CHALMERS | UNIVERSITY OF GOTHENBURG

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

<Title of your thesis work>

Sarosh Nasir: *Completed courses relevant for thesis work: DAT220, DAT231, DIT201, DAT246, ...*

Vamsi Ravi: *Completed courses relevant for thesis work: DAT220, EDA397, DAT246, DAT231 & TDA594*

Academic Supervisor: *Mazen Mohamad, Jan-Philipp Steghöfer*

1 Introduction - help

An introduction provides readers with the background information for the research proposed (or reported in the paper), with the purpose to provide an understanding of how the research is related to other research (Wilkinson 1991). In an introduction, the writer should (Creswell 2002):

- Create reader interest in the topic
- Lay the broad foundation for the problem that leads to the study
- Place the study within the larger context of the scholarly literature
- Reach out to a specific audience

With the new standard ISO/SAE 21434 on Road Vehicles Cybersecurity Engineering is under development[1], the need for security assurance cases is now becoming more apparent for companies in the automotive industry. Modern day automotive vehicles have moved on from traditional mechanical connections in vehicles to using more computer-controlled systems with sensors to introduce systems such as adaptive cruise control and self-steering. This progress in the automotive industry has been going on for a couple of decades now to the point where we've gone from systems working offline (private networks) to now having connected cars where they rely on real-time networking. This puts the risk of cyber attacks at a higher degree and there has not been as much progress into making assurance cases for claims about security, particularly in regards to cybersecurity. Although there is a lack of using SACs in the industry, there has been a lot of research done into how to approach the creation of SACs in different domains, including automotive development processes (ADPs).

Security assurance cases (SACs) are structured bodies of evidence that support claims about systems with the use of arguments. While this does sound similar to assurance cases,

[1] https://www.iso.org/standard/70918.html

security assurance cases are specialized in cyber security. The cases take a top-level approach where a claim about a system is set and is supported by objective arguments and evidence to support the claim, not to mention that top level claims can also be supported by sub-claims. Creating an SAC is no simple task though, especially when working with large complex systems such as the systems in automotive vehicles. [SAC example here?]

The goal of this study is to construct two artifacts that improve upon the knowledge about SACs and one artifact that aims to support practitioners in monitoring SACs. The first artifact will be in the form of a library that will hold valuable data about SACs in the scope of ADP. This library will assist practitioners when constructing SACs and exploring SAC approaches. The second artifact will provide insight to researchers and practitioners about the gap between industry and research in the same scope as before, ADP. Lastly, the final artifact will be a proof of concept support tool which will aim to let practitioners monitor continuously updating SACs.

2 Statement of the problem - help

The statement of the problem is the foundation for the construction of any research proposal. In addition to being an integral part of selecting a research topic, it also helps to select research design. It serves as the bases for determining research objectives, formulation of research hypotheses or research questions, and planning the research design (Booth et al 2003). It allows the researcher to describe the problem systematically, to reflect on its importance, its priority and to point out why the proposed research on the problem should be undertaken.

A problem might be defined as the issue that exists in the literature, theory, or practice that leads to a need for the study. It is important in a proposal that the problem stands out and that the reader can easily recognize it.

- A problem statement should be presented within a context, and that context should be provided and briefly explained, including a discussion of the conceptual or theoretical framework in which it is embedded.
- Clearly and succinctly identify and explain the problem within the framework of the theory or line of inquiry that supports the study.
- State the problem in terms intelligible to someone who is generally sophisticated but who is relatively uninformed in the area of your investigation.

Effective problem statements answer the question: Why does this research need to be conducted? If the writer is unable to answer this question clearly and succinctly, the statement of the problem will be perceived as vague and diffuse.

During an automotive development process, a lot of artifacts are created. These artifacts can be used to create arguments and evidence of SACs. Examples of such artifacts could be controls (mitigation strategies) to vulnerabilities found in the system or assets of value in an automotive system. This study aims to provide valuable artifacts about Security Assurance Cases in the scope of automotive development processes for practitioners as well as SystemWeaver, a product manufactured by Systemite.

Problem 1

Currently, there is no online documentation of artifacts created during an automotive development process making it difficult for practitioners to keep track of the artifacts that exist and potential artifacts that will be created. Systemite has identified this challenge and thus this is something that we aim to resolve: to identify and collect the evidence artifacts involving the creation of SACs into one place, a library, to be integrated into SystemWeaver.

