CHALMERS
UNIVERSITY OF TECHNOLOGY

UNIVERSITY OF GOTHENBURG

Leveraging a Traceability Information Model in order to enhance the maintenance of automotive Safety Assurance Cases

Master's thesis in Software Engineering & Management

Yulla Ibrahim & Mikaela Törnlund

Department of Computer Science and Engineering
CHALMERS UNIVERSITY OF TECHNOLOGY
UNIVERSITY OF GOTHENBURG
Gothenburg, Sweden 2020

Master's thesis 2020

Leveraging a Traceability Information Model in order to enhance the maintenance of automotive Safety Assurance Cases

Yulla Ibrahim & Mikaela Törnlund

UNIVERSITY OF
GOTHENBURG

CHALMERS
UNIVERSITY OF TECHNOLOGY

Department of Computer Science and Engineering
Chalmers University of Technology
University of Gothenburg
Gothenburg, Sweden 2020

Leveraging a Traceability Information Model in order to enhance the maintenance of automotive Safety Assurance Cases

Yulla Ibrahim & Mikaela Törnlund

Supervisor: Riccardo Scandariato, Department of Computer Science and Engineering & Mazen Mohamad, Department of Computer Science and Engineering
Advisor: Joakim Ohlsson, Volvo Group Trucks Technology
Examiner: Jennifer Horkoff, Department of Computer Science and Engineering

Master's Thesis 2020
Department of Computer Science and Engineering
Chalmers University of Technology and University of Gothenburg
SE-412 96 Gothenburg
Telephone +46 31 772 1000

Cover: Description of the picture on the cover page (if applicable)

Typeset in LaTeX
Gothenburg, Sweden 2020

Leveraging a Traceability Information Model in order to enhance the maintenance of automotive Safety Assurance Cases

Yulla Ibrahim & Mikaela Törnlund
Department of Computer Science and Engineering
Chalmers University of Technology and University of Gothenburg

Abstract

In safety critical systems, Safety Assurance Cases are created in order to provide argumentation as to why a system is reasonably safe. In the automotive industry, the ISO 26262 standard is complied with in order to provide comprehensive and structured argumentation for developed electrical and/or electronic (E/E) systems in regards to function safety. Previous research, while seeing initial results in improving traceability in Safety Assurance Cases, has expressed the importance of creating trace-link between the safety related artefacts and elements in order to provide the argumentation of as to why the complex real-world systems are safe. By utilising the Design Science Research methodology a Traceability Information Model emerged as the design artefact, which has been validated in an industrial setting. The aim is to contribute in how traceability of Safety Assurance Cases can be represented and what the appropriate relationships are. In this paper, the artefacts which are important to traceability and the relevant relationships among them in Safety Assurance Cases are presented and discussed. The results of this study could help future research in identifying the important trace-links required to facilitate the maintenance, by introducing traceability, in other industrial cases and provides a starting point for work in automation of the creation of Safety Assurance Cases.

Keywords: Safety Assurance Cases, Traceability Information Model, Functional Safety, ISO 26262, Traceability.

Acknowledgements

We would like to thank our supervisor Riccardo Scandariato for guiding and supporting us during our study and for gently pushing us when needed. Additionally, a huge thank you to Mazen Mohamad for your interest, help and because without you this thesis would not have been written. Finally, we would like to thank Joakim Ohlsson and Olof Bridal for your commitment and for making this thesis possible.

Yulla Ibrahim & Mikaela Törnlund, Gothenburg, June 2020

Contents

List of Figures

1
Introduction

In safety critical systems, it is important to provide extensive evidence that the product is up to safety standards, this can be expressed in a Safety Assurance Case (SaAC)[3]. A top level approach is taken by decomposing safety requirements and providing argumentation in order to argue that a certain part of a system is safe. The argumentation is concerned with claims about a system, some of these claims are tightly related to the safety requirements, but the requirement hierarchy is not identical to the argumentation hierarchy. A SaAC includes and organises claims, arguments and evidence [4]. A claim refers to a safety specification that needs to be achieved in order to prove attained safety in that particular part of the system. Arguments express how the evidence provided satisfy those claims. Evidence usually consist of information in various shapes and types of documents and is often contained in an artefact, which refers to an ISO 26262 work product [5]. These documents can be, but are not limited to: test cases, reviews and safety concepts. This study and the SaAC refers to what ISO 26262 refers to as safety cases.

For automotive functional safety, in order to comply with appropriate safety standards, the ISO 26262 series of standards [5] must be met. The ISO 26262 is an instrument to secure that developed electrical and/or electronic (E/E) systems are safe in relation to functional safety. This means arguing that the system does not malfunction, causing unreasonable risks [6]. Safety cases in this environment are required to provide argumentation and evidence for the achievement of functional safety. In order to achieve this, the safety case needs to progressively contain the ISO 26262 work products. A work product is documentation that is produced throughout the Safety life-cycle in order to facilitate the management of functional safety [5] e.g., functional safety concept, software verification reports) [7]. 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 and evidence, nor how to evaluate the quality and completeness of a safety cases. SaACs have the potential to aid in the maintenance, consistency and support evolution of safety critical products [8]. Therefore, from a safety perspective 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.

A vital aspect to achieve these goals is traceability and therefore the goal of this study is to improve upon the traceability of SaACs in a practical, industrial setting. Attempts have been made in order to introduce traceability to the documents by

keeping version control up to date over multiple sources [9]. While experiencing positive results in research, the adoption of these practises in industry has seen some initial but not yet any comprehensive results. Traceability is a key attribute that is difficult to achieve using currently utilised workflows and methodologies in industry. By proposing a new model for creating and maintaining SaACs which benefits said attribute, a more streamlined and risk-averse workflow will be created for use in industry [9]. Additionally, this research intends to close a gap between research and industry by applying your research in an industrial context. Managing a safety case through life is not a trivial process, as it needs to be maintained on an accurate account of a system's safety, through assessing various challenges that has impact on the safety argument[10]. This study will focus on the industrial problems faced by Volvo Group Trucks Technology, a Swedish OEM company, as the main source of challenges faced in a real world environment. Three key challenges in regards to maintaining SaAC will be addressed:

1) The first challenge directly involves the maintaining of the SaACs, where they the lack supportive trace links information. Practitioners experience the main obstacles in SaAC maintenance particularly in keeping the relevant documents consistent and the traceability of information between artefacts and elements. This is especially true in situations regarding changing requirements but also changes in the product under development. Traceability become particularly difficult to attain in SaACs as they grow too large and the complexity increases [11]. The main problem in terms of maintenance is the lack of traceability. When a change is made, even a small one, it takes a significant amount of time to trace the impacted artefacts and elements of that change if traceability is not integrated [3].

2) The second challenge pertains to the difficulties that are faced to provide traceability between the SaAC and the referenced artefacts. It is important for the validity of a SaAC that all artefacts used in order to build the SaAC are up-to-date [12]. 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. It is also important to ensure that the SaAC reflects the physical reality of the product, in regards to functionality and behaviour. Any change should have a traceability link to the impact on the corresponding safety argumentation.

3) The third and final challenge is to attempt to contribute to minimising the gap between theory and real-world practices. Issues regarding traceability between the various documents in a SaACs during the evolution of the product have been the focus of some initial research, but have not yet been efficiently addressed [11]. 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 traceability 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 [12]. 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

This study focused on improving SaAC maintenance efficiency by the devel-

opment of a Traceability Information Model (TIM). A new solution is proposed that suggests a model to introduce traceability in SaAC that could be applied in an industrial setting, using the case company as a primary data point on which to develop the TIM. The focus was on facilitating the maintenance of SaACs by providing the ability to manage change by introducing traceability in the context of continually changing artefacts. Even though the focus of this study was on a specific industrial case, an attempt was made to produce results that are generalised and has the possibility be used in different real-world settings.

2
Background

In order to provide the necessary background information needed for this study, this section is divided into three different topics. The first topic describes what a SaAC is, the benefits to the organisation, recommended method to work with SaAC, the ISO 26262 standard and the Goal Structuring Notation (GSN). The second topic introduces the strong connection between Maintainability and Traceability and how introducing traceability can improve the maintenance of SaACs. Finally, the third topic describes what a TIM is and how it can help improve maintenance of SaACs.

2.1 Safety Assurance Cases & ISO 26262

In systems where safety is a critical aspect, an extensive argumentation for its compliance to safety standard is important. In roadside vehicles, the safety of a systems functional safety is expressed in a SaAC [3]. The SaAC should communicate an argument, regarding that the system is acceptably safe for the user to operate in a given context, which is both comprehensive and defensible [13].

SaACs are important to an organisation not only to reduce safety related risks but also to decrease commercial risks. The creation of SaAC also provides a platform for stakeholders to get involved and provide their reviews. Additionally, creating SaAC provides a great incentive to focus on improving safety related activities, present the use of accepted guidelines and standards and a means to express that known potential vulnerabilities have been investigated [4].

In order to decrease the overhead of working with SaAC, to achieve an efficient workflow, the implementation of the idea of continuous assurance cases is of upmost importance. These assurance cases are created, and updated, as part of the development process instead of an item that is created after the development cycle is complete. Warg et al. [14] argue that integrating assurance cases more tightly with development and having the same support for versioning and product lines for both activities is one crucial part of enabling continuous assurance. Separation of Concerns, which is a design principle used to manage complexity and facilitate re-use, enables the use of component-based assurance case fragments. It is advised not to limit the handling of assurance cases to solely the experts in this domain but the development teams need to be able to keep the assurance cases up to date as part of releasing new functionality [14].

In order to comply with the ISO 26262 standard, which comprise guidelines to secure that the functional safety in electrical and/or electronic (E/E) systems is acceptably safe, safety cases are created. To comply with the standard, the safety

cases need to consecutively contain the ISO 26262 work products. A work product in ISO 26262 refers to a document or a set of documents that are produced during the safety life-cycle of a product [5].

One well known technique to express a SaAC is with the GSN [15]. It is a graphical argumentation notation made to represent and visualise elements in a SaAC (claims, arguments & evidence) and the relationships between them. The main purpose of representing the elements in a SaAC utilising the GSN is to visualise how the claims about the system are broken down into sub-claims until the claims can be supported by a direct evidence regarding the system safety [13].

2.2 Maintenance & Traceability

The creation and approval of SaAC is a challenge for practitioners, especially when the cases become large and complex. Explicit and implicit dependencies are introduced and the SaACs become increasingly hard to maintain [3]. Without traceability to and between the artefacts and elements of a SaAC, a small change can take a significant amount of time to both trace and update throughout the case. Additionally, the confidence in that all effects of a change have been addressed is decreased without the assurance from implemented traceability [3].

Guiding developers to identify parts of SaAC that can be affected by a change can aid in maintenance of the cases. This can be done by establishing relationships between different components of the system. When a change occurs, it will be visible for practitioners which the sensitive elements and their dependencies are. The established relationships will indicate which other elements might have been affected by the change, which will reduce maintenance time in terms of identifying which elements should be examined after a change is made [16]. Traceability plays a very important role in identifying the evidence required in a SaAC but also becomes important when assessing if all the evidence needed is available in the case [17].

2.3 Traceability Information Models

Previous research has shown the need for traceability in SaACs. Some results have been produced in this area but few attempts have been made in order to implement these in an industrial setting. Traceability in SaAC focuses on establishing relationships between artefacts 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 need 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. The traces between claims, arguments and evidence regards traceability within the SaAC. Traces between claims/evidence and artefacts regards traceability between the SaAC and artefacts external to the case [12].

Nair et al. [12] created a “Traceability Information Model for Safety Evidence” called SafeTIM. It builds upon creating class diagrams and classes with certain

predefined attributes such as version and references. However, the authors states that this model is still in need of additional tool support in order to simplify the adoption by industrial cases [12]. 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.

Taguchi et al. [18] present their TIM which is related to the GSN and criteria for how to validate and evaluate if the traceability is adequate in a safety case. The GSN diagram is divided into the various phases of development and traceability links are created both between and within the phases. The validation criteria proposed for traceability with respect to ISO 26262 is summarised as follows: A collection of GSN diagrams has complete traceability coverage if all traceable artefacts fed to the TIM are referenced in the diagrams as evidence. The collection has forward coverage if indexed diagrams reference a traceable unit in one solution (S2) with a reference to the previous version of the traceable unit in solution (S1).

In this study, an attempt was made to build upon existing solutions [12, 18] in order to create a TIM at the case company which would help the practitioners to improve the maintainability, by introducing traceability, of their SaACs. Although these two TIMs were the main sources of inspiration, we did investigate additional TIMs that were created for other domains. However, the focus was on vehicle related TIMs and the automotive industry.

3
Research Questions

By reviewing currently employed methods by the case company to implement traceability in their SaACs and the existing body of knowledge in the area, the following research questions emerged.

- **RQ1: How can we trace the relevant relationships in SaAC and the containing elements to their relevant development artefacts?**
  - **RQ1.1: How can we describe the relevant relationships among artefacts and elements of the SaAC?**
  - **RQ1.2: What are the relevant relationships among artefacts and elements of the SaACs?**

Based on findings from previous studies, it is clear that traceability is a substantial aspect of maintainability in SaACs. It is also evident that research regarding traceability in SaAC is a pressing and important topic as of today. There have been significant results in attempting to introduce traceability in SaAC but the differences between findings in research and the real-world settings that SaACs are developed in has not yet been entirely addressed. This study will focus on how traceability can be utilised in SaACs created and developed in an industrial setting, in order to improve the maintenance of these cases. Traceability regards the relationships that is, or can be created between different elements or components in a system [16]. Identifying these relationships are key to answer RQ.1 on how can we trace the relevant relationships in SaAC and the containing elements to their relevant development artefacts. Therefore, by answering the two sub-questions on how the relationships can be described and what the relationships are, we can make an attempt to answer RQ.1

Answering RQ.1.1 required analysing existing studies and identifying the most suitable solution for the case company and answering the RQs. A suitable model to present this information and provide a solution for better maintainability built on traceability information for the SaAC was needed.

Answering RQ.1.2 required identifying the structure utilised for a SaAC. Furthermore, the structure needed to be analysed in order to provide the list of elements within it and additional elements needed to be identified. The additional elements regards the ones that are necessary references from within the development process and are required to support the SaAC artefact to provide trace information for accomplishing tasks regarding maintainability. Further analysis was needed in order to specify the nature of the relationships among identified elements and artefacts.

In order to answer RQ.1, the identification of a way to enhance traceabil-

ity presentation within specific environment was required. The analysis took into consideration that any solution available needed to focus on supporting the maintainability of SaACs. In order to validate the approach, information was collected regarding the system deployed in the case company. A synchronisation of the evolution of the product and the evolution of the SaACs was executed. This was done in order to support Maintainability, which would through this synchronisation be affected and improved. How this was addressed was through the implementation of traceability.

The guidelines in the paper written by Agee [19] have been adhered to. 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.

4
Methods

This thesis was conducted in collaboration with the Swedish OEM company Volvo Group Trucks Technology (GTT), in particular with their Functional Safety department. The case company is one of the largest heavy-duty truck brands in the world; with trucks sold and serviced in over 140 countries.

The Design Science Research (DSR) methodology [20] was utilised. The process of a design science research is an iterative approach that consists of a number of cycles. Each one comprises five phases: Awareness of Problem, Suggestion, Development, Evaluation and Conclusion. When a cycle is complete, the generated output is used as input for the upcoming one [21].

The DSR method was chosen because it is a solution-oriented approach to a business problem, which is stated as one of Hevners [20] guidelines on DSR. An additional reason for choosing the DSR method was because this would enable the development of the solution backed by existing studies that also fulfils the company's requirements, which clearly indicated that the study would need to take on an iterative approach with an artefact as the generated solution.

Three iterations were conducted at the case company with the goal to provide the company with a solution that they could utilise in order to facilitate the maintenance of their SaACs in regards to traceability. Another goal was to propose a general solution that can be utilised in safety critical systems when creating SaACs.

4.1 Iterative cycle

The following is a description of what each cycle in the iteration entails.

4.1.1 Awareness of Problem

The first phase of the cycle is focused on achieving an in depth understanding of the problem domain in order to enable the attempts to propose relevant solutions for said problem. During this phase of the study, the focus was on eliciting a deeper understanding of traceability in SaACs, traceability information models and the particular problems faced in industry in relation to this study.

4.1.2 Suggestion

In the second phase of the cycle, different solution proposals are explored and evaluated based on the findings in the awareness of the problem phase. If a proposed

suggestion is found to be suitable it is carried over to the next phase. However, the possibility that no suggestion is appropriate is also a possibility. In this study, the suggestion comprised of different solution artefacts in the various iterations. In the first iteration, the proposed suggestion comprised of a list of methods that could be utilised by the case company in order to introduce traceability to SaACs, and subsequently improve maintainability of these cases. In the second iteration, the suggestion was a TIM that was developed in order to increase traceability and improve maintainability in SaACs, while also being feasible in an industrial setting. In the third iteration the suggestion comprised of a proposal of a way to conduct an analytical evaluation of the TIM by applying it on existing SaACs. The aim was to identify issues both with the model, but also current practises in industry that inhibits traceability and maintainability of SaACs.

4.1.3 Development

The fourth phase, the development phase, is conducted by taking the suggestion proposed in the previous step of the cycle and carrying out the development of said suggestion. This was performed by presenting the methods to SaACs, functional safety and ISO 26262 experts at the case company, refining and extending the proposed TIM solution and by applying the TIM on existing SaACs as mentioned in the previous section.

4.1.4 Evaluation

In the fourth phase, the artefact generated from the development phase is evaluated against the problem or problems found in the awareness of problem phase of the cycle utilising appropriate evaluation methods. The primary method of evaluation utilised in this study was expert evaluation of the developed artefact. Additionally, in the final iteration, a focus group evaluation was conducted. The evaluation was carried out by experts in SaACs, functional safety and the ISO 26262 standard in combination with findings of previous studies in relation to traceability in SaACs.

4.1.5 Conclusion

Finally, in the fifth and final phase of the cycle, the focus is on concluding the results of the evaluation phase in order to answer the research questions of the study. The conclusion is also utilised as the problem investigation phase for the following cycle.

4.2 Data collection

Five different techniques for data collection was utilised: Document review/analysis, Participant observation, Focus Group, Expert evaluation and a Workshop. These techniques were chosen due to both their applicability and the amount of data that could be elicited. The participant observation technique was used mainly in meetings and workshops with the case company's employees and experts in SaACs and functional safety to achieve triangulation of the data elicited from the document review

and vise versa. The workshops and expert evaluation methods were used primarily as evaluation techniques but were also utilised as data collection techniques. Triangulation of data is used to validate and compare data collected between at least two different methods to identify any biases or divergence between the different sources of data collected [22].

4.2.1 Document analysis

The primary method of data collection was document analysis. As expressed by Bowen [23], document analysis is utilised to *"elicit meaning, gain understanding, and develop empirical knowledge"*. The benefits of this technique are the availability of documents and time efficiency of the data elicitation. The documents analysed in this study comprised of, but were not limited to, instructions on how to write SaACs according to the ISO 26262 standard, SaACs under development at the case company, strategies regarding the company's safety assurance process, process documents and templates. A significant amount of documents were provided by the case company and an extensive amount of data could therefore be elicited using the document analysis method which would not have been so readily accessible using other methods.

Analysing the instructions and template documents on how to write SaACs according to the ISO 26262 standard made it possible to analyse the ongoing process at the case company and the current state of implementing traceability to their SaACs. A better understanding of the company's structure and development process was obtained, which would be useful in order to propose a solution that would benefit the practitioners who would possibly be affected by the solution.

