



Applying and Maintaining Security Assurance Cases in the Medical Domain

A Case Study at AstraZeneca

Master's thesis in Computer science and engineering

Adam Andersson, Max Fransson

MASTER'S THESIS 2022

Applying and Maintaining Security Assurance Cases in the Medical Domain

A Case Study at AstraZeneca

Adam Andersson, Max Fransson



UNIVERSITY OF
GOTHENBURG



CHALMERS
UNIVERSITY OF TECHNOLOGY

Department of Computer Science and Engineering
CHALMERS UNIVERSITY OF TECHNOLOGY
UNIVERSITY OF GOTHENBURG
Gothenburg, Sweden 2022

Applying and Maintaining Security
Assurance Cases in the Medical Domain
A Case Study at AstraZeneca
Adam Andersson, Max Fransson

© Adam Andersson, Max Fransson, 2022.

Supervisor: Mazen Mohamad, Department of Computer Science & Engineering
Advisor: Anders Löfgren, Software Engineering Lead Digital Health, AstraZeneca
Examiner: Robert Feldt, Department of Computer Science & Engineering

Master's Thesis 2022
Department of Computer Science and Engineering
Chalmers University of Technology and University of Gothenburg
SE-412 96 Gothenburg
Telephone +46 31 772 1000

Cover: A Venn diagram representing the intersection of safety and security, inspired by the MDCG guidance document [1]

Typeset in L^AT_EX
Gothenburg, Sweden 2022

Applying and Maintaining Security
Assurance Cases in the Medical Domain
A Case Study at AstraZeneca
Adam Andersson, Max Fransson
Department of Computer Science and Engineering
Chalmers University of Technology and University of Gothenburg

Abstract

As there are constant innovations within the medical field, it should come as no surprise that software is often included in new medical technology. Concurrent with this, there are also actors who for different reasons want to gain access to, or to use a product in malicious ways. As their actions may have serious effects on end user safety there are strict regulations, such as ISO 14971, that these products need to comply with. One way for companies to show compliance with these regulations is through detailed documentation.

Security Assurance Cases, is a structured argument used for documenting the security of a system through the use of claims supported by evidence. CASCADE is an approach for creating such cases, which introduces a block based methodology, with an emphasis on arguing quality for the supplied evidence, as well as arguing completeness for the decomposition of claims. While the CASCADE approach was developed in close collaboration with the automotive industry, a knowledge transfer to the medical domain might be possible, as they are both safety critical domains with security critical systems. To investigate this, a case study at AstraZeneca was performed, which utilized interviews, focus groups and a regulatory documentation analysis. These showed significant overlap between the requirements in the medical domain and the properties of CASCADE. However, they also showed the need for CASCADE to incorporate patient safety to some degree. An incorporation method found was through the use of risk assessment matrix ratings as these are already used for similar purposes in the domain.

As software is continuously evolving and any changes made to a system will require a reevaluation of the associated assurance case in order for it to be up to date. Such a process is not yet included in agile work approaches, however the hypothetical inclusion has been found feasible mainly through the addition of a role responsible for ensuring that the *Security Assurance Case* (SAC) is updated before the feature begins development, and before the feature is released, utilizing input from other roles involved in system development.

All things considered, this study has found CASCADE a beneficial and potentially desirable tool for complying with several requirements posed in the medical domain given that traceability to safety related risks is provided. It has also been concluded that the iterative process at the case company can host a maintainability mechanism for CASCADE but that lack of knowledge among the practitioners involved might require the introduction of a new role.

Keywords: security assurance cases, medical domain, SAC, CASCADE, case study, maintainability, knowledge transfer

Acknowledgements

We would like to thank **Mazen Mohamad** for supervising us during our work on this thesis, and providing valuable context and input, especially regarding Security Assurance Cases and CASCADE.

We would also like to thank our industry supervisor **Anders Löfgren** for his work in making this thesis collaboration with AstraZeneca possible, as well as for providing an excellent setting for conducting a case study, and for important input throughout the case study.

Our examiner **Robert Feldt** provided guidance that was required to complete our thesis, and gave input that in turn increased the quality of the final report, for which we are very grateful.

Thanks are also in order for **David Mason** and **Marcus Wallin**, who often took time out of their day to sit down with us on numerous occasions, and provided information and data which led us forward throughout our thesis work.

Finally, we would like to thank **Marcus Olofsson**, **Tomas Pagerup** and **Tobias Terstad** for their participation in our focus groups, and for their eagerness to participate in focus group discussions.

Adam Andersson, Max Fransson, Gothenburg, June 2022

Contents

List of Figures	xv
List of Tables	xvii
1 Introduction	1
1.1 Research questions	3
2 Background and Related Work	5
2.1 Background	5
2.1.1 Security Assurance Cases	5
2.1.2 Fault tree analysis	6
2.1.3 CASCADE	8
2.1.4 Standards and guidelines in the medical domain	12
2.1.4.1 Software as a Medical Device (SaMD)	12
2.1.4.1.1 Meaning of trustworthiness	12
2.1.4.1.2 Post market management document (2016)	12
2.1.4.1.3 Pre market management document (2018)	13
2.1.4.2 Guidance on Cybersecurity for medical devices (2019)	13
2.1.4.3 ISO 14971:2020	13
2.1.4.3.1 ISO 24791:2020	13
2.1.4.4 ISO 62304:2006	14
2.1.4.5 Good Clinical Practice (GCP)	15
2.1.5 Guideline on computerised systems and electronic data in clinical trials	15
2.1.5.1 NIST 800-30 (Revision 1)	15
2.1.6 Risk assessment matrix	16
2.2 Related work	16
2.2.1 General overview of Security Assurance Cases and current research	16
2.2.2 Security Assurance Cases in relation to agile development	17
2.3 Case Study environment	19
2.3.1 System documentation	19
2.3.2 Architecture introduction and mobile app platform	19
2.3.3 Product/system Case Study study suitability	19
2.3.4 Roles at AstraZeneca	20
3 Methods	23

3.1	Case Study	23
3.1.1	Case Study motivation	23
3.1.2	Overview of participants	24
3.1.3	Initial case creation	24
3.1.4	Interviews	24
3.1.4.1	Interview structure	25
3.1.4.2	Interviews round #1	25
3.1.4.3	Interviews round #2	25
3.1.5	Benchmark case creation	25
3.1.6	Documentation and regulation analysis	26
3.1.7	Focus group	26
4	Results	29
4.1	Suitability of CASCADE in the medical domain	29
4.1.1	Identified use cases for CASCADE in the medical domain	29
4.1.2	Overlap with existing practices	31
4.1.3	Identified overlap between CASCADE and regulatory documentation for the medical domain	31
4.1.3.1	Post market	33
4.1.3.2	Premarket	34
4.1.3.3	NIST 800-30	35
4.1.3.4	Medical Device Coordination Group 2019-16	35
4.1.3.5	Good Clinical Practice (Good Clinical Practice (GCP))	37
4.1.3.6	ISO 14971	37
4.1.3.7	ISO 62304	38
4.2	Extension of existing CASCADE approach	39
4.3	CASCADE case maintenance using existing work methodology	41
4.3.1	Existing workflow and practices at AstraZeneca	41
4.3.2	Possible incorporation of SAC maintenance in existing workflow at AstraZeneca	42
5	Discussion	45
5.1	Adaptability of CASCADE to a medical domain context (RQ1.1)	45
5.1.1	Field observation at case study company	45
5.2	Domain specific requirements compelling CASCADE modifications (RQ1.2)	46
5.3	Utilize and extend existing agile processes to accommodate SAC maintainability (RQ2)	47
5.4	Cybersecurity domain volatility	49
5.5	Alternative methodology	49
5.6	Threats to validity	49
5.6.1	Internal Validity	50
5.6.1.1	Limited existing SAC and CASCADE knowledge	50
5.6.1.2	Potential bias	50
5.6.2	External Validity	50
5.6.2.1	Generalizability	51
5.6.2.2	Partial documentation analysis	51

5.6.2.3	Documentation and standard volatility	51
5.6.2.4	Result validation concerns	51
6	Conclusion	53
6.1	Future research	53
	Bibliography	55
A	Appendix 1	I
A.1	Interviews with SaMD Coordinator at AstraZeneca	I
A.1.1	Interview questions	I
A.2	Interview with Software engineering lead at AstraZeneca	II
A.2.1	Interview questions	II
B	Appendix 2	III
B.1	Questions and answers from maintainability focus group questionnaire	III
C	Appendix 3	VII
C.1	Example Raspberry Pi web server SAC	VII
C.2	Resulting benchmark case	VII
D	Appendix 4	IX
D.1	EMA enquiry	IX
D.1.1	Question	IX
D.1.2	Response	X

Glossary

AZ AstraZeneca. 30, 31

CAE Claims, Argument and Evidence Framework. 5

CIA Confidentiality, Integrity and Availability. 9

DoD Definition of Done. 43, 53

EMA European Medicines Agency. 1, 15, 32

FDA U.S. Food and Drug Administration. xv, 1, 12, 13, 32, 35, 40, 46

FMEA Failure Mode and Effects Analysis. 2, 54

FTA Fault tree analysis. xv, 2, 7, 8, 31, 38, 45, 50, 54

GCP Good Clinical Practice. x, 15, 37

GSN Goal Structuring Notation. xv, 1, 5, 6

ISO International Organization for Standardization. 51

MDCG Medical Device Coordination Group. xv, xvi, 13, 32, 35, 36, 39, 40

NIST National Institute of Standards and Technology. 15, 32

PMD Postmarket Management Document. 12, 13

PreMD Premarket Management Document. 13

SaAC Safety Assurance Case. 2, 38, 50

SAC Security Assurance Case. v, xv, 1–3, 5, 6, 8, 16–18, 24–27, 29–31, 34, 38, 41, 43, 45, 46, 48–50, 53

SaMD Software as a Medical Device. 12, 13, 25, 32, 45, 46, 51, 52

SDD System Design Document. 19

SOP Standard Operating Procedure. 30, 36

SOUP Software Of Unknown Provenance. 14

List of Figures

2.1	The different elements provided by Goal Structuring Notation (GSN). GSN can make up the building blocks for a SAC utilizing this kind of notation	6
2.2	A partial example SAC created for Raspberry Pi web server	6
2.3	An example Fault tree analysis (FTA) case from ISO 61025 [19] . . .	7
2.4	Subset of the notation used in the FTA case from ISO 61025 [19] . .	8
2.5	The structure for the CASCADE approach displaying all the different blocks	8
2.6	A partial example of the white hat block for a Raspberry Pi web server	9
2.7	A partial example of the black hat block for a Raspberry Pi web server	10
2.8	A partial example of the resolver block for a Raspberry Pi web server	10
2.9	A partial example of the generic subcase for a Raspberry Pi web server	11
2.10	Examples for both types of quality claims, the first one (in blue) for arguing completeness of decomposition and the second one (yellow) for arguing quality in evidence attached to the same claim	11
2.11	Definition of a trustworthy system according to the FDA premarket guidance document [11]	12
2.12	Example from ISO 24791 [22] of concrete hazards (risk) and their potential impact on patient safety	14
2.13	Illustration from Pascarella et. al [24] showing how a risk matrix is used to classify a risk level depending on the risk's probability and impact	16
3.1	A Figure outlining the methods used for the case study in chronological order	23
4.1	Derived use cases from the second focus group	29
4.2	High level overview of findings in the documentation and their overlap with the blocks of CASCADE	33
4.3	Requirements taken from the PMD document by U.S. Food and Drug Administration (FDA) [11]	35
4.4	Mapping between important areas introduced in MDCG Annex I and CASCADE blocks	37
4.5	Outline of risk management process flow in ISO 62304 [8]	39
4.6	A visual representation of the relevant intersection between security and safety, based on the Medical Device Coordination Group (MDCG) guidance document [1]	40

4.7	An illustration from the MDCG guidance document, [1] showing risk management process for security and safety side by side with the addition of arrows showing connections between these.	40
4.8	A subset of a table from ISO 62304 [8], displaying which parts of the requirements outlined in the standard applies to which classes	41
4.9	Overview of the workflow at AstraZeneca regarding Jira [37] status transitions of features for the BOOST platform, triage team approval gates highlighted in blue	42
5.1	An potential example for how risk assessment ratings could be incorporated with the CASCADE approach	47
5.2	Overview of the workflow at AstraZeneca regarding Jira [37] status transition for features of the BOOST platform, and suggestions to where amendments can be made	48
C.1	The resulting SAC after using the SAC creation guidelines by Carnegie Mellon University [13]	VII

List of Tables

2.1	Overview of different relevant roles at AstraZeneca	20
3.1	Participants in the case study activities	24
4.1	Overview of identified use cases for Security Assurance Cases	30
4.2	Prominent standards and guidance documents in the medical domain and their identified overlap with CASCADE	32

1

Introduction

The need for increased cybersecurity is growing rapidly across domains that rely on the use of software [2], as data and systems have a significant risk of receiving attention from malicious actors [3]. These actors seek access to the data or systems for a plethora of reasons, with one prominent reason being financial gain [4], and another being the deliberate destabilization of infrastructure [5].

The medical domain is seeing an increase in the digitization of medical devices, where software can sometimes be responsible for therapeutic choices [6]. Medical devices are also increasingly becoming more connected [7], which increases both the possibility and the probability of cybersecurity risks. These cybersecurity risks have the potential to have a negative impact on the health and safety of the patient using the device, when a medical device is not functioning according to its specifications [8].

There are therefore strict requirements from multiple parties regarding cybersecurity and safety in the medical domain. These parties include government regulatory entities, such as European Medicines Agency (EMA) and FDA that have an interest in protecting assets that could be deemed sensitive (such as personal medical data), as described in the Guideline on computerised systems and electronic data in clinical trials [9]. Medical devices can also have a potentially hazardous impact on the patient using the device [10], and providing evidence that risks that have the potential to result in patient harm have implemented relevant mitigation measures (which is one area outlined in ISO 14971, Application of risk management to medical devices [10]) is important for getting marketing approval for medical devices [11] [12].

One way to enable such regulatory compliant handling of medical devices is the ability to break down the system into manageable, granular parts which can then be subjected to further analysis. These granular parts can then be used when creating security claims about the system and its artefacts, that can in turn be used to structure and form an argument about the security of the system as a whole, which is one of the primary elements of a SAC [13].

Security Assurance Cases provide the structure needed for breaking down a high level security claim into further security sub claims about a system artefact, in a recursive process, using notation (such as GSN) suitable for SACs. This is performed until a granularity is reached where concrete evidence supporting the sub claims validity can be assigned [13]. These sub claims are then structured to form an argument,

where the validity of the argument is supported by previously provided evidence. A more elaborate explanation of SACs is provided in the background chapter (chapter 2).

There are many different and diverse approaches when using SACs, where each one varies in applicability given a certain domain (automotive, financial, medical etc.) [14]. Furthermore, depending on the system undergoing inspection (and for example the desired/required abstraction level), this further impacts which of the approaches that is the most suitable for the task. Choosing the right approach is key, as each approach garners different tools, meant to tackle the domain-specific goals and challenges that can be encountered while documenting a system using SACs. That is not to say that an approach catered for one domain cannot be useful in another domain, given proper validation and potential adjustments. Creating a new approach from the ground up brings with it a potentially higher workload and time investment, and so being able to transfer knowledge from one domain to another can have the benefit of not only preserving resources, but also the benefit of ensuring some initial quality due to prior validation in its originating domain.

The automotive domain presently includes the use of Safety Assurance Cases (SaACss) and SACs [15], whereas the medical domain sees frequent use of tools and processes such as FTA [10] (and Failure Mode and Effects Analysis (FMEA), which is also used in several risk analysis approaches, including the automotive domain). FTA, SaACs and SACs all use the notions of “claims” to argue for properties of the system in question.

Software systems are also prone to changes and updates, and these changes could potentially affect the security of the system, thus requiring a re-evaluation of the current security state of the system. Claims and evidence used in SACs need to be re-evaluated to address any potentially required updates, which is something that requires resources, attention and relevant knowledge from the maintainers of the system.

Handling the aforementioned changes and updates to software systems is often done through using agile work methodology. Agile approaches are increasingly becoming the current preferred way to handle software development in general, as well as the updated requirements and feature set of a software system [16]. These approaches do not currently have a closely coupled approach for handling the need for maintaining SACs, and the process of updating/re-evaluating them. Since SACs are an emerging approach for assuring the security of software systems in several different domains [14] (with a lot of current focus on the automotive domain), they are consequently not well established in industry.

There are techniques that are similar in nature to SACs that have had a presence in industry before, and still do, in the form of SaACs. However, a key difference in their approaches is that the involved elements in a SaACs are more static in nature (such as light bulbs, battery circuits, wire durability etc.), not prompting continuous updates or amendments to them, at least not to the same extent as software based components.

This is in contrast to SACs where there is a pressing need for the facilitation of maintainability, as IT systems are constantly evolving and adapting leading to potential gaps in the completeness and quality of the previously created SACs. This urges further investigations into the maintainability regarding SACs in general, as well as their applicability to software based solutions/products in the medical domain.

1.1 Research questions

Given the potential benefits of SACs, there is an interest from entities in the medical domain, as well as in the cybersecurity domain, to investigate whether a knowledge transfer about SACs is possible or feasible. There is also data and research needed on the maintainability of SACs, and whether they are able to be accommodated into an existing agile workflow. So, to provide information on the matter, the following research questions have been established.

