A., Khoshmanesh, S., Vierhauser, M., Rahimi, M., Cleland-Huang, J., & Lutz, R. (2019, May). Leveraging artifact trees to evolve and reuse safety cases. In Proceedings of the 41st International Conference on Software Engineering (pp. 1222-1233). IEEE Press.

Chen, J., Goodrum, M., Metoyer, R., & Cleland-Huang, J. (2018, May). How do practitioners perceive assurance cases in safety-critical software systems?. In Proceedings of the 11th International Workshop on Cooperative and Human Aspects of Software Engineering (pp. 57-60). ACM.

Nair, S., De La Vara, J. L., Sabetzadeh, M., & Briand, L. (2014b). An extended systematic literature review on provision of evidence for safety certification. *Information and Software Technology*, *56*(7), 689-717.

Nair, S., de la Vara, J. L., Melzi, A., Tagliaferri, G., De-La-Beaujardiere, L., & Belmonte, F. (2014a, April). Safety evidence traceability: Problem analysis and model. In International working conference on requirements engineering: Foundation for software quality (pp. 309-324). Springer, Cham.

Born, M., Favaro, J., & Kath, O. (2010, April). Application of ISO DIS 26262 in practice. In Proceedings of the 1st workshop on critical automotive applications: Robustness & safety (pp. 3-6). ACM.

Crnkovic G.D. (2010) Constructive Research and Info-computational Knowledge Generation. In: Magnani L., Carnielli W., Pizzi C. (eds) Model-Based Reasoning in Science and Technology. Studies in Computational Intelligence, vol 314. Springer, Berlin, Heidelberg

H. J. Holz, A. Applin, B. Haberman, D. Joyce, H. Purchase, and C. Reed.(2006) Research Methods in Computing: What are they, and how should we teach them? ACM Special Interest Group on Computer Science Education (SIGCSE) Bulletin,

Agee, J. (2009). Developing qualitative research questions: a reflective process. *International journal of qualitative studies in education*, *22*(4), 431-447.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. MIS quarterly, 75-105.

Wieringa, R. (2009, May). Design science as nested problem solving. In *Proceedings of the 4th international conference on design science research in information systems and technology* (p. 8). ACM.

Jaradat O., Bate I. (2016) Systematic Maintenance of Safety Cases to Reduce Risk. In: Skavhaug A., Guiochet J., Schoitsch E., Bitsch F. (eds) Computer Safety, Reliability, and Security. SAFECOMP 2016. Lecture Notes in Computer Science, vol 9923. Springer, Cham