One of the disadvantages with the document analysis method for data collection is that the contents of the documents might contain insufficient detail, as they are created for a certain purpose [23]. In order to mitigate this participant observation was chosen as another technique for data collection in the study in order to obtain more details about what was learnt and discovered in the document analysis.

4.2.2 Participant Observation

The secondary method of data collection was conducting participant observations at the case company. Participant observation can be expressed as the researcher or researchers becoming a part of the team that works with the area regarding the study. The researchers will observe the actors and derive relevant data from the work being done and said [24]. This method was used as a lot of relevant information, especially on a strategic level, is expressed in these meetings between experts while interacting with each other. A number of workshops were attended, information and strategy meetings regarding the company's development of SaACs and ISO 26262 in relation to said SaACs. By attending these meetings and workshops insights into the process was gained, goals and current strategies at the case company that would have otherwise been difficult to obtain. The guidelines to participant observation expressed by Mack [25] were followed. These guidelines include how to manage the ethical, observational, note taking and analytical aspects of conducting participant

observation. The guidelines were adhered to regarding taking notes during the different observation occasions and field notes were expanded on accordingly (See Appendix, A.9-A.12).

In this study, the participant observation data collected were focused on what was being discussed among employees at the case company in meetings and workshops held for each other. This was done in order to gain insights into how the organisation and their employees reason and work with SaACs and the ISO 26262 standard. In addition to the data gathered through documents' review, the participant observation data highlighted the difference between guidelines that were created and how far the organisation had come in order to adhere to these guidelines while working with SaACs.

4.2.3 Expert Evaluation

The third method of data collection was Expert evaluation. This is a qualitative method where experts can contribute freely with comments without pre-defined heuristics. It is a fast and cost effective evaluation method [26]. Experts Evaluation took place in form of meeting sessions, Where experts where invited into scheduled sessions to address each iteration evaluation practice. In the expert evaluation the researchers took the role of moderators to lead the session and assess the results, while the evaluation from the experts was monitored. Expert evaluation was utilised for the evaluation of the development of the TIM. The structure of the sessions were designed to provide insights to the knowledge regarding the models applicability and usefulness in terms of providing needed traceability information required for maintenance tasks for the SaACs. Various factors have been considered following the guidelines expressed by Klas [26] approach for performing the evaluation in each session.

The first factor is the task, which is designed based *"on the information need to express the unknown"* [26]. The task for each session was reviewing each of the models classes in terms of reflecting a clear representation of elements that explore a connection to the SaAC structure and availability of the trace links to the dependent elements provided in the development process. The task also included evaluating the associations between the classes, in order to determine if they represent the correct connections and if they flow in a the right directions of how traceablity information is available in the company's systems.

The second factor was determining the group that would be preforming the evaluation. An important aspect to consider here is that the group task and target group that will be using the model should be an accurate reflection, meaning that the *"evaluators should be experts from the same community as the intended audience"* [26]. Therefore, the experts were employed at the case company and their field of expertise were; SaACs, functional safety, R&D and the ISO 26262 standard. The third factor is to be able to create comparable results within the intended framework, which was theoretically oriented to address important relations among the SaAC elements. Multiple versions of the TIM were developed and were presented to the experts in each evaluation session with a highlight on the new changes. The final factor was specifying the period to use the expert evaluation. This type of data

collection was assigned to be a formative evaluation. Therefore, it has been carried out during each stage to evolve with the TIM design [26].

4.2.4 Workshop

The fourth method of data collection was a Workshop used as an approach to ensure the transparency of analysing proposed solutions in the domain of maintainability of safety cases. A workshop consist of an arrangement where a group of people learn, acquire new knowledge, perform creative problem-solving or innovate in relation to a domain-specific issue [27]. Workshops are arranged events of a limited duration targeted to participants who share a common domain, e.g., work in the organisational change domain [28] [29]. In this study this method was utilised to create a discussion between experts in the relevant areas in order to derive useful insights into the case company and the possible solutions proposed. The workshop posed as a form of expert evaluation with additional focus on creating a discussion among the experts to fill any knowledge gap, to illuminate their differences and similarities with respect to goals, outcomes, phases, roles, and organisation.

Following the recommendations of Ørngreen and Levinsen [27], the participant group was kept small in order to allow everyone's personal attention and the chance to be heard. The workshop was conducted with the case company and included ten participants. They were from the E/E and Chassis departments. That summarises the expertise that is needed to evaluate ideas regarding the way they build and construct their SaACs, while also including the opinions of the experts of the functions that those safety cases are built to assure.

The workshop topic was a discussion of the literature review of solutions related to SaAC maintainability, in particular traceability improvements. Based on the discussions among the attending experts, prioritisation of the solutions connected to traceability of various artefact information was possible. The scope was narrowed down to focus on maintenance and modelling traceability information to support agile change management for the SaACs. Based on the description provided by Ørngreen and Levinsen [27] of participation modes, the workshop has a collaborative context whereby researchers and participants work together but with the researchers in control. As the solutions were pinpointed and discussed based on the related work application in the literature review, the participants discussions has helped the researches as observers to choose which approach to follow.

4.2.5 Focus Group

In a focus group, only a small amount of problems are addressed. Questions are open ended but selected to continuously lead the answers towards the determined problems. A moderator is chosen as a guide for the group in order to direct the answers to focus on the topic [30].

For design science research, focus groups are used to elicit feedback from the participants regarding the utility of the study's generated design artefact. For the purpose of evaluating the TIM, a confirmatory focus group was created and conducted. A "confirmatory focus group" is a focus group utilised to evaluate a design

artefact and its utility in a real world setting in design science research rather than the "exploratory focus groups" in which the aim is to gather quick feedback for improving the artefact [31].

The smaller group of participants were chosen in order for all members to have room to discuss their thoughts and to facilitate the interaction between the participants. The meeting was held on a video call and therefore a smaller set of participants was helpful as social queues when someone is about to talk is less evident and people tend to start talking over each other.

The guidelines on conducting evaluation with focus groups provided by Tremblay et al. [31] were adhered to. The authors provide guidelines on how to conduct focus group evaluation for design research. The first step that was performed was to formulate the research problem, which was the evaluation of the TIM and its applicability in an industrial setting at the case company. The reason for the focus group instead of an expert evaluation in the shape of individual interviews was; since these people are working with SaAC at the company but with different aspects of it, in different steps of the process, their collaboration and ideas of how this model will be utilised by them collaboratively was an important aspect to discuss. Because the participants had different knowledge about SaAC another reason behind the evaluation and the focus group environment was to allow them to discuss these topics as well as evaluating the TIM itself. This method also allowed for probing questions that helped the participants delve deeper into any statement that they made that were insightful but had the potential to provide more in depth information.

The participants were chosen based on how they relate to the SaAC in their work and how their roles fit together. The same goes for the questioning route, the goal of the evaluation was to also focus on the TIM on its own, how it would fit into their development process and how the different employees would work with it in their collaboration.

The questions were asked in a specific order according to Tremblay et al. [31] guidelines. The questions were ordered to start with the most general ones down to the narrowest but also relative to the importance of the question, asking the most important ones first. One of the researchers acted as the moderator for the focus group and the other one as an observer taking notes.

The questions that were asked can be found in Appendix A.14

4.3 Iteration 1

In the first iteration, the primary goals were to lay the foundation of this study in term of gathering the knowledge from previous research and to find a suitable method to use in order to introduce traceability to SaACs. Said model also had to be in line with the case company's established workflow, structure and practises in regards to SaACs.

4.3.1 Awareness of Problem

In the Awareness of Problem phase of this iteration a literature review was conducted focusing on traceability in SaACs, traceability in safety assurance evidence

and maintainability of SaACs. This was done in order to gain a better and deeper understanding of the problem domain but also of the solutions that have already been proposed in the area. The majority of papers that were found states the need for increased traceability within SaACs and between the SaAC and the artefacts it references. The main obstacle is that the evidence is spread across various locations and exist in different formats. In the most relevant paper found and reviewed, there were various different solutions proposed. These solutions were, among others, Traceability Information Models, tools, different analysis methods and process models [12, 18, 9, 32, 16, 33, 34, 14]. These solutions were often tailored to a specific case, not attempted in industry or only proof of concepts. However, these solutions were important in order to gain knowledge of possible solution, draw inspiration from and build upon to fit the real-world scenario. A list and a brief description of those solution is included in the Appendix, Figure A.17 and Figure A.18.

4.3.2 Suggestion

The previous studies found that proposed relevant solutions to the traceability and maintainability problem were analysed deeper. The suggestion in this phase comprised of a set of existing solutions that could be applicable as a foundation for this study. In order to develop and evaluate the chosen solutions found, an extensive presentation was prepared for the relevant experts at the case company. The goal of the presentation was to get a better understanding of what type of solution would fit the case company's need and what would work in the development structure that they were employing at the time. The suggestion comprised a document and a presentation containing different methods that could be utilised in order to develop a solution for the case company. The suggestions would be subject to an evaluation from experts at the case company in the shape of a workshop where each proposal was evaluated in terms of the feasibility of implementation in the case company's structure and way of working but also on the potential to improve traceability in SaAC overall.

4.3.3 Development

In order to propose a solution it became evident that the scope needed to be narrowed down. A document was created summarising all relevant research and solutions in order to facilitate the presentation creation and to ensure that the key principles from each solution were understood. The final presentation and the solutions proposed were only related to traceability in SaACs. The presentation/workshop was held present the findings from the literature review and the analysis of the existing solutions. The participants of the presentation were industry experts in SaACs, functional safety, Research and Development (R&D) and ISO 26262 standard and totalled at a number of ten people. Their roles at the case company were the following: Functional Safety Manager, Senior Principal Functional Safety Engineer, Principal System design engineer, Specialist Functional Safety, GTM E/E Platform, Lead System Design Engineer, System Architect HW, Acting Manager and Development engineer (See Appendix, A.16). The solutions which were identified in

the awareness of problem and suggestion phase were presented in dept in order for the experts to provide informed and valuable feedback both based on their existing knowledge in the area but also on their understanding of existing solutions.

4.3.4 Evaluation

The presentation resulted in a large amount of questions and feedback from the experts in regards to the various solutions. The solutions proposed by Nair et al. [12] and Taguchi et al. [18] were the main focus of both questions and interest. The potential for the case company was clearly present in a Traceability Information Model compared to many of the other solutions. The majority of the experts agreed that the company had the opportunity and potential to improve the traceability in their SaACs evidence and documentation by implementing a TIM suited for their organisation and workflow. The experts did also point out that, in regards to traceability, many of the other solutions that were presented had potential to help the development and creation of SaACs. However, it was evident that they did not have the same applicability in terms of maintainability as the TIM which then became both the researchers and their main focus of this study.

4.3.5 Conclusion

Based on the result from the evaluation phase with the experts at the case company, the next step was to make an attempt to build a TIM inspired by Nair et al. [12] and Taguchi et al. [18] TIMs and findings. Combining the two solutions with the data elicited from the safety case template and instructions, workshops and meetings at the case company enough information was gathered in order to start designing the TIM. The model had to be tailored to the case company which meant work would have to be closely conducted with the experts available at the company in order to understand their processes and tools that were utilised to store the information needed to build a safety case.

In regards to the research questions, finding an appropriate method to develop a solution indicated the path to answer RQ.1.1.

4.3.6 Artefact evolution - Iteration 1

The decision to create a Traceability Information Model was made. The decision was based on the study of existing research in traceability for SaACs along with the evaluation from the experts in SaACs and functional safety at the case company. A TIM was chosen for its potential to benefit the company and to contribute to identify the relationships among artefacts and elements which will in turn contribute to improve maintainability in SaACs.

After pinpointing what type of solution that this study would attempt to produce together with the experts at the case company, two solutions were identified, in particular the two that was utilised as a starting point to begin building the TIM upon. Changes would have to be made in order to fit the needs of the case company, the ISO 26262 standard and the automotive products that the model would be created for. While these solutions have been implemented in an industrial setting,

both TIMs were applied on SaACs related to railway and not automotive systems. The two TIMs that were utilised as a starting point were developed by Nair et al. [12] and Taguchi et al. [18]. These TIMs were created as class diagrams which would facilitate the visualisation of relationships between the artefacts (ISO 26262 work products) and elements that are present in the SaACs and provide a clear overview of the case. Together with SaACs and functional safety experts at the case company an attempt was made to build upon existing solutions and augment these it to suit the case company's needs and facilitate the need to address the ISO 26262 standard.

4.4 Iteration 2

In the second iteration the first goal was to draw inspiration from and tailor the TIMs developed by Nair et al. [12] and Taguchi et al. [18] to create a TIM suited for the case company. This TIM would also be based on the conclusions of the first iteration and evaluated against the old traceability strategies employed by the case company.

4.4.1 Awareness of Problem

During this phase of the cycle various documents provided by the case company were analysed. Two of these documents were a template and a set of instructions on how to build a SaAC so that it reference work products needed to comply with the ISO 26262 standard on functional safety. These documents are used internally for the developers and safety assurance experts who create and maintain the SaACs in order to ensure that all relevant and required pieces of evidence are present in the SaAC. This helped identify the artefacts and elements that are required or could be used to provide evidence for the safety case.

The case company also provided a SaAC which they were developing at the time of this study. The case was analysed in order to obtain a better understanding of what a developed SaAC looks like, is structured and if there was information of where all relevant documents could be found in their various systems and repositories. The studied SaAC provided by the case company was incomplete in the sense that it only covered parts of the overall argumentation structure. The SaAC provided was built after the development of the function was complete which is not the process that the case company will utilise to create and maintain future SaACs nor the most efficient way to develop a SaAC [14]. Once their process and structure for building safety cases is better established within the company, the SaACs will be developed in parallel to the development of the safety critical function the case will relate to. What was required was the existence of some elements and artefact that relate to each other. In conclusion, the results of the study was not negatively affected by the state of the SaAC provided. However, this was kept in mind when performing the final evaluation of the case company's practises and to further mitigate the implications of the issues regarding the incomplete SaAC. The decision was made to rely more heavily on the template and instructions that summarised what information and evidence was needed to create a complete SaAC in order to propose solutions for the identified problems.

In the ISO 26262 functional safety standard, a hierarchy of claim and arguments are established in order to reason that the system is safe. This hierarchy is correlated to the safety goals, which are then broken down into functional safety requirements, which are in turn broken down into technical safety requirements. The technical safety requirements are then finally broken down into hardware and software requirements [8]. However, during this phase insights were gained into the main issues the case company faced in regards to traceability in their SaAC process. As mentioned above, functional safety requirements are broken down to technical safety requirements. The problem arise when, more often than not, one safety critical function can have multiple technical requirements that are broken down into further technical requirements and this can be done multiple times for each new technical requirements creating additional levels in the hierarchy. A pressing challenge is adhering to the traceability between these levels of requirements and their respective evidence. Another obstacle faced by the case company is the vast amount of documents and information spread across various tools and in different formats which is a problem that was also identified by Nair et al. while evaluating their TIM [12].

4.4.2 Suggestion

While analysing the SaAC provided by the case company an attempt was made to trace the information back to its source to evaluate the current level of traceability in their SaAC. This exercise also helped investigate what information the case company needed to be traceable and to keep this in mind while attempting to create possible solutions on how to solve the issues. Alongside the knowledge gathered from the literature review and the data provided by the case company the shaping of the TIM could begin, focusing on solving the existing traceability issues. The company did not utilise TIMs in any aspect of their development process and the concept was new to the majority of employees the researchers came in contact with. Which could have been valuable information since the SaAC related TIMs we identified were created like any other TIM. Therefore, there was no knowledge about TIMs and how to develop or work with them available at the case company to elicit any insights from.

The foundation of the solution is derived from previous work in the area. Especially previous studies in which the authors have created and utilised a TIM which laid the foundation for this study [12, 18]. The TIMs were studied closely in order to completely understand the terminology used and the argument behind choosing the classes or artefacts. A first attempt was made to create a safety related TIM that could suit the case company based on the data gathered from the company as well as from existing studies. Together with the case company an attempt was made to combine previous work with their needs regarding their SaACs creation and maintenance while also complying with the ISO 26262 standard and the automotive industry.

It was found that Nair. et al. [12] TIM is most similar to the solution to the case company's needs. However, an important aspect of Taguchi et al.[18] paper is the trace link created to the requirements involved as was identified as a key issue

in the Awareness of Problem phase of this iteration. This was not considered in [12] TIM. The case company has expressed the importance of all SaACs to be related to at least one safety requirement and therefore the trace links to the requirements is vitally important for the proposed TIM. Taguchi et al. [18] also include the acceptance criteria, plan and measurements in their TIM which is not available in Nair et al. [12] TIM. Based on the knowledge that was accumulated the assumption was made that these three would be important to establish if a safety case is complete and therefore included them in this study's version. It was assumed that these classes could be useful, not only because it could introduce important traceability information but also because it could help the case company to improve their structure and process working with safety cases.

The suggestion for this iteration boiled down to using Nair. et al. [12] TIM as an inspiration to develop a TIM tailored to the case company and to include some elements of Taguchi et al.[18] TIM.

4.4.3 Development

Two iterations of developing and evaluating the TIM were performed with the experts at the case company. 4.1 displays the nested phase within the DSR methodology to express the process that was performed.

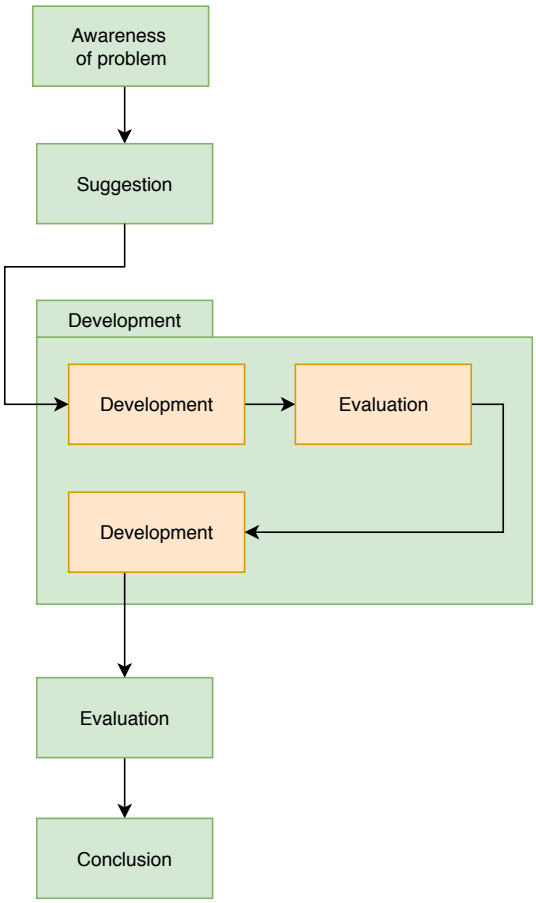

Figure 4.1: Nested development phase, DSR process

The nested development and evaluation phases was done in order to create a quicker feedback loop, still within the context of the same problem for the iteration. Since the problem space was the same, this structure was created rather than conducting a new iteration for each development/evaluation phase.

An attempt was made in order to create the first version of the TIM for the case company. Data was gathered from the documents provided by the case company of their SaACs process and instructions. Additional data was elicited from participant observations conducted in various meetings where the workflow and steps in the safety process for an “end user function" were discussed. Combining the two sources of data, the first version of the TIM emerged (See Appendix, A.1).