RQ1. To what extent can knowledge about assurance cases be transferred from other domains to the medical domain?

RQ1.1 To what extent can the CASCADE approach be adapted to a medical domain context?

RQ1.2 What domain specific requirements exist in the medical domain that require changes to CASCADE in order for it to function adequately in a medical context?

RQ2. How can existing agile processes be utilized or extended to accommodate the maintainability process of a Security Assurance Case in an iterative workflow in the medical domain?

RQ1 investigates if CASCADE, an approach developed for the automotive domain for creating SACs, can be applied to the medical domain to the same extent that it has been applied to the automotive domain [17]. Depending on the extent to which applicability can be achieved, changes to the approach will be investigated for the knowledge transfer to be viable. As this is a case study, the focus for the compatibility will be on the workflow and practices currently used at AstraZeneca, which is a large multi-national company in the medical domain.

RQ2 aims to investigate whether there are elements that can be added or amended to existing processes in agile work methodology, with a focus on Scrum (as this is the most prominent agile work methodology used at the case company), which would make it more compatible with the maintenance of SACs. As Scrum itself can be used to improve the maintainability of a system on a work methodology level, incorporating potentially beneficial elements could have a positive effect on the maintainability regarding SACs. As changes to the code base are handled using regular Scrum, there needs to be an additional step in the workflow, handling the need for updates in regards to the relevant SAC elements that have been affected by the changes.

2

Background and Related Work

This chapter aims to convey the literary and scientific background of Security Assurance Cases, the maintainability of Security Assurance Cases, and Security Assurance Cases in the context of the medical domain, for which the purpose of this thesis work is to take into consideration, investigate, and build further upon. It will also introduce important concepts and artefacts for the study such as Security Assurance Cases, the existing CASCADE approach for creating Security Assurance Cases and important regulatory documentation for the medical domain. Finally it will provide information about the case study environment.

2.1 Background

This section aims to present and provide an overview of Security Assurance Cases and CASCADE, that are the main subject of analysis in this report, in moderate detail in order to convey their basic purpose and motivation for being relevant in the context of (cyber)security. Regulatory documentation from the medical domain which is significant to the study is also outlined in this section. It will also describe Fault tree analysis, which is an approach used in the medical domain that is in some ways similar to SACs.

2.1.1 Security Assurance Cases

A SAC is a structured body consisting primarily of security claims and evidence for these [13]. GSN (see Figure 2.1), and is often used as the medium through which the claims and evidence are formed into an argument regarding the security of a system. There are however several ways that an assurance case can be created, it can for instance be created using plain text, or using the Claims, Argument and Evidence Framework (CAE) notation [18].

The creation of a case starts of with a top claim for the security of the entire system, which is then used to derive security sub claims. This is a multi-stage process that can use GSN strategies as an intermediary step to describe on what basis the decomposition is performed. This is repeated until the claims are broken down to a sufficiently granular level, where concrete evidence can be assigned to them. When evidence has been assigned for all low level claims, and given that the derived claims are exhaustive for the system, the case helps argument for the existing

2. Background and Related Work

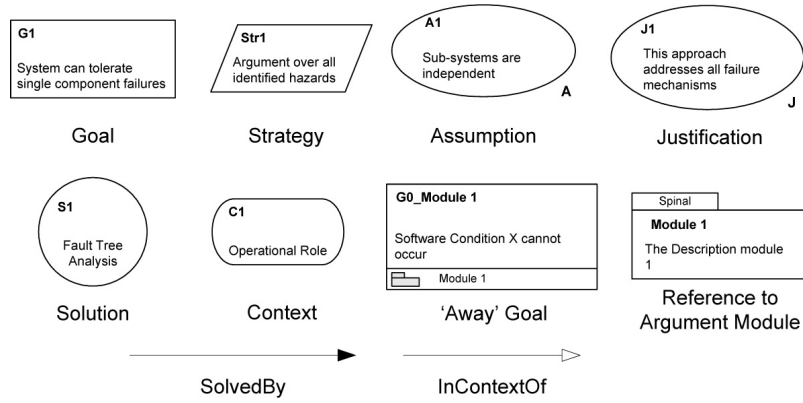


Figure 2.1: The different elements provided by GSN. GSN can make up the building blocks for a SAC utilizing this kind of notation

security posture of the system. As an example, a partial case for a Raspberry Pi web server is displayed in Figure 2.2, where the relation between claims, strategies and evidence can be seen. It also shows an instance of a context element which is used to help set the scope for the claim (where the scope can for example consist of product security requirements, and standards that need to be complied with).

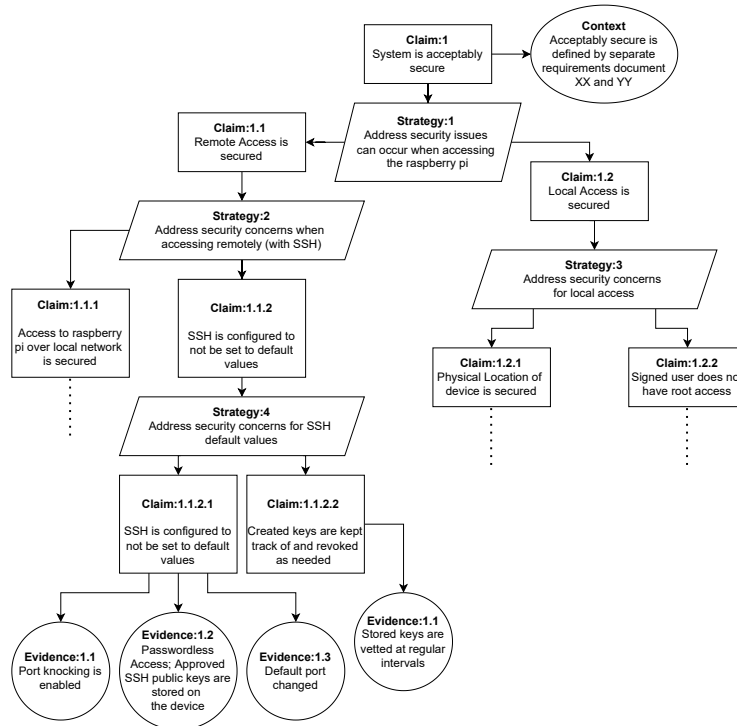


Figure 2.2: A partial example SAC created for Raspberry Pi web server

2.1.2 Fault tree analysis

An approach that is in some ways similar to SACs is the Fault tree analysis [19], which is a top-to-bottom approach to investigate causes of system level failure, which

uses boolean logic operators, such as OR, AND, XOR (as shown in Figure 2.4), in conjunction with event symbols. These event symbols and operators represent component level failures, which are needed to reach the top claim, which is the system level failure (such as the system not acting according to specifications). An example of an FTA case can be seen in Figure 2.3. The approach currently sees use in the system engineering field, including the avionics domain, the automotive domain and the medical domain [20], as they all handle safety critical elements. It is also in place at AstraZeneca in order to trace potential failures that could have an impact on the user of the device/product, and result in a violation of established patient safety practices/specifications and requirements, which could lead to patient harm.

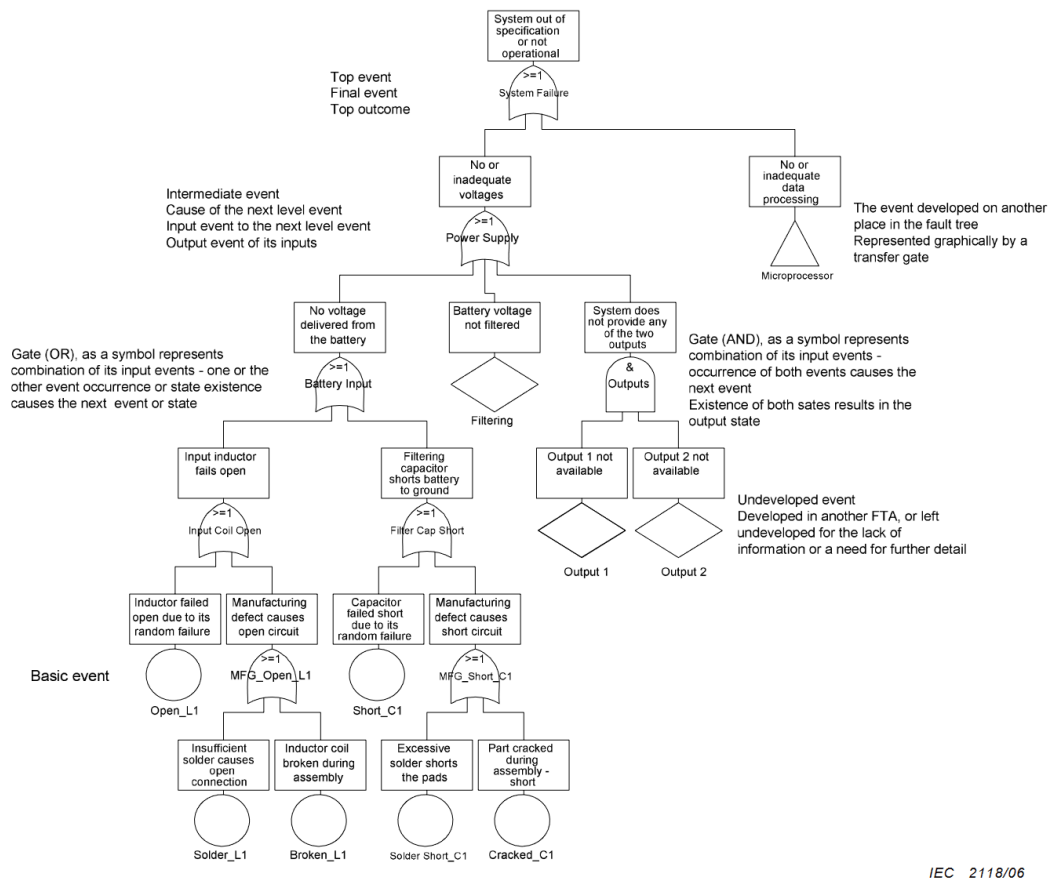


Figure 2.3: An example FTA case from ISO 61025 [19]

2. Background and Related Work



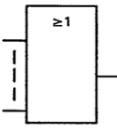

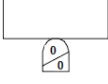
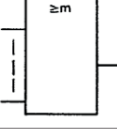

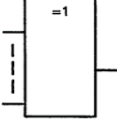


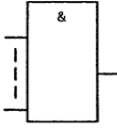
	Symbols		Name	Description	Reliability correlation	Number of inputs
			OR gate	The output event occurs if any of the input events occur	Failure occurs if any of the parts of that system fails – series system	≥ 2
			MAJORITY VOTE GATE	The output occurs if m or more inputs out of a total of n inputs occur	Redundancy k out of n , where $m = n - k + 1$	≥ 3
			EXCLUSIVE OR gate	The output event occurs if one, but not the other inputs occur	A failure of the system occurring only if one, not both of the two possible failures happens	≥ 2
			AND gate	The output event occurs only if all of the input events occur	Parallel redundancy, one out of n equal or different branches	≥ 2

Figure 2.4: Subset of the notation used in the FTA case from ISO 61025 [19]

2.1.3 CASCADE

CASCADE is an approach created through a study [14] made at Volvo, by Mohamad et al., which aims to provide an approach for creating security assurance cases, including a "block based" structure which is depicted in Figure 2.5. As can be seen, CASCADE keeps the usage of a top claim and evidence, however it has divided the rest of the case into three blocks and a subcase that gives the case more structure and an inherent flow, in contrast to a more generic SAC.

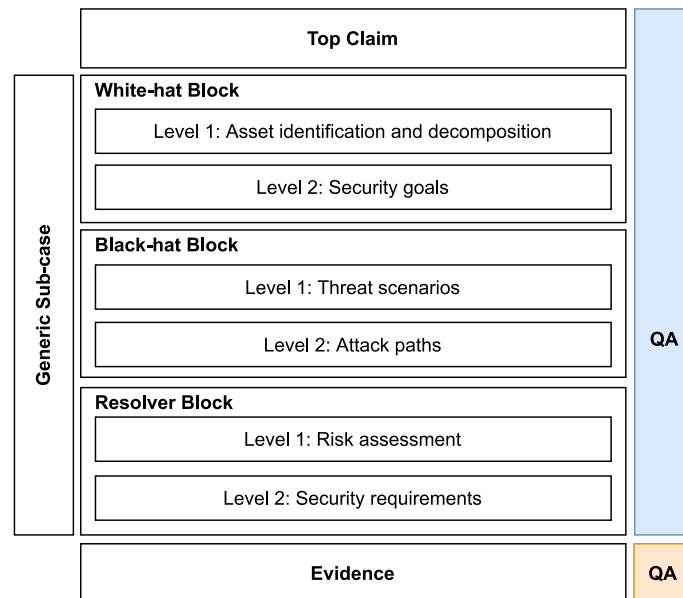


Figure 2.5: The structure for the CASCADE approach displaying all the different blocks

White hat block: This block contains all identified assets, assets in this case refers to artefacts deemed important in the system, and their decomposition as well as security goals that are placed on these [14]. These security goals connect to the decomposed assets and often have ties to the Confidentiality, Integrity and Availability (CIA) triad where the case argues that one or many of the CIA properties are assured for the specific asset. A created example for the white hat block can be seen in Figure 2.6.

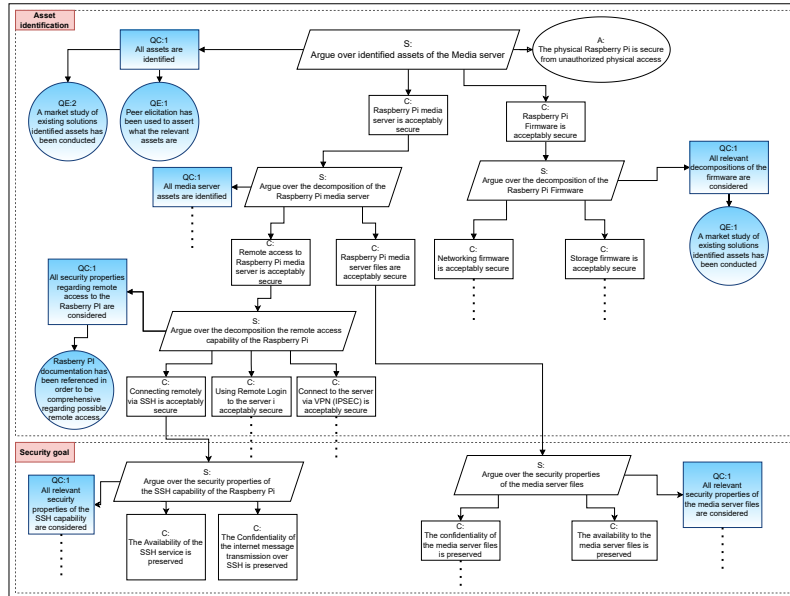


Figure 2.6: A partial example of the white hat block for a Raspberry Pi web server

Black hat block: This block defines claims about threat scenarios that could compromise the security goals defined in the white hat block, and then goes on to specify claims about attack vectors that could realise these threat scenarios [14]. An example of the black hat block can be seen in Figure 2.7.

2. Background and Related Work

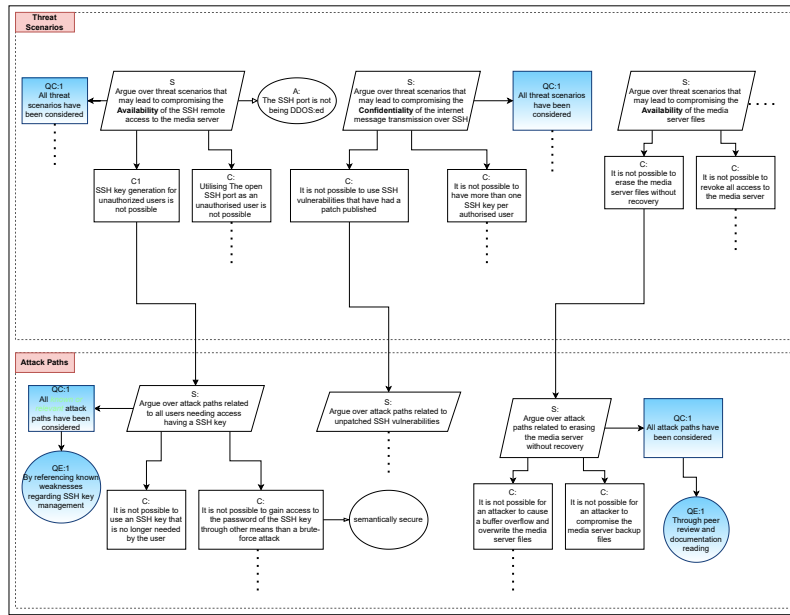


Figure 2.7: A partial example of the black hat block for a Raspberry Pi web server

Resolver block: This block defines claims about the assigned risk treatment to the previously defined attack vectors and then depending on the assigned treatment it provides specific security requirements that need to be fulfilled for the treatment to be effective [14]. Valid treatments would be to *Accept*, *Mitigate* or *Transfer* the risk. A created example for the resolver block can be seen in Figure 2.8.

