Developing the Safety Case based SQAD-methodology to handle a risk/margin profile by integrating methods for risk assessment

Jonas Åström

Department of Fire Safety Engineering and Systems Safety
Lund University, Sweden

Avdelningen för Brandteknik och Riskhantering
Lunds Tekniska Högskola
Lunds Universitet

Report 5351, Lund

This report has been sponsored by Solvina AB and the Swedish Radiation Safety Authority

Developing the Safety Case based SQAD-methodology to handle a risk/margin profile by integrating methods for risk assessment

Jonas Åström

Lund 2011

Title:

Developing the Safety Case based SQAD-methodology to handle a risk/margin profile by integrating methods for risk assessment

Author:

Jonas Åström

Report 5351

ISSN: 1402-3504

ISRN: LUTVDG/TVBB--5351--SE

Number of pages: 47

Keywords

SQAD, Safety Case, Preliminary Hazard Analysis, Risk/Marginal

Abstract

The aim of this thesis is to present a proposal for an evolved SQAD (Safety/Quality Assurance and Demonstration)-methodology. SQAD is a Safety Case-based methodology with the main purpose of supplying an effective tool for organizing and demonstrating system safety. Just as Safety Case, SQAD is designed to be a document that proves series of claims with the purpose to declare a system safe. This thesis looks into the possibility to grade and visualize the level of claim significance using recognized methods for risk management.

Brandteknik och Riskhantering
Lunds tekniska högskola
Lunds universitet
Box 118
221 00 Lund

brand@brand.lth.se
http://www.brand.lth.se

Telefon: 046 - 222 73 60
Telefax: 046 - 222 46 12

Department of Fire Safety Engineering
and Systems Safety
Lund University
P.O. Box 118
SE-221 00 Lund
Sweden

brand@brand.lth.se
http://www.brand.lth.se/english

Telephone: +46 46 222 73 60
Fax: +46 46 222 46 12

Acknowledgements

I want to give a great thanks to all the people that have made the work with this thesis possible. Special thanks to Solvina and Pontus Ryd for taking initiative to the project and giving me the possibility to write this thesis and for offering great support through the work of writing the report.

Thanks to all the personnel at Solvina for all your help and your patience when answering my many questions about high and low.

I also want to thank my supervisors at LTH, Kurt Petersen and Henrik Hassel and Tage Eriksson and Bo Liwång at SSM.

Jonas Åström
Lund 2011

Summary

Conducting risk assessments has become an important part of many activities, for some it is a requirement of governmental institutions, for others it is a way for the industry to on its own increase safety and availability in its organization and further develop their products. Whatever the purpose, it is important that the risk analysis can be presented in such a way that the result is easy to interpret so that the reviewer can be sure that no risks have been ignored or valued incorrectly.

SQAD is a Safety Case based methodology that is used to ensure safety and/or quality in a system by explicitly proving a set of claims about the systems safety/quality functions. The objective is to prove that the formulated claims are fulfilled, which is answered with either yes or no. When all claims are fulfilled the system is considered meet the desired requirements. This black and white way of looking at claim fulfillment makes the method blunt in some ways though as there in reality are certain claims indicating a greater grade of uncertainty than others.

This thesis aims at investigating whether established methods of risk analysis can be integrated into the SQAD-methodology to enable ranking of claims after their impact on system safety and accessibility so that focus and resources can be directed to where they do the most use.

To be able to integrate methods used in traditional risk management into SQAD the first step in attacking the problem was to identify the similarities and differences between SQAD and the traditional risk concept. Traditionally risk is seen a product of probability and consequence but how do they fit into SQAD? The answer is that they don't, at least not in their current form. The solution was to introduce the importance and urgency factors to replace the concepts of consequence and probability. Importance replaces consequence by estimating the importance a claim has for overall system safety/quality by identifying which consequences could arise if the functions handled by a claim would fail to function. Importance has thereby a certain relation to traditional consequence. Probability is replaced by urgency which is less related its counterpart. Urgency consists of two parts: Strength of Evidence (SoE) and Exigency where SoE is an estimation of how good the evidence is believed to be and Exigency a compensation of how soon the claim needs to be fulfilled.

As the risk management-method chosen for integration into SQAD, the Preliminary Hazard Analysis was chosen. The reason being its possibility for adaptation for current needs and relatively ease of learning for persons not usually working with risk management.

By assigning claims importance and urgency and grading them on a scale from 1 to 5 the claim significance can be derived using a traditional risk matrix. The claim significance is a measure of how significant a single claim is for total system safety/quality related to other claims. The claim significance could thereby be used to decide into which areas of a system attention should be focused to reach the goal of reaching a desired level of safety or quality.