4.4.4 Evaluation

The TIM that was chosen for evaluation in this cycle (See Appendix, A.1) displays the suggestion that emerged from combining the knowledge acquired from the previous studies conducted in regards to creating TIM for safety cases and the issues which were identified at the case company.

A meeting was held with the people responsible for functional safety and safety cases at the case company (See Appendix, A.16) in order to conduct an expert evaluation and to determine what changes that needed to be made in order for the TIM to better suit their needs and on what abstraction level the TIM should be represented at. The abstraction level of Nair et al. [12] TIM is on a high level, providing an overview of how all pieces of the safety case is related. Compared to dividing the evidence into different types like Agrawal et al. [9] who has, for example, divided the evidence into Acceptance test, Code and tests, simulation and others. Since SaACs can be enormous in size, the initial assumptions were that the level of granularity would contribute greatly to the size and complexity of the TIM. This was confirmed by the experts at the case company who expressed that the showcased TIM was too granular even though it was developed on an abstraction level similar to Nair et al. [12].

A.2 in the Appendix displays the updated TIM after the first round of evaluation with the functional safety, SaACs and ISO 26262 experts at the case company.

In the second iteration of the evaluation phase, the experts (See Appendix, A.16) explained their process of working with safety plans. At the case company they utilise the safety plan to define activities which in turn will be performed using appropriate techniques that will result in the artefacts. Finally, the proposed TIM included the classes Acceptance Plan, Acceptance Process and Acceptance criteria based on Agrawal et al. [9] TIM to enable trace links back to the tolerable risk that is allowed for the end user function. This however, was deemed to granular and too complex for the experts that expressed that it would not provide value for the SaACs or the creation of it.

A.3 in the Appendix displays the updated TIM after the second round of evaluation with the functional safety, SaACs and ISO 26262 experts at the case company.

4.4.5 Conclusion

Based on the expert evaluation it's arguable that the results could be used as a starting point to identify the relationships between the artefacts and elements present in the SaACs developed by the case company. By introducing the class *storage location* it will also be possible to keep track of evidence regardless if the evidence is stored across different tools.

4.4.6 Artefact evolution - Iteration 2

In the initial version of the TIM (see Appendix, A.1) the main differences from Nair et al. [12] solution was that in the case company, the "project" class is not applicable in their case as all SaACs stems from an 'end user function'. A product comprise of a multitude of end user functions but a SaAC never covered more than one of these functions and the need to trace the evidence all the way back to the product was questioned but not immediately dismissed. The proposed changes in the TIM included a 'end user function' as a class related to the artefact and to a product type that would be the topmost traceable unit to adhere to. From Taguchi et al. [18] solution the main inspiration was from their focus on the processes related to SaACs and while identifying which processes were utilised at the case company Acceptance criteria, process and plan were added. With the knowledge gained from the data elicitation through participant observation, document analysis and the literature review it seemed like the best method was to initially create an inclusive solution and remove from there in order to utilise the maximum amount of existing solutions. This meaning, the initial TIM included many classes that would presumably be removed or edited in order to narrow down the TIM in the attempt to make it appropriate for the case company. This was done since the existing solutions had already been tested and verified and therefore thought it better to evaluate with the experts at the case company to determine the importance to traceability rather than ourselves.

The second version of the TIM (see Appendix, A.2) emerged based on the result from the first expert evaluation session. As mentioned above, according to Birch et al. [8] safety assurance is comprised of a hierarchy where safety goals are the topmost level, followed by the different types of requirements. At the case company they adhere to the same practise since it is a cornerstone of working with the ISO 26262 standard [8]. Therefore, the representation of safety goals and safety requirement specification in the TIM became a main focus. The "product" class was removed in the second evaluation round as the importance in terms of evidence traceability was equivocal. Each SaAC is created based on an end user function which is the element that encapsulates the entire SaAC. Meaning, the SaAC is build for a particular end user function and evidence is provided in order to argue for the safety of that function. Therefore, the "product" class was changed to "end user function" to correlate to the case company's traceability structure of the SaAC. Additionally, multiple products at the case company might utilise the same end user function, making the linking to the product even less important.

The third version of the TIM (see Appendix, A.3) was further developed based on the result of the second round of expert evaluation. Granularity was a significant

issue expressed during expert evaluation in iteration 2 which led to the removal of the acceptance process, plan and criteria which were deemed unsubstantial to the traceability of a SaAC and out of scope for the TIM. The experts expressed that although the acceptance process is important to validate the safety of the product, no direct links are needed in order to maintain a safety case in relation to its evidence.

As mentioned in section 1, one obstacle in creating traceability in SaACs is that artefacts are spread out over different locations [12]. In the third version of the model, a solution is proposed by adding a class called “Storage location" that is connected to the artefact (see Appendix, A.3). This class will specify in which system the artefact can be found as well as where in said system it can be located. By introducing the class “storage location" it will also be possible to keep track of evidence regardless if the evidence is stored across different tools.

An additional change that was made was the indirect connection between safety requirement specification and both claims and evidence. As discussed in the awareness of problem phase in iteration 2, the traceability between evidence and requirements can become very complex and convoluted. Therefore, it was shown that the link between the safety requirement specifications to both the claim and evidence is vital for establishing traceability.

One complication that was expressed in the expert evaluation of the TIM was that Safety requirement can be connected to an artefact in a very vague way but can also be the artefact itself. This creates a confusion in the TIM on how to address the trace links to Safety requirements so it can be generalised. This was solved by connecting the safety requirement specification class indirectly to both the claim and the evidence in the TIM.

4.5 Iteration 3

In the third and final iteration of the study the focused was on improving the TIM that emerged from the previous iteration while also making an attempt to generalise the findings.

4.5.1 Awareness of Problem

In addition to the insights gathered from the previous iteration on how to improve on the TIM, finding existing SaAC from other organisations in order to generalise the findings and the TIM was realised.

4.5.2 Suggestion

In order to generalise the TIM it was needed to apply the solution on other SaACs and implement those changes as a result from this iteration. The goal was to create something general within the space for automotive, but also looked at outside resources to get inspired. It is something the researchers learned by sitting at the case company, they look at other domains to see how different industries solve the same or similar problems.

To do so, the researchers went online to look for existing, open source, SaACs that could be utilised in order to gain additional insights in how to improve and generalise the TIM.

The following search terms were used on Google scholar:

- Automotive safety case
- Safety assurance case in automotive
- Safety assurance case
- UAV Safety assurance case
- Railway Safety assurance case
- Safety assurance case example
- Safety case example
- Example data safety assurance cases
- Sample safety assurance cases
- GSN safety assurance cases

Although the amount of appropriate results were relatively scarce and the final selection of SaAC was five additional SaAC. The selection criteria on which cases to include or exclude the SaACs that were found from the search were the following:

Size and complexity: The size and complexity was a plausible indication on if the SaAC was a made up example or based on a real world example. A larger and more complex case would have a higher possibility to be a real world example rather than an example used to prove a point. This metric alone would of course not be enough to validate the relevance of the case but was a determining factor. Larger and more complex cases would also help validate one of the greatest issues in SaACs maintenance and could, in that regard, help determine if the TIM has the possibility to be useful in such an industrial setting.

Level coverage, existence of a context for the safety case: Level coverage was determined based on if the SaAC includes all the different components of a safety case. These components being claims, arguments and evidence. The lack of existing evidence, compared to the other two components, was noted but not excluded. The lack of evidence in these cases found online was suspected as the companies or organisations would not be expected to share that level of confidential information. These cases was, however, still utilised to validate and evaluate the other aspects of the TIM since the structure and other elements were still available.

Covering Evidence relationship: An interesting aspect that was learned from the evaluation at the case company in the previous iteration was the relationship between pieces of evidence and their relationship to safety requirements, which was one of the main issues the company faced in regards to traceability. It was important to find other occurrences regarding the evidence relationship in order to see how and if other solutions attempted to solve this problem.

Source credibility: Another aspect that was evaluated was who made the cases and what company created them. An investigation was conducted into the organisations who created the cases when the name was not recognised. Ensuring that

only trustworthy cases were included in the evaluation of the TIM was important.

Relevance to Safety: A a couple of assurance cases were found that were implemented for security and the relevance to safety was negligible. These cases were excluded in order to keep the TIM safety related since some aspect of these two areas differ and it is outside of the scope of this thesis to create a TIM that is generalised to that extent.

Automotive relevance: An attempt was made to find SaACs relevant to the automotive industry but since the main focus was to identify cases that were safety related the industry the cases were utilised in was not an excluding factor.

4.5.3 Development

The result of the search yielded in five additional SaACs [35] [2] [34] [15] [36] apart from the case company's case. All six SaACs were analysed in order to identify the elements and artefacts available or not in relation to the TIM. The addition of a "context" were present in multiple SaACs that was not considered before. Several of the cases had a context in terms of Automotive Safety Integrity Level (ASIL) that were connected both to the top claim, claims and arguments. ASIL is an important aspect of the ISO 26262 standard [5] and could have a positive impact on the traceability of SaACs.

A spreadsheet of available elements in the SaACs was created in order to visualise frequent available classes to determine how often each class is referenced in a typical SaAC. The availability of each class in the SaACs are visualised as a bar chart (See Appendix, A.13).

Three SaACs, were selected as candidates for applying the TIM (See Appendix, A.5-A.7) [34] .

The steps taken in order to apply the TIM on the SaACs were as follows:

- Identify which ISO work product/artefact the Safety case was attempting to produce
- Start modelling the relationships between the different GSN specific classes (Argument, Claim, Evidence, Top claim/Goal and Context)
- Analyse the content of the GSN specific classes to identify important traceable information that relates to the development process classes. E.g., Activity, technique, storage location, artefact provenance and relationship, analysis document and version.
- Draw the associations between these classes and the GSN specific ones
- Identify the End user function or any pointers towards a product or similar.
- Note down which classes in the TIM were missing/not available

Applying the TIM on the case company's SaAC (See Appendix, A.5) was done not only to evaluate the TIMs applicability but also to aid the evaluation of the TIM for the experts at the case company with whom the final evaluation was conducted. In this visualisation, the scale and complexity that begin to emerge when SaACs become large and complex becomes increasingly visible.

4.5.4 Evaluation

When the data was collected from applying the TIM on the various SaACs, identification of which classes in the TIM were rarely or never present could be done (See Appendix, A.13) , the existence of additional classes that were not available in the TIM and other relevant insights that were important aspects of evaluating the model. The classes, or reference to classes, which were found missing from the SaACs were all related to the development process. Information about the development process of companies is often sensitive information or might not be explicitly referenced in the SaAC. To mitigate this gap existing literature was explored in order to provide argumentation for if the missing classes should be kept or removed from the TIM in relevance to establishing traceability in SaACs, more information about this is available in the results section 5.1.2.1. The classes that were available in the SaACs and were already represented in the TIM was decided to be evaluate in terms of the importance for improving traceability. The fourth version of the TIM (See Appendix, A.4) emerged from the analysis of the SaACs, applying the TIM to the cases and the result from the extended literature review regarding each class and its relation to traceability, especially the classes related to the development process.

In addition to the evaluation based on existing cases and the extended literature review, a focus group evaluation was conducted. In preparation for this focus group, an abstract view of the artefact class in the TIM was created. The TIM was also divided into two parts, one including the development process elements and the other one containing the safety case structure elements. This was done in order to facilitate the understanding of the TIM and its element in depth and to help the experts better understand what artefacts and processes are encapsulated by the model.

The focus group was conducted with four experts at the case company with different areas of expertise in regards to SaAC. One was a Specialist in functional safety another one a safety case manager, the third one Principal system design engineer and functional safety specialist and the last one had the role of Senior principal functional safety engineer (See Appendix, A.15). The questions that were asked in the focus group related to the TIMs applicability in an industrial setting, the challenges that the practitioners foresaw, the understandability and accuracy of the model, how the TIM could be augmented to further facilitate the integration to their organisation and the current support that the company has for creating the necessary links to utilise the model (See Appendix, A.14).

Based on their feedback, a final version of the TIM emerged (See Appendix, A.8).

4.5.5 Conclusion

By conducting the focus group, applying the TIM on the existing SaACs and analysing the results with relevance to previous studies in safety assurance, traceability and ISO 26262 a final version of the TIM was produced. Since multiple SaACs were utilised, created by different organisations, it can be assumed that the developed TIM is more generic than only suitable for the case company.

The focus group resulted in some proposed changes to the TIM which were

implemented in the fifth version of the model (See Appendix, A.8). Furthermore, positive discussions emerged on what work could be conducted at the case company in order to improve their current way of working by implementing the TIM.

Additionally, with help from existing literature and the findings during this study, a list of recommendations was produced for participants who want to utilise a TIM in order to improve the traceability of their SaACs.

These methods of evaluation provided insights into RQ.1.2 that bridged the knowledge gap that was left from completing the second iteration. The research question could now be answered based on the outcome of this iteration.

4.5.6 Artefact Evolution - Iteration 3

The fourth version of the TIM (see Appendix, A.5) was created based on analysing the six different SaAC, including the company's SaAC, that were searched for and found online in order to identify which classes were directly or indirectly available in these SaACs. Directly meaning the SaAC structure elements (Claim, Argument, Evidence etc.) and indirectly meaning the development process elements (Storage location, version, participant, activity etc.). After analysing all six cases, the classes that were represented in the SaACs and which were not were identified (See Appendix, A.13). Additionally, the identification of one reoccurring element in the cases that were not available in the TIM was made. This class was context, which was related to the claim and the argument. Based on the varying results from analysing the six cases, the importance of traceability of each and every class included in the TIM was ensured. The search into existing literature was extended in regards to traceability in SaAC and its evidence. The following section includes argumentation for keeping or removing classes from the TIM based on their relevance to traceability based on existing literature. Both types of classes were evaluated, the ones that were available and the ones that were missing, since their availability does not directly correlate to the traceability of the element. The argumentation is available in the results section 5.1.2.1.

Analysing the cases showed which classes in the TIM were most important based on their availability (See Appendix, A.13) and their importance to traceability found in existing studies (See Appendix, A.13). This led to the examination and investigation of further regarding their relevance to traceability which, If not correct, would decrease the quality of the TIM.

An additional activity that was performed, in order to create the fourth version of the TIM, consisted of applying the TIM to three different SaACs (One of those being the case company's SaAC). This was done in order to mitigate the problem of the case company's SaAC being incomplete but also to make an attempt to generalise the TIM to fit other projects. This helped to evaluate the TIMs classes, relationships and associations in comparison with other SaACs.

One of the SaAC that was picked to apply the TIM to was the Ubers SaAC for their self-driving vehicles [2] (See Appendix, A.7). This case was picked not only because its level of detail but also since it is a real-world case that the company has published as an open source document on their website. Additionally, another benefit of using this case was that the SaAC is developed for the automotive industry.

The case comprised of five top claims or safety goals that divided the case in to five different parts. In order to keep the model of the SaAC readable it was decided that the TIM would only be applied on one of these goals. In this case it showed similarities between the implementation of case company's SaAC and Ubers SaAC. In both these cases they have adjusted the artefact to fit the company's need and which then represented an ISO 26262 work product instead of consisting of one. In the application of this case, it contained the existence of multiple techniques combined in to one activity. Additionally, the existence of multiple "EvidenceProvenance" elements linked to one piece of evidence was found in the SaAC.

The other SaAC that the TIM was applied to was an automatically generated SaAC developed by Denney et al. at NASA [35] (See Appendix, A.6). It is a SaAC that is made from *"automatically generated instance arguments"* [35]. The case was developed for Unmanned Aerial Vehicles (UAS). No other open source SaAC was found that was related to the automotive industry. However, this case is for another type of vehicle and therefore has many of the same characteristics as both of the automotive cases. Even though the ISO 26262 standard is only for *"Roadside vehicles"* [5], there are similar standards for UAS. The case was also created using the GSN structure and included the same elements as the automotive cases. The same thing was found in this case as with the Uber case, which is that multiple techniques can together be used to perform one activity. An additional insight from applying the TIM to this SaAC was that multiple activities can be utilised to create one artefact.

Applying the TIM on the case company's SaAC (See Appendix, A.5), it was found that the previous assumption that a Safety requirements specification did not always relate to a claim to be false. The safety requirement specification was in all three cases connected to at least one claim. Artefact provenance, that describes the characteristics that relates to the information of the life-cycle and management responsibility of the artefact was only available in one of the three cases that the TIM was applied to. Meaning the association assuming that the artefact was associated with one Artefact provenance was incorrect and was subsequently updated to a zero-to-many relationship.

Applying the TIM to the three SaACs did provide with further insight into the associations and relationships rather than more information regarding the available classes. With just the three cases that the TIM was applied to, much of the same patterns were seen in terms of the relationships and associations. The other two SaAC were chosen from the available five based on their level of detail. The most detailed options were picked, including as many links and elements as possible.

For the final evaluation and augmentation of the TIM a focus group was conducted with experts at the case company. The results from the focus group evaluation that was conducted as the final evaluation of this study were very insightful. The questions and subsequently, the answers covered discussions regarding the applicability and quality of the TIM.

The experts expressed that the model should include more annotations, the model classes needs a more detailed description in order for everyone to understand the purpose of each class. This will enable a wider range of users to read and understand the TIM. A few of the participants expressed that once the classes were

explained to them, it made a lot more sense. The model abstraction, dividing the classes into SaAC structural classes and development process classes was deemed helpful and increased their understanding of the model and they could more easily map the classes to the real-world components. The associations between the classes were discussed. The relationships between classes were deemed accurate as far as they were concerned but they did however, suggest a few changes to the associations. One of these suggestions was that the argument aggregates a claim, or that the argument is owned by the claim. Another observation made by the experts that was discussed in detail in the focus group was the relationship between the claim and any development process class that was missing in the TIM. This feedback was used to create the final version of the TIM.

The changes made between each TIM is listed in Appendix A.0.2

4.6 Threats to Validity

To discuss the threats to validity in this study, the threats to validity that Runeson and Host [37] has identified were utilised. The types of threats are: Construct validity, Internal validity, External validity and Reliability.

4.6.1 Construct Validity

In order to ensure that all participants in this study were fully aware of the aim of the study and what, in the evaluation phases, was being evaluated. All employees that contributed or took part in the expert evaluations or workshops had previous knowledge in SaAC or worked in the team the researchers of this study were assigned to at the company. At the beginning of each meeting, evaluation or workshop with any of the employees a short introductory presentation was held in order to ensure everybody understood the purpose of the activity, what the goal with it was and what information was desired to extract from it. Any questions that arose were always addressed immediately so that any uncertainty was not carried through the entire meeting but rather clarified directly so that the participant could continue the meeting with a clearer picture of the situation and better understand the study and the purpose.

When conducting participant observations, there is a possibility of misunderstanding and forgetting information. This was mitigated by always having both researchers on site during these sessions. Note taking could therefore be delegated to one of the researchers while letting the other one focus solely on observing the scenario and interactions that took place. After each session, the researchers sat down together to expand on the notes that were taken during the observation (See Appendix, A.9-A.12), added more data that was overlooked or missed and filled in information based on the available notes. This method was useful not only to remember and understand the session better at a later date but also enabled the examination and analysis of the data while discussing and expanding the information.

4.6.2 Internal Validity

Due to time constraints and the long process for each new product at the case company, this study will be unable to cover the utilisation of the solution on a product within the company during the designated time period. Although the results will undergo expert evaluation in order to measure the success of the findings, the remaining work after this study is to apply the findings in an actual project to ensure that the desired outcome is achieved. The artefact did go through multiple rounds of expert evaluation and in addition, existing studies were investigated in traceability in relation to SaAC in order to evaluate the appropriateness of the model that was created.