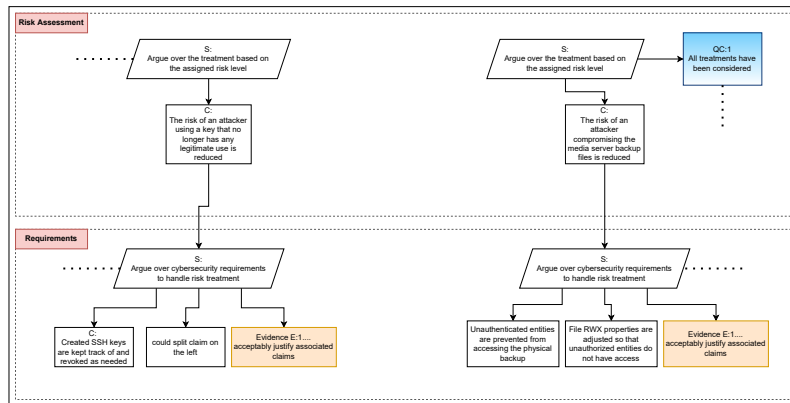


Figure 2.8: A partial example of the resolver block for a Raspberry Pi web server

Generic subcase: This part of the case is used for claims that are non-specific to the case context and could apply to other systems at the company as well [14]. Some usages for this is to express things like "mandatory security training", "company security policies", "thorough workstation firewalls" etc. A created example for the generic subcase can be seen in Figure 2.9.

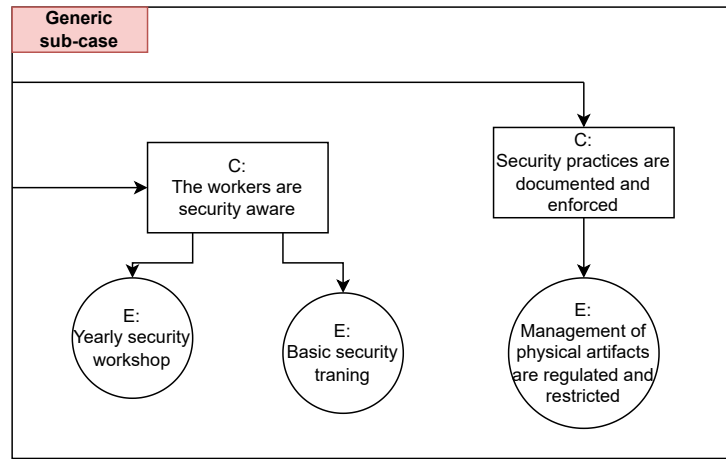


Figure 2.9: A partial example of the generic subcase for a Raspberry Pi web server

In addition to this block structure, another extension *CASCADE* makes (in comparison to conventional Security Assurance Cases) is the usage of quality claims to argue for the completeness of the decomposition of sub claims, as well as for the quality of the provided evidence. Examples for these can be seen in Figure 2.10

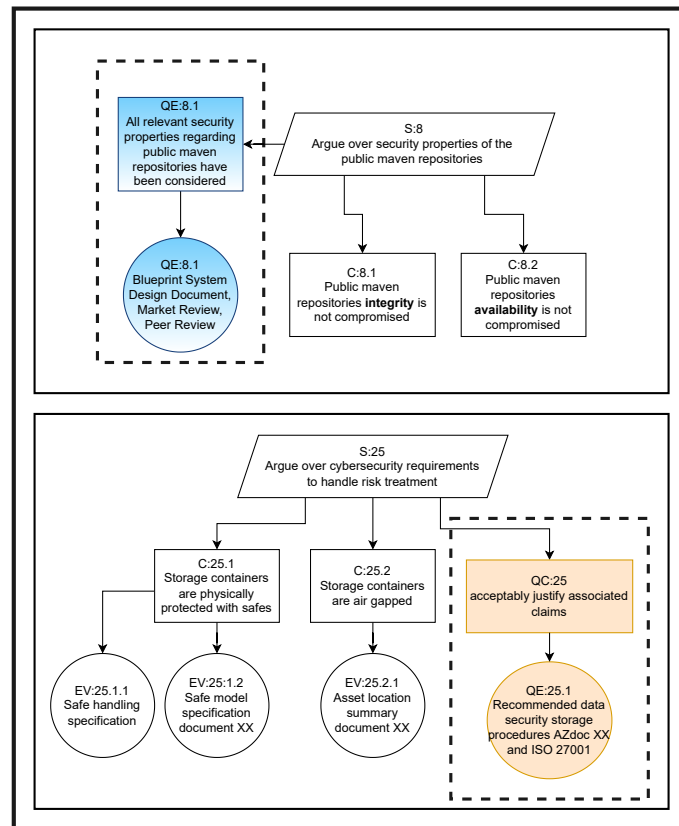


Figure 2.10: Examples for both types of quality claims, the first one (in blue) for arguing completeness of decomposition and the second one (yellow) for arguing quality in evidence attached to the same claim

For the completeness aspect the aim is to provide assurance that the strategy used has decomposed all relevant sub claims (to the best of the creators knowledge), and that it has taken the relevant aspects and assets into consideration. In the case, claims that aim to argue completeness are colored blue, and so is their evidence. For the quality aspect the aim is to argue for the soundness and quality of all evidence assigned to a claim. In the case, claims that aims to argue quality are colored yellow and so is their evidence [14].

2.1.4 Standards and guidelines in the medical domain

This section provides descriptions about the role and purpose of the documentation, standards and guidance documents analysed, in regards to the applicability of CASCADE in the medical domain.

2.1.4.1 Software as a Medical Device (SaMD)

Software as a Medical Device is a new standard from the IMDRF [21] that imposes requirements on different types of software, when used in the context of a medical device (a device/product with medical concerns or goals). This standard retains importance throughout the life cycle of a product as it imposes regulations both before and after the release of a product onto the market.

2.1.4.1.1 Meaning of trustworthiness

Within the Software as a Medical Device (SaMD) guidance documents the word trustworthiness is used several times in relation to the medical devices that the documents apply to. In this context the term “Trustworthiness” has a very specific meaning, and the FDA has defined it as follows:

Computer hardware, software and procedures that:
(1) are reasonably secure from intrusion and misuse;
(2) provide a reasonable level of availability, reliability, and correct operation;
(3) are reasonably suited to performing their intended functions; and
(4) adhere to generally accepted security procedures.

Figure 2.11: Definition of a trustworthy system according to the FDA premarket guidance document [11]

Knowing the exact definition for this word is crucial when assessing a tool’s ability to conform to the guidelines proposed by these documents.

2.1.4.1.2 Post market management document (2016) The Premarket Management Document (PreMD) [12] issued by the FDA is a guidance document that focuses on the measures a company has to take in order for SaMD compliance to be continued after a system or product has reached the hands of consumers. The

document places its focus on encouraging manufacturers to address risk during different stages of the products life cycle in order to lower the likelihood that any of these will cause concerns to users health when the device is in use.

2.1.4.1.3 Pre market management document (2018) The Premarket Management Document (PreMD) [11], also issued by the FDA, fills a similar role to the PMD. However, this document places its focus on the processes that a company has to go through in order for their product to be deemed SaMD compliant before being able to reach consumers (i.e before being available on the market). This creates an incentive for companies in the medical domain, like AstraZeneca, that want their products to be SaMD compliant, to refer to the guidelines of this document throughout their design process.

2.1.4.2 Guidance on Cybersecurity for medical devices (2019)

The “Guidance on Cybersecurity for medical devices” document [1] issued by the MDCG focuses on guiding manufacturers on how to conform with the most important requirements posed by the “MDR Medical Devices Regulation; EU 2017/745” (MDR) and the “In Vitro Diagnostic Medical Devices Regulation; EU 2017/746” (IVDR). As these two regulations aim to ensure that that new devices are capable of facing current technological demands in regards to risk management and cybersecurity, the focal point of this document is to provide guidance on how to achieve this.

2.1.4.3 ISO 14971:2020

ISO 14971 [10] is a standard that specifies requirements for the application of risk management to medical devices. It is an important standard in the medical domain to comply with, as it handles topics and requirements that are often needed for regulatory authorities to be able to issue marketing approval. These requirements stay relevant throughout the life cycle of the product and can be applied to not only medical devices, but also other systems involved with medical devices. A central piece of ISO 14971 is an artefact called the “risk management file”. This file serves to provide traceability for hazards/risks identified to a risk management process and consists of a risk analysis, risk evaluation, risk control and verification of risk control measures. The document also states that “The risk management file can be in any form or type of medium.” and that “Compliance is checked by inspection of the risk management file.”.

2.1.4.3.1 ISO 24791:2020

ISO 24791, Medical devices – Guidance on the application of ISO 14971 [22], contains advice regarding the process of being compliant with ISO 14971.

It further mentions hazardous situations (including those that could result in physical harm) that could stem from cybersecurity risks, and put these in the context of Confidentiality, Integrity and Availability.

- Loss of confidentiality can lead to the disclosure of personal health information.

2. Background and Related Work

- Loss of integrity can lead to incorrectly represented lab results or malfunction of the medical device.
- Loss of availability can prevent the use of critical functionality of a medical device or can stop the use of a medical device altogether.

<i>Hazard</i>	<i>Sequence of events</i>	<i>Hazardous situation</i>	<i>Harm</i>
Loss of data integrity	1) The vulnerability of unnecessarily opened network port is exploited. 2) Dose setting data of infusion pump is modified by unauthorized access.	Incorrect dosage data leading to infusion fluid not being delivered as intended.	Deterioration of health. Death.
Loss of data integrity	1) The vulnerability of unnecessarily opened network port is exploited. 2) Patient data or diagnostic results are modified by unauthorized access.	Modified data leading to incorrect clinical decisions or <i>procedures</i> , or lack of treatment.	Deterioration of health. Unnecessary surgery.
Loss of data availability	1) The vulnerability of unnecessarily opened network port is exploited. 2) <i>Medical device</i> performance is reduced or is terminated by DDoS attack or ransomware.	Delay of therapy. Inability of diagnosis.	Loss of <i>medical device</i> functionality. Deterioration of health.
Loss of data confidentiality	1) The vulnerability of unnecessarily opened network port is exploited. 2) Disclosure of personal health information.	Denial of insurance coverage leading to lack of treatment.	Psychological stress. Deterioration of health.

Figure 2.12: Example from ISO 24791 [22] of concrete hazards (risk) and their potential impact on patient safety

2.1.4.4 ISO 62304:2006

The ISO 62304 [8] standard has strong ties to ISO 14971 [10] regarding the risk management process, with a few additions. These additions consist of additional processes and requirements with a focus on hazards (where a hazard is the risk of causing physical harm). They introduce the concept of Software Of Unknown Provenance (SOUP), and highlight SOUPs as a potential cause for failure and unexpected results. The notion of SOUP is based on the fact that an existing software artifact that could be needed for a medical device might not always be developed in-house by the company manufacturing the medical device, and that they opt for using “off-the-shelf” software that another entity has created.

The SOUP might not have records regarding the development process taken for the creation of the software artifact, and not have any documentation supporting that they have followed certain existing standards and requirements for the development process, hence the “unknown provenance”. They further mention that a risk management file should be created in accordance with ISO 14971 and used during the

risk management process, and that there is an emphasis on traceability of the hazard (safety) risk and the risk control measure that has been put in place (such as a software item), as well as verification of the risk control measure in place (evidence).

A safety class of identified software items in the medical device is needed, where the safety class is derived from the possible hazard from the software items, and categorized as Class A, Class B and Class C. The meaning of each safety class can be seen in the bullet list below.

- Class **A**: No injury or damage to health is possible
- Class **B**: Non-SERIOUS INJURY is possible
- Class **C**: Death or SERIOUS INJURY is possible

2.1.4.5 Good Clinical Practice (GCP)

GCP is a quality standard introduced by the EMA [23], which outlines ethical and scientific concerns regarding clinical studies and/or trials, posing requirements on the design, recording, and reporting of these studies/trials that involves the participation of human subjects. The GCP quality standard is relevant in the medical domain, as companies can conform with the GCP standard in order improve the effectiveness and the ability of regulatory authorities to review the data and results of the clinical study.

2.1.5 Guideline on computerised systems and electronic data in clinical trials

The Guideline on computerised systems and electronic data in clinical trials [9] highlight the GCP position on the handling (collection, storing, archiving) of data, which has implications on the required security for this process, since the data handled could be deemed highly sensitive. Improper handling of the data could have consequences such as severe legal repercussions for the responsible entity, if for example the data in the clinical trial were to be accessed by an unauthorized party.

2.1.5.1 NIST 800-30 (Revision 1)

The Guide for Conducting Risk Assessments, published by the National Institute of Standards and Technology (NIST), is a guideline highlighting strategies and approaches for risk analysis, which is used across several domains where there is a need for handling risks related to cybersecurity. It introduces both qualitative and quantitative approaches for risk assessment, where the likelihood of occurring and impact of the risk is taken into consideration. It calls for the identification of assets, security goals and attack vectors as part of the risk assessment.

2.1.6 Risk assessment matrix

Risk assessment matrix is a tool used in the medical domain [24] with the purpose of assigning a rating and color to patient safety risks. This system rates risks as either green, yellow or red, where green denotes a low risk and red denotes a high risk. This rating is dependent on two main factors, the probability of the risk occurring and the impact should the risk occur. An illustration showing a risk assessment matrix as well as a calculated example can be seen in Figure 2.13.

		IMPACT/CONSEQUENCE LEVELS				
		SLIGHT / NEGLECTIBLE [1]	MINOR [2]	MODERATE [3]	MAJOR [4]	CATASTROPHIC [5]
LIKELIHOOD DESCRIPTORS		Injuries requiring no treatment or first aid	Minor injury, first aid only required	Injury requiring medical treatment and some lost time	Serious injury, hospital treatment required	Death or permanent disability
RARE / REMOTE [1]	May happen only in exceptional circumstances	1 VERY LOW	2 VERY LOW	3 LOW	4 MODERATE	5 MODERATE
UNLIKELY [2]	Could happen some time	2 VERY LOW	4 LOW	6 MODERATE	8 MODERATE	10 MODERATE
POSSIBLE / OCCASIONALLY [3]	Might occur occasionally	3 LOW	6 MODERATE	9 MODERATE	12 MODERATE	15 HIGH
LIKELY [4]	Will probably occur in most circumstances	4 LOW	8 MODERATE	12 MODERATE	16 HIGH	20 VERY HIGH
ALMOST CERTAIN [5]	Expected to occur in most circumstances	5 MODERATE	10 MODERATE	15 HIGH	20 VERY HIGH	25 VERY HIGH

RISK EXAMPLE	LIKELIHOOD	IMPACT	RISK LEVEL	RISK GRADING
PATIENT INJURY	LIKELY [4]	MAJOR [4]	16	HIGH

RISK GRADING COLORS				
1-2 VERY LOW RISK	3-4 LOW RISK	5-12 MODERATE RISK	15-16 HIGH RISK	20-25 VERY HIGH RISK

Figure 2.13: Illustration from Pascarella et. al [24] showing how a risk matrix is used to classify a risk level depending on the risk's probability and impact

2.2 Related work

This section aims to list literature that has been reviewed for the purpose of finding current gaps in research regarding SACs current usage and limitations as well as maintainability of SACs, SACs used in an iterative workflow.

2.2.1 General overview of Security Assurance Cases and current research

Arnab Ray and Rance [25] presents security assurance cases as an approach to increase security for medical devices. With this security improvement a safety enhancement may follow as security breaches may lead to malfunction or denial of service for these devices causing potentially harmful consequences for the user. They

also propose that the usage of SACs can be a driving force for the development and documentation for medical devices regarding the design, implementation and verification etc. By creating the assurance case alongside the development desirable security practices can be achieved and the case itself may be used as a thorough representation and motivation for the device security. This is in contrast to current observed usage where assurance cases for medical devices are often created after development as a means to satisfy regulatory bodies. Cases created in this manner are often viewed as more of an unnecessary use of resources, than an actual method aimed to enhance security.

Mohamad et al. [14] provides a comprehensive view of the increasing research regarding SACs through a Systematic Literature Review (SLR), covering the topic. This is performed by analysing and discussing 51 research papers applied in different domains, and with different focal points of research. The papers provides categorisation for the different studies according to metrics such as the type of study, which domain it was conducted in, what came out of the study (including the approach, tools used) etc. The review also provides guidelines for the creation workflow of a SAC as well as a reading guide, providing papers that covers all blocks included in the creation of a SAC.

Mohamad et al. [17] describes an approach for creating SACs, CASCADE, that is driven by assets. An example case is also outlined where CASCADE is applied to an example use case available in ISO/SAE-21434 [26]. The approach aligns with the requirements from ISO/SAE-21434 and needs from automotive Original Equipment Manufacturers (OEM). CASCADE adds two elements to the primary list used in SAC, these being Case Quality claims (CQ-claims) and Case Quality evidence (CQ-evidence). CQ-claims works to assure quality in a case such as completeness and relevance and CQ-evidence works the same but for evidence. This approach is split into six blocks, top claim, evidence, generic subcase, white hat, black hat and resolver block, each containing a part of the case. Through expert discussion performed at Volvo trucks a requirement for SACs not covered by CASCADE were identified, this being the ability to maintain the SAC during the products life cycle, specifically traceability between artefacts and the SACs elements as this would help with an impact analysis following changes and therefore aid maintainability.