Also within the purpose of this thesis was to propose a method for communicating the result of an evolved SQAD-analysis. Two methods are suggested as possible ways to achieve this; the risk matrix and the radar chart. The risk matrix is the same used to produce the significance factor that was found useful for communicating the analysis result in a quick way. The radar chart offers a possibility to compare several SQAD analyses and thereby following how claim significance is changing during the system life cycle.

Sammanfattning

Riskanalyser har kommit att bli en viktig del av många verksamheter, för vissa är det ett krav från tillståndsgivare, för andra är det för att ge den egna organisationen möjlighet att kvalitetssäkra och vidareutveckla sin produkt eller organisation. Oavsett syfte är det viktigt att riskanalysen kan redovisas på ett sådant sätt att resultatet är lätt att tolka så att granskare kan vara säker på inga risker förbisetts eller värderats felaktigt.

SQAD är en Safety Case-baserad metodik som har till syfte att påvisa att tillräklig säkerhet och/eller kvalitet uppnåts i system genom att bevisa att ett antal påståenden som ställts upp angående systemts pstådda säkerhets- eller kvalitetsnåvå. Målet är att bevisa att de uppställda påståenden är uppfyllda, vilket besvaras antingen ja eller nej. När alla påståenden är bevisade kan systemed påstås ha nått en tillräklig nåvå av säkerhet/kvalitet. Detta svart-vita sätt att se på ett påståendes uppfyllnad är trubbigt på så sätt att det inte värderar de enskilda påståendenas inverkan på den totala säkerheten/kvaliteten.

Detta exjobb syftar till att undersöka om etablerade riskanalysmetoder kan integreas i SQAD för att möjliggöra en rangording av de enskilda påståendenas påverkan på systemet i stort så att fokus och resurser kan riktas dit de gör mest nytta.

Första steget i processen med att integrera en traditionell riskanalysmetod var att identifiera likheter och skillnader mellas SQAD och hur man traditinellt ser på risk. Risk ses vanligtvis som en produkt av consekvens och sannolikhet men hur passar de in i SQAD? Svaret är att de gör de inte, åtminståned inte i deras nuvarende form. Lösnignen blev att introducera imporance- och urgency-faktorerna för att ersätta konsekvens och sannolikhet. Importance ersätter konsekvens genom att ett påståendes viktighet för systemet uppskattas genom att identifiera vilka konsekvenser som kan uppstå om de funktioner som ett påstående hanterar skulle fallera. Importance har därmer en viss likhet med hur man traditionellt ser på konsekvens. Sannolikhet ersätts istället av urgency som är lite mer olik sin föregångare. Urgency består av två delar: Strength of Evidence (SoE) och Exigency där SoE är ett mått på bevisets styrka och Exigency en kompensation efter hur brottom det är att få påståendet bevisat.

Den riskanalysmetod som valdes för integration i SQAD var preliminär riskanalys, eller grovanalys. Den valdes på grund av dess möjlighet att anspassas efter rådande behov samt relativa enkelthet att sätta sig in i för personer som vanligtvis inte arbetar mer riskhantering.

Genom att tilldela påståendena importance och urgency graderade efter en skala från 1 till 5 kan man uppskatta påståendets significance genom plottning i en riskmatris. Påståendets significance är ett mått på hur signifikant påståendet är för den totala säkerheten/kvaliteten jämfört med andra påståenden i samma system. Signifikansen kan därmer användas för att avgöra var insataser skall riktas för att nå det uppsatta målet gällande systemets säkerhet/kvalitet.

Det låg även inom exjobbets ramar att förelå en metod för att kommunicera resultatet av en SQAD-analys. Två metoder har föreslagits för detta: riskmatrisen och radardiagrammet. Riskmatrisen är densamma som används för att ta fram signifikansen och är ett snabbt sätt att kommunicera vilka påståenden som har högst signifikans. Radardiagrammet erbjuder bättre möjligheter att följa upp hur flera påståendens signifikans förändras genom systemed livscykel.

Contents

1 Introduction

1.1 Background

Risk assessment has become an important part of many industries, for some it is a requirement from regulators, for others it is ways for an organization to secure quality and to further develop their product or organization. For whatever the purpose, it is important that a risk analysis is presented in such a way that the result is easy to interpret so that examiners can assure that no risks are overlooked or incorrectly valued.