As mentioned, the generated solution will not be utilised during the study on a project at the case company. The solution should be applied continuously during the development of a product and knowledge regarding how to utilise a TIM is vital for the employees at the company in order to reap the possible benefits. Therefore, guidelines were provided on how to work with a TIM in order to achieve substantial results. The recommendations available on how to increase traceability is further guidance and help in order for the case company to implement the TIM in their daily business.

There is a risk that during the first iteration, additional relevant studies were not found in the search. Due to the time constraint on this study, only recent papers (from max ten years back) were investigated in order to build a case that is up to date. Older studies were looked into but not as thoroughly. Important research might have been missed because of the targeted focus. For future research in this area, an extensive literature review is recommended and should be performed.

Selection of the participants, especially in the evaluation activities, was done with the aid from the company supervisor assigned to this study. There is a risk that the participants, even though possessing relevant roles in the company, might have been picked based on their availability and therefore not entirely without bias. An attempt was made to include existing literature and SaAC as a means to evaluate the TIM from outside sources. However, to fully mitigate this, further research in this area should look into including experts from multiple organisations.

4.6.3 External Validity

An attempt was made to generalise the results. However, since this thesis was 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. In order to mitigate this and make the results and findings more generalised, the decision was made to evaluate and apply the generated solution on other Safety Assurance Cases available online and in other existing studies. The results will be tailored to the automotive industry but applying and modifying the model based on other SaAC will augment the TIM from being limited to the structures and systems of the case company.

Additionally, the unique aspects of other industries in terms of SaACs has not been fully explored in this study because the external SaACs analysed and the case company are mainly from the automotive industry. Although the results were

aimed to be generalised, future studies should attempt to analyse and include other industries in order to further generalise the results.

4.6.4 Reliability

Since the authors of this study had no previous knowledge about the case company's practises, a significant amount of time was spent on identifying those practises and instructions. The process of data elicitation and analysis took a significant portion of the available time for this study. This also meant that some focus of the evaluation phases became dedicated to further explanation from the experts in how the process of working with SaAC, the ISO 26262 standard and general practises were conducted at the company. This did not suppress the evaluation of the TIM but did extend the time of the evaluation. Other researchers who wants to make an attempt to reproduce this study could possibly spend less time in this step if they are already familiar with the company that would serve as their case company and has all the appropriate access to data at the very beginning of the study.

4.7 Ethical considerations

In terms of the ethical considerations in this study the guidelines specified in Andrews and Pradhans paper [38] *"Ethical issues in empirical software engineering: the limits of policy"* was adhered to.

In order to conduct the study with the case company, all information that will be relevant to the study should be revealed to the researchers. In order for the company to provide this information, a non-disclosure agreement was signed to create the boundaries for revealing information in the report and for the company to protect sensitive information regarding its organisation and procedures. In order to facilitate the adherence to this agreement, a company supervisor was assigned to the project and continuous progress reports were held to both the academic and company supervisors on a bi-weekly schedule. In terms of publishing the report and the findings in it, the report was presented to the company for approval and for communicating what information was needed to be anonymous or excluded in the published report.

All participants of the workshops, expert evaluation, participant observations and focus group were employed by the case company. In terms of ethical consent, all information gathered in these sessions were orally approved for use in the report by the participants. Additionally, while making sure all data regarding the participants were anonymous the employees got a chance to review the study and the information presented in order to give them an additional chance to approve the information to be published.

5
Final Results

5.1 Traceability Information Model

A TIM was applied to support SaAC traceability in order to describe the relations among all artefacts that construct and specify the functional SaAC. The TIM is also used to documents reference links to the development process elements that are required for maintaining a SaAC. The purpose of this approach is to create a fundamental method in order to establish traceability among the artefacts in a system. Integrating the TIM could provide improvements in the maintenance of SaAC by implementing trace links.

The TIM has evolved through five versions, by which multiple evaluation methods have been conducted in order to improve the model. Experts working with SaAC were involved throughout the entire study. The final model is showcased in three different abstraction levels in order to provide a more descriptive concept of the TIM and present the reader with more in dept information of the model and its context. Based on the experts recommendations, this model could be used by various stakeholders within the company, where their interest and fields of experience vary.

TIM Abstract View Model
The top level abstraction was a way of divide the TIM elements into two blocks: Safety Case Structure Elements (SCSE) and Development Related Elements (DRE). This view concentrates on the general associations between the two categories and it provides an understanding of how SaAC elements are related to the development process elements, in the context of supporting the SaAC. The list of associations and their logical direction is presented in Figure 5.1: they provide an indication of nature of actions triggered from the DRE side regarding creating a new element or updating one in the SCSE side, while it is a referencing nature the other way around.

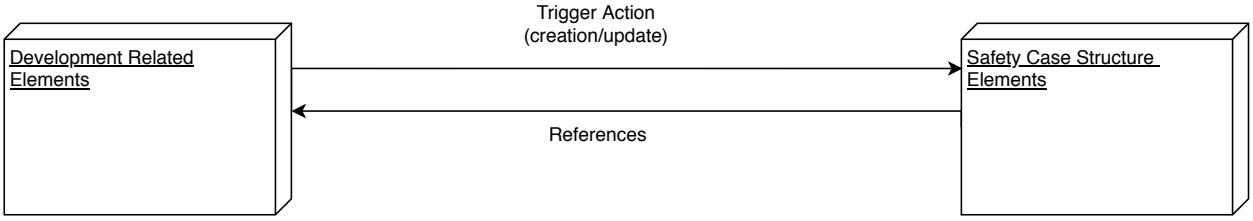

Figure 5.1: Final Result - TIM Abstract View

The next level of abstraction focuses on each block in a more detailed and

independent view.

5.1.1 Detailed View - Safety Case Structure Element (SCSE)

The detailed view of the SCSE visualises the traceability among the safety case elements and can be seen in Figure 5.2. The classes in the diagram represent the structure of a GSN [15] SaAC, they are represented because they are the main building blocks of a SaAC. These elements includes; Top claim, Claim, Argument, Piece of evidence and Context. Additional classes were added in order to provide better information regarding traceability, including; Evidence Provenance and Analysis Document. The associations towards the artefact class and in between classes are defined in Figure 5.2, the diagram is also provided with a colour map that shows the origin of each class.

The definition of the classes in the detailed view are defined as follows:

Claim: A statement that is defended within argument, where the assessment of this statement could end up true or false.

Top Claim: This class is inheriting the claim class in order to represent the Top-Claim type of claims, this class is used to show a complete structure of the safety case structure.

Sub-Claim: This class is inheriting the claim class in order to represent the Sub-Claim type of claims, this class is used to show a complete structure of the safety case structure.

Argument: A description of information that includes an argumentation with the intention of supporting a claim.

Piece Of Evidence: A reference to presenting an evidence to support a claim or an argument.

Context: Present an assumption about the system and working environment.

Evidence Provenance: Provide the history information about an evidence in regards of its provenance and how it was congregated.

Analysis Document: A document that relates to a Claim in order to contextualise it. It's the type of supporting documents that are needed to be referenced in association to an artefact to give a complete trace information to the situation. an example is a simulation result document. Information in the Analysis Document is however often used as evidence.

Classes that was inspired by Nair et al. [12] and Taguchi et al. [18] are claim,

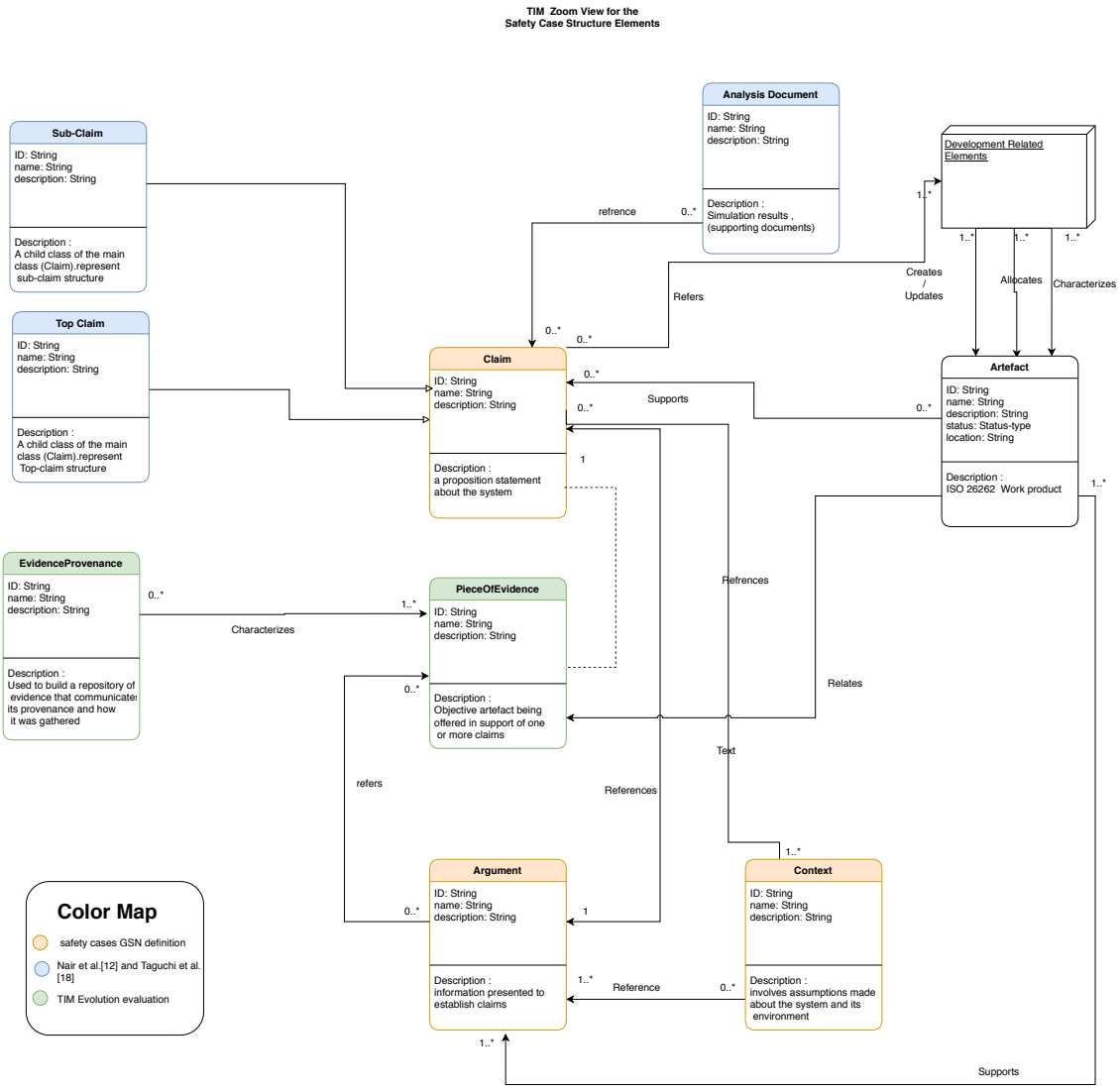

Figure 5.2: Final Result - TIM SCSE View

argument, piece of evidence and evidence provenance. The associations between classes were altered as a substantial part of the TIM evolution. Additionally, the context, analysis document and the safety requirement specification classes were added to support the model's ability to capture trace-link information needed for SaAC maintainability.

5.1.2 Detailed View - Development Related Elements (DRE):

The detailed view of the DRE elements provides traceability information among development elements referenced by the SaAC artefact and can be viewed in Figure 5.3. These classes are; Participant, Storage location, Artefact Provenance, End user function, Activity and Technique. the associations towards the artefact class and in between classes are defined in Figure 5.3, the diagram is also provided with a colour

map that shows the origin of each class.

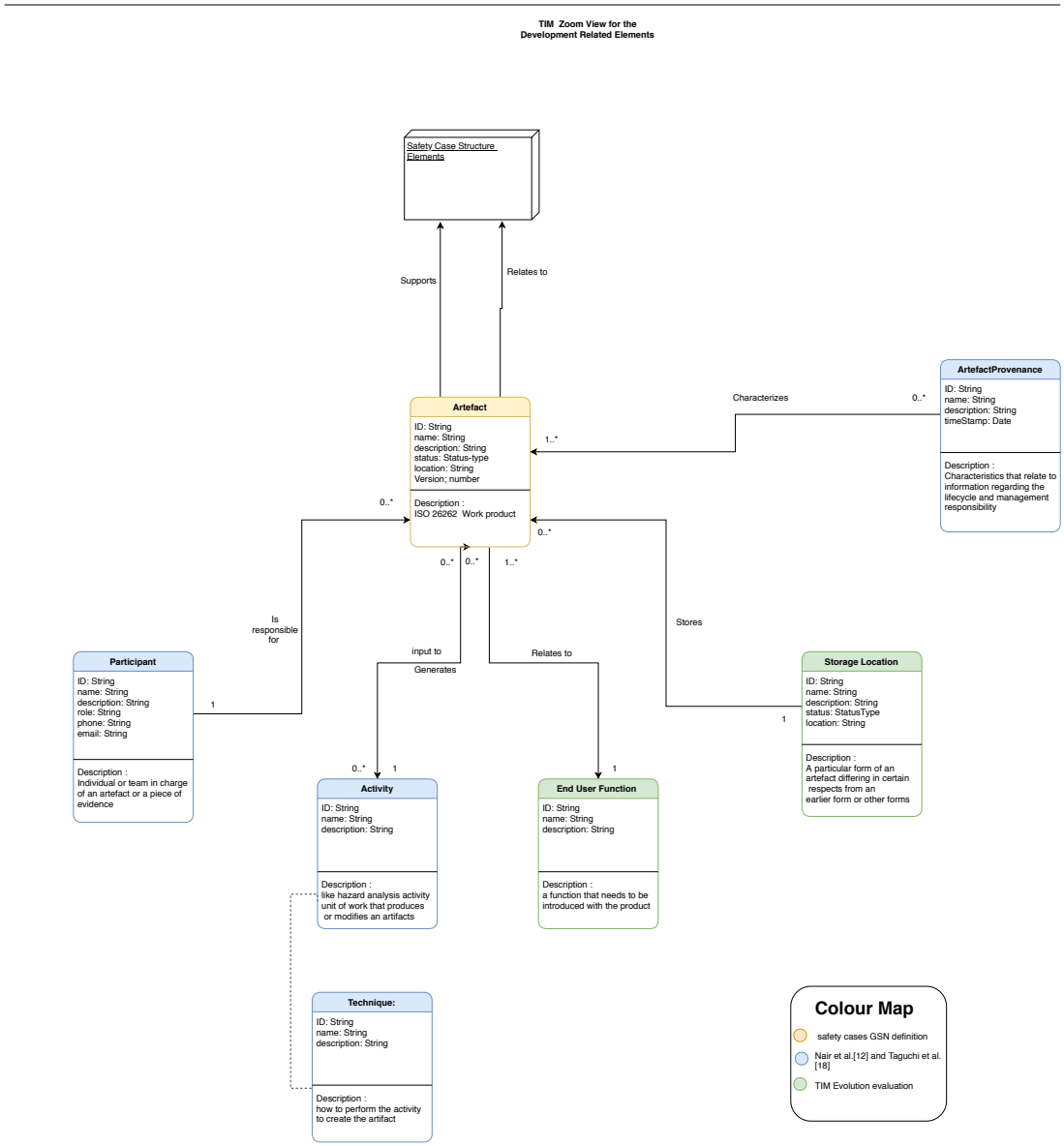

Figure 5.3: Final Result -TIM DRE View

The definition of the classes in the detailed view are defined as follows::

Participant: Used to specify parties who are responsible of creating and managing an artefact or an artefact asset.

Storage Location: Indicated where a certain file or document can be located across multiple applications.

Artefact Provenance: Provides historical information about the artefact provenance regarding how it was created and managed during its life cycle.

End User Function: The feature or function that the SaAC evidence is collected in order to argue that it is safe.

Activity: Units of actions that affect the artefacts or an artefact assets, in terms of creation or management changes.

Technique: Provides a procedure description on how an activity affecting an artefact is performed.

The Participant, Artefact Provenance, Activity and Technique were inspired by both Nair et al. [12] and Taguchi et al. [18] papers. The different approaches employed in using those classes were based on multiple rounds of expert evaluation. The associations were augmented in order to support traceability in regards to the artefact. The motivation for these changes is discussed in section 4 in this report. Adding the End User Function class was done in order to support the functional safety cases structure at the case company and a reason as to why the project class was removed in the TIM. The Storage Location class was introduced as a reference to the physical location of the artefact, which enables the traceability to various systems involved in the SaAC development.

5.1.2.1 DRE and their importance to traceability

The results from applying the TIM on the existing cases produced a list of what classes or references existed in the SaACs. In order to argue for keeping or removing the classes that were either missing or existing in the cases, existing literature was investigated. For each class, missing or existing it was found that at least one source showing evidence for the importance of the element to a SaAC in relation to traceability. The following contains the argumentation for altering or keeping each one of the classes in the DRE detailed view of the TIMs classes. The classes that were removed based on lack of supporting tractability information connection to the SaAC elements and/or added increased complexity to the model.

Participant Participant information in a TIM regards to the team or person who is responsible for an artefact. This is included, among other reasons, in order to know where the artefact stem from but also who to contact when changes are needed. This is available in the case company's SaACs provided, but not in any other case that were found online. There are sources stating the importance of including a participant in relation to the artefact [12] and based on the experts at the case company, is a very important aspect of the SaACs traceability. Therefore, the assumption for the missing participant data in the other cases are that this information was omitted before submission due to GDPR [39] or that information about the teams are sensitive data.

Artefact Provenance Artefact provenance is described as follows, *"Shows how the artefact was created and managed over their life cycle, and what techniques and resources were used in their generation"* [40]. In terms of its importance to traceabil-

ity, when a change is made and an artefact needs updating its important to identify when in the life-cycle the artefact was created and how.

End User Function Since we are addressing a function safety scenario and all SaACs in the case company stems from an 'end user function', this class can not be omitted. In the industrial setting this study was conducted in, the product was described as comprised a multitude of end user functions but a SaAC never covered more than one of these functions. Outside of the particular setting of this study, all SaAC contain argumentation for why a particular function or system is deemed appropriately safe [3]. Indicating that the traceability to this artefact is vital for the model.

Context A context is an encapsulation of an argument, top claim or a claim which determines the scope of the element. E.g., a context can be the ASIL level given to the claim. Some changes, such as a minor operational role change, may seem innocuous at first when given superficial consideration, but actually have a significant impact with respect to the context and argument of the safety case. Hence, Changing a context element challenges not only the most immediate associated goal or strategy but also all of the child goals and strategies underneath that item within the goal structure [10]. Including a trace link to the context has potential to be beneficial in order to track dependable changes. Since this justifies its importance to maintainability and traceability in SaACs, it becomes an important element to be included in the TIM.

Storage Location The storage location is a representation of the links to where an artefact in the SaAC are available throughout the various systems that might be involved. Since artefacts and evidence can be created with and stored within different tools [41] it is often difficult for practitioners to manage change in SaAC maintenance. Therefore, keeping the representation of the artefacts physical location is valuable. Storage location will provide a dependency link to where a change should be applied, those links are used in order to track the composition of objects and manage the repercussion of changes in one on other object that depends on it [41].