2.2.2 Security Assurance Cases in relation to agile development

Johan Peeters [27] introduces in the article “Agile Security Requirements Engineering” another way of thinking about threats, called Abuser Stories, which provide a ranking approach similar to User Stories (which can be ranked in terms of value), where the Abuser Stories can instead be ranked in terms of potential damage and successful attack likelihood. Effective means, and key components of writing quality abuser stories (in relation to agile work methods), are highlighted.

Ben Othmane et al. [28] consider the difficulties in using an iterative approach (Scrum), while developing security features meant to mitigate different security threats, and investigates using Assurance Cases in combination with Scrum. One

particularly apparent challenge is that the target code artifact that the security feature is meant to cover and mitigate threats against, could be updated, and thus requiring another security patch. From the other side of the spectrum, applying security coverage to an existing feature could have an impact on several software quality measures, such as effectiveness (as security layers often introduce computation overhead). The paper also argues that a lot of these problems could be mitigated through avoiding incomplete security tests.

To ensure completeness when it comes to the security tests of a security feature, the authors address this problem through security assurance cases. They highlight a few key concerns when using SACs in conjunction with an iterative approach.

- Component updates could invalidate previously created SAC claims
- New components requires re-evaluation of all related SAC claims
- Changing the use context of the software requires re-evaluation of all related SAC claims
- Adding a new claim requires re-evaluation of all related SAC claims

When it comes to using an iterative approach, they propose a process/method which is focused on enabling incremental work on a security feature, preventing the redevelopment of security mechanisms already in place. The approach consists mainly of creating a high level architecture, create an incremental road map highlighting the increased complexity, and iteratively develop the feature while applying the knowledge gained in previously completed steps. They provide additional goals for each of the Scrum phases (“pregame”, “game”, “postgame”), aimed to mitigate, or ease the amendment of the aforementioned concerns.

An example Case Study regarding secure communication between a mobile device and a remote device, using the proposed process is featured, documenting the process being used in an applied real world context.

Ben Othmane et al. [29] discuss the usage of a SAC in relation to incremental software development and how changes invalidate previous security assurance. These changes are divided into three categories: security requirements changes, code changes, and security mechanism changes. The authors also outlines a prototype of their creation for designing Security Assurance Cases and tracing the impact of code changes in said case. Its composition is divided into three parts, one tool and two eclipse plugins. The tool, Penetration Testing Engine (PTE), extracts parameters for a test case from a given XML file and performs a test with these parameters. The two plugins for eclipse are, Security Assurance Case Plug-in (SACP) that is used for designing SACs in the eclipse environment and User Story Security Mapping Plug-in (USSMP) that allows for mapping between user stories, claims in the security assurance case and security tests that are then matched and performed by the PTE.

2.3 Case Study environment

The case study is performed at AstraZeneca, a large multinational pharmaceutical company in the medical domain with 76100 employees as of 2020 [30]. They have for the past decade increased their focus on the production of software, often in the context of data gathering for clinical studies, as well as for the development of medical devices. The primary department that the study will be conducted in is called Digital Health, which includes the ongoing development of the AstraZeneca BOOST platform, which is used to handle patient and medical practitioner data, in regards to clinical studies.

2.3.1 System documentation

For all of the software products at AstraZeneca, a System Design Document (SDD) [31] is kept, which is called a “Blueprint”. This document contains all information about the system architecture and design and helps the developers through providing this information. The blueprint is incrementally updated during the products life cycle through its tight connections to the iterative workflow at AstraZeneca. This means that new features and artefacts introduced in the software system design phase have to be reflected in the blueprint.

2.3.2 Architecture introduction and mobile app platform

There is currently a surge in the need for a mobile app platform at AstraZeneca, for which the main purpose is to facilitate data collection in regards to ongoing clinical studies - which in turn generates a large amount of data. This data is used by several services and components that have distinct purposes, for which the data that each component needs varies, and there is sometimes a need for duplication of data for these components to work correctly.

2.3.3 Product/system Case Study study suitability

The BOOST platform is one of the larger systems in place at AstraZeneca, that is being developed across several of their sites in different countries, but with the bulk of the platform development responsibility being placed in Sweden, and their sites in Mölndal and Södertälje. This system was deemed suitable for this study due to multiple reasons:

- The system has ties to several highly regulated areas in the medical domain, such as patient- and practitioner data handling and connected medical devices. This means that the system requires a high degree of conformance with applicable standards and compliance with applicable laws, and can be regarded as a benchmark for the suitability of CASCADE in the domain.
- It is under development, meaning that there is a lot of iterative work being performed by several teams allowing for RQ2 related discussion

- The industry supervisor at AstraZeneca is one of the lead software engineers for the BOOST project, for which the bulk of development takes place in Sweden, which allows for better coordination of interviews, focus groups and requirement elicitation, in order to facilitate the case study at AstraZeneca.

2.3.4 Roles at AstraZeneca

As AstraZeneca is a large multinational company, there are highly specific roles in place to fulfill the domain specific operational needs and business needs, as well as the product development needs of the company. These roles are outlined in Table 2.1 below, with the role name, and a brief description of the responsibility of the role.

Table 2.1: Overview of different relevant roles at AstraZeneca

Role	Responsibility
IT Project Manager	Agrees the SaMD life Cycle process with PO, DRP, ITQM & SaMDQM, ITPMs and BPM. Responsible for the successful execution of all IT deliverables.
Product Owner (PO)	Ensures the product is developed to meet the business requirements
	Owns, defines and prioritizes services/functionality that delivery business value.
SaMD Quality Manager(SaMDQM) Device Quality	Ensures activities that fall under SaMD procedures meet quality requirements and SaMD quality input into the project.
Business Quality Management (BQM) Clinical Quality	Reviews and approves non SaMD validation documentation in accordance with ITQMF
	Ensuring GCP compliance for validation activities.
	Provides GCP quality input into the project.
Quality Technical Manager R&D IT (SWQE)	Ensures SaMD quality processes are implemented according to the quality strategy for the project/product
IT Quality Manager (IT QM)	Assures activities that fall under IT procedures meet IT quality requirements.
	Provides IT quality input into the project.

Table 2.1 continued from previous page

Role	Responsibility
Device Responsible Person (DRP)	Accountable for ensuring that development activities meet the medical device requirements.
Risk Management Lead (RML)	Lead risk management activities
	Responsible for establishment of the Risk Management File and maintenance throughout the development project
	Review and approve relevant design controls deliverables
Device Regulatory Lead (DRL)	Provides regulatory guidance and strategy for the development of the SaMD.
End-to-End Service Capability Manager (E2E CSM)	Responsible for developing service and support models for deployment.
Operational Service Manager (OSM)	Service Management for the Boost service. Plans and manages changes for the system or service. Monitor and manage the support processes.
Business Analyst (BA)	Responsible for developing user requirements and ensuring requirements meet the business need
Solution Architect (SA)	Works with the business and BA to understand functional, non-functional and infrastructure requirements. Responsible for high-level design.
Test Lead (TL)	Responsible for creating test scripts and executing UAT and traceability to user requirements
	Responsible for reviewing test scripts and executing UAT and traceability to user requirements
Test Manager (TM)	Responsible and supporting test scripts creation and executing UAT and traceability to user requirements Responsible and supporting and reviewing test scripts and executing UAT and traceability to user requirements Responsible for generating final test summary and traceability reports

Table 2.1 continued from previous page

Role	Responsibility
Configuration Manager (CM)	Handles the configuration management and updates the System index.
IT/SW Dev Lead (DEV) (Squad Lead)	Responsible for the Software Design, API Specifications, and Software Detail Design Plan Responsible for code reviews and checklist compliance, unit and integration tests execution and proper traceability
Patient Safety Medical Device Lead (PSLMD)	Responsible for patient safety input
IT Release Manager (ITRM)	Responsible for the successful execution of all IT deliverables during the release process. Manage release process for external/internal partners/clients

3

Methods

This chapter describes the utilized methods for this study and details the steps taken when executing these. It also provides rationale as to why these methods were chosen and deemed appropriate for answering the research questions posed by this study.

3.1 Case Study

A case study was conducted at AstraZeneca, with the goal of investigating the suitability of CASCADE in the medical domain, and the ability of the created case to be maintained in an agile workflow. This study composed of several different activities outlined in Figure 3.1.

3.1.1 Case Study motivation

A “Field Study” type was deemed as the most suitable study type, given the real-world context and setting at AstraZeneca and our research goals. The Case Study method was deemed as a suitable, as we did not want to make any changes to the setting or control any variables [32].

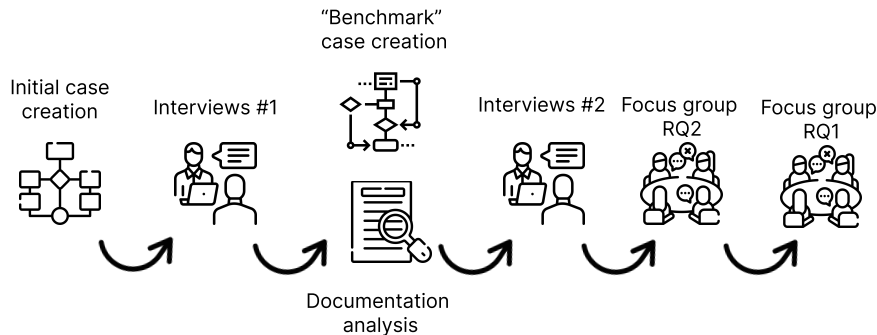


Figure 3.1: A Figure outlining the methods used for the case study in chronological order

The initial case creation was used as an internal tool for learning the workflow behind creating a SAC and a SAC using CASCADE. With this knowledge the first round of interviews were used to elicit the system information necessary to create the benchmark case as well as elicit the documents for the documentation analysis.

The second round of interviews served as initial validation for the documentation analysis results and as data gathering for RQ2. This was meant to be followed up with a focus group for the RQ1 results, however focus group RQ2 was performed before focus group RQ1. This was due to the second focus group being given a longer time-slot which was deemed necessary for validating RQ1. Finally focus group RQ1 was performed which brought together the results for interviews #1, benchmark case creation and the documentation analysis.

3.1.2 Overview of participants

Several actors were included in the different activities performed and these are outlined and mapped to respective activity in Table 4.2. As can be seen from the Table, the participants had roles that varied significantly, which helped to excel discussions and provide opinions grounded in different parts of the studied system.

Table 3.1: Participants in the case study activities

ID	Company	Role	RQ1 Suitability	RQ2 Maintainability	Focus group #1	Focus group #2	Benchmark case	Interviews #1	Interviews #2
1	AstraZeneca	Software Engineer Lead	✓	✓	✓	✓	✓	✓	
2	AstraZeneca	Software Engineer Lead	✓	✓	✓	✓	✓	✓	
3	AstraZeneca	SaMD Quality Lead	✓	✓	✓	✓		✓	✓
4	AstraZeneca	Senior Software Engineer	✓	✓	✓	✓			
5	AstraZeneca	Project Manager		✓	✓				
6	AstraZeneca	Test Manager		✓	✓				
7	Chalmers University of Technology	Researcher	✓						
8	Chalmers University of Technology	Researcher	✓	✓		✓			

3.1.3 Initial case creation

Initially a generic SAC was created in accordance with the guidelines and definitions provided by a paper on security assurance cases from Carnegie Mellon University [13], describing the SAC creation process. The context for this SAC was a hypothetical Raspberry Pi web server, the case can be viewed in Appendix C. This served as a basis for hands on learning about SAC creation and a starting point for internal discussions. After receiving feedback on the generic case, another case was created with a similar context, but this time using the CASCADE approach, which is outlined by Mohamad et al. [17]. This case can be viewed in Appendix C. Not only did the process of creating these two cases help with understanding the practical application of SACs, but they also served as a stepping stone in the creation of the benchmark case that was to be created together with engineers and security experts at AstraZeneca. They were used as a reference and example tool to explain how a case could look and what the different parts of the case should contain.

3.1.4 Interviews

Interviews were used in the process of answering the first research question and were carried out in two separate rounds containing several interviews each. The questions for the interviews can be found in Appendix A.

3.1.4.1 Interview structure

The interviews were conducted in a semi structured way as this would provide qualitative information while still ensuring that the interviews stay close to the problem of interest. Using a semi structured approach also helped with the interview technique as predefined questions worked as the backbone of the interviews and a framework to fall back on when the currently discussed topic reached an adequate saturation. Keeping to a few loosely defined questions also helped with the analysis that followed the interviews as the data was more comparable between subjects in contrast to data generated from a more unstructured interview approach.

3.1.4.2 Interviews round #1

The first round of interviews were conducted with a software engineering lead working on the BOOST system and the SaMD coordinator at AstraZeneca, with the focus of getting a deeper insight into the regulations and requirements placed on the documentation of the BOOST system and security demands from regulatory authorities. They were also used in order to elicit important areas of the system that would serve as the ground for the benchmark CASCADE case.

3.1.4.3 Interviews round #2

The second round of interviews focused on validation for findings in the documentation that were relevant to CASCADE. In practice this meant interviewing the SaMD coordinator as this is the role with the most knowledge about the specific requirements and applications that are stated by the standards important to the medical domain. Interviews for data gathering regarding possible approaches for accommodating a process involving the maintenance of the created CASCADE case, into AstraZenecas workflow were planned but could not be executed due to time constraints. This data gathering was transferred to the first focus group.

3.1.5 Benchmark case creation

A case was made to serve as a benchmark (in the sense of evaluating domain suitability) for the applicability of CASCADE in the medical domain and it was created over several sessions with different software engineers at AstraZeneca. The elicitation was performed through unstructured discussions about the system and was primarily done in a top down manner to utilize the inherent flow of CASCADE. This meant first working out the relevant assets and what their security goals were then looking at threats and risks relating to these then assigning treatments and requirements to the risks and finally providing evidence for the requirements. As creating a complete SAC following any approach is a very labor intensive process and beyond the scope of this thesis the case was created to be partially complete but containing enough information to be used to assess the performance of CASCADE in the medical domain.

3.1.6 Documentation and regulation analysis

From an initial elicitation, several policies and regulations placed on the project were identified. These regulations exist on a spectrum both in regards to their connection to the medical domain and the stringency that they impose on the project (through compliance with applicable requirements being mandatory for product marketing approval). For this study, the focus of the analysis is placed on regulations that handle the medical domain in a direct manner, as these serve as a deciding factor whether CASCADE is an applicable approach to the medical domain in its current form, or if alterations are necessary.

When assessing the suitability of the CASCADE approach in relation to the documentation, it was divided into its fundamental parts as these are outlined by Mohamad et al. [17]. Their individual ability to provide value for the requirements introduced by identified standards and regulations in the medical domain were then examined. The Top Claim apparent in the CASCADE approach was not a candidate to take into consideration, as the existence of a White hat block implicitly implies the existence of a Top Claim. The fundamental parts taken into consideration are as follows:

- White hat block
- Black hat block
- Resolver block
- Evidence
- Case quality assurance
- Generic sub-case

3.1.7 Focus group

Focus groups were utilized on two different occasions. The first focus group session was utilized for data gathering for RQ2, regarding the inclusion of a maintainability process for a CASCADE case in the medical domain. The participants for the session were composed of six experts from AstraZeneca with different roles and areas of responsibility in the company, which can be seen in Table 4.2, with varying degree of expertise regarding their iterative workflow. The session started with a short presentation that explained the research question in focus as well as a brief description of SACs and CASCADE. Following this, all participants filled in a questionnaire, see Appendix B, where the questions and answers served as a basis for initial discussions. After these discussions had been concluded to an appropriate degree (i.e the discussion simmered down and data gathered was deemed enough), the focus changed towards answering RQ2 through brainstorming between the participants. For this part the focus group organizers assumed a more passive role, letting the focus group participants discuss their experiences about their workflow and key project processes apparent at AstraZeneca.

The second focus group was used as validation for the results generated from the interviews, documentation analysis and case creation in regards to RQ1. The group was composed of four participants from AstraZeneca with knowledge about the system of interest, and a Chalmers researcher with vast CASCADE knowledge (specific roles can be seen in Table 4.2). The session began with a quick repetition of SACs and CASCADE which then transferred into discussions about the findings and results for RQ1. These were presented one by one and discussed among the participants. An additional activity that took place during the session was for use case creation where the participants discussed potential use cases of SACs in regards to the existing roles at AstraZeneca.

4

Results

The result section aims to convey key findings regarding overlap of concerns when it comes to the CASCADE approach, and existing standards and guidance documents prevalent in the medical domain. Assessments of overlap regarding processes and tools currently in use in the medical domain (at AstraZeneca) will also be conveyed. And finally, findings regarding the process of maintaining a Security Assurance Case in the medical domain will be presented.

4.1 Suitability of CASCADE in the medical domain

This section will present the results with ties to the adaptability of the CASCADE approach to a medical context. This includes the derived use cases and the overlaps found in the documentation analysis.