One tool that offers possibilities to analyze and present a risk analysis in a structured way is the Safety Case methodology. The purpose of a Safety Case is to prove that an operation satisfies safety requirements by formulating a set of explicit claims about safety and quality, evidence that claims have been met and a set of arguments linking the claims to the evidence.

Solvina AB is a Swedish consulting company in the power and process industry. They are working closely with Swedish nuclear power industry, and have been engaged in projects in all currently active nuclear plants in Sweden. During an extensive modernization project in the *Ringhals* power plant the need for an effective method to organize safety work and keeping track on work emerged and thus the Safety Case-methodology was adopted to the project. Since then *Solvina* has worked actively, both with *Ringhals* and other clients to further develop the Safety Case-methodology to fit the industry needs and expectations. The result from this is SQAD (Safety and Quality Assurance and Demonstration) which is a Safety Case-based methodology for analyzing the status in safety and quality related projects. SQAD (and SC) is based on a number of claims that are made about the safety and quality in a systems which is to be proved during the project to ensure safety and quality. This thesis has its base in the wish to evolve this methodology to enable a grading of how important individual claims are for total safety/quality by introducing tools from traditional risk management.

1.2 Goal and purpose

The purpose of this thesis is to evolve the SQAD-methodology from producing the black and white output of today to an output that is gradable. The goal is to integrate recognized risk analysis methods in the SQAD-methodology to enable a possibility to rate each claim towards how significant it is for total system safety. A more precise description of the problem will be discussed in chapter 3.

1.2.1 Problem formulations

The problem formulation has been summarized in three questions that this thesis aims to answer:

- How can recognized risk management methods be used to compare and assess different claims significance regarding total system safety.
- Can claims be ranked after how great the margin for claim significance is?
- How can the resulting margins be efficiently illustrated and communicated?

1.3 Method

The work will be divided into two main parts were the first part is an explanation of the Safety Case and SQAD methodologies and a formulation of the problem. The second part handles the problem and the proposed solution to the problem.

1.3.1 Part 1 – Safety Case, SQAD and the problem formulation

This part of the report contains the problem formulation and a brief introduction to Safety Case in general and SQAD in particular. Information about Safety Case methodology and experiences in general is relatively easy to find through scientific papers and journals which isn't the case with SQAD. SQAD is a new methodology that is developed by, and only in use by *Solvina* and their clients. The documentation isn't very comprehensive and therefore most knowledge about SQAD has to be obtained through reports from projects where SQAD has been applied and orally from *Solvina* employees.

1.3.2 Part 2 – The problem itself

This is the problem solving part of the thesis. The aim is to integrate existing risk management methods in the SQAD methodology. This will be done by first doing a coarse selection of available methods from which a smaller number of appropriate methods will be chosen using a number of selection criteria. The selected methods will then be evaluated separately.

It is also part of the problem to find a suitable method to illustrate and communicate the result from a SQAD-analysis. This part of the problem will be explored in cooperation with *Solvina.*

1.4 Project stakeholders

There are two stakeholders in the project. *Solvina* is the main stakeholder and owner of the SQAD-concept and are responsible for initiating this project. The Swedish Radiation Safety Authority (SSM) is the main regulatory body within the nuclear industry in Sweden. SSM has also showed interest in the further development of the SQAD-methodology.

1.5 Limitations

- The SQAD-methodology is supposed to be applicable to any system but in this thesis focus will be on nuclear power plant safety/quality as this is the only area in which SQAD has been applied so far.
- The thesis does not aim at developing methods of assuring completeness in the safety case definition itself.
- The main objective is to evolve the SQAD methodology to also handle risk/margin assessments, not to identify or correct other possible shortcomings of SQAD as presently applied.
- The assignment from *Solvina* is to evolve SQAD by integrating tools from traditional risk management. This is seen as main prerequisite and therefore no other possibilities to evolve SQAD will be discussed.
- Eventually it will be of interest to analyze how claim significance propagate in the area-claim structure but this will not be handled in this thesis as it is to complex and time consuming.

2 The Safety Case-methodology

This chapter aims at explaining what a Safety Case is, what it does and what it does not do. Focus will be on SQAD which is *Solvina's* own adaptation of Safety Case methodology but to fully understand SQAD the original idea behind Safety Case must first be explained.

2.1 What is a Safety Case?

Originally the term Safety Case was adopted from the legal business and had the same practical meaning; making a case that proves a claim. In a Safety Case the claim is stating that a system is safe (or at least safe enough) (Zotov, 2007). When talking about Safety Cases one would have to distinguish between the Safety Case as a logical concept that describes a way to document safety and the physical text that actually describes the safety of a system (Kelly, 1998). In this thesis the term "Safety Case" will be referring to the logical concept, as the way to document a Safety Case differs from case to case as will the way to refer to it.