Activity and Technique The activity together with the technique contains the information that help practitioners identify the event generating each artefact and the process that specify the steps in order to modify or create it. Event information was found to be important for the purpose of change management for SaAC maintenance. *"Change event recognition is useful because it can provide a high-level documentation of the changes implemented in the requirements specification. This complements existing change management practices by supporting the process of updating entities related to the change""* [42].

5.1.3 The Artefact Model

From both the papers this study was inspired by Nair et al. [12] and Taguchi et al.[18], the artefact was kept as the main focus of the TIM. The artefact represents an ISO 26262 work product, which is what SaACs will produce in order to comply with the ISO 26262 standard.

Before the final evaluation of the TIM, the experts expressed that it was not clear as to what the Artefact class represented. Therefore, the inclusion of an explanatory model (See figure 5.4) has been made, which represents the artefact abstract class encapsulating additional classes that are inherited from the main artefact. This helped the experts in the focus group, the final evaluation, to understand what the artefact class represented in the TIM in regards to instantiating the artefact class.

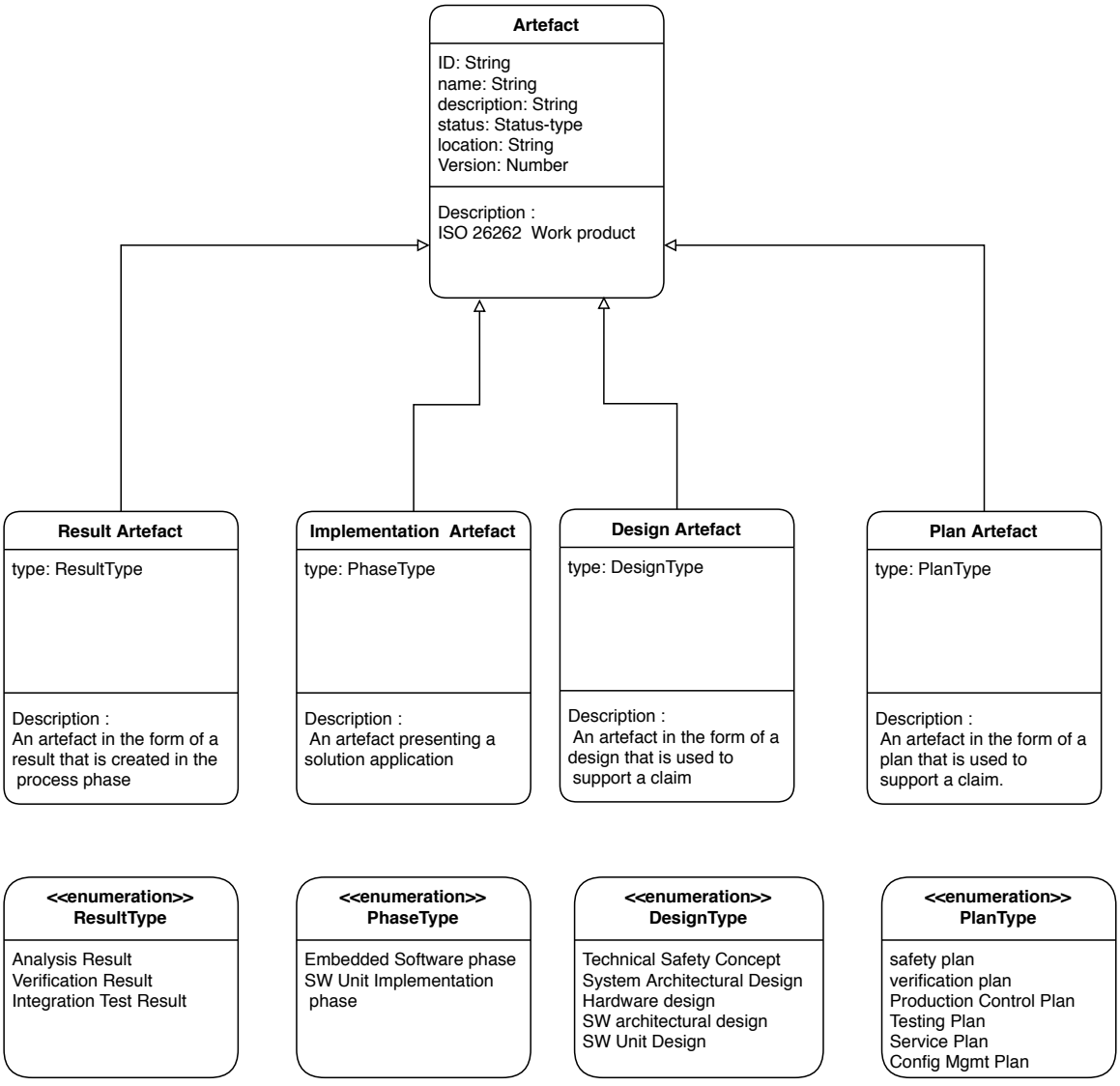

Figure 5.4: Artefact Model - a decomposition of the artefact class in the TIM

The Artefact sub-classes are defined as follows:

Artefact: "represents the distinguishable units of data used in a structured assurance case" [40].

Result Artefact: An artefact in the form of a result that is created in the process phase. This class uses the enumeration types that includes: Analysis Result, Verification Result and Integration Test Result.

Implementation Artefact: An artefact presenting a solution application. This class uses enumeration types that includes: Embedded Software phase and SW Unit Implementation phase.

Design Artefact: A design that is used to support a claim. This class uses enumeration types that includes: Technical Safety Concept,System Architectural Design, Hardware design, SW architectural design and SW Unit Design.

Plan Artefact: A plan that is used to support a claim. This class uses enumeration types that includes: Safety plan, Verification plan, Production Control Plan, Testing Plan, Service Plan and Configuration Management Plan.

The types used in these classes are extracted for the ISO26262 work products list provided by the case company.

5.1.4 TIM Links and Associations relations

Using the abstract view enabled further detailed identification of the relationships between elements included in the safety case structure and the development related ones. It was found that the DRE contributes to the SCSE in terms of creating, updating information to the SCSE. This indicated that the DRE have an action oriented effect on the SCSE. In the other direction, the SCSE provides reference information which are supported in the DRE.

The associations in the SCSE are introduced in order to provide a complete representation of the structure of the SaAC in the case company and traceability among the SaAC elements. This is especially demonstrated in the following links:

- Claim - Argument, relation association
- Claim - Piece of Evidence, dependency association
- Claim - Top Claim, inheritance association
- Claim - Context, contextual association
- Argument - Context, contextual association

The remaining associations are necessary in order to provide supporting reference provenance information.

The associations in the DRE are built around the artefact specification and the

connection between each type of development process entity towards the core artefact class of the diagram. These associations are directly connected to it, as they represent the explicit traceability information between them.

In terms of the activity and techniques, the findings indicate that the technique has an implicit relation to the artefact through the activity. The activity is responsible of generating and updating artefacts while the techniques specifies the procedures required in order to conduct the activity. The activity and technique classes were available in both referenced papers [12, 18]. From a maintenance perspective, being able to quickly identify which activity and technique was utilised in order to perform a rerun of said activity and technique e.g., code tests when a change has occurred is important.

In regards to the participant class, the case company did have trace links available to the reviewer of the SaAC but not to the developer or team responsible for an artefact. Regarding maintenance of the SaAC, introducing an ownership trace link to the artefact is beneficial for when artefacts has to be updated. The classes that are added, in addition to the TIM that this study gathered inspiration from Nair et al. [12] and Taguchi et al. [18], are: Storage location, End user function and Analysis document. These classes were added based on a combination of data gathered from the case company's expert evaluations, available documents, identified problems and important aspects in existing research on traceability in SaACs.

6
Conclusion

6.1 Discussion

The following contains a discussion about the result and answer to the research question and how they relate to existing studies.

In order to answer the first RQ, the focus of this study became to develop a TIM based on existing literature and the need from the case company to improve the maintenance, in particular traceability, in their SaAC. Existing research was investigated and an attempt was made to translate the findings into a solution that can be utilised by practitioners in an industrial setting, especially the case company. Industrial settings contain a lot more variables that are not considered in an artificial or selective setting that are often simulated in studies in order to test possible solutions. This study is inspired by Nair et al. [12] and Taguchi et al. [18] but has been altered substantially in order to be tailored to the automotive industry with influences from the case company and their needs, but also applied and augmented based on five open source SaAC from other organisations to validate and to generalise the findings and results.

In order to build upon these existing solutions in terms of attempting to solve existing problems regarding SaAC and traceability, the focus have been on the issues revolving evidence and documents of SaACs are spread over different tools [12, 11]. Introducing traceability to the tools has the potential to facilitate this known issue. Additionally, an issue that was heavily focused on is the requirement hierarchy that SaAC are built around and has to adhere to. Implementing traceability between requirements, claims and evidence is vital for the practitioners in order to facilitate their work in maintaining SaAC.

In regards to the problems faced by the case company in terms of maintainability, the experts in the case company agree on that the study and its results, in particular the TIM, has made them realise gaps in their current guidelines and instructions which the TIM will aid them in solving. These issues are mainly regarding the maintainability of the SaACs that has been overlooked until now. Introducing the traceability links established in the TIM will help them improve the guidelines to not only cover creation but also maintenance. The model will also help in identifying which traceability links are already available in the company's systems and enable the identification of the missing links.

In terms of generalise-ability, the model was deemed general enough to be applied on different types of products. This was just the experts' impression but it was expressed that this would of course have to be tested in order to verify but

no initial issues with the model in terms of generalisation internally in the company was expressed. The TIM has the possible potential and is general enough to be implemented on any SaAC with minimum changes depending on the structure and safety standard that each industrial setting will comprise of.

Research Question 1.1 asks, *How can we describe the relevant relationships among artefacts and elements of the SaAC?* As discovered in the first iteration of the study, there are many possible solutions to introduce traceability in SaAC but based on the results from existing literature and the experts at the case company, creating and implementing a TIM has seen the most promising results in this area.

Mader et al. [43] describes the reasons for implementing and benefits of using a TIM to introduce traceability in any system as follows; In projects with multiple stakeholders, the implementation of a TIM will ensure consistency in the result. Tracing information can be very complex and a TIM will facilitate creating the trace links and improve the process of validating changes made to the elements that are encapsulated in the model. Additionally, the author states that a TIM is necessary for automated traceability handling.

Based on the findings from the first iteration the assumption can be made that creating a TIM and implementing it into the structure of the way of working with SaAC will aid in identifying and maintaining traceability between the elements of an SaAC. Both the structure of the SaAC and the GSN elements required to create a case but also to link these structural elements to the evidence and documents created during the development process related to safety assurance will facilitate maintenance of SaACs in an industrial setting.

Research Question 1.2 asks, *What are the relevant relationships among artefacts and elements of the SaACs?* After finding a sound method on how to implement a structure for realising the relationships between element and artefacts in a SaAC it was needed to figure out how these relationships can be identified and subsequently be implemented in the TIM. The development of the TIM and the evolution of the model based on the expert evaluation in the second iteration of the study progressed the study towards the goal of identifying the correct relationships and what classes are relevant for traceability in SaACs. The work was closely conducted with the case company to identify the structure and elements used for SaAC creation in order to translate those aspects in to the TIM.

For the third and final iteration an attempt was made to generalise the findings based on existing literature and other SaAC available online. Some interesting insights were found in applying the TIM to these cases and the changes made to the TIM in order to adhere to those structures did not conflict with the application of the TIM to the case company's SaAC, but rather improved upon it. Indicating that a more generalised solution could be beneficial to the application of the TIM in an industrial setting even though not tailored to a specific case. Additionally, applying the TIM on a SaAC [2] that was substantially larger and more complex than the case company's SaAC strongly verified the known issue expressed in previous studies that both maintenance of a SaAC and the implementation of a TIM can take a substantial amount of time to utilise. This indicates that it is important to find a way to integrate the trace links and the model into the industrial cases in a manner as to not create a considerable amount of overhead, which would be an interesting

topic for any future work performed based on the insights made in this study.

Additionally, the focus group evaluation with the experts in different areas of working with SaACs at the case company helped provide insights into by whom this model will be used and how it could improve their way of working. To utilise this model it is first important to assess the structure and hierarchy of an industrial setting. In the case company's structure, there are process developers whom will apply the model and integrate it into the way of working at the company. The developers will have to adapt their development process to adhere to these new guidelines but will probably not be interacting directly with the TIM. The instructions and guidelines on how to write SaACs at the company will be augmented and enhanced with the help of the TIM together with the findings and insights from the results of this study. This insight is in unison with one of the reasons to implement a TIM described by Mader et al. [43] as follows; Practitioners, who did not create the model, who will be interacting with the TIM in one way or another need to know how it is defined and what to expect from working with it. By integrating the TIM in to the guidelines and instructions at the case company the model will be utilised indirectly by developers and fewer drastic changes in the way of working will have to be implemented.

The TIM created is a part of a much bigger scope in terms of maintainability, there are processes and methods that needs to be put in place in order to further improve the maintainability of a SaAC and additionally to fully utilise the TIM. For the sake of a viable scope for this study, the TIM was the only part of the bigger picture that was fully investigated and created.

The links between some artefacts and work products were expressed as already available and used at the case company. Versions of all the artefacts are available in their version control system. The practitioners discussed implicit and explicit traceability. The implicit traceability was referred to as elements and components having the same name, which was said to be non ideal. The experts sees potential with the TIM to explicitly identify which links are available in the systems and that they would not be sure about what links they already have until the model has been implemented. "We have some of these (links), but definitely not all the links that we want and are needed" was expressed by one practitioners on which the rest agreed. Development process elements are not traced at all in the current state of the company.

The company's goal for the future is to implement the TIM into their development platform for embedded systems. In that scenario the Tool developers of the company will work to integrate the model into their tool and the TIM will then become an integral and fundamental map of how each element regarding their safety culture and safety assurance is structured and linked together. Every company structure is different and the presence of a development platform tool is not a given.

Even though it is plausible the TIM can be utilised in a beneficial way regardless of company structure and the availability of tools to support it, the additional workload that will have to be done is unsure and out of scope for this study. It is however, an interesting question that should be investigated in the future.

Answering both sub-questions, has led to an answer for RQ.1, *How can we*

trace the relevant relationships in SaAC and the containing elements to their relevant development artefacts? In order to be able to maintain a SaAC, one needs to be able to update the case when a change occurs. A big aspect of this updating process is to easily be able to identify what parts of the case could have been affected by the change. Traceability between the elements and artefacts in a SaAC will tell the practitioner(s) working on the case which other elements, linked to the element in which the change was made, might have been impacted.

In the focus group evaluation session, a participant stated how the TIM would help them redefine their structure in terms of working with SaAC creation by introducing, based on the insights made from the TIM, a maintainability structure in to their way of working from these trace links. If the model contains all the correct links between elements in the SaAC, this would mean that every one of those links represent that a change will have an impact on its linked elements when a change is made. E.g., If an element is connected by an association to three other elements, all three of those elements should be analysed and updated accordingly when a change is made to the first element. Subsequently, the links connected to those three elements will also have to be checked for any impact of the change. The TIM facilities this chain of changes and has the potential to decrease the time to update the cascading change impact on the elements that are linked together.

In addition to the answers to our RQs, a few interesting topics were uncovered that are worth discussing.

First, even though the TIM was seen as possessing potential to help increasing maintenance and traceability in the SaAC at the case company, the practise of utilising the TIM for the creation and maintenance of safety cases were thought to add a lot of extra time to create the trace links between all components and artefacts across tools and formats. The findings in this study and the TIM created could be the base of future studies focusing on automating the creation and instantiation of the trace links expressed in the TIM. This would address one core issue in SaAC expressed by multiple existing studies that is creating and maintain SaAC is a cumbersome and time consuming task which often become very complex as the product grows in size. This is an important issue that has to be solved in order to facilitate the work practitioners are doing with SaACs.

Second, while there were strong indications of the value of the Traceability Information Model produced within this study, there is a need to utilise it in a ongoing project to see how it fares during a normal project life-cycle instead of a simulated environment such as the workshop performed for the evaluation. A comparison between utilising the TIM as solely a maintenance model, implementing it on an already finished product, versus an ongoing product during the development phase would evaluate in which state of the product and its life-cycle the TIM is most optimal to introduce. While the focus of the study was maintenance in SaAC, the TIM should tested in the development of a product in order to establish the trace links between the elements as a continuous process. Since the TIM will grow in sync with the product, attempting to implement the TIM once the product is complete and enters the maintenance phase will take a lot of time and effort which will perhaps be off putting for many practitioners.

Finally, the case company has expressed their desire to move all documents,

processes and information storage to the application utilised at the company. The tool is a development platform for embedded systems. As of the date of publication, the case company has only expressed the wish for moving everything in to the utilised tool while the state of their documents and information is still spread over multiple tools and sources. Future work in this area of this study and a way to simplify the associations and increase the maintainability of a product is to introduce the TIM and its trace links into the development platform along with all documents and information stored in the application as well. This would enable practitioners to link the classes in the TIM to the documents in the application and make the trace links not just between the artefacts and elements but also link everything to the TIM in a simple and straightforward way, using the TIM as an embedded model of their tool to structure and link all relevant information together. Implementing the appropriate trace links into the development platform will however be manual work, but since the model only represents the elements and the relationships between those elements this model is independent of which tool an organisation utilise.

6.1.1 Recommendations to improve Traceability

In terms of implementing traceability, there are existing studies that advocate a more brute-force approach in which all requirements are thoroughly traced across the life cycle of a system or product [44, 41]. The aim for these recommendations were to find a more pragmatic approach. A list of recommendations in the paper 'Strategic Traceability for safety-Critical Projects' has been provided to apply traceability strategically in safety-critical projects to systematically build a case for product safety and support the assessment process [45]. The recommendations introduce practices which can be used in order to establish traceability that is cost-effective and provides effective support for constructing a safety-critical system and assessing its safety.

In addition to these guidelines, the following are a few suggestions that are proposed based on the work conducted in this study and the main takeaways that have been discovered along the way. It is important to include stakeholders with different roles, when developing the TIM design. As seen when the model was evaluated, experts of different roles provide comprehensive feedback on the trace link information that would otherwise be difficult to attain. It is important to represent how these trace-links are constructed in the TIM and investigate the strategic value of representing that information in the TIM. These practices are particularly important as they provide a sustainable solution that consider traceability from the very beginning of the development life cycle of any product. In order to ensure that the added value of using a TIM is achieved, providing information about the relationships among artefacts and elements of the SaAC is crucial. The information is needed both initially and continuously during the life cycle of a SaAC, starting from structuring the SaAC and the development process.

The potential users are the people working on process development, development of "the way of working", the employees that audit and review SaACs and the ones who develop the instructions and guidelines to create and maintain SaACs. In order to establish how to work with the TIM, the model needs to be integrated

into the way of working and the process related to creating and maintaining SaAC. The process developers will therefore be directly affected by the model and most possibly will be the ones to implement the TIM. Indirectly affected by the TIM and the process revolving it will be the developers. They will only be affected in the way the process of how their work is done will be performed. Other potential users of the TIM will be the tool developers. A possibility that was explored and discussed in the focus group was that the company will be able to utilise the currently used tool to integrate the traceability model into. Tool support to create SaAC is important to the case company and utilising the TIM will help describe and capture the important aspect of implementing traceability in the SaACs. The model will also be useful to identify what traceability links are not available or created today. This solution is by no means constrained by the development process tool utilised at other industrial settings and integrating the TIM into the utilised tool is recommended if this possible solution is desired.