4.1.1 Identified use cases for CASCADE in the medical domain

Use cases for SAC in the domain were created in order to show its practical applicability. The SaMD coordinator created 15 use cases for SACs in the medical domain seen in Figure 4.1. These show that SACs have the potential to prove useful for several of the roles utilized at AstraZeneca. During the second focus group use cases was also discussed and two additional ones elicited were:

“As a test manager I would use SACs in order to elicit what needs to be tested for a specific software artifact in order to facilitate traceability to user requirements”

“As a SaMDQM, I would provide applicable evidence (test cases and test suite results) to claims in the SAC case, in order to increase the quality and argumentative power of the SAC case, which in turn provides an increased ability to argue for the quality of the product”

Figure 4.1: Derived use cases from the second focus group

In the Table 4.1, the SAC use cases created by the SaMD coordinator at AstraZeneca

4. Results

are presented. The roles mentioned in the use cases can be seen in Table 2.1.

Table 4.1: Overview of identified use cases for Security Assurance Cases

ID	Use Case Description
1	As a Device Regulatory Lead (DRL), I would use top-level SAC to prove to the regulatory agencies that the company has considered all relevant security aspects of the final product, and has enough evidence to claim that it has fulfilled them to meet the Intended Use claims of the medical device.
2	As a member of the Risk and Cybersecurity teams, DRP & RML, I would use detailed SAC to prove to AstraZeneca (AZ) compliance, and regulatory teams that the project has complied to AZ Risk & Cybersecurity Standard Operating Procedure (SOP)s, ISO 14971 standard, FDA Guidance in addressing patient safety and cybersecurity concerns and show them evidence of my claim of compliance.
3	As a member of the AZ's compliance team, SaMDQM, BQM, SWQE, ITQ I would use detailed SAC to review and ensure compliance to AZ Risk & Cybersecurity SOPs, ISO 14971 standard, FDA Guidance in addressing patient safety and cybersecurity concerns and document the effectiveness of the QA review.
4	As a project manager or RM, I would use SAC to make sure that a project is ready from a security point of view to be closed and shipped to production.
5	As a project manager or RM, I would include SAC in my project plan. I would make sure the project has the needed resources and time for creating the case (argumentation, evidence collection, etc).
6	As a project manager I would use sac to monitor the progress of my project when it comes to fulfillment of security requirements.
7	As a product owner, I would use SAC to make an assessment of the quality of my product from a security perspective, and make a roadmap for future security development.
8	As a product owner, responsible for my project's handling threats and vulnerabilities, I would use SAC to evaluate the effect of new threats and vulnerabilities, and evaluate whether a change is needed to the product or product lines.
9	As a member of the supplier assessment team, I would include SAC as a part of the contracts made with suppliers, in order to have evidence of the fulfillment of security requirements at delivery time, and to track progress during the supplier's development time.
10	As an cybersecurity Subject Matter Expert, SME on a project team, I would use detailed and visual SAC to communicate with the risk owner, and decide how to update the product security in the rightway (to know what to do).

Table 4.1 continued from previous page

ID	Use Case Description
11	As a system leader or solution architecture on a project, I would use SAC to make an assessment of the quality of my system from a security perspective, and make a roadmap for future security development.
12	As a software developer responsible for implementing cybersecurity controls on my project, I would use SAC from previous similar projects as a guideline for secure development practices.
13	As a corporate QA owner, I would use SAC during a EU or FDA inspection if a regulatory issue is raised against the company for security related issues. I would use the SAC to prove that sufficient preventive actions were taken.
14	As a member of the corporate communication team, I would use SAC as a reference to answer security related questions.
15	As a member of the Patient Safety team, I would use detailed SAC to prove AZ compliance and effectiveness of addressing any patient safety concerns with respect to cybersecurity threats that have the potential of any patient safety concerns.

4.1.2 Overlap with existing practices

One of the more prominent practices/tools used for risk management at AstraZeneca is the Fault tree analysis, which is used to identify causes that could impact the user in some way, and result in some type of hazard/patient harm. This has overlap in the sense that some of the component failures that need to be taken into consideration in the FTA stem from cybersecurity concerns, and that the approach also relies on notion claims (and a so called “top claim”). However, since the FTA also takes non-cybersecurity concerns into consideration (such as safety hazards), the general scope for use cases with FTA is wider. Potential safety hazards, such as a medical device battery running out, or a short-circuit occurring in the system, are also apparent in the FTA artifacts available at AstraZeneca. However while the scope is wider, the created FTAs are generally smaller in size and scope, as there is no underlying structure (like the block based one provided by CASCADE), that can support a huge case. The structure for FTAs is also defined through events regarding failures in a system, without any inclusion of evidence or measures for remediating failures. This is in contrast to SACs where the structure is defined through claims about the system and accompanied with evidence for the correctness of the claims on the lowest level.

4.1.3 Identified overlap between CASCADE and regulatory documentation for the medical domain

The overlap between all of CASCADEs parts and the most prominent regulatory standards and guidance documents in the medical domain has been identified, and is detailed in this section. The investigated documents were elicited through interviews with a safety expert at AstraZeneca. The list of documents is comprised of the

4. Results

SaMD pre- and postmarket guidance documents issued by the FDA, the pre- and postmarket guidance documents issued by the MDCG, EMA, FDA, several ISO standards and NIST 800-30. The specific overlaps for each CASCADE part found in these documents are presented in Figure 4.2 and the compiled findings in regards to each CASCADE part can be seen in Table 4.2.

Table 4.2: Prominent standards and guidance documents in the medical domain and their identified overlap with CASCADE

Artifact			Categorization					
Reference	Type	Market	White hat	Black hat	Resolver	Generic	Evidence	Quality claims
ISO 14971:2019 [10]	Standard	International	✓	✓	✓	✓	✓	✓
ISO 62304:2006 [10]	Standard	International	✓	✓	✓	✓	✓	
MDCG 2019-16 [1]	Guideline	EU	✓	✓	✓	✓	✓	
SaMD Premarket [11]	Guideline	US	✓	✓	✓	✓	✓	✓
SaMD Postmarket [12]	Guideline	US	✓	✓	✓		✓	
NIST 800-30 [33]	Guideline	US	✓	✓				
EMA/226170/2021 [9]	Guideline	EU	✓	✓		✓	✓	

In Figure 4.2, each concrete part of CASCADE has been given a specific color, and the corresponding finding in each document that relates to the concrete part of CASCADE has been given the same color.



Figure 4.2: High level overview of findings in the documentation and their overlap with the blocks of CASCADE

4.1.3.1 Post market

In the postmarket management document (PMD) [12] there are several requirements stated that directly tie into different parts of CASCADE. Early on, it states that manufacturers are required to have a "cybersecurity vulnerability and management approach" [12] in place. They then proceed to outline the concrete parts required for such an approach. These are as follows:

1. Identification of assets, threats, and vulnerabilities;
2. Assessment of the impact of threats and vulnerabilities on device functionality and end users/patients;
3. Assessment of the likelihood of a threat and of a vulnerability being exploited;
4. Determination of risk levels and suitable mitigation strategies;
5. Assessment of residual risk and risk acceptance criteria.

Looking at the first item there is a clear use case for the white hat block and the black hat block, with a special emphasis on the first level of both, these being, for the white hat block "*asset identification and decomposition*", and for the black hat block, "*threat scenarios*". These are, as the names imply, used for identifying and

breaking down the assets that compose the system, and stating what the potential threats to these assets are.

When looking at the second, third, fourth and fifth item there is a connection to the resolver block, which handles risk assessment, and what the treatment for a specified risk should be (mitigation, transfer etc.).

The PMD also states a recommendation for manufacturers to perform cybersecurity risk analyses, and as a part of this analysis, the inclusion of threat modeling is proposed. As explained by Mohamad et al. [17], a *Threat Assessment and Remediation Analysis* (TARA) [34] performed using the threat model STRIDE [35], was used to create the black hat block in a case study at Volvo, which indicates that a TARA, like the one proposed by this document, could be expressed in terms of a black hat block in CASCADE.

It also urges manufacturers to perform software validation, taking the form of software testing (such as unit tests, integration tests etc.), in conjunction with the previously mentioned risk analysis. It then proceeds to elaborate on the main purpose of the software validation, this being the assurance that the remediation applied to identified risks was successful. Not only would CASCADE provide a logical approach for displaying these tests and their results through evidence, but it would also allow for the designer of the case to specify the connection between the risks and their specific testing using risk treatment and concrete requirements as an intermediary step.

4.1.3.2 Premarket

The premarket management document (PreMD) [11], contains the same, identical, bullet list (bullet list 5.) as the one presented in the PMD and so the same connections that were made between the PMD and CASCADE related to that list can be made for this document as well.

However, something that is stressed in the PreMD that is not brought up in the PMD, is the need for devices to be trustworthy, stating that "Manufacturers should design trustworthy devices and provide documentation to demonstrate the trustworthiness of their devices in premarket review" [11]. CASCADE has the means to provide this documentation, but a prerequisite to this is that the system already needs to be adequately tested and verified, since the role of SACs is to provide documentation that demonstrates what security measures have already been taken. Having performed rigorous testing and risk proofing of a system does not provide trustworthiness (as outlined in Figure 2.11) itself, unless it can be properly portrayed through proper documentation, validation and argumentation. This is where CASCADE has the ability to create confidence in cybersecurity contributing towards trustworthiness through the case itself, as this conveys all known and relevant (as scoped in terms of "acceptably secure") cybersecurity measures taken and through the use of "case quality assurance". "Case quality assurance" is an element to CASCADE that tries to verify that breakdowns made in the case are exhaustive/complete, meaning that all assets, risks, mitigation strategies etc. have been identified and accounted for. It is also used to show that claims with evidence assigned uphold a certain

amount of quality. These two aspects serve to create more trustworthiness in the documentation, which in turn helps to provide trustworthiness for the device.

Just as with the PMD, there are several mentions of software validation and why this is necessary, stating reasons such as reasonable assurance of the safety and effectiveness for the system/product in question. However, the PreMD goes a step further than the PMD by outlining specific design implementations that they recommend (for the submission to be approved by FDA).

The kind of specific implementations include:

“Limit access to devices through the authentication of users” [11]

“Verify the integrity of all incoming data” [11]

Figure 4.3: Requirements taken from the PMD document by FDA [11]

Given a concrete list of required implementations (with a base in cybersecurity, like in Figure 4.3), any potential SAC approach could prove beneficial for demonstrating compliance with these. The list of implementations can first be used together with the context element, to help set the scope of the case, and further aid in defining what the reoccurring “acceptably secure” means for the case. If this list has been kept in mind during the product creation, then the case can be used to show that these implementations truly have been taken into consideration for all relevant assets.

Finally the PreMD outlines a list of best practice activities, such as password handling and user authentication. Adherence to best practice elements like these that are relevant throughout the company and incorporate several products can be documented in the generic subcase part of CASCADE.

4.1.3.3 NIST 800-30

The NIST 800-30 guidance document outlines a risk management process that includes identifying security goals for assets, identifying vulnerabilities, and gives examples of concrete attack vectors (such as phishing attacks, DDoS attacks), in conjunction with suggestions on how the severity of attack vectors can be measured. The identification of assets and security goals align with the purpose of the white hat block in CASCADE, and the identification of vulnerabilities and attack vectors has an overlap with the black hat block in CASCADE.

4.1.3.4 Medical Device Coordination Group 2019-16

The MDCG guidance document [1] contains similar connections to CASCADE as the FDA issued guidance documents. It explicitly points out the usage of risk management system and threat modeling and security verification and validation through testing. There are also a requirement taken from Annex 1 in the same document regarding information security stating that devices incorporating software should be developed using state of the art risk management and verification. Along

with this they provide a definition from ENISA for the information security domain “Protection against the threat of theft, deletion or alteration of stored or transmitted data within a cyber system”. This definition ties in to all parts of CIA and through extension the security goals in the white hat block.

However, the MDCG also includes a statement that urges healthcare providers to learn and adhere to best practices when it comes to general cybersecurity measures. A list from the MDCG document [1] of what is meant by best practices is specified in the list below:

1. Good physical security to prevent unauthorised physical access to medical device or network access points.
2. Access control measures (e.g. role based) to ensure only authenticated and authorised personnel are allowed access to network elements, stored information, services and applications.
3. Network access controls, such as segmentation, to limit medical device communication.
4. General patch management practices that ensure timely security patch updates.
5. Malware protection to prevent unauthorised code execution;
6. Security awareness training.
7. Auditability that supports non-repudiation, i.e. the ability to reliably determine who made what changes to the system and when to assist with forensics.

Viewing these from the perspective of CASCADE, a strong connection can be made between the implementation of these, and the block of CASCADE known as the “generic sub case”. As the main purpose of the generic sub case is to abstract and document general practices and SOPs that are prevalent at the entity in question (such as a pharmaceutical company), that in turn lead to an improved security at the entity. The incorporation and conformity of the above mentioned items would be displayed in the generic sub case. This is due to all of them relating to general non-product/system specific practices (or practices that span over for example a family of products).

In the MDCG guidance document, there is also a section dedicated to how documentation should be handled. In this section it specifically states that documentation should conform with the requirements stated in “Medical devices regulations, Annex I”. Showing that conformity has been achieved given specific regulations is one of the key features of a SAC approach, and as explained earlier having concrete requirements are crucial for scoping the case (which is immensely important when the main focus is demonstrating compliance or conformance to specific requirements, as SACs in general have a tendency to grow very large when the scope is large). Looking closer at Annex I [1], there are requirements that regard risk and impact assessment, security awareness training and data integrity that would be part of the resolver block, generic sub case and white hat block in that order.

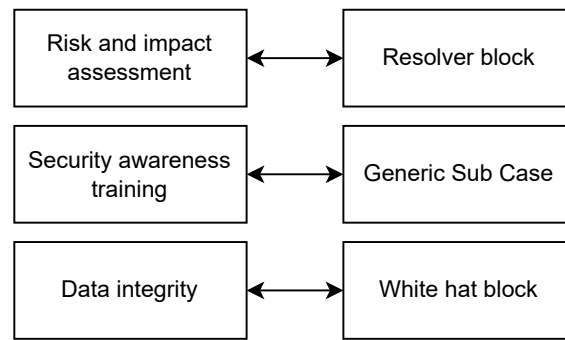


Figure 4.4: Mapping between important areas introduced in MDCG Annex I and CASCADE blocks

4.1.3.5 Good Clinical Practice (GCP)

In response to an enquiry made to the European Medicines Agency, regarding the cybersecurity requirements imposed by the GCP quality standard, the response (which can be seen in appendix D) outlined important sections of the “Guideline on computerised systems and electronic data in clinical trials”.

It mentions an array of best-practices for a good cybersecurity posture, including the use of data backups, network firewalls, anti-virus software and authentication policies. At one point the sentence “There should be documented training on the importance of security” is used. Showing conformance with best practice requirements like these can be achieved through the generic sub case. The best practices present in the document are motivated through threat scenarios/attacks that could occur if the implementation of the best practices is not successful.

It further stresses the importance of data integrity, as any unauthorized or uncontrolled changes to the data can jeopardize the results of the clinical trial, as well as impact the privacy and integrity of the participants in the clinical trial. This property is something that could be shown through the white hat block (through security goals, i.e the integrity is not compromised).

4.1.3.6 ISO 14971

A central piece to the ISO 14971 [10] is an artefact called the “risk management file”. The way this file is specified ties into several of CASCADEs usage areas. The specification consists of a risk analysis defined as documentation of intended usage and foreseeable misuse, identification of safety related characteristics and identification of hazards.

Certain safety related characteristics can then be expressed in the white hat block, such as properties that need to be preserved (security goals) in order to prevent hazardous situations, namely security risks with properties that could have a safety impact. There are also safety related characteristics that can be expressed in the black hat block, but then of the kind that relates to the concrete situations that could potentially result in a violation of the established properties that need to be preserved (threat scenarios). However, there are some safety related characteristics

that have no connection to cybersecurity (such as short-circuits or battery damage) that do not belong in a SAC.

Risk control is indirectly performed through assigning risk treatments in the resolver block and then providing evidence, that ensures that the risk has reached an acceptable level. In regards to the requirement of providing traceability between risks and the “risk management process”, it is one of the core functionalities of CASCADE and any other SAC approach, as they are explicitly tied together in the assurance case. The same reasoning goes for using the risk management file as a way to show compliance during an inspection.

The document also stresses the importance for completeness when doing risk management as “An incomplete task can mean that an identified hazard is not controlled and harm can be the consequence.” CASCADE tries to control for this by utilising quality claims that involves gathering evidence that all risks/hazards have been accounted for, and argues for the achieved completeness. It further calls for the identification of characteristics related to safety, as well as identification of hazards, which are tied to the identification of assets that the medical device consists of.

There are also mentions the requirement of competence of the personnel responsible for carrying out the risk management process and application of ISO 14971, and that they have the necessary skills, education, training and experience of the applicable medical device, as well of the technologies and the risk management techniques used during the risk management process. These properties tie in to the “Generic Sub Case” of CASCADE, and that there are skills and practices in place that carry over between different (separate) applications of SAC creation using CASCADE.

A noteworthy statement that ISO 14971 makes is that the standard can be used to assess all types of risks that are related to medical devices, not only cybersecurity related ones. As CASCADE is a SAC approach, only cybersecurity based risks are to be recorded in the case, meaning that purely safety based risks need to be handled with another process (such as FTA and SaAC).