So, what is a Safety Case? Basically a Safety Case is a way to document and prove that a system is adequately safe by systematically showing that a set of explicit claims about a systems properties have been met. Specifically a Safety Case consists of the following components:

- *Claims* about the property of a system.
- *Evidence* that confirms that the claims made about an elements are true.
- *Arguments* that links the evidence to the claim.
- *Inference rules* that tie multiple (inconclusive) evidences together to an argument that proves a claim.

The claims are what defines a Safety Case and what is to be proved to declare a system safe. The claims should reflect the system in such a way that all the claims need to be fulfilled for the system to be safe. Different claims can handle different safety related aspects called attributes. Examples of attributes are e.g. reliability, security (from external attack), functional correctness, maintainability, fail-safety, usability (by the operator) (Bishop & Bloomfield, 1998). Of course there are more possible attributes but these give a good idea of how a Safety Case claim is constituted.

The evidence is the basis of the argument structure in a Safety Case. The source of the evidence can be either facts, assumptions or other claims in the Safety Case-structure. The arguments can utilize evidence from one of the following main sources: the design, the development process, simulated experience or prior field experience (Bishop & Bloomfield, 1998). The choice of evidence depends on the availability and the application. For new or untried designs, simulations might be necessary. If the design however is known from earlier applications the evidence could be to refer to prior experience.

The arguments are what link the evidence to the claim. Arguments can be deterministic, probabilistic or qualitative.

Figure 1 shows the basic outline of a Safety Case structure. Note that a Safety Case does not have to be presented in a tree like structure like the figure below, one should therefore be careful of drawing any conclusions that a Safety Case is a defined way to present information.

The purpose of a Safety Case is to prove a systems safety and therefore the output from a Safety Case will be either "yes, the system is safe enough" or "no, the system is not safe yet". The output could thus be said to be black and white in the sense that it is not possible to compare different claims to each other regarding claim fulfillment, this will be discussed further in chapter 3.

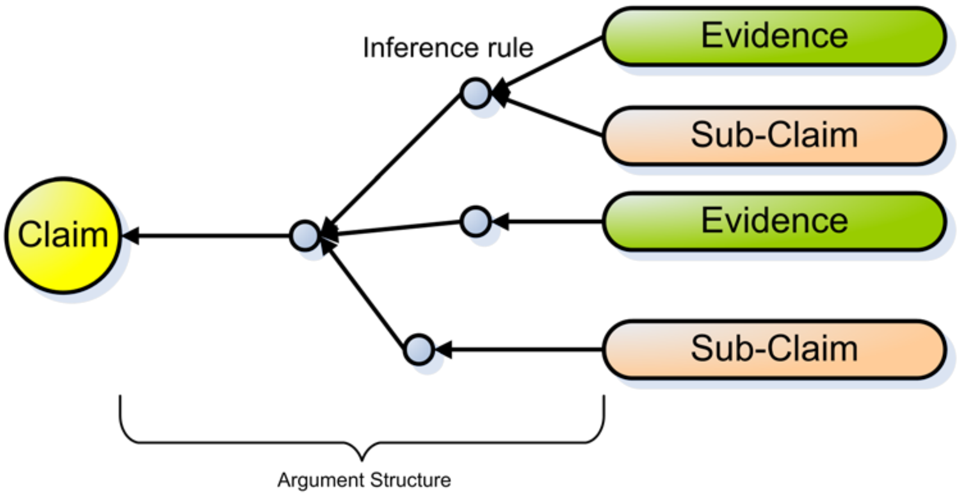


Figure 1 - The Safety Case structure.

It is up to the analyst conducting the Safety Case to define "safe enough". How this is done differs from case to case. In the UK regulations requires certain industries, e.g. the nuclear and off shore-industries, to operate within a Safety Case (Bishop & Bloomfield, 1998). The Health and Safety Executive that regulates nuclear installations in the UK defines a Safety Case as:

> *"The safety case is a suite of documents providing a written demonstration that risks have been reduced to a level that is as low as reasonably practicable. The safety case is not a one-off series of documents prepared to obtain a nuclear site license. It is intended to be a living dossier which underpins every safety related decision made by the licensee. The safety case is required to be updated regularly and as plant and organizational changes dictate. Safety cases can apply to whole plants or to modifications and encompass some aspects addressed in management prospectuses"*
> (HM Nuclear Installations Inspectorate, 2008)