Problem 2

There is an obvious gap between research and real-world practice in the approach to create SAC. This is clear to us by the amount of papers that exist about SACs but the lack of SACs used in the industry (Mohamed et al. 2020a).

Problem 3
Support tool - not a problem but rather a challenge

Can statements about creation of SAC be taken from 'Continuous maintenance' paper? For example the fact that currently, practitioners are manually building SACs with a document-based approach. Does Systemite feel the same way?
This thesis feels similar to the proposal about "Continuous maintenance of an ISO 26262 Safety Case".

3 Purpose of the study - draft

The purpose of this study is to improve upon the existing knowledge of creation of SACs, and investigate a scenario where it could be used in the real world. Our aim is three-fold, where we (1) create a library to hold information on the creation of SACs, (2) investigate the gap between research and industry in regards to SAC approach, and (3) investigate and construct a proof of concept support tool for SACs which could be applied in an industrial setting, especially at Systemite. The gap analysis will have its focus on suggested approaches in literature versus automotive industry in the scope of automotive development processes (ADP).

The library constructed in (1) will be used to build the support tool for the practitioners at Systemite. Additionally, the support tool will be used to monitor continuously updating

SACs in real-time. Even though the focus of this study will be in the automotive domain, namely automotive development processes, we hope to produce results that can be generalized in other real-world settings.

4 Review of the literature - draft

In a systematic literature review (SLR) called Security Assurance Cases - State of the Art of an Emerging Approach (Mohamad et. al, 2020a), Mohamad et al. discuss the importance of Security Assurance Cases by doing an in-depth analysis and comparing 51 research papers. This study was conducted due to the momentum that SAC has gained in recent years, as well as the importance of being able to follow security standards and regulations. Based on the results of this systematic literature review, a workflow is created for working with SACs which is a useful tool for practitioners and also provides guidelines on how to approach SAC from the point of view of literature. The authors propose a workflow that consists of different stages involved in creating security assurance cases and provide relevant papers to each stage. Furthermore, the results of the SLR showed that there's a gap between usage scenarios and approaches of SACs in literature and their applicability in the real world.

Mohamad et al. (Mohamad et. al, 2020b) analyses and discusses the requirements to use security assurance cases in the automotive domain in the paper Security Assurance Cases for Road Vehicles: an Industry Perspective. The study was conducted in collaboration with one academic institution, two original equipment manufacturers (OEMs), and stakeholders to identify the internal organisational needs and opportunities for adopting SACs. Based on their observations, the authors have translated the results into a number of pragmatic recommendations for OEMs. Although, these recommendations are not complete solutions but rather provide a ground to integrate SAC with the company's way of working and help different stakeholders to make use of SAC. While the industry still lacks in using sound methodology to create SACs, this study has investigated the external constraints and internal needs that security assurance cases have to satisfy in the context of the automotive domain. The outcomes of this study will help us to analyse the constraints for phase two.

When snowballing the SLR, the study found that 26 of the studied literature suggested GSN notation as the most common notation in representing arguments. (Spriggs et. al, 2012) (GSN) introduces notations. The study gives an overview of how assurance cases are defined by GSN standards. The author describes GSN notation as (1) Claim (also called goal) (2) Context (3) Strategy (4) Assumption (also called justification) (5) Evidence (also called solution). Each node is crucial for the creation of a successful SAC. Finally, the author discusses each node and how they are defined with respect to SACs. This will be helpful to understand the nodes and their purpose, as well as get a better understanding of the topic.

Another paper of interest to us is the Asset-driven Security Assurance Cases with Built-in Quality Assurance by Mohamad et al.[2] This study demonstrates about developing

[2] Paper is accepted and will be published in June 2021.

CASCADE, the asset-driven approach for creating SACs. Being asset-driven means the resulting SACs will have assets as the drivers of the structure of the security arguments. This allows in creating security assurance based on what is valuable in the system. The study also mentions integrating quality assurance in SACs created with CASCADE by differentiating between product-related claims and quality claims, as well as building arguments for them. The authors describe an approach as (1) Top claim (2) Generic sub-case (3) White-hat block (4) Black-hat block (5) Resolver block (6) Evidence (7) Case quality assurance. Each block contains certain levels, for instance, black-hat blocks need to identify threat scenarios and attack paths in order to fulfill the block. The researchers found that quality assurance of SACs is missing in reported approaches in literature. Additionally, they identified that the lack of industry involvement is a significant issue in current approaches.