4.1.3.7 ISO 62304

As ISO 62304 requires that a risk management process is applied in accordance with the specifications in ISO 14971 “The **MANUFACTURER** shall apply a **RISK MANAGEMENT PROCESS** complying with ISO 14971.”, the same connections to CASCADE that was made for that standard in regards to the risk management process can be made for ISO 62304 as well.

The ISO 62304 standard also requires that documentation providing traceability be created, the sought after traceability is described as: hazardous situation -> software item -> software cause -> risk control measure -> verification of measure (as shown in Figure 4.5). This way of showing traceability is almost identical to the flow in CASCADE going from an asset (software item) in the white hat block, through the other blocks, to finally reach a level where evidence is provided.

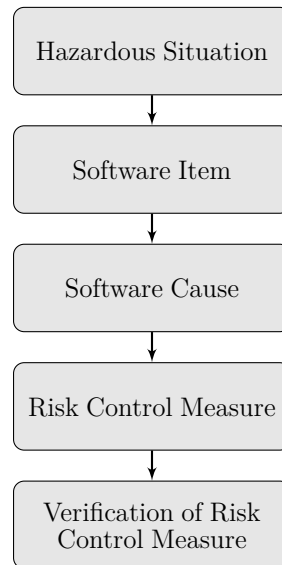


Figure 4.5: Outline of risk management process flow in ISO 62304 [8]

4.2 Extension of existing CASCADE approach

This study has during several stages found a need for CASCADE to include traceability for safety related security risks. This does not imply that additional claims needs to be included in a created case, rather it calls for the need to include safety risk ratings, and distinguish the safety related security risks from purely security based risks included in the case.

The MDCG document contains two illustrations that are used to convey the need for this type of traceability and in what part of the design process the concerns are accounted for. The first illustration, a Venn diagram, illustrated in Figure 4.6, displays the relation between security and safety, and the different types of risks that arise from their relation depending on what is impacted and what the attack surface is. One part that is of particular interest is the intersection between safety and security, “Security risk with safety impact”, as is it is the need for special treatment of the risks contained by this intersection that is being investigated. As for the section named “Security Risk” in the venn diagram (which represents purely security based risks), MDCG urges no further need for investigation or mitigation, as these risks are not imposed with any special requirements from them.

Regarding the section named “safety related risks”, it falls outside the scope of a Security Assurance Case (which only handles security aspects), and is therefore not taken into consideration in this study. Along with this illustration, the document states that “there is a need to consider the relationship between ”safety and security” as they relate to risk ... safety may be compromised due to ”security issues” which may have safety impacts” [1].

In the second Figure 4.7 the focus is on the arrow going from “cybersecurity risk evaluation” to ”risk evaluation”. This arrow denotes the need for traceability between these two processes as they are connected through security risks that also

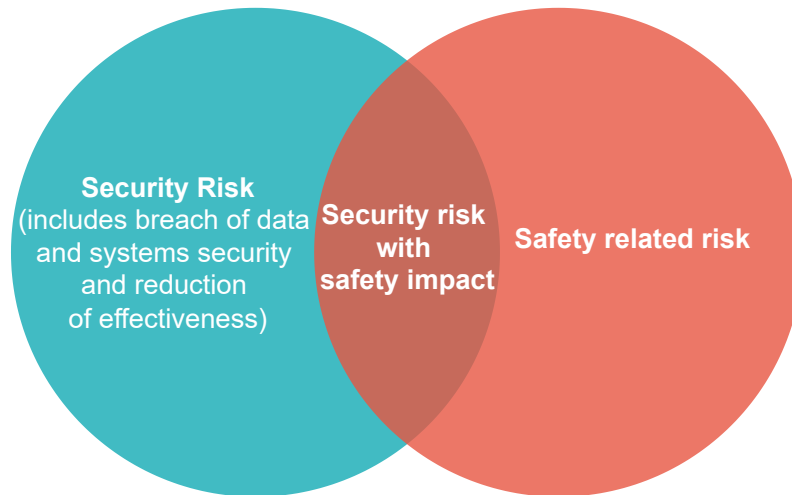


Figure 4.6: A visual representation of the relevant intersection between security and safety, based on the MDCG guidance document [1]

have safety risks.

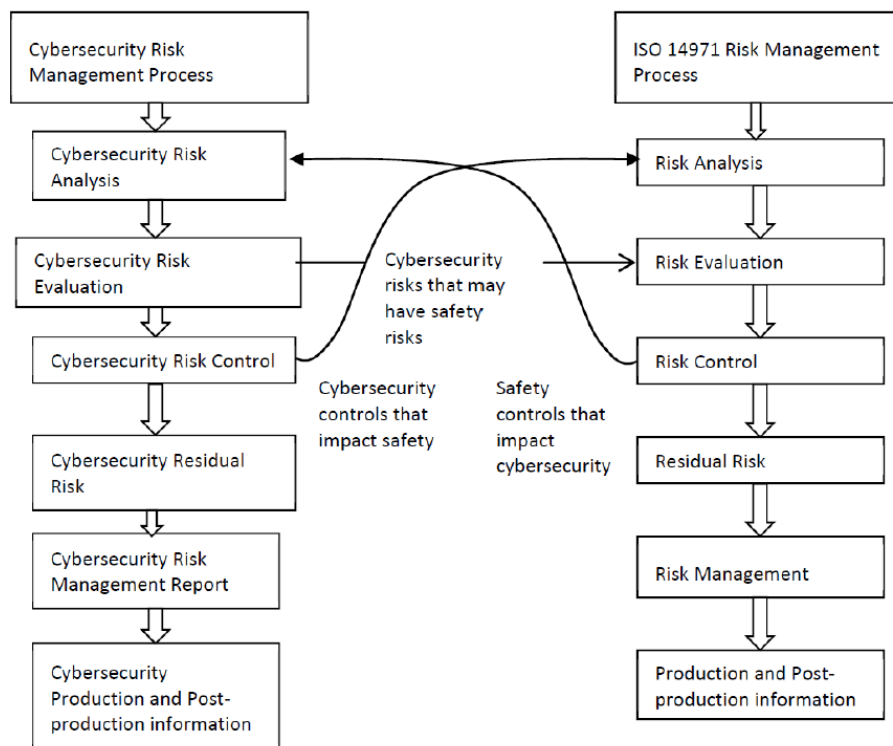


Figure 4.7: An illustration from the MDCG guidance document, [1] showing risk management process for security and safety side by side with the addition of arrows showing connections between these.

The FDA issued postmarket guidance document states the need for assessing the severity of patient harm should a cybersecurity risk be exploited. It then goes on to reference an approach outlined in ISO 14971, involving “qualitative severity levels”,

that can be used for conducting such an assessment. Taking this into consideration when looking at ISO 14971, it states that assessing and documenting the severity and probability of occurrence for risks with safety implication should be performed as part of risk estimation. It further states that manufacturers shall identify and document risks that may lead to hazardous situations (situations involving patient harm) during both intended use and foreseeable miss-use. While these statements apply to all safety related risks, they will only be taken into consideration for safety related security risks in this study, as pure safety risks fall outside the scope of what is covered in SACs.

ISO 62304 [8] states that manufacturers of medical device software are required to document a software safety class for all software items (partial assets), that denotes the severity of the outcome should a hazard occur for that item. Assigning such classes is required in order to comply with the standard, as the type of class dictates what measures need to be taken for a given software item to be deemed secure and safe, see Figure 4.8. The need for these classes ties into the need for showing traceability in CASCADE between software security and the potential safety implications, should the security fail in some manner.

Clauses and subclauses		Class A	Class B	Class C
Clause 4	All requirements	X	X	X
5.1	5.1.1, 5.1.2, 5.1.3, 5.1.6, 5.1.7, 5.1.8, 5.1.9	X	X	X
	5.1.5, 5.1.10, 5.1.11		X	X
	5.1.4			X

Figure 4.8: A subset of a table from ISO 62304 [8], displaying which parts of the requirements outlined in the standard applies to which classes

It was proposed during the interviews that an approach for distinguishing safety critical security claims in the case would be to incorporate the assessments from a "risk assessment matrix" [24]. This tool was explained by the interviewee as an established system in medical domain for rating and flagging risks in a medical context that have an inherent patient safety concern. Including these ratings and flags in CASCADE would mean that the case creators should assign color to identified safety critical security claims in accordance to their calculated rating from the matrix.

4.3 CASCADE case maintenance using existing work methodology

This section will present the results produced from the first focus group as this was the primary methodology used for investigating the incorporation of an maintainability process for CASCADE into AstraZenecas current iterative workflow.

4.3.1 Existing workflow and practices at AstraZeneca

The current workflow at AstraZeneca is built upon existing frameworks such as Scrum and phase-gate processes [36]. Before a feature can be moved into production,

they have a comprehensive list of criteria that need to be fulfilled before it can be deemed complete and ready for release.

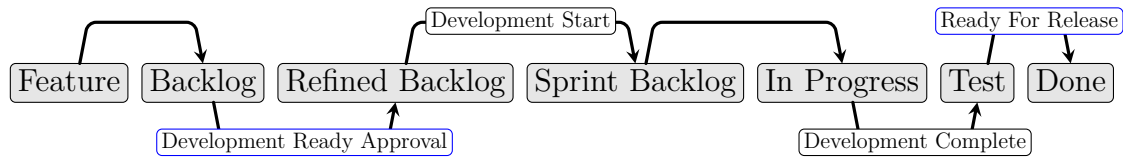


Figure 4.9: Overview of the workflow at AstraZeneca regarding Jira [37] status transitions of features for the BOOST platform, triage team approval gates highlighted in blue.

One of the major processes involved is what is called a “triage approval”, where the triage consists of several important roles:

- Product Owner
- ITPM
- Solution Architect
- Product Analyst
- ITQM
- Squad Lead

These roles are involved during several stages of product development, and not only for the purpose of the triage team. The triage team does not currently include any roles responsible for cybersecurity.

The roles of triage team have different areas of concerns, and want certain properties to be fulfilled, before being able to give their approval. In order for a feature to receive a triage approval, all roles need to give their individual approval. The approval from the triage team is currently needed for:

1. A feature to be able to be moved from the “Refined Backlog” into the “Sprint Backlog”, and thus deemed ready for development
2. A feature to be able to be moved from “Test” to “Done” and deemed ready for release

An overview of the feature transition flow at AstraZeneca can be seen in Figure 4.9.

4.3.2 Possible incorporation of SAC maintenance in existing workflow at AstraZeneca

During the focus group dedicated to the maintainability issue there was a consensus that incorporating a maintainability process for CASCADE into the workflow would require several experts as no one in the scrum teams would have all the required knowledge to manage all the levels of CASCADE. In regards to when in the iterative process the maintenance should take place, one suggestion was to add suggested

changes to the created assurance case as a part of a feature approval criteria, with a main focus on the White hat block, and the topic of asset identification.

As part of the design review, suggested changes to the product Blueprint document are needed in order for a feature to pass the review, and be marked as ready for development. The proposed changes to the Blueprint could introduce new assets, and the suggested changes to the Blueprint can be used as an aid in finding assets that need to be added in the assurance case.

At a later stage, after the feature has been marked as completed by the development team and is pending triage approval, a suggestion was made to include a security architect as one of the roles, which would need to approve the suggested changes to the Security Assurance Case (with a corresponding SAC related property added to the Definition of Done (DoD)), in order for the feature to fulfill the DoD and triage team feature acceptance criteria at AstraZeneca.

5

Discussion

This chapter aims to summarize the findings of this master thesis, and to provide a discussion of various, important aspects that were discovered during the different phases of the study. It will also look at identified threats to validity for the study and how these have been mitigated.

5.1 Adaptability of CASCADE to a medical domain context (RQ1.1)

All of the results from the methods used to assess the adaptability of CASCADE have indicated that CASCADE has a place in the medical domain, and that there is significant overlap and practical usability regarding the original CASCADE as it is outlined by Mohamad et al. [14]. The use cases derived by the SaMD coordinator at AstraZeneca, and the use cases from the focus group, have shown that CASCADE has the potential to be a useful tool for several of the roles at AstraZeneca, both for external and internal needs. Judging from the numerous interviews conducted with the SaMD coordinator, there was an expert assessment that CASCADE would be able to provide the necessary documentation to comply with requirements posed by the most relevant and stringent standards and guideline documents for cybersecurity in the medical domain. The documentation analysis later confirmed this assessment, by finding requirements in all of the studied standards that could be fulfilled with one, or several parts of CASCADE. However, it also showed that there is a need to address safety related security risks in a separate manner, which will be discussed in section 5.2. Summarily, the case study has shown that CASCADE could be adapted to the medical domain, to a significant extent.

5.1.1 Field observation at case study company

During one of the focus group sessions, a participant mentioned that they had been inspired by the block based approach that CASCADE offers. They had during the creation of FTA artifacts kept this in mind when structuring the different elements of FTA (which can be seen in figure 2.3), to provide a sense of structure. This has the potential to improve the readability of the FTA artifacts, as they can get large and messy quite quickly. It further signifies that the structure that a block based SAC creation approach has, is something that is desired in the medical domain.

5.2 Domain specific requirements compelling CASCADE modifications (RQ1.2)

The results from the study have shown that all of the parts of CASCADE have the ability to provide both internal and external value through being a thorough documentation tool, and a way to show compliance with requirements stated by regulations imposed on systems in the medical domain. They have also indicated that there is a need for traceability/linkage between security and patient safety concerns that stem from insufficient security measures.

During several stages of this study, the need to distinguish safety related security risks from purely security based risks was brought up. This was firstly discussed during the benchmark case creation, followed by the SaMD coordinator interviews. During the documentation analysis, requirements were found that stated the need for this distinction, with the motivation that safety based security risks are to be treated more strictly, as in terms of risk mitigation, and verification of the risk mitigation measure. In terms of SACs and CASCADE, this requirement does not prompt the need for any additional elements to be added to a created case, rather it urges the need for distinction between the purely security based risks and the safety related risks included. This requirement was discussed with the SaMD coordinator, and a derived solution was to include the ratings (1-5) and color (gradient from green-yellow-red) usage from the "risk assessment matrix".

Adopting this would fulfill the need for CASCADE to provide a level of traceability for security risks with an inherent safety risk to patients (as these are judged separately and require greater mitigation efforts and mitigation effort verification by some regulatory authorities, such as the FDA). Utilizing the same rating and color system used in other approaches in the medical domain for CASCADE has the benefit of not increasing the required labour for the case creation, as these ratings are being calculated anyway, as well as not increasing the complexity of understanding the case, as these ratings are already well established and used within the medical domain. Both of these factors tie in to two highlighted internal factors from the interview, namely that "a tool or approach deployed in the medical domain needs to have, "ease of creation" and "ease of use". This does not mean that creation and use cannot be complex but it does mean that unnecessary complexity is an undesirable trait.

As the inclusion of these ratings had not been planned in the initial scope there were no time to try and validate potential approaches with domain experts, however a potential example for including these ratings can be seen in figure 5.1. Looking at figure 5.1 the inclusion of the risk assessment ratings is placed on the individual risks on the attack path level. There are both possible positives a negative with this approach. Positives are that:

- When these ratings are created they are assigned for individual risks with safety aspects. This makes the inclusion of these ratings in the case trivial as you only have to find the risk in the case and apply the assigned rating.

- As regulatory authorities will examine flagged risks separately, it is beneficial to differentiate between purely security based risks and safety related security risks (by flagging individual risks).
- The assigned risk levels for the decomposed risks that stem from a specific threat scenario or security goal might vary, and having the ability to have risks with different ratings under the same threat scenario will make these distinguishable from one another.

A negative is the lost potential for abstraction, should all risks associated with a threat scenario or a security goal be safety related risks with the same risk rating. Such abstraction could be achieved through the usage of these ratings on claims in higher levels such as threat scenarios or security goals.