This definition is quite precise unlike other Safety Case definitions as it dictates that the risks must be ALARP (As Low As Reasonably Practical and that the Safety Case should be a living dossier that is updated as the system evolves. Other definitions are more elementary:

> *"A documented body of evidence that provides a convincing and valid argument that a system is adequately safe for a given application in a given environment"*
> (Bishop & Bloomfield, 1998)
> *"A structured argument, supported by a body of evidence, that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given environment"*
> (Ministry of Defence, 2007)

The last two definitions above are less detailed than the first and show how vague the term Safety Case really is. All three definitions however share the common idea that a Safety Case is a documentation that proves a systems safety. How this documentation is performed is not a standardized method and thus it varies with who performs the analysis.

2.2 SQAD – Solvina's adaptation of the Safety Case methodology

Solvina has, together with their clients, in the resent years applied the Safety Case methodology in three major modernizations projects in Swedish nuclear power plants. The methodology used by *Solvina* is a customized adaptation of the Safety Case-methodology, going under the name "Safety/Quality Assurance and Demonstration" (SQAD). SQAD has been developed by *Solvina* in cooperation with their clients and is, as the name suggests, designed to manage both safety and quality demonstration within a project. The following chapter aims at giving a description of SQAD.

2.2.1 SQAD in general

SQAD is in essence an evolved version of the Safety Case-methodology with the main purpose of supplying an effective tool for assessing and demonstrating system safety. If applied from the beginning of- and practiced throughout a project, SQAD offers possibilities to ensure that involved parties in a project are working together in an efficient manner and understand how their piece fits in the whole as well as their role in the organization. The main aspect that distinguishes SQAD from the original Safety Case-idea is the concept of areas which is an essential part of the SQAD-methodology. The general idea is that the entire project is categorized by safety subject areas (SSA:s) that can be overlooked by a group of specialists in each area. The areas are supposed to cover the entire scope of the project and in some extent overlap each other to ensure sufficient scope coverage. How many areas and what they enclose differs from project to project, but there are some that are generally applicable. For example in project TWICE[1] 14 areas were defined, ranging from soft areas handling subjects such as quality assurance, design process and competence assurance to more technical areas dealing with subjects such as design requirements completeness and correctness, codes & regulations compliance, plant installation and product qualification (See Appendix 1 for a complete list of safety subject areas from project TWICE). Figure 2 illustrates the concept of areas.

In the future there is also a wish to utilize SQAD in systems that are built and taken into operation in order to further increase its safety and quality. This would be accomplished in a similar order as for systems under construction. It is believed that SQAD would be of great help here as it makes it possible to encompass an entire plant, factory or similar in one analysis.

[1] Ringhals TWo Instrumentation and Control Exchange. The project purpose was to modernize the entire instrumentation and control system including the main control room in the Ringhals Unit 2 where the old analog systems replaced by modern digital equipment.

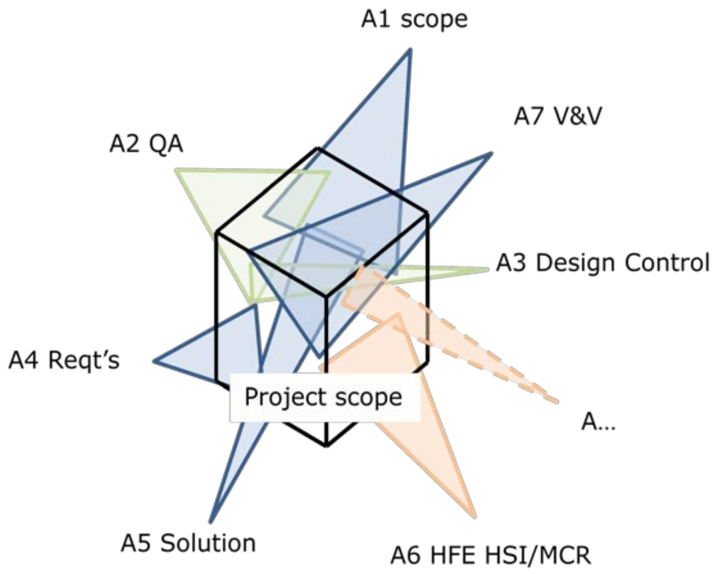


Figure 2 - The area concept of SQAD. The complete scope of the project (represented by the cube) is illuminated by the beams of light, each representing a specific area. The areas have different width and are

Within each area a structure of relevant claims and sub-claims are defined, preferably in cooperation with expertise from both supplier and system owner to ensure that the claims necessary are defined to cover the safety scope as completely as possible. Figure 3 shows the logic behind an area-claim structure; note that this is not an actual way to present such a structure but rather an illustration of how claims can be linked to each other in a tree structure.