While the TIM might not see the best results in the hands of the developers, but rather to the process developers. A simplified model, based on the TIM could possibly be given to the developers to facilitate their work with the new guidelines for traceability.

6.2 Conclusion

The results of this study has provided substantial indications of the importance of implementing a TIM to support SaACs maintainability. This was accomplished by investigating available literature findings in this area, supported with an evaluation in the shape of a workshop with experts working with SaAC. Using a TIM has been found to be an suitable model to describe the relationships among SaAC elements and artefacts. Working through three iterations, the TIM design has been able to evolve in a fundamental way. The evolution process included mapping the TIM to various sources which were; the SaAC from the case company and another five SaAC form various organisations and research papers. This accomplished a generalised solution, which has shown indications to the identification of what the relationships among SaAC that should address and represent in the TIM. The developed TIM comprises two types of traceability information, which are: traceability among the SaAC elements and traceability information that references development artefacts and elements required to support the SaAC. This representation visualises how the structure of a SaAC, that is used in an industrial setting, has a strong impact on specifying the traces which should be created and maintained between SaAC artefacts and development process elements. Developing a TIM to document this information has provided a clear view to various stakeholders regarding the importance of traces to the SaAC and how this approach could be integrated into the development platform and process. A strategic planing of how to use the TIM is needed to make sure that appropriate stakeholders are informed and included from the very beginning, as well as defining working procedures that integrates the TIM.

6.2.1 Future Work

Even though this study has dealt with plausible progress in terms of the issue of dealing with evidence found in various tools and formats, the issues regarding complexity and scale is still very present. A possible viable future solution to this is to make an attempt to utilise the TIM created and the insights gained to automate the creation and maintenance of SaACs. This is a necessary implementation in order to save time and increase efficiency. Additionally, work regarding the integration of the TIM into the strategic planing and work process guidelines in the automotive industry is required.

Bibliography

[1] E. Denney and G. Pai, "Tool support for assurance case development," *Automated Software Engineering*, vol. 25, no. 3, pp. 435–499, 2018.

[2] Safety assurance case, uber self-driving vehicle safety. https://uberatg.com/safetycase/gsn. Accessed: 2020-04-07.

[3] R. Hawkins, I. Habli, T. Kelly, and J. McDermid, "Assurance cases and prescriptive software safety certification: A comparative study," *Safety science*, vol. 59, pp. 55–71, 2013.

[4] R. Bloomfield and P. Bishop, "Safety and assurance cases: Past, present and possible future–an adelard perspective," in *Making Systems Safer*. Springer, 2010, pp. 51–67.

[5] "International standardization organization," *ISO/IEC*, pp. 5–6, 2018.

[6] G. Schildbach, "On the application of iso 26262 in control design for automated vehicles," *arXiv preprint arXiv:1804.04349*, 2018.

[7] Y. Luo, A. K. Saberi, and M. van den Brand, "Safety-driven development and iso 26262," in *Automotive Systems and Software Engineering*. Springer, 2019, pp. 225–254.

[8] J. Birch, R. Rivett, I. Habli, B. Bradshaw, J. Botham, D. Higham, P. Jesty, H. Monkhouse, and R. Palin, "Safety cases and their role in iso 26262 functional safety assessment," in *International Conference on Computer Safety, Reliability, and Security*. Springer, 2013, pp. 154–165.

[9] A. Agrawal, S. Khoshmanesh, M. Vierhauser, M. Rahimi, J. Cleland-Huang, and R. Lutz, "Leveraging artifact trees to evolve and reuse safety cases," in *2019 IEEE/ACM 41st International Conference on Software Engineering (ICSE)*. IEEE, 2019, pp. 1222–1233.

[10] T. P. Kelly and J. A. McDermid, "A systematic approach to safety case maintenance," in *International Conference on Computer Safety, Reliability, and Security*. Springer, 1999, pp. 13–26.

[11] J. Chen, M. Goodrum, R. Metoyer, and J. Cleland-Huang, "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*, 2018, pp. 57–60.

[12] S. Nair, J. L. de la Vara, A. Melzi, G. Tagliaferri, L. De-La-Beaujardiere, and F. Belmonte, "Safety evidence traceability: Problem analysis and model," in *International working conference on requirements engineering: Foundation for software quality*. Springer, 2014, pp. 309–324.

[13] T. Kelly and R. Weaver, "The goal structuring notation–a safety argument notation," in *Proceedings of the dependable systems and networks 2004 workshop on assurance cases*. Citeseer, 2004, p. 6.

[14] F. Warg, H. Blom, J. Borg, and R. Johansson, "Continuous deployment for dependable systems with continuous assurance cases," in *2019 IEEE International Symposium on Software Reliability Engineering, WoSoCer workshop*. IEEE Computer Society, 2019.

[15] K. Attwood, P. Chinneck, M. Clarke, G. Cleland, M. Coates, T. Cockram, G. Despotou, L. Emmet, J. Fenn, B. Gorry *et al.*, "Gsn community standard version 1," *Origin Consulting (York) Limited*, 2011.

[16] O. Jaradat and I. Bate, "Systematic maintenance of safety cases to reduce risk," in *International Conference on Computer Safety, Reliability, and Security*. Springer, 2016, pp. 17–29.

[17] V. Katta, C. Raspotnig, and T. Stålhane, "Presenting a traceability based approach for safety argumentation," *Proceedings of ESREL 2013*, pp. 2037–2046, 2013.

[18] K. Taguchi, S. Daisuke, H. Nishihara, and T. Takai, "Linking traceability with gsn," in *2014 IEEE International Symposium on Software Reliability Engineering Workshops*. IEEE, 2014, pp. 192–197.

[19] J. Agee, "Developing qualitative research questions: a reflective process," *International journal of qualitative studies in education*, vol. 22, no. 4, pp. 431–447, 2009.

[20] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design science in information systems research," *MIS quarterly*, pp. 75–105, 2004.

[21] V. Vaishnavi and B. Kuechler, "Design research in information systems/association for information systems. 2005," 2011.

[22] N. K. Denzin, *The research act: A theoretical introduction to sociological methods*. Transaction publishers, 2017.

[23] G. A. Bowen *et al.*, "Document analysis as a qualitative research method," *Qualitative research journal*, vol. 9, no. 2, p. 27, 2009.

[24] T. C. Lethbridge, S. E. Sim, and J. Singer, "Studying software engineers: Data collection techniques for software field studies," *Empirical software engineering*, vol. 10, no. 3, pp. 311–341, 2005.

[25] N. Mack, "Qualitative research methods: A data collector's field guide," 2005.

[26] C.-P. Klas, *Expert evaluation methods*. Facet, 2012, p. 75–84.

[27] R. Ørngreen and K. Levinsen, "Workshops as a research methodology." *Electronic Journal of E-learning*, vol. 15, no. 1, pp. 70–81, 2017.

[28] L. Darsø, *Innovation in the Making*. Samfundslitteratur, 2001.

[29] S. E. Jackson, A. Joshi, and N. L. Erhardt, "Recent research on team and organizational diversity: Swot analysis and implications," *Journal of management*, vol. 29, no. 6, pp. 801–830, 2003.

[30] R. Krueger and M. Casey, "Focus groups: a practical guide for applied research," Sage Publications, Inc., Tech. Rep., 2000.

[31] M. C. Tremblay, A. R. Hevner, and D. J. Berndt, "Focus groups for artifact refinement and evaluation in design research." *Cais*, vol. 26, no. 27, pp. 599–618, 2010.

[32] W. Ridderhof, H.-G. Gross, and H. Doerr, "Establishing evidence for safety cases in automotive systems–a case study," in *International Conference on Computer Safety, Reliability, and Security*. Springer, 2007, pp. 1–13.

[33] R. Hawkins, I. Habli, D. Kolovos, R. Paige, and T. Kelly, "Weaving an assurance case from design: a model-based approach," in *2015 IEEE 16th International Symposium on High Assurance Systems Engineering*. IEEE, 2015, pp. 110–117.

[34] S. Kokaly, R. Salay, M. Chechik, M. Lawford, and T. Maibaum, "Safety case impact assessment in automotive software systems: an improved model-based approach," in *International Conference on Computer Safety, Reliability, and Security*. Springer, 2017, pp. 69–85.

[35] E. Denney and G. Pai, "Tool support for assurance case development," *Automated Software Engineering*, vol. 25, no. 3, pp. 435–499, 2018.

[36] C. Cârlan, T. A. Beyene, and H. Ruess, "Integrated formal methods for constructing assurance cases," in *2016 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW)*. IEEE, 2016, pp. 221–228.

[37] P. Runeson and M. Höst, "Guidelines for conducting and reporting case study research in software engineering," *Empirical software engineering*, vol. 14, no. 2, p. 131, 2009.

[38] A. A. Andrews and A. S. Pradhan, "Ethical issues in empirical software engineering: the limits of policy," *Empirical Software Engineering*, vol. 6, no. 2, pp. 105–110, 2001.

[39] General data protection regulation (gdpr). https://gdpr.eu/. Accessed: 2020-05-14.

[40] O. SACM, "Structured assurance case meta-model," 2020.

[41] B. Ramesh and M. Jarke, "Toward reference models for requirements traceability," *IEEE transactions on software engineering*, vol. 27, no. 1, pp. 58–93, 2001.

[42] J. Cleland-Huang, C. K. Chang, and Yujia Ge, "Supporting event based traceability through high-level recognition of change events," in *Proceedings 26th Annual International Computer Software and Applications*, 2002, pp. 595–600.

[43] P. Mader, O. Gotel, and I. Philippow, "Getting back to basics: Promoting the use of a traceability information model in practice," in *2009 ICSE Workshop on Traceability in Emerging Forms of Software Engineering*. IEEE, 2009, pp. 21–25.

[44] O. C. Gotel and C. Finkelstein, "An analysis of the requirements traceability problem," in *Proceedings of IEEE International Conference on Requirements Engineering*. IEEE, 1994, pp. 94–101.

[45] P. Mäder, P. L. Jones, Y. Zhang, and J. Cleland-Huang, "Strategic traceability for safety-critical projects," *IEEE software*, vol. 30, no. 3, pp. 58–66, 2013.