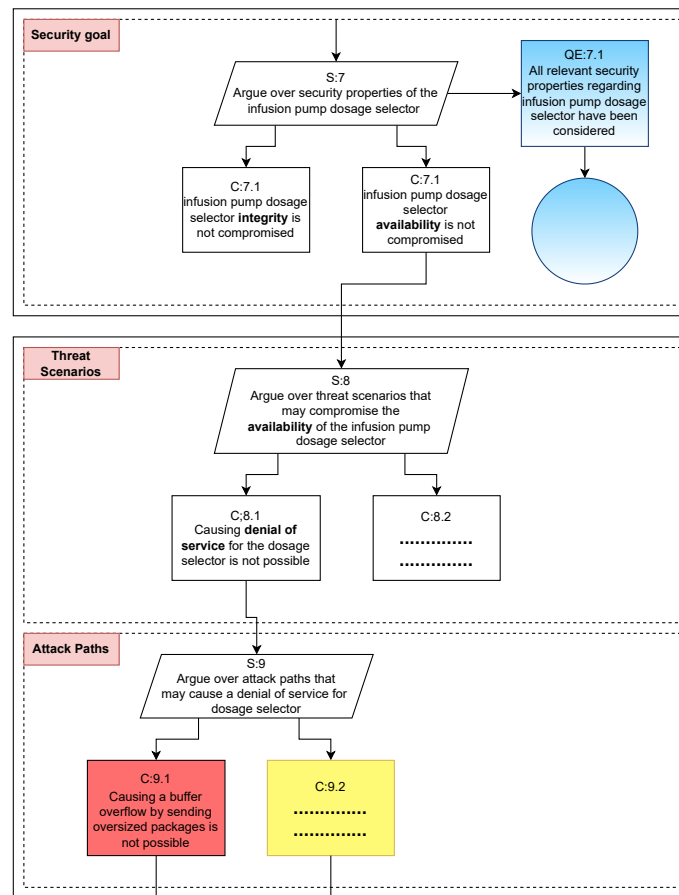


Figure 5.1: An potential example for how risk assessment ratings could be incorporated with the CASCADE approach

5.3 Utilize and extend existing agile processes to accommodate SAC maintainability (RQ2)

As elicited during the focus group session, there were indications of a need for the introduction of a new role, to fulfill the responsibility of security related needs,

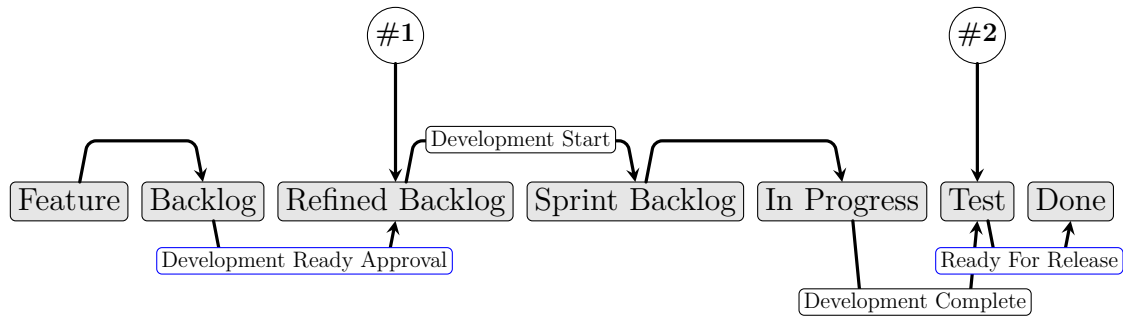


Figure 5.2: Overview of the workflow at AstraZeneca regarding Jira [37] status transition for features of the BOOST platform, and suggestions to where amendments can be made

measures, and documentation. This role was suggested to take on the form of a “security architect”, which would also join the triage team and have a say during the different phases of development, as a feature is moving through the different stages, as outlined in figure 4.9. The most crucial changes to the actual workflow are proposed to take place in **#1** and **#2**, shown in figure 5.2, as this is when the triage team is involved, and a triage approval is issued, which works as a gate (as in the phase-gate process [36]).

The developers and other roles involved during the development of the feature could have suggestions to where in the assurance case that changes are needed, as the feature is being developed. The development of a feature could involve the introduction of a new asset, that could potentially bring with it additional needed security goals, and open up for additional threat scenarios (and attack vectors).

It is possible that the “Blueprint” document (a System Design Document) at AstraZeneca could be aligned with the SAC maintainability process, as the document contains a high level description of the architecture of the system under development, including the different assets that the system is composed of. As features are added to the system, this also needs to be reflected in the Blueprint document, before the feature can be approved for development. It could therefore be utilized to some degree as a basis for adding changes to the SAC, which could streamline the process of SAC maintainability.

For example, a developer could in the design process of a feature see the need for the addition of a new asset, and would proceed add the asset to the Blueprint, and then add the corresponding changes to the SAC, to reflect the addition, in order for it to be considered accurate and up to date (which could be one of the new properties required in order for the proposed security architect role to be able to issue their individual approval).

The suggested changes would need to be vetted, confirmed, and potentially changed by the security architect, in order for the feature to be able to move to the “In Progress” phase. As development goes on, additional changes could be needed, and it is therefore important that the security architect is involved before a feature is deemed “Ready For Release”, and is put into production. After the feature has been

approved and the required changes to the SAC have been added, these changes are then merged into the main SAC.

5.4 Cybersecurity domain volatility

The cybersecurity domain is volatile in nature, due to the constant addition and discovery of attack vectors, which can be found in old versions, updated versions and even when patches for other attack vectors are published. Different frameworks used in a software product can easily introduce a huge security risk if a critical bug or attack vector is found, with one applicable example being the Log4j framework vulnerability [38].

This means that amendments to existing standards and laws are being updated constantly in order to keep up with the rapid pace of evolution and development of products including software. Taking this into consideration, updates to documents, standards, and laws published after **2022-04-20** are not included in this study. This date was chosen due to time constraints imposed on the thesis work, as the focus shifted from generating data toward interpreting the already acquired results.

5.5 Alternative methodology

The focus of this thesis was to carry out a case study at AstraZeneca to be able to find as much relevant information and applicable results about the targeted research area as possible. The goal was to capture information regarding the applicability of CASCADE and maintainability of SACs in a real world setting, in the medical domain. As the **availability** of applicable results to achieve the goals established with this thesis is very much related to the real world setting, and is not something that can be calculated or simulated to any significant degree, the case study research method was selected.

Sample studies was an alternative approach, and could to some degree be motivated as an alternative method, as data analysis of existing data (such as questionnaire responses, existing documentation) has the potential to yield results that aligns with the goals of this thesis. However, pre-existing data (with a focus on qualitative data from interviews) available regarding SAC approaches in the medical domain, is to the best of the thesis authors' knowledge, scarcely available. This solidifies the choice of a case study as the most applicable research method for having the means required for results that align well with the posed research questions.

5.6 Threats to validity

This section will discuss the various threats to validity identified in all the steps of this study as well as the methods used to minimize these threats.

5.6.1 Internal Validity

This section covers all the identified threats to the internal validity of this study. This means threats that relates to the validity of the gathered results [39].

5.6.1.1 Limited existing SAC and CASCADE knowledge

No one at AstraZeneca had heard of assurance cases, CASCADE, SaACs or SACs before having the concepts introduced to them, in conjunction with the case study. This means that the bulk of the case study participant knowledge about assurance cases, CASCADE, SaACs and SACs came from the case study authors, potentially introducing a form of bias in regards to the extent of SAC information introduced, and the motivation behind using SACs. Most of the case study participants were familiar with the notion of FTA, which shares some common factors with SaACs and SACs, which means that they had pre-existing knowledge of alternative, and in some ways similar, tools available during risk management and risk analysis. The case study participants were also experienced with approaches for documenting safety/security properties and ensuring compliance with applicable standards, which meant that they had a good understanding of the different needs that security assurance approaches have.

5.6.1.2 Potential bias

Three of the main sources for potential bias come from the:

- Thesis authors
- The supervisor from the university
- The supervisor from the case study company

These three "entities" all have different goals with the thesis, which could influence the direction of where the thesis is headed. However, one of the aspects that have been utilized in order to reduce bias include the fact that this study had two authors, meaning that all choices and interpretations made during the study have been thoroughly discussed before being taken. This way of working limits the amount of individual bias introduced into the study as all choices require a motivation that satisfies both authors before being introduced into the study. Another aspect is that no advice received from the university supervisor and the company supervisor have been treated as pure dogmatic facts, but as a starting point for conversation and further discussion.

5.6.2 External Validity

This section covers all the identified threats to the external validity of this study. This means threats that relates to generalizability of the study, how well the results could be applied to a similar context outside of the study environment [40].

5.6.2.1 Generalizability

As this case study has taken place at a single company (AstraZeneca) in the medical domain, the generalizability of the results might be limited. However, the documents and standards referenced are domain-wide, meaning that all companies in the medical domain will have to consider and comply with these standards to a varying degree, depending on the product line available at the company in question, which speaks for a greater ability of generalization of results.

5.6.2.2 Partial documentation analysis

While several standards and guidelines were considered, there are still more in use that touch upon security within the medical domain, that were not included in the study. While these could potentially contain requirements that would require further adaptations to CASCADE, there have been efforts to confirm that the selected standards are those of critical importance to cybersecurity in the medical domain and that the requirements posed by these are the ones that shape what the cybersecurity needs are in the medical domain. This confirmation has been carried out together with the SaMD coordinator at AstraZeneca and it has indicated that the selected ones fulfill the previously stated properties.

While analysing the selected standards it was also observed that they have an innate cohesion by referencing and building upon each other (especially the International Organization for Standardization (ISO) standards) meaning that the requirements posed by the more narrow standards not studied are a sub-set of the requirements in the studied ones. This also meant that requirements were shared for several of the standards leading to similar connections to CASCADE.

5.6.2.3 Documentation and standard volatility

The current pattern of updates that can be observed is that guidance documents from U.S. Food and Drug Administration tend to be updated every 2 years, whereas the International Organization for Standardization standards tend to be updated every 5-6 years. This means that further extensions or revisions to the CASCADE approach then those proposed in this study might become beneficial or necessary after later revisions of the documents are released, depending on the amendments made to the the document in question.

5.6.2.4 Result validation concerns

The results have been validated at one single company, AstraZeneca, and some of the results were validated by only one person at AstraZeneca, the SaMD compliance coordinator. The SaMD compliance coordinator had the greatest/deepest knowledge of applicable medical domain standards, and general knowledge of compliance requirements that are imposed on some of the products (medical devices) available at AstraZeneca. Given the resources available for this masters thesis, it was infeasible to include additional compliance coordinators. However, the content of the standards and guideline documents were vetted by the thesis authors, and conveyed

to the thesis supervisor at Chalmers, with the intention of getting a good posture on the general soundness of the results, before getting validation by the SaMD compliance coordinator, and validation through discussions with participants in the second focus group.

6

Conclusion

The first major subject that this thesis aimed to investigate, was to what extent a SAC approach developed for the automotive industry, CASCADE, could be transferred to (and used in) the medical domain. To achieve this, major regulations and standards imposed on the medical domain were elicited from domain experts. These were then subject to study and evaluation regarding their overlap with CASCADE, as well as their potential additional needs, which would require extensions to the approach. Experts in different areas at the target company, AstraZeneca, were also inquired about the utilization of this approach for their specific roles.

The assessment for CASCADE is that it would be both conceivable and desirable to introduce the approach into the medical domain, given that safety related security risks be given visual indicators according the risk assessment matrix ratings, to provide traceability regarding safety risks.

The second subject for study was how CASCADE could be incorporated into an iterative workflow, utilizing the existing agile processes at the case company for this workflow. Through focus group discussions and insights into the established processes at AstraZeneca, it was deemed that in order for this inclusion to function adequately during the product development process, there would need to be certain additions. These additions would be in the form of additional properties for the DoD of features (which would include that proper amendments have been made to the SAC), and the inclusion of a new role which would have the responsibility of the security documentation of the system.

This new role would play a deciding factor in the gates of the phase-gate adapted workflow, and would ensure that the SAC is updated before receiving approval to begin development of the feature, and before receiving approval to release the feature into production. It is also important that other involved roles of the product development (such as software developers) aid in the identification of potential changes needed to the SAC, as development takes place.

6.1 Future research

For potential future research subjects, one area could be to investigate whether there are processes and tools in the medical domain which could fit directly into a SAC creation approach (potentially CASCADE), such as incorporating the results

6. Conclusion

or providing traceability of FTA artifacts or FMEA results.

Bibliography

- [1] Medical Device Coordination Group (MDCG). *Guidance on Cybersecurity for medical devices*. Dec. 2019. URL: https://ec.europa.eu/health/system/files/2022-01/md_cybersecurity_en.pdf.
- [2] HIMSS Healthcare Cybersecurity Survey | HIMSS. en. Nov. 2020. URL: <https://www.himss.org/resources/himss-healthcare-cybersecurity-survey> (visited on 12/15/2021).
- [3] William Stallings and Lawrie Brown. *Computer security: principles and practice*. en. Fourth Edition. New York, NY: Pearson, 2018. ISBN: 978-0-13-479410-5.
- [4] Monica Lagazio, Nazneen Sherif, and Mike Cushman. “A multi-level approach to understanding the impact of cyber crime on the financial sector”. en. In: *Computers & Security* 45 (Sept. 2014), pp. 58–74. ISSN: 01674048. DOI: 10.1016/j.cose.2014.05.006. URL: <https://linkinghub.elsevier.com/retrieve/pii/S016740481400087X>.
- [5] United States Government. *Federal Register, Executive Order 13636*. Feb. 2013. URL: <https://www.govinfo.gov/content/pkg/FR-2013-02-19/pdf/2013-03915.pdf>.
- [6] EMA. *Medical devices*. en. Text. Nov. 2018. URL: <https://www.ema.europa.eu/en/human-regulatory/overview/medical-devices> (visited on 06/02/2022).
- [7] Minhee Kang et al. “Recent Patient Health Monitoring Platforms Incorporating Internet of Things-Enabled Smart Devices”. en. In: *International Neurology Journal* 22.Suppl 2 (July 2018), S76–82. ISSN: 2093-6931. DOI: 10.5213/inj.1836144.072. URL: <http://einj.org/journal/view.php?doi=10.5213/inj.1836144.072> (visited on 04/07/2022).
- [8] *IEC 62304:2006/Amd 1:2015*. en.
- [9] *Guideline on computerised systems and electronic data in clinical trials*. en. URL: https://www.ema.europa.eu/en/documents/regulatory-procedural-guideline/draft-guideline-computerised-systems-electronic-data-clinical-trials_en.pdf (visited on 05/23/2022).
- [10] 14:00-17:00. *ISO 14971:2019*. en. URL: <https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/27/72704.html> (visited on 05/06/2022).
- [11] Center for Devices and Radiological Health. *(Draft) Content of Premarket Submissions for Management of Cybersecurity in Medical Devices*. Oct. 2018.
- [12] Center for Devices and Radiological Health. *Postmarket Management of Cybersecurity in Medical Devices*. Dec. 2016. URL: <https://www.fda.gov/>

- regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices.
- [13] Charles B Weinstock, Howard F Lipson, and John Goodenough. “Arguing Security – Creating Security Assurance Cases”. en. In: (), p. 22. URL: https://resources.sei.cmu.edu/asset_files/whitepaper/2013_019_001_293637.pdf.
 - [14] Mazen Mohamad, Jan-Philipp Steghöfer, and Riccardo Scandariato. “Security assurance cases—state of the art of an emerging approach”. en. In: *Empirical Software Engineering* 26.4 (July 2021), p. 70. ISSN: 1382-3256, 1573-7616. DOI: 10.1007/s10664-021-09971-7. URL: <https://link.springer.com/10.1007/s10664-021-09971-7>.
 - [15] Mazen Mohamad et al. “Security Assurance Cases for Road Vehicles: an Industry Perspective”. In: *arXiv:2003.14106 [cs]* (Mar. 2020). arXiv: 2003.14106. URL: <http://arxiv.org/abs/2003.14106> (visited on 05/31/2022).
 - [16] M. Coram and S. Bohner. “The Impact of Agile Methods on Software Project Management”. en. In: *12th IEEE International Conference and Workshops on the Engineering of Computer-Based Systems (ECBS’05)*. Greenbelt, MD, USA: IEEE, 2005, pp. 363–370. ISBN: 978-0-7695-2308-8. DOI: 10.1109/ECBS.2005.68. URL: <http://ieeexplore.ieee.org/document/1409937/>.
 - [17] Mazen Mohamad et al. “Asset-driven Security Assurance Cases with Built-in Quality Assurance”. In: *2021 IEEE/ACM 2nd International Workshop on Engineering and Cybersecurity of Critical Systems (EnCyCriS)*. Madrid, Spain: IEEE, June 2021, pp. 1–8. ISBN: 9781665445535. DOI: 10.1109/EnCyCriS52570.2021.00012. URL: <https://ieeexplore.ieee.org/document/9476061/>.
 - [18] CAE / Adelard. URL: <https://www.adelard.com/asce/choosing-asce/cae.html>.
 - [19] *ISO 61025:2006 Fault tree analysis (FTA)*. Standard. International Organization for Standardization.
 - [20] “Model-based System Engineering for Fault Tree Generation and Analysis:” en. In: *Proceedings of the 1st International Conference on Model-Driven Engineering and Software Development*. Barcelona, Spain: SciTePress - Science, 2013, pp. 210–214. ISBN: 978-989-8565-42-6. DOI: 10.5220/0004346902100214. URL: <http://www.scitepress.org/DigitalLibrary/Link.aspx?doi=10.5220/0004346902100214> (visited on 06/02/2022).
 - [21] *International Medical Device Regulators Forum (IMDRF)*. en. URL: <https://www.imdrf.org/international-medical-device-regulators-forum-imdrf> (visited on 04/14/2022).
 - [22] *ISO 24791:2020 Medical devices – Guidance on the application of ISO 14971*. Standard. International Organization for Standardization.
 - [23] EMA. *European Medicines Agency*. en. Text. URL: <https://www.ema.europa.eu/en>.
 - [24] Giacomo Pascarella et al. “Risk Analysis in Healthcare Organizations: Methodological Framework and Critical Variables”. en. In: *Risk Management and Healthcare Policy* Volume 14 (July 2021), pp. 2897–2911. ISSN: 1179-1594. DOI: 10.2147/RMHP.S309098. URL: <https://www.dovepress.com/risk->