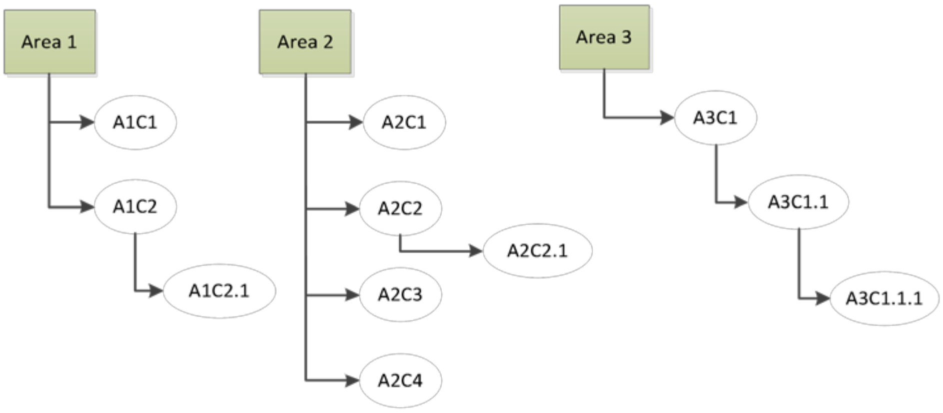


Figure 3 - The Area-Claim structure.

The main difference between an ordinary Safety Case and SQAD is described in Figure 4. A Safety Case is in some sense similar to a fault tree (except the only logical gate possible is AND) where the claims in the bottom of the hierarchy in the Safety Case represent the basic events in the Fault Tree. As shown in Figure 4 the difference between Safety Case and SQAD is that the claim hierarchy between the top claim (overall system safety) and the sub-claims have been cut off and replaced by the concept of Safety Subject Areas and overall conclusions made from assessment. The reason for doing this is mainly to rationalize the process of building the claim hierarchy as the system with SSA:s allows grouping of similar claims into a relevant area. The consequence of this is that the strict logic chain between the individual SSA:s and the top claim are broken in such a way that probabilities and consequences can't propagate "mathematically" in the same way as in for example a fault tree. This won't be a problem in this thesis though as the focus is on comparing specific first level claims towards each other a not how the "risk" propagate through the area-claim structure.