5 Research question and/or Hypotheses - draft

This thesis will aim to answer the following three research questions.

RQ1. Which artifacts are created during an automotive development process that can be used in Security Assurance Cases?
   a. What are the assets, vulnerabilities, and controls which can support the creation of SAC arguments?
   b. What evidence exists that can support the claim of the arguments?

RQ2. To what extent do these artifacts cover the needs in the approaches suggested in literature?

RQ3. To what extent can security assurance cases be created and maintained as a continuously updating document?

For RQ1, we aim to create a library for assets, vulnerabilities and controls (mitigation strategies) in the scope of cyber security in the automotive development processes that will be open and maintainable over time, which will lead us into RQ2. However, by itself it should be a source of knowledge for safety-critical industries (e.g., automotive).

In RQ2, an investigation will be done on the gap between literature and industry. In particular, how the approach of SACs is being suggested by researchers and to what extent the automotive development process covers the needs of the suggested approaches. With new standards coming out, this investigation will provide insight into whether the approaches suggested today need to be modified to fulfill the requirements set by the new standards.

Finally, in RQ3, we aim to create a proof-of-concept support tool. The support tool will provide a library (constructed in RQ1) on SACs in the scope of cyber security in automotive development processes in order to monitor continuously updating SACs.

6 The Design – Methods and Procedures - draft

The structure and procedure of the thesis project will be split into three phases. Each phase will use the design science research methodology by Hevner et al, using the model by Vijay Vaishnavi and Bill Keuchler (Vaishnavi et. al, 2004).

Phase One - Research Question 1

This question not only focuses on identifying artifacts in the automotive development process that can be used for creating SACs, but also the creation of a library that can hold information regarding those artifacts. An artifact in the automotive development process is an artifact in an automotive system that can be used to create arguments and evidence of SACs. The examples of these artifacts can be assets of value to the automotive company, vulnerabilities, and controls (mitigation strategies). Additionally these artifacts include evidence to support the claims of an argument in an assurance case, such as analysis and testing reports.

The structure of the Design Science methodology is planned as follow:
Awareness of the problem: Here we focus on understanding the current state- and the challenges of creating SACs in the automotive development processes, documenting the artifacts we find along the way. We have the SLR by (Mohamad et. al, 2020a) and the standards UNECE WP.29 GRVA and ISO/SAE 21434 (under development) that will assist us in this problem awareness step. Additionally, we will be working in collaborating with Systemite to learn about the practical work involved. For this, we plan to use interviews and focus groups as an additional source of data.
Suggestion: When current state and challenges are better understood, we still start to build a provisional design of a library that will hold the data about artifacts gathered in the previous step. We plan to collaborate with Systemite in this phase as well in order to gather possible necessary requirements for the library as the library is planned to be integrated with their product SystemWeaver. Here, focus groups will be used more to gather data.
Development: In this step, the artifacts identified will be categorized and translated into a structure that conforms to the structure and design of the library. After which we will further develop and implement the tentative library design into an artifact. Systemite will be involved to assist in the development to some degree.
Evaluation: The evaluation of the artifact created will be conducted by subject matter experts at Systemite after the library has been implemented and is in a stable state. The evaluation will consider what was mentioned in "*awareness of the problem*".
Conclusion: After the evaluation is conducted and results are documented, we will be able to conclude our work, answer the research question and move on to phase two.

Phase Two - Research Question 2

This phase focuses on doing a gap analysis by identifying the gap between literature and the industry. We will be looking into two aspects of this: (1) What are the suggested approaches in literature when creating SACs and (2) How well the automotive

development processes (ADP) cover the needs of the approaches suggested in literature. The artifacts that will be considered here will be those identified in RQ1.