- analysis-in-healthcare-organizations-methodological-framework-and-peer-reviewed-fulltext-article-RMHP (visited on 05/03/2022).
- [25] Arnab Ray and Rance Cleaveland. "Security Assurance Cases for Medical Cyber-Physical Systems". In: *IEEE Design & Test* 32.5 (Oct. 2015), pp. 56–65. ISSN: 2168-2356, 2168-2364. DOI: 10.1109/MDAT.2015.2468222. URL: <http://ieeexplore.ieee.org/document/7194764/>.
 - [26] ISO - ISO 21434 — Road vehicles — Cybersecurity engineering. en.
 - [27] Johan Peeters. "Agile Security Requirements Engineering". en. In: (), p. 4.
 - [28] Lotfi ben Othmane, Pelin Angin, and Bharat Bhargava. "Using Assurance Cases to Develop Iteratively Security Features Using Scrum". en. In: *2014 Ninth International Conference on Availability, Reliability and Security*. Fribourg, Switzerland: IEEE, Sept. 2014, pp. 490–497. DOI: 10.1109/ARES.2014.73. URL: <http://ieeexplore.ieee.org/document/6980323/>.
 - [29] Lotfi Ben Othmane and Azmat Ali. "Towards Effective Security Assurance for Incremental Software Development the Case of Zen Cart Application". In: *2016 11th International Conference on Availability, Reliability and Security (ARES)*. Salzburg, Austria: IEEE, Aug. 2016, pp. 564–571. ISBN: 9781509009909. DOI: 10.1109/ARES.2016.86. URL: <https://ieeexplore.ieee.org/document/7784620/>.
 - [30] AstraZeneca plc. *Full year and Q4 2021 results*. Feb. 2022. URL: <https://www.astrazeneca.com/content/dam/az/PDF/2021/full-year/Full-year-2021-results-announcement.pdf>.
 - [31] ISO 12207:2018 Software life cycle processes. Standard. International Organization for Standardization.
 - [32] Klaas-Jan Stol and Brian Fitzgerald. "The ABC of Software Engineering Research". en. In: *ACM Transactions on Software Engineering and Methodology* 27.3 (July 2018), pp. 1–51. ISSN: 1049-331X, 1557-7392. DOI: 10.1145/3241743. URL: <https://dl.acm.org/doi/10.1145/3241743> (visited on 06/13/2022).
 - [33] Joint Task Force Transformation Initiative. *Guide for conducting risk assessments*. en. Tech. rep. NIST SP 800-30r1. Edition: 0. Gaithersburg, MD: National Institute of Standards and Technology, 2012, NIST SP 800-30r1. DOI: 10.6028/NIST.SP.800-30r1. URL: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf> (visited on 05/06/2022).
 - [34] Jackson Wynn. "Threat Assessment and Remediation Analysis (TARA)". In: 2014.
 - [35] *Threat Modeling Process* / OWASP Foundation. en. URL: https://owasp.org/www-community/Threat_Modeling_Process (visited on 04/26/2022).
 - [36] Jeffrey K. Pinto. *Project management: achieving competitive advantage*. eng. Fifth edition, global edition. Harlow, England: Pearson, 2020. ISBN: 9781292269146.
 - [37] Atlassian. *Jira / Issue & Project Tracking Software*. en. URL: <https://www.atlassian.com/software/jira> (visited on 05/26/2022).
 - [38] NVD - CVE-2021-44228. URL: <https://nvd.nist.gov/vuln/detail/CVE-2021-44228> (visited on 05/30/2022).

- [39] *APA Dictionary of Psychology*. en. URL: <https://dictionary.apa.org/internal-validity>.
- [40] *APA Dictionary of Psychology*. en. URL: <https://dictionary.apa.org/external-validity>.

A

Appendix 1

A.1 Interviews with SaMD Coordinator at AstraZeneca

A.1.1 Interview questions

1. Relevant standard and requirement elicitation

- 1.1. Which regulations or standards exist that impose requirements on cybersecurity in the medical domain?

2. Pre-existing internal documentation regarding AZ SaMD practices

- 2.1. What documents/documentation has been created that is tailored for SaMD compliance at AZ (preferably with a focal point in security)?

3. Safety in combination with security

- 3.1. Do you believe that the combination of safety and security would be necessary for CASCADE to be useful in the medical domain?
- 3.2. Are there any pre-existing documentation practices in the medical domain that uses safety in combination with security?
- 3.3. Do you have any concrete examples of these?

4. Impressions for SACs and CASCADE

- 4.1. Do you know of any current usages of SACs or ACs?
- 4.2. Do you believe that SACs would be beneficial for the domain, why?
- 4.3. Do any scenarios where SACs could be used within the domain come to mind?

5. Volatility in the field

- 5.1. How volatile would you say the standards and regulations are around cybersecurity in the medical domain?
- 5.2. How does requirement and standard updates/additions impact existing methods in the field?

A.2 Interview with Software engineering lead at AstraZeneca

A.2.1 Interview questions

- 1. Relevant standard and requirement elicitation**
 - 1.1. Which regulations or standards exist that impose requirements on cybersecurity in the medical domain?
- 2. Pre-existing internal documentation regarding AZ SaMD practices**
 - 2.1. What documents/documentation has been created that is tailored for SaMD compliance at AZ (preferably with a focal point in security)?
- 3. Impressions for SACs and CASCADE**
 - 3.1. Do you know of any current usages of SACs or ACs?
 - 3.2. Do you believe that SACs would be beneficial for the domain, why?
 - 3.3. Do any scenarios where SACs could be used within the domain come to mind?
- 4. The BOOST system**
 - 4.1. *Questions related to the benchmark case*
- 5. Best practices employed at AZ**
 - 5.1. What are some of the “best practices” for cybersecurity employed at AZ?

B

Appendix 2

B.1 Questions and answers from maintainability focus group questionnaire

What is your title at AstraZeneca?

6 responses

Samd quality lead

Release manager & Project manager

Software Engineering Leader

Senior Software Engineer

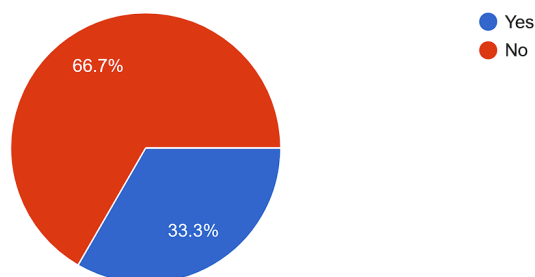
Software Engineering Lead

Test Manager

Have you heard of Security Assurance Cases before today?

[Copy](#)

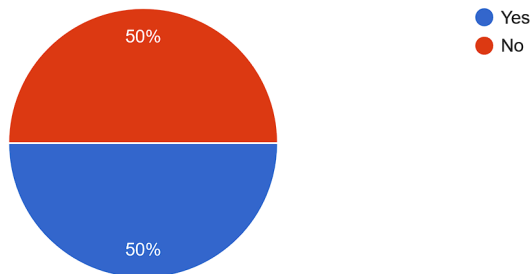
6 responses



Have you heard of Safety Assurance Cases before today?

 Copy

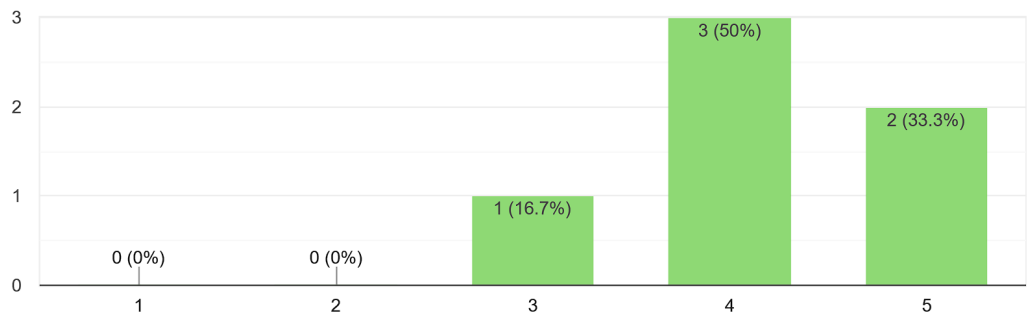
6 responses



How familiar are you with agile work methodologies?

[Copy](#)

6 responses



What work methodology do you primarily use in your team at AstraZeneca?

6 responses

Being developed
adf, safe, scrum, samd sop
SAFE Scrum
Agile / Scrum
Scrum / SAFe
Scrum

Are there any documents available at AstraZeneca that you use to support your workflow? If so, which ones?

5 responses

adf website

We have a full framework called ADF with loads of documents

yes, ADF

Many within Adaptive Delivery Framework

ADF- workflow

Which standards/requirements/documents regarding security or safety do you use in your workflow at AstraZeneca?

6 responses

See chat

cyber security standrds, outcome of the rid ends up in non func requirements

Loads of different

Unsure, we have some tools scanning images and codes

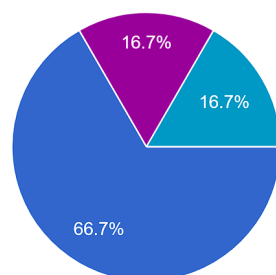
Part of ADF

There is a bunch of them in the standard training

At which stage (if any) do you evaluate the security state of the system/product being worked on?



6 responses



- Continuously
- Before each sprint
- At the end of each sprint
- Before it is placed into production
- Both continuously in some extent and also annually
- There is a yearly review, but static analysis are performed within the CI pipeline

Do you have a suggestion on where in the process a security review would be suitable?

5 responses

Sdlc
At design review and at feature complete gateway
During testing of the software, at many levels
Design review for each Feature should include security aspects, but at delivery of the Feature the real security review should happen.
Before every release

C

Appendix 3

C.1 Example Raspberry Pi web server SAC

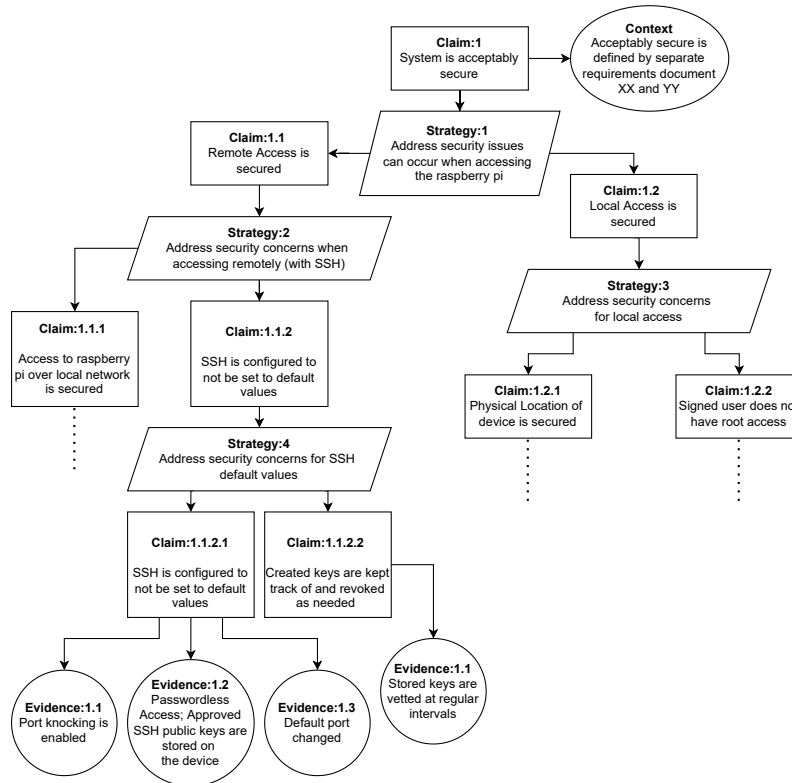
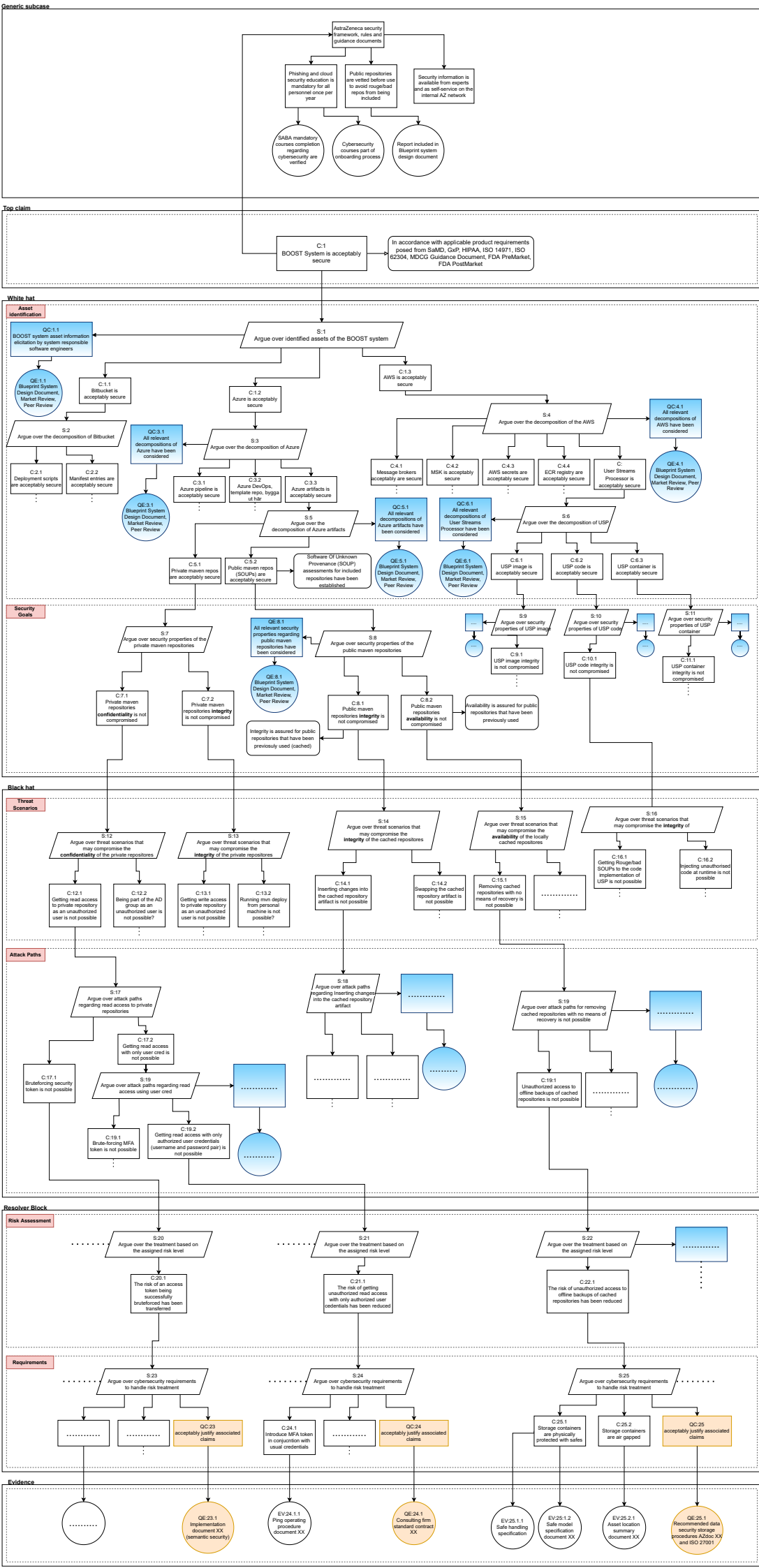


Figure C.1: The resulting SAC after using the SAC creation guidelines by Carnegie Mellon University [13]

C.2 Resulting benchmark case

The case created in collaboration with domain experts at AstraZeneca, that was meant to serve as a "benchmark" case as mention in the methodology section, can be seen on the page below.



D

Appendix 4

D.1 EMA enquiry

D.1.1 Question

Hello,

We are two students from Chalmers University of Technology who are conducting a case study at AstraZeneca regarding the documentation of security (of medical devices or systems that handle for example data in relation to clinical trials), and how the documented security of a system can be shown to be compliant with requirements from different regulatory authorities and standards. We have taken a look at the Good Clinical Practice standard and have seen mentions of Confidentiality and Integrity, but are having a hard time finding these in the context of (cyber)security. Would it be possible to get some help in this regard?

Are there for example specific requirements in regards to cybersecurity available in the GCP quality standard? Is there some other standard that you think would be more applicable in this case?

Thanks in advance!

Best regards,
Max and Adam

D.1.2 Response

Dear Mr Fransson,

Thank you for contacting the European Medicines Agency (EMA). You have asked about the requirements in regards to cybersecurity available in the GCP quality standard and any further guidance.

IT (or cyber) security is briefly addressed in the current ICH GCP E6 (R2) 5.5.3:

d) Maintain a security system that prevents unauthorized access to the data

Preventing unauthorized access to clinical data involves a number of measures including but not limited to management of accesses, firewalls and platforms.

Further guidance can be found in annex 3 and 4 of the draft Guideline on Computerised Systems, although this document is currently in review after public consultation:

https://www.ema.europa.eu/en/documents/regulatory-procedural-guideline/draft-guideline-computerised-systems-electronic-data-clinical-trials_en.pdf

Draft guideline on computerised systems and electronic data in clinical trials

Guideline on computerised systems and electronic data in clinical trials
EMA/226170/2021 Page 5/47 122 Glossary and abbreviations 123 Generally used terms 124 Unless otherwise specified (e.g. "source data" or "source document") and in order to simplify the text,
www.ema.europa.eu

We hope you find this information useful.

Kind regards,

European Medicines Agency