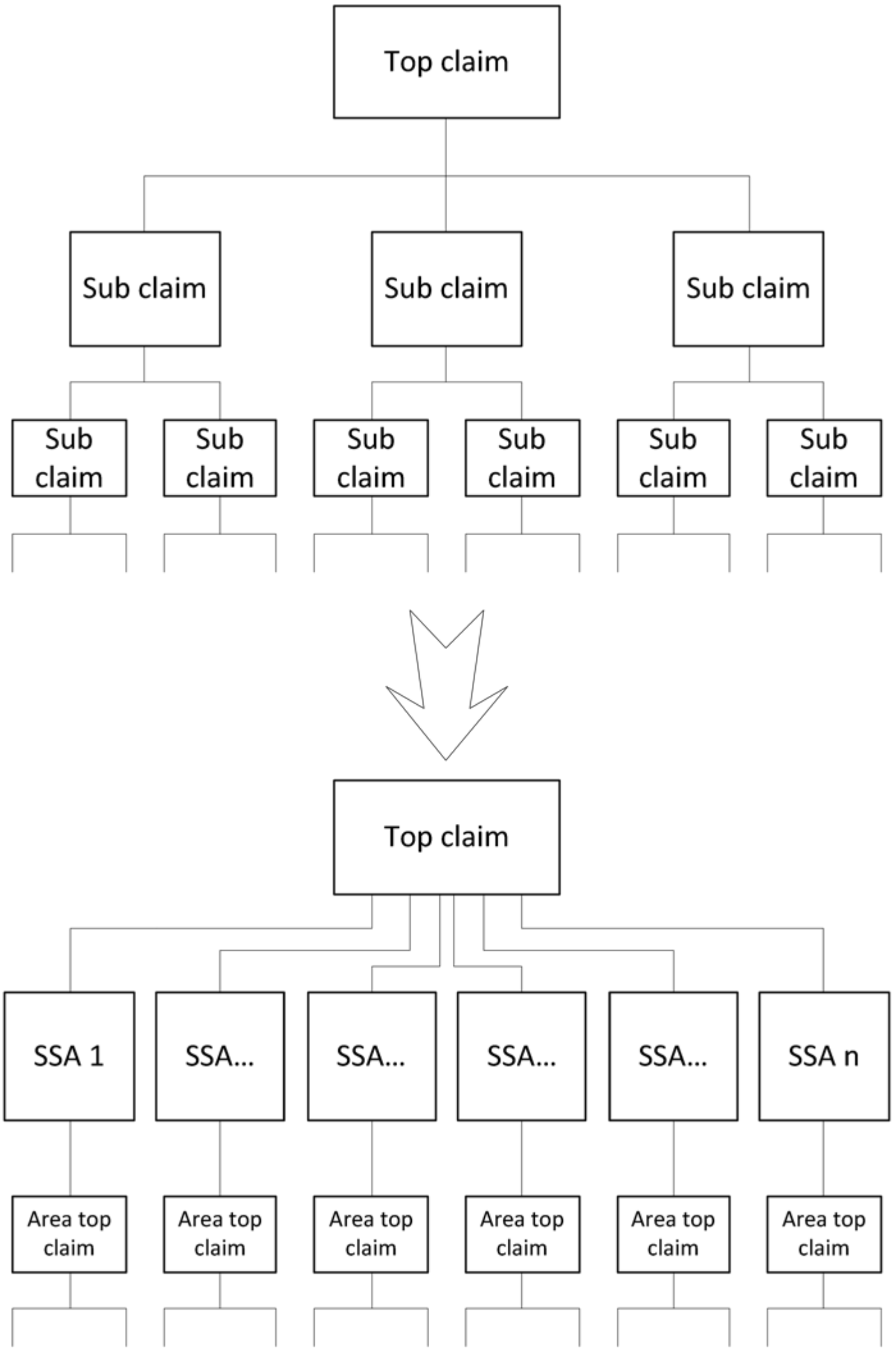


Figure 4 - The difference between an ordinary Safety Case and a SQAD. There is not necessarily a straight forward logic (and/or) from the SSA to the top claim(s) on overall safety conclusion, as there is in a normal Safety Case. The resulting safety conclusion is a comprehensive assessment.

3 Limitations with the current Safety Case and SQAD-methodologies

The output from SQAD and Safety Case claims in general, is basically one of two possible answers; it's either "yes, the claim is true" or "no, the claim is false". This is natural since the entire purpose of the Safety Case is to prove that an explicit claim, such as "This product is safe to use", is true. There are simply no "maybes" or "don't knows" and this may be fully satisfactory in many cases but in some circumstances the need for a more nuanced output is needed. This can be compared to assessing risk to find weak spots in a system in order to prioritize where to put greatest assurance effort. The following chapter will discuss the limitations in the current methodology and what an evolved methodology that allows a more nuanced output could achieve.

3.1 Lack of nuance in the binary output

The output from a Safety Case is binary. A claim is made about the property of a system or a system component that is then proven either (sufficiently) true or false. If false, adequate measures are taken to correct the shortcoming until the claim can be shown fulfilled. This binary output makes it hard to differentiate one claim from another because in a Safety Case no difference is made between two claims if they are both proven true (or false). But just because they are both true doesn't mean they necessarily have equal safety impact. Picture this; a claim is made that a building site is safe. The argument that proves the claim is that a railing is mounted on the scaffolds to stop workers from falling. The evidence for this could e.g. be compliance demonstrations to codes from a government regulator. Having the railings are probably safer than not having a rail at all, but what if you also make the workers wear harnesses? This would increase safety further but in either case a Safety Case would declare the claim as equally true. In reality however the two cases would show different levels of safety.

If this margin between the two cases could be visualized it would further increase the possibility to use the Safety Case-methodology as a tool for improving both safety and quality as it would provide possibilities to choose specific safety/quality areas that could be further ameliorated. Take the same example as above and let's say that the construction company also gives their workers an education in high altitude working as a complement to having physical barriers to prevent accidents. If the company later would like to further improve safety they would need to know where to put the effort, should it be in more physical barriers or in education? These two safety barriers could be in two different SSA:s in a SQAD and it is here an evolved methodology that makes it possible to compare claims from different areas could prove to be useful.

4 Evolving the methodology

To be able to understand if and how SQAD could be further developed in the desired direction it is important that the problem is fully understood. The previous chapter gave an initial description of the problem and the desired goal but a more precise breakdown of the problem is necessary. This chapter further describes the problem and presents a possible solution.