The planned structure of the Design Research methodology is as follows:
Awareness of the problem: In this step we will focus on investigating the aspects (1) and (2). We will explore literature reviews by looking at current approaches that have been suggested in ADPs. The starting point for this step will be the Industry Perspective by (Mohamad et. al, 2020b) that points out the external constraints and internal needs that SACs have to satisfy in the context of the automotive industry. By collaborating with Systemite, we will get insight into the industry perspective in terms of how well the artifacts created in the ADP fulfill the needs of the suggested approaches in literature. We plan to use interviews and focus groups to gather data from Systemite and its customers.
Suggestion: When the problem is well understood, we will start to analyse the existing approaches from literature studies and come up with a preliminary plan as to how to modify those approaches if needed. Additionally, we will also look at the gap from an ADP perspective, in terms of artifacts created in the ADP versus artifacts required by the suggested approaches in literature.
Development: In this step, we will implement the identified modifications to suggested approaches, as well as document the gap between industry and literature in the scope of ADP as artifacts.
Evaluation: The evaluation of artifacts identified will be conducted by subject matter experts at Systemite and their customers. The evaluation will reflect what was mentioned in the *"awareness of the problem"* step.
Conclusion: After the evaluation is conducted and results are documented, we will be able to conclude our work, answer the research question, and move on to phase three.

Phase Three - Research Question 3

The focus for this phase is to develop a proof-of-concept support tool based on the artifacts created during ADP that can be used in creating SACs. Since this is a proof of concept, the approach will be of the exploratory kind where we will investigate the possibility and approaches to such a support tool. The main objective for the support tool will be to make it work as a tool to monitor continuously updating SACs in real-time. We will work closely with Systemite to gather the requirements for the prototype.

The planned structure of the Design Research Methodology is as follows:
Awareness of the problem: This phase will focus on the challenges of a support tool that will allow subject matter experts to monitor continuously updating SACs. That is, to see the status of a SAC and be notified if there's anything amiss in real-time. The support tool will most likely be a kind of web service. Additionally, we will investigate possible system architectures for this service, as it's planned to be integrated with SystemWeaver. We plan to use interviews and focus groups to gather the data and requirements for this support tool (database, web framework, etc).
Suggestion: When the challenges have been identified, we will build a tentative design for the support tool and the system architecture. The library artifact constructed in RQ1 will be the data source. We plan to use focus groups in this step to gather feedback about the initial designs of the tool and architecture.

Development: The tentative designs constructed in the "*suggestion*" step will be further developed in this step. We will consider the system architecture design as well and attempt to make a stable first prototype of the designs.
Evaluation: After the design has been stabilized, the evaluation will be conducted by subject matter experts at Systemite.
Conclusion: We will be able to conclude our work on this prototype once the evaluation has been conducted. We will gather the results and answer our research question.

7 Limitations and Delimitations - draft

Limitations

The main limitation is that we rely heavily on literature as the main source of data and some data will be gathered via interviews and focus groups. We also don't know whether we will be able to have interviews about this topic with actual practitioners in the automotive industry. Although, we do have Systemite which has experts that have been working with security assurance cases in their product SystemWeaver. Thus, we rely on them to give their expert evaluation on the artifacts produced in this study.

To identify possible internal and external validity threats, we looked at Experimentation in Software Engineering by (Wohlin et. al, 2012).

- **Internal validity:** As the only subjects we will have during our research are subjects of interviews and focus groups, we believe if there is a threat to internal validity it would there. Of course, we won't know about our subjects until we actually prepare for the interviews and focus groups, therefore we can say that there's a possibility of single group threats, such as *maturation* where the subjects react differently as time passes (if the subjects are bored/tired vs interested), as well as *testing* where the subjects respond differently at different interviews/focus groups as they know how those will be conducted. In that sense, any sub-threat under single group threat can be considered here.
- **External validity:** We will make an attempt to generalise the results. However, as the thesis is limited to one company, results will be specific to one case which raises the concern of *interaction of selection and treatment* where the subject population does not represent the population we want to generalize. This will be completely based on the company's organisational structures and development processes which may not cover all the aspects in general. We would make sure to evaluate the results with other companies in the automotive industry, such as Systemites customers, to make sure the results are reliable. Another validity threat is that we will only be looking at a set of approaches in our research for RQ2, which affects the reliability of the results as they don't consider enough approaches to be reliable. What we can do to mitigate this is to select a set of approaches that can represent a generalization for the majority of the approaches that exist. In this way, although it's only one or two approaches, they are a little bit more reliable.