A

Appendix 1

A.0.1 Traceability Information Models

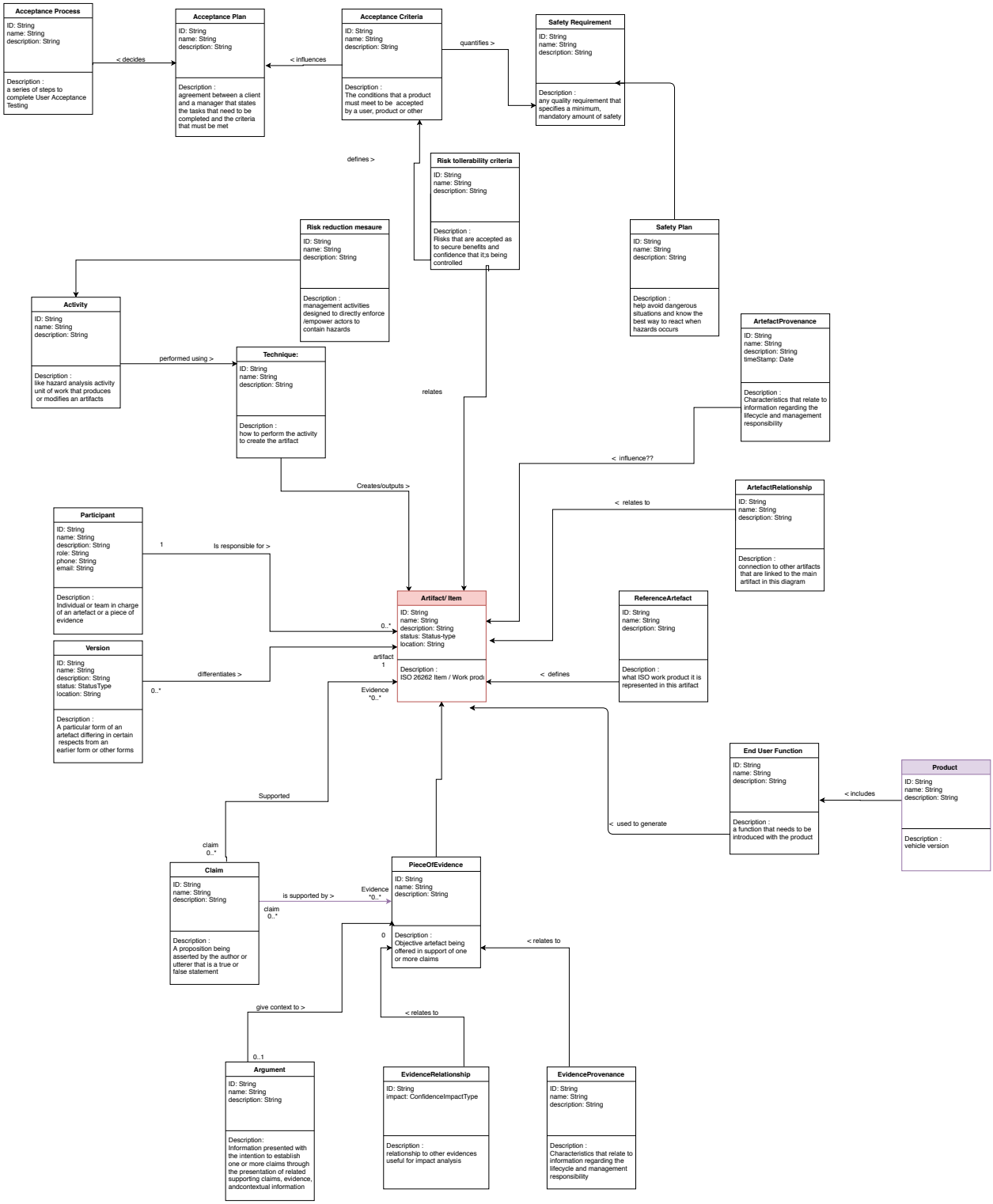

Figure A.1: Iteration 2 - First development

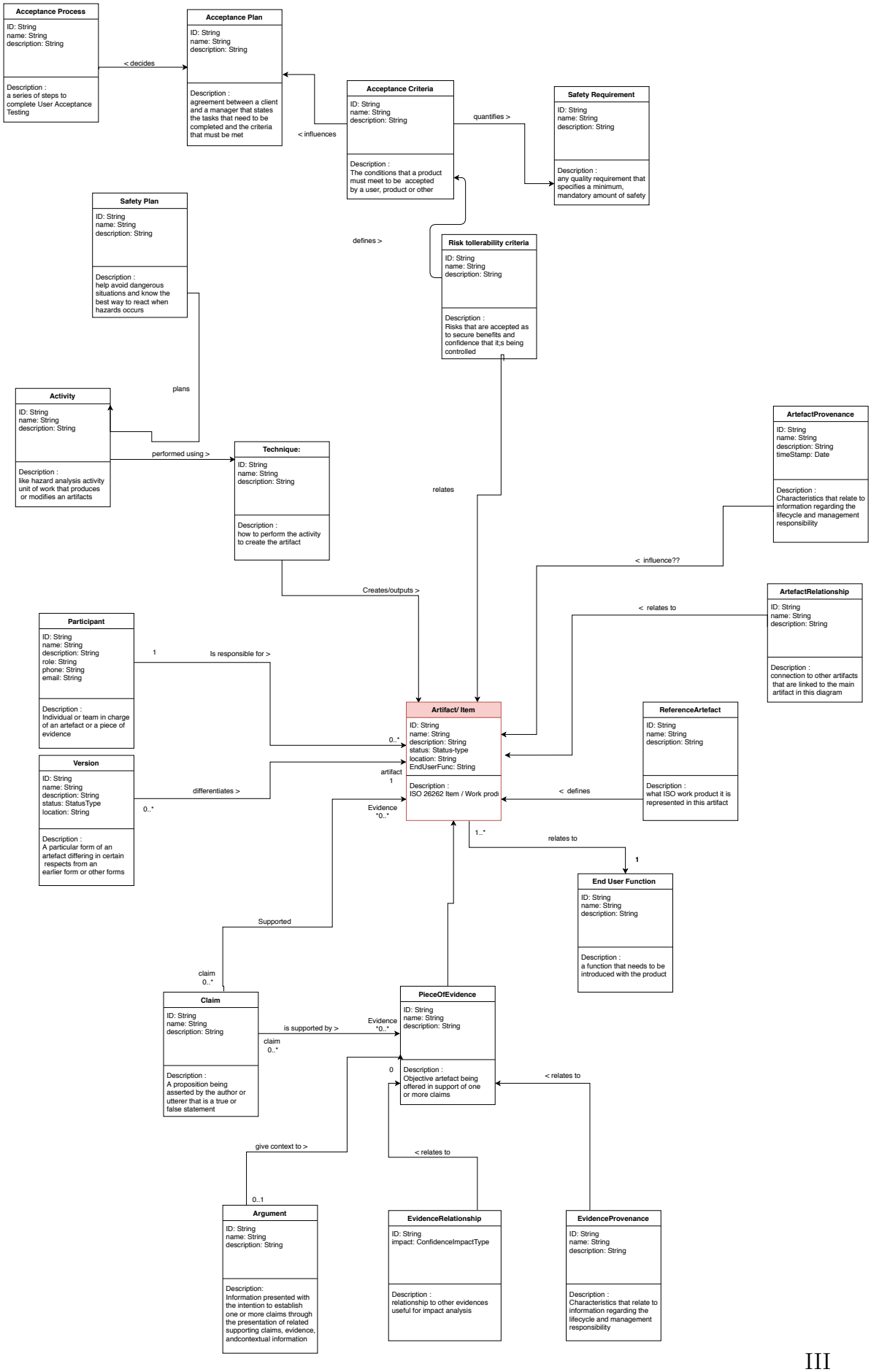

Figure A.2: Iteration 2 - Second development

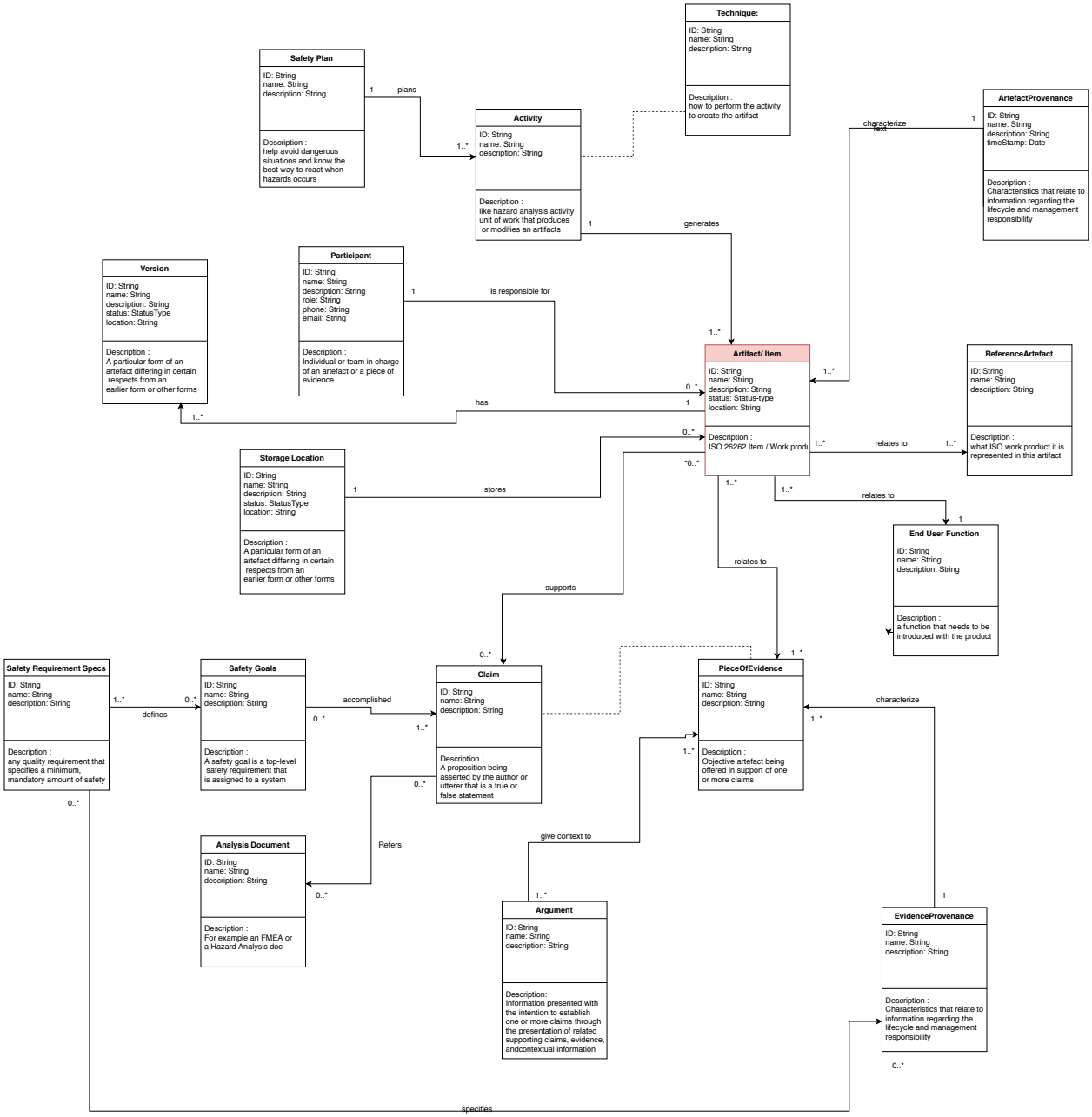

Figure A.3: Iteration 3 - First development

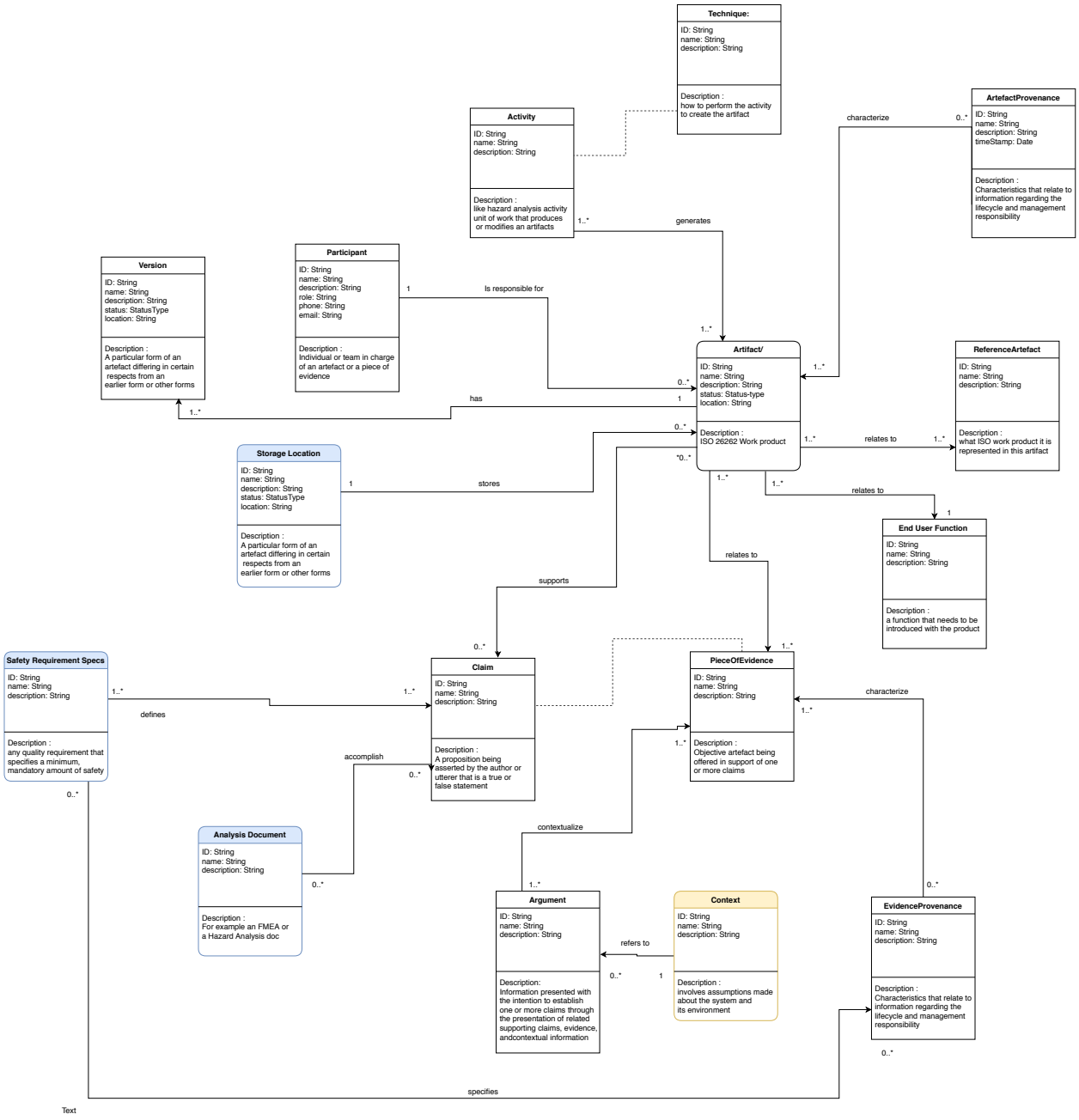

Figure A.4: Iteration 3 - Second development

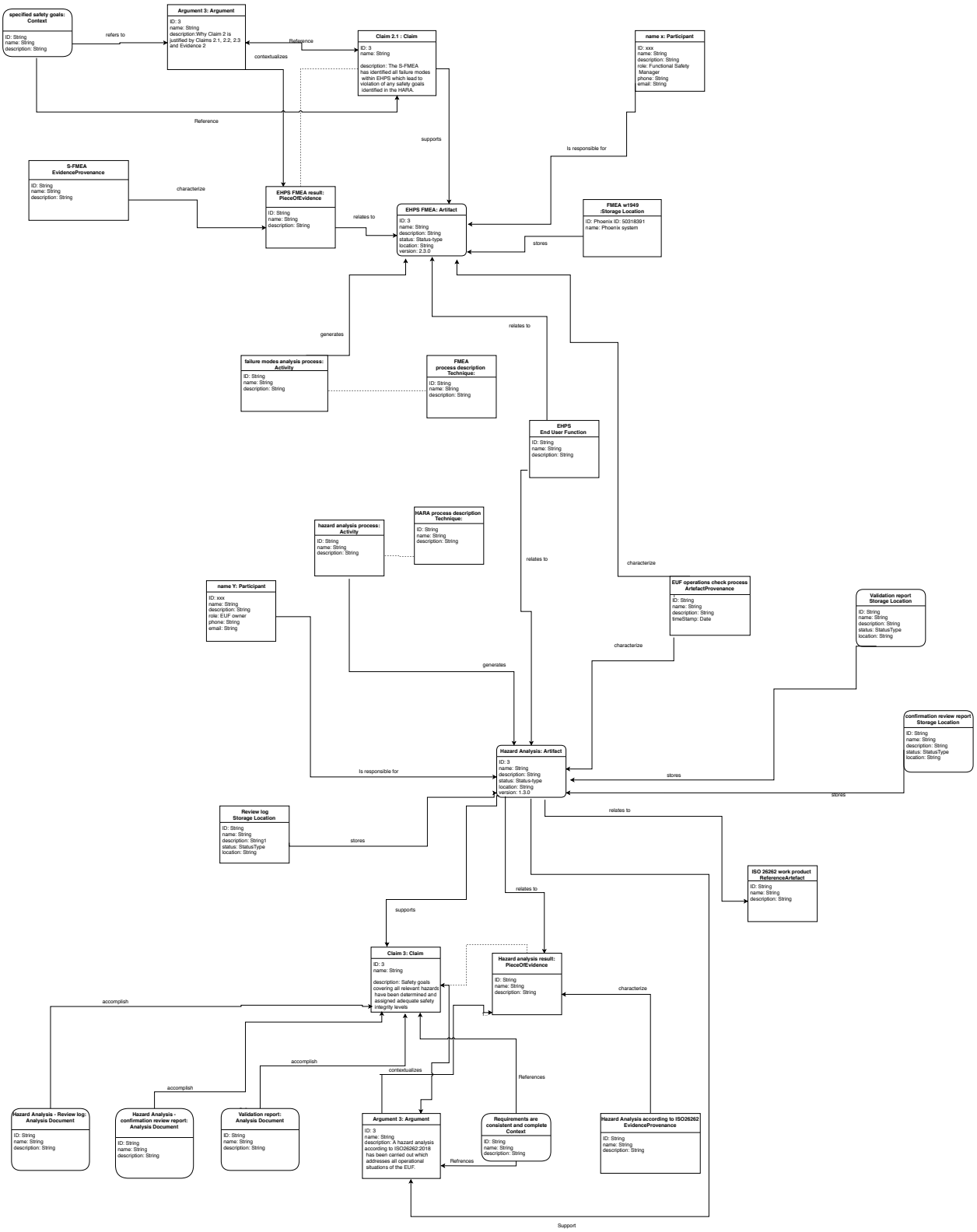

Figure A.5: Iteration 3 - Applying TIM to case company's SaAC

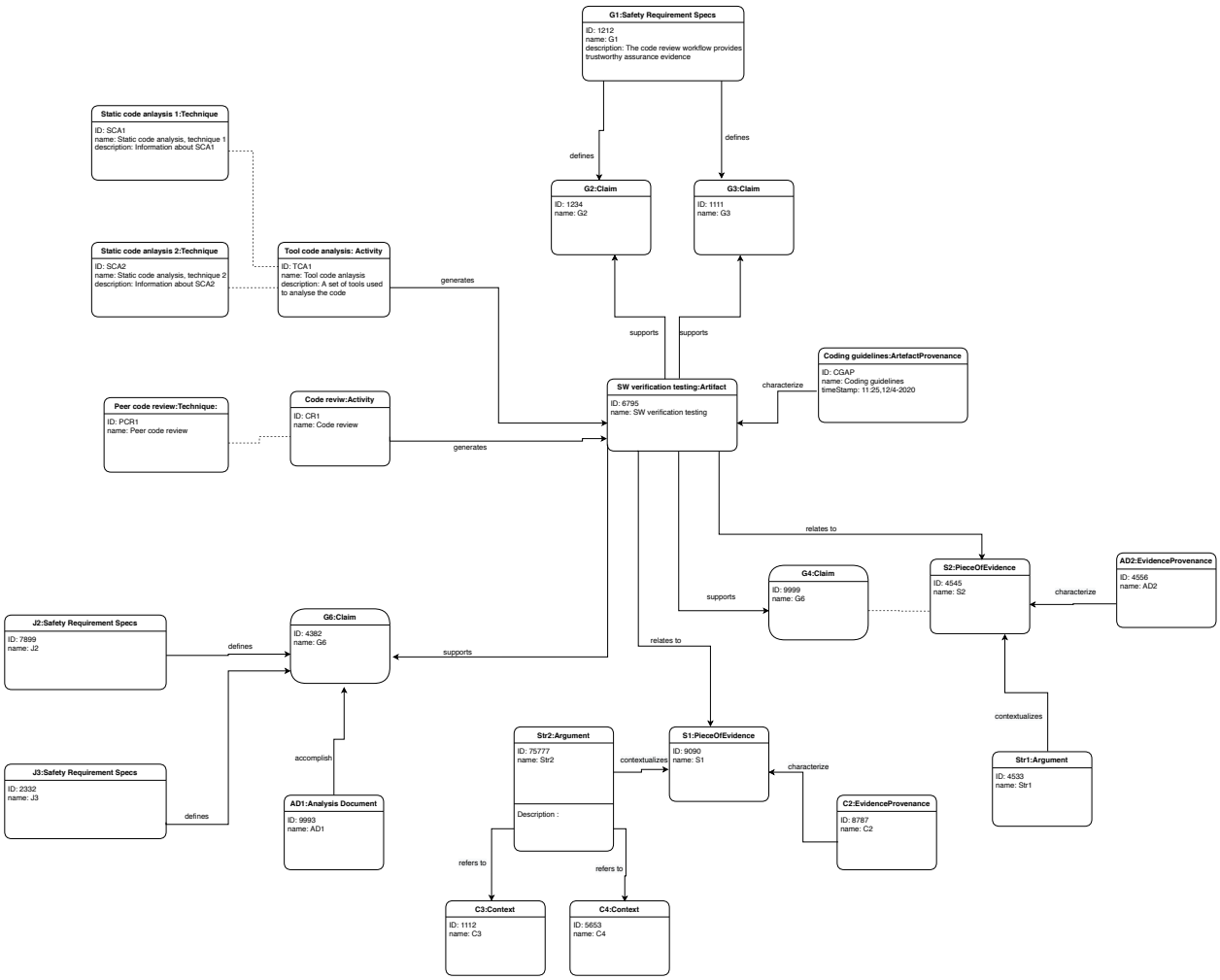

Figure A.6: Iteration 3 - Applying TIM to SaAC [1]

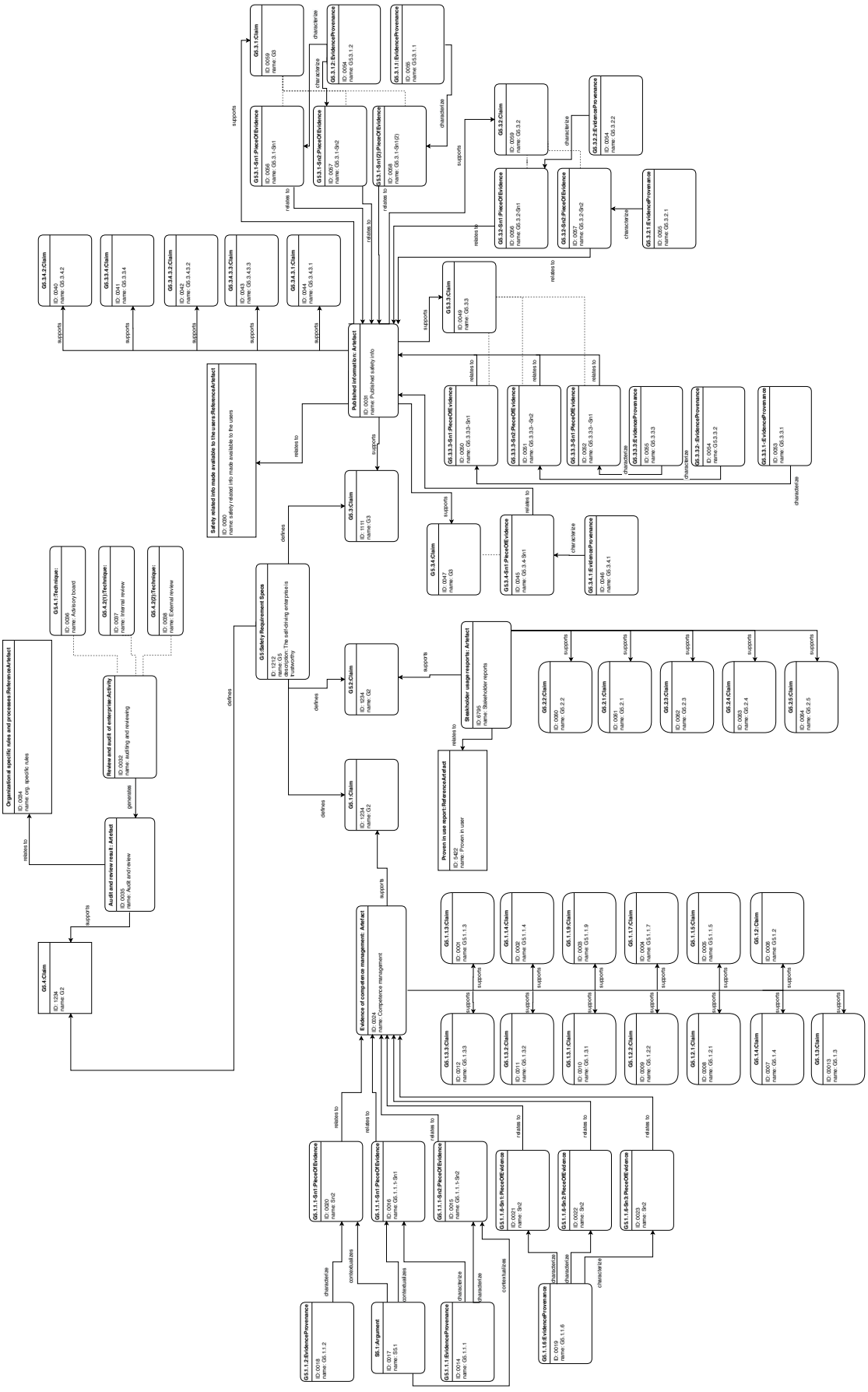

Figure A.7: Iteration 3 - Applying TIM to SaAC [2]