Delimitations

Security Assurance Cases in the scope of cyber security is very large. We will not be looking into everything in that scope. Instead we will focus on the automotive domain, namely automotive development processes (ADP) due to the new standards on cyber security and automotive vehicles. Apart from the gap analysis, we will attempt to construct both a library for SAC creation and a proof of concept support tool for SACs in order to improve upon that existing knowledge on SACs and approaches and explore the gap between research and industry. The study will focus on gathering practical data from Systemite and their customers only. This will allow us to keep to their structure for SACs and approaches as most of the artifacts from this research will be used by them.

8 Significance of the study - draft

Our study aims to contribute with artifacts which are not apparent in research and in practice so far. Each research question will produce an artifact that we hope will extend and possibly refine existing knowledge about the creation of SACs in the scope of our thesis. The library artifact from the first research question will benefit both researchers and practitioners. The library provides a way for both parties to more efficiently look up components for creating SACs for their own respective purposes. This could be to identify, for example, what artifacts are of interest in an automotive development process during the creation of SACs

The main challenges in SACs creation is that there is an explicit gap between research and industry in terms of usage of approaches. Even though there are studies available about usage of different approaches, they do not translate well into the industrial settings of maintaining proper SAC documents. The second research question will construct an artifact that takes a deeper look into this gap. Additionally, by looking at a couple of the existing approaches, we will look into how to modify them so that they follow the new standards and can be used in the ADPs.

The last artifact that will be constructed is the one from the last research question where we will attempt to construct a proof of concept support tool for SACs. The aim of the support tool will be to provide a way for practitioners to monitor continuously updating SACs in real-time. We believe this to be not only an extension of existing knowledge, but also a revision of how practitioners monitor SACs today.

9 Risks - draft

There are numerous risks to this study. This section of the proposal will contain the most significant expected risks along with ways to mitigate them.

- First of all, we will be creating a library or database for assets,vulnerabilities and controls which will be open and maintainable over time. Secondly, we will develop a

proof-of-concept support tool to maintain SAC's. These will be done in collaboration with Systemite. During the creation, the obvious risk would be the ongoing pandemic and what if the work with the company doesn't continue. The probability will be low but will impact the creation of a library and support tool. As a mitigation we could probably send surveys to other companies apart from Systemite and its customers to collect the data we need. This can be done with the help of an academic supervisor as he has collaboration with other companies in the automotive domain.

- Time limit is another risk to this study. As this study will be done as a master thesis project, it has a limited time of approximately 20-22 weeks. We believe that there is a risk that the approach of building a web service based on the knowledge extracted from the SystemWeaver and integrating with it will be time consuming, as it involves some technical implementation. To mitigate this risk, we have our aim to produce a proof of concept and we have technical support from systemite, the company that produced and maintains SystemWeaver. This would be helpful for us to overcome the technical problems and speed up the development process.

- Data gathering is one potential risk in this thesis time frame. If the data is not collected from the company in time for phase one and phase two then there might be a risk when implementing a support tool for phase three. As a mitigation, we will constantly be in touch with the Systemite team by updating the progress of work.

10 Time Frame - draft

The initial estimations on the timeframe assume the start date being April 1st with the duration being about 20 weeks from then. This would make the end date be August 12th.

Week	Task
1-2	Familiarizing with the Systemite, what they do, and a closer look into how we will be working together with the company.
3-7	Phase one - working on RQ1
8-11	Phase two - working on RQ2
12-17	Phase three - working on RQ3
18-20	Finalizing the thesis report. Drafts ready and sent to supervisor, opponent, and examiner. Present the final report to the company and prepare for thesis defence.

The table above shows what we will do each week, the first week starting on April 1st.

References - incomplete

Mohamad, M., Steghöfer, JP. and Scandariato, R. (2020a) Security Assurance Cases - State of the Art of an Emerging Approach.

SYSTEMITE AB. (2014) SystemWeaver [Computer Program]. Available at http://www.systemweaver.se/

Mohamad, M., Äström, A., Askerdal, Ö., Borg, J. and Scandariato, R. (2020b) Security Assurance Cases for Road Vehicles: an Industry Perspective.

Vaishnavi, V. and Kuechler, W. (2004/5). "Design Research in Information Systems" January 20, 2004, last updated August 16, 2009. URL: http://desrist.org/design-research-in-information-systems

Spriggs, J. (2012) GSN - The Goal Structuring Notation: A Structured Approach to Presenting Arguments.

Wohlin, C., Runeson, P., Höst, M., Ohlsson, MC., Regnell, B. and Wesslén, A. (2012) Experimentation in Software Engineering