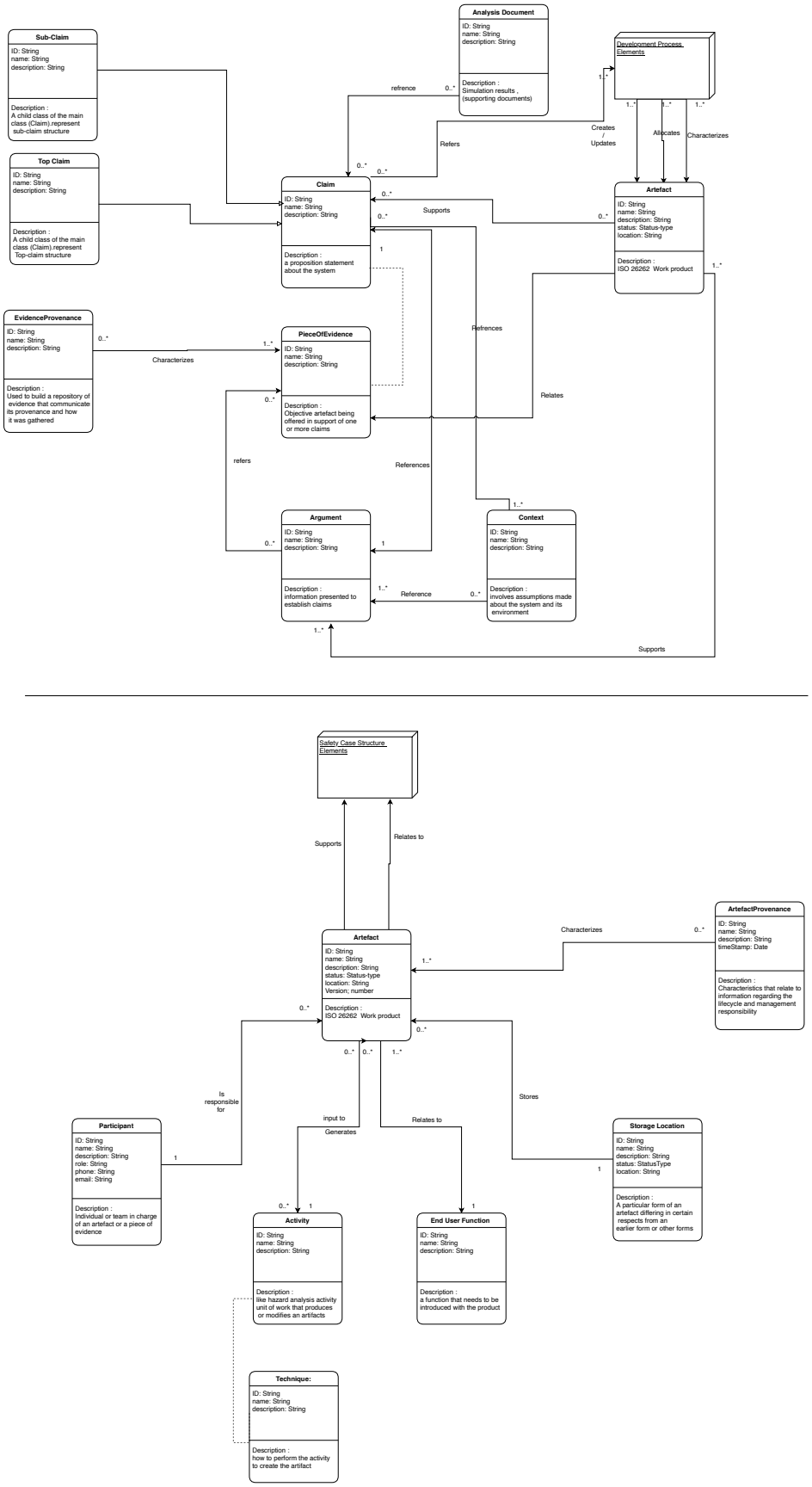

Figure A.8: Iteration 3 - After focus group, final version

A.0.2 Change log - TIM

A.0.2.1 Changes TIM v.1-2

List of changes between TIM version 1 to 2 (A.1-A.2):

- Removed the class “Risk reduction measure“
- Removed the class “Product“
- Added association between the classes “Safety plan“ and “Activity“
- Removed association between the classes “Safety plan“ and “Safety requirement“
- Changed the association between the classes “Artefact“ and “End user function“ to be “relates to“ instead of “used to generate“

A.0.2.2 Changes TIM v.2-3

List of changes between TIM version 2 to 3 (A.2-A.3):

- Added the class “Safety goals“
- Added the class “Analysis document“
- Added the class “Storage location“
- Removed the class “Acceptance critera“
- Removed the class “Acceptance plan“
- Removed the class “Acceptance process“
- Removed the class “EvidenceRelationship“
- Removed the class “Risk tollerability criteria“
- Added association between the classes “Activity“ and “Artefact“
- Added association between the classes “Safety requirement specification“ and “Safety goals“
- Added association between the classes “Safety requirement specification“ and “EvidenceProvenance“
- Removed association between the classes “Technique“ and the class “Artefact“
- Changed the association between the classes “Technique“ and “Activity“ to a dependency association
- Changed the association between the classes “Claim“ and “PieceOfEvidence“ to a dependency association
- Changed the association between the classes “EvidenceProvenance“ and “PieceOfEvidence“ from “relates to“ to “characterize“
- Changed the association between the classes “Version“ and “Artefact“ from “differentiates“ to “has“
- Changed the association between the classes “ArtefactProvenance“ and “Artefact“ from “influence“ to “characterize“
- Changed the association between the classes “ReferenceArtefact“ and “Artefact“ from “defines“ to “relates to“
- Renamed the class “Safety Requirement“ to “Safety requirement specification“

A.0.2.3 Changes TIM v.3-4

List of changes between TIM version 3 to 4 (A.3-A.4):

- Added the class “Context“
- Removed the class “Safety plan“
- Removed the class “Safety Goals“
- Added association between the classes “Safety Requirement Specification“ and “Claim“
- Changed the association between the classes “Activity“ and “Artefact“ form “1“ to “1..*“
- Changed the association between the classes “PieceOfEvidence“ and “EvidenceProvenance“ form “1“ to “0..*“

A.0.2.4 Changes TIM v.4-5

List of changes between TIM version 4 to 5 (A.4-A.8):

- Added the class “Top Claim“
- Added the class “Sub Claim“
- Added the class “Development process element“
- Removed the class “Version“
- Removed the class “Safety Requirement Specification“
- Removed the class “ArtefactReference“
- Added bi-directional association between the classes “Artefact“ and “Activity“
- Added association between the classes “Claim“ and “Argument“
- Added association between the classes “Context“ and “Claim“
- Added association between the classes “Claim“ and “Claim“
- Added inheritance association between the classes “Top claim“ and “Claim“
- Changed the association between the classes “Claim“ and “Analysis document“ from “accomplish“ to “reference“
- Changed the association between the classes “Artefact“ and “Activity“ from a 1..* relationship to 0..*

A.0.3 Particpant observation field notes

#1

Site: Redacted
Date: 23/11-2019
Start: 13:00
End: 15:00

Notes: In a meeting with five employees from the case company, they are discussing the current state of their SaACs process and what they have in terms of data so far. The team that is discussing the topic is the functional safety team at the organization and they are holding this meeting in order for everyone to have the same information about the current state and situation at the company. There are no complete safety cases at the company right now that adheres to the ISO 26262 safety standards, but they are working on it. To comply with this standard became mandatory last year (2018) so it is important that they start adhering to the standard as soon as possible and that everyone is aware of this. The senior staff of the team is sceptical to utilizing any tools and have themselves looked into a range of these but were not impressed. They think it is better to focus on their own process and structure to fully comprehend the scope of this standard and how to work with it before introducing any tools. They are using word documents to write their safety case but expresses that this is an issue for traceability and maintainability. They want to find something else to use that is easier to trace the documents between each other and to easily keep them up to date. The modelling structure they are using for their SaACs is and will be GSN, this will not change since it is a very common modelling language for SaACs and they want to go with the standards. In terms of the work process, the case company does not develop their SaACs as a parallel thing to the development for function safety, it is part of the normal development process and the developers working on a safety related feature or part of a feature will then write that part of the SaAC. That is also a reason why they do not want to introduce too many tools since these developers are doing it and would have to learn a lot in addition to their development process which they want to avoid.

Reflection: The case company is now forced to adhere to new safety standards and are trying to figure out a process for doing so that is efficient but also does not impose too many new tools on their developers. Some pilot attempts have been made, but are not complete, to develop SaACs using the Goal Structuring Notation modeling structure and have been faced with some difficulties. These difficulties include the traceability and maintenance for the cases.

Figure A.9: Participant observation, 23/11/2019

#2

Site: Redacted
Date: 26/11-2019
Start: 13:00
End: 15:00

Notes: This meeting was a continuation of the one held three days prior since it turned out there was a lot to discuss and make sure everyone was up to speed. The focus of this meeting is what structures and processes they have in place but also what they need to implement. The instructions and guidelines on how to write a safety case exist and has been validated and it is clear what information is needed to fill a SaAC. However, what is not clear is how to build a SaAC that is easy to maintain or what methods are needed to do so. The most important part of this to the company is how to improve the traceability and make updates accordingly when changes occur. The most difficult changes to handle today is the change to requirements because their structure is quite complicated. Other aspects of traceability which are difficult today but which are also very important is the traceability to the level of part numbers that needs to be included in the SaACs. The solution the company is looking for is for us to improve traceability in order to see what artefacts are impacted if one changes and where to find all the artefacts across the different storage tools that are used in the company. For their SaACs in the company they are looking for some kind of generalization to cover the safety of all the products they are developing. Again the people are reminded that they do not want to introduce any tools to work with safety as of today and it is stated that it is first important to know exactly what you want to do and how it is done before introducing tools to do it for you. Although, whatever process and methods are chosen in order to implement this, it is important that it is possible to integrate them with the development lifecycle. The goal is when the product reaches production, everything should be consistent. This meaning the SaACs and the product itself should be consistent, complete and up to date.

Reflection: The focus of the case company in terms of improving their process of SaACs is not how to structure the cases or what information is needed, but where to find the information in the various tools they use and the connection/traceability between the different information. The connection between the various documents and resources are very important to the company so they can easily see which parts might be impacted during a change and where to find these parts.

Figure A.10: Participant observation, 26/11/2019

#3

Site: Redacted
Date: 27/2-2020
Start: 14:00
End: 16:00

Notes: In this meeting, between four employees at the case company, a progress report was held by the Safety Case Manager in the department where one of the SaACs was being developed. The manager states that the SaAC is close to complete. However, the instruction and SaAC might not fully match because the case is not complying with all of what is included in the ISO 26262 standard. Why? Because the SaAC was started on before the instructions and guidelines were complete. The instructions are built in order to comply with the standard. While working on the SaAC the main issues regards the process of functional safety requirements being broken down into technical safety requirements. Traceability is the main problem. Linking the different levels of requirements to the evidence is very difficult with this requirement structure. The available safety case instructions do not address how to handle changes to the features nor claims. Even a small thing as new part numbers can trigger a complete redoing of the validation process for a SaAC. There are continuously a lot of changes to these products and therefore the SaACs.. Changes on feature level will impact the SaAC, changes to requirements, new part numbers and many other aspects can cause great impact on the case. Changing small stuff will force rerun of tests and validations (for example changing part number). It doesn't have to be a big change to the entire case but just a part of it. If we could clearly see which artefacts of the SaAC are connected to the other documents, we could save time and might not have to redo it all.As of today, word and excel templates are used to write SaACs at the company but they aim to move towards using an application called system weaver instead to store everything in the future. Today they only generate reports from the tool and store some of it in a long term database/storage called Phoenix. Other information is stored in, among others, JIRA, Github and sharepoint. Traceability between requirements and technical artefacts are handled different in different teams.There are some traceability guidelines that are about to be adopted

Reflection: The employees discussed the current state of the SaACs under development but also talked about the difficulties and strategies to move forward with their work in this area. The compliance with the ISO 26262 standard is lacking in the current cases. They discussed their main issue which is how the requirements are broken down and the traceability issues that arise from that structure in relation to the evidence in the SaACs. Another big issue they are facing with the lack of traceability is when changes occur. Complete reruns of the validation process are carried out because the practitioners are not sure which parts of the case possibly got affected by the change because they do not have the trace links which would show which of the parts that are connected.

Figure A.11: Participant observation, 27/2/2020

#4

Site: Redacted
Date: 5/3-2020
Start: 13:00
End: 16:00

Notes: A function safety workshop was held by one of the senior members of the functional safety team at the case company. This workshop was conducted in order to educate the function safety staff and managers about the ISO 26262 standard and how to write SaACs that comply with said standard. Eight people attended the workshop excluding the researchers of this study. The ISO lifecycle model was explained and that the results would produce the work products that would later be used as evidence in a SaAC. The lifecycle comprise of the following steps:

1. Item definition
2. Hazard analysis
3. Specification of functional safety concept
4. Specification of technical safety concepts
5. Development and verification SW & HW
6. Item testing and integration
7. Safety validation
8. Functional safety assessment
9. Production
10. Operation, service, decommission

This means that a complete safety case would always produce the work products needed in order to comply with the standard. The next thing discussed is the requirement hierarchy utilized at the company. The top-most requirement in this scenario is called a safety goal which is allocated to an item. An item being the ISO 26262 work product. To make one function many safety goals are grouped to cover all safety related concerns. These safety goals are then broken down into different functional safety requirements which are then allocated to main elements (subsystems) of the items. When that is done, functional safety requirements are broken down into technical safety requirements which are then allocated to elements at different levels. The complexity increases since technical safety requirements can be further broken down into smaller technical requirements. Technical safety requirements are then broken down into hardware safety requirements and software safety requirements which are then allocated to hardware and software elements respectively. The importance of developing a safety case as a continuous process during development was expressed clearly.

Reflection: A thorough presentation of the ISO 26262 standard and the company's strategies and issues were given. In the E/E systems that the company develops and work with, with the ISO 26262 standard, a pressing issue is the requirement hierarchy and how to address that in a SaACs.

Figure A.12: Participant observation, 5/3/2020

A.0.4 Safety Assurance Case comparison

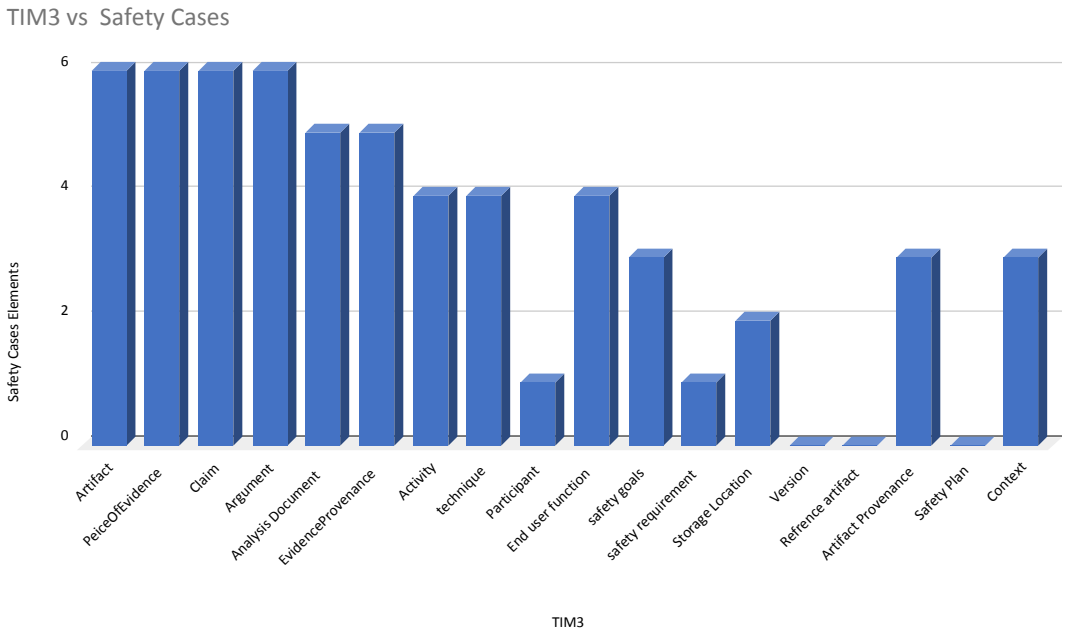

Figure A.13: Availability of TIM classes in analysed SaACs

A.0.5 Focus group

Focus group questions:

-
- What are the potential uses of the model?
    - Where?
    - How?
- What value do you see in using this model?
    - If not: what is missing in order to create value for the company and your process?
    - Is there something missing and/or is there something that is not needed
- Are the classes in the model clear?
- What do you think they represent and how do they relate to the safety cases?
- Are the associations clear and make sense?
    - If not, elaborate
- Do you have tools that support creating the links represented in the model?
- Are the information of the links already available in the Volvo systems?
- What are the challenges you foresee using this model?
- Any additional comments/insights?

Figure A.14: Focus group questionnaire

ID	Current Position	Years of SaAC Experience	Interests related to SaAC
1	Specialist Functional Safety - System Engineer at Powertrain Engineering (PE), acting safety manager for a project at PE. Formal specialist role in embedded SW (specifically functional safety), my task is to implement and drive functional safety (ISO 26262) at PE.	ST: 6 years, since 2014. Also worked functional safety for off road vehicles/machines for a year long time ago.	ST: I review safety cases from suppliers. It is common that the safety case is a list of work products, like test reports etc. It is interesting to compare with the way where we work with claims.
2	Senior Principal Functional Safety Engineer at Electrical Department (ESA) at Volvo GTT	20+	maintenance, reuse and automatic creation
3	Principal System Design Engineer, Functional Safety Specialist	~25 years	Structure and contents (including relationships between claims, arguments and evidence) of the reasoning in the safety assurance case. Maintenance of an existing safety assurance case when changes are made in the associated system.
4	Functional Safety Manager – Chassis Technology department – Volvo GTT	4,5 years	Efficient creation of cases, traceability, maintenance/re-use, safety cases for automated driving applications

Figure A.15: Focus group participant information

A.0.6 Study Participants

ID	Role	Workshop-face-to-face	Expert Evaluation 1 - face-to-face	Expert Evaluation 2 - Online	Focus group - Online
1	Specialist Functional Safety	X			X
2	Senior Principal Functional Safety Engineer at Electrical Department (ESA) at Volvo GTT	X	X	X	X
3	Principal System Design Engineer, Functional Safety Specialist	X	X	X	X
4	Functional Safety Manager	X	X		X
5	Functional Safety Manager	X	X		
6	Acting Manager in the Functional Safety Team at GTT	X			
7	Development engineer	X			
8	Global Technology Manager, Electrical/Electronic Platform	X			
9	Lead System Design Engineer	X			
10	System Architect Hardware	X			

Figure A.16: Participant information, evaluation methods

A.0.7 Related work methods and approaches for traceability to support SaAC

Reference	solution	Description
[12]	SafeTIM, traceability information model for safety evidence	A study based on a systematic literature review and a survey
[9]	Safety Artifact Forest Analysis (SAFA),	leverages traceability to automatically compare software artifacts from a previously approved or certified version with a new version of the system. Where they identify, visualize, and explain changes in a Delta Tree.
[14]	component-based design, contracts, modular assurance cases, and continuous assessment to enable continuous deployment in the context of product lines.	combining the use of component-based design, contracts, and modular assurance cases with agile practices, we can achieve continuous assurance cases that evolve and are assessed in the same pace as,and together with, the product.
[16]	present two techniques that utilise safety contracts to facilitate the maintenance of safety cases, • Sensitivity Analysis for Enabling Safety Argument Maintenance (SANESAM) • SANESAM+	apply sensitivity analysis on FTAs to measure the sensitivity of outcome A (e.g., a safety requirement being true) to a change in a parameter B SANESAM+: consider the change's impact on: (1) intermediate events of FTAs, (2) multiple events, and (3) duplicated events.
[18]	meta-model which describes the relationship between the two and present a case study taken from IEC 62278/EN 50126 from railway systems to show how	linking traceability to GSN (Goal Structuring Notation) using the Traceability Information Model (TIM). They built a TIM and GSN diagrams

Figure A.17: Additional tools for traceability approaches for SaAC

[18]	meta-model which describes the relationship between the two and present a case study taken from IEC 62278/EN 50126 from railway systems to show how traceability and safety cases benefit each other	linking traceability to GSN (Goal Structuring Notation) using the Traceability Information Model (TIM). They built a TIM and GSN diagrams new criteria for validation of GSN in terms of traceability and showed a partial evaluation in the case study based on those criteria.
[32]	introduce a methodology and a tool chain for establishing a safety argument, plus the evidence to prove the argument	use the goal structuring notation to decompose and refine safety claims into sub- claims until they can be proven by evidence. The evidence comes from tracing the safety requirements of the system into their respective devel- opment artifacts in which they are realized.
[33]	Exploit the weaving model for automated generation of assurance cases.	discuss how a seamless model- driven approach to assurance cases can be achieved and examine the utility of increased formality and automation.
[34]	present six precision improvement techniques illustrated on a GSN safety case used with ISO 26262.	Used wordGSN-IA: GSN Impact Assessment Algorithm

Figure A.18: Additional tools for traceability approaches for SaAC