4.1 Applying risk management methods to SQAD and problems related to this

The task is to evolve SQAD to enable a gradable output by integrating conventional and established risk management methods to the current SQAD-methodology. This is to be accomplished by in some way estimating the probability and consequence of not fulfilling each claim in the claim/evidence structure and thereby produce an estimation of how important a claim is for total system safety - or "risk" to unfulfillment. This is however associated with certain problems related to how consequence and probability would fit into the SQAD-concept and also how the method would work differently depending if it is applied to a system under construction or taken into operation.

4.1.1 The problem with applying consequence and probability to SQAD

The first problem arises when trying to understand how to relate consequence to the concept of claims utilized in SQAD. The thing is that it is not really of any meaning trying to assign a consequence as such to the claims in SQAD as they can't be seen as sources of risk themselves. A claim is rather a statement saying that if certain things can be proven about a system the risk of an unwanted event could be held to an acceptable level. What this means however is that if it can be established which unwanted events could come as a result from an unfulfilled claim a consequence could be established for these events. The concept of consequence is thereby not far away when dealing with SQAD but it would still be wrong trying to apply consequence directly to claims. The reason being that it isn't the consequence of claims not being fulfilled that is measured but rather the consequence of a possible failure in a component/function that is handled by the claim. The solution is to introduce claim importance. By assessing what the consequences would be if functions/components handled by a claim malfunctioned the grade of importance that claim have for the overall system can be established. For a system to work as imagined all claims of course need to be fulfilled, this is the entire purpose of a Safety Case/SQAD. But that isn't to be said that a system won't work at all even if some claims are not entirely fulfilled. Therefore claims could possibly be graded after their importance to the system as a whole.

Just as consequence, probability is an important piece in the risk concept. And also, just as consequence, probability doesn't entirely fit the concept of SQAD. The problem is how to fit probability into the model as it isn't clear what the probability would measure. Should it measure the probability for a claim to be unfulfilled or should it measure the probability of failure for a function that a specific claim concern? Neither idea is satisfactory as they are extremely hard to answer and might also be too complex – or just wrong. So a new approach to probability is needed to allow evolution of SQAD. Instead a combination of "margin of claim fulfillment" (or rather an estimation of evidence strength) and a factor that states "how soon the claim needs to be fulfilled" will be introduced. This would in some meaning describe the urgency of a claim to be fulfilled.

What is to be established is, in other words, a factor that measures the importance (here-from *importance factor*) of a claim for the system as a whole and a factor that estimates the evidence strength of a claim compensated for how urgently the claim need to be fulfilled (here-from *urgency factor*). This will be further discussed later on in 4.6.3.

4.2 The difference between systems under construction and taken into operation

The idea behind SQAD is that it should be possible to apply to a system during its entire life span from planning and construction to decommissioning. However this introduces a problem with the urgency factor introduced above as it would differ from systems under construction and systems put into operation as the urgency factor relies on that there is a time frame available from which one could estimate urgency. During construction this time frame exists as a distinct time plan for the project and it is relatively easy to determine how well fulfilled a claim is, as it is described in detail in project documentations what is to be done to achieve claim fulfillment. When a system have been finalized and put into operation however there may be no obvious time table to follow. So if SQAD is to be used as a tool for quality/safety improvement for a system in operation where all the claims are already intended to be fulfilled the approach to handling the urgency factor needs to be modified under these circumstances. The problem is thereby in essence to find a method to produce the urgency factor for claims in a system taken into operation. This is an important part of the problem.

4.3 Requirements for potential risk evaluation methods

Seeing that most of the evidence in a typical SQAD is of a qualitative nature focus will be put on exploring qualitative risk management methods. This is also desirable seeing that the areas in a SQAD is of such a broad perspective ranging from technical aspects to the level of education among operators, that trying to incorporate a quantitative method would be hard and probably not solve the problem. It is favorable that the method selected is easy to use and understand by personnel that are not used with conducting risk management tasks. A more detailed set of requirements are given below:

The output must be gradable

This is the most important requirement as it is the core of the entire thesis. The output from the SQAD must by gradable to allow individual claims to be compared to each other.

Easy to understand and manage

Conducting a SQAD involves people from many different backgrounds with different experience in risk management. Most people involved may be experts in their field but doesn't for that sake have to be experienced in risk management. It is therefore important that the methodology is easy to use so that performing the SQAD doesn't become a cumber.

Allowing for easy communication

To be able to use SQAD as a tool for safety and quality improvement, it must be possible to visualize and communicate the result in an effective manner. This would be best accomplished if the method resulted in a numerical output that could be visualized graphically.

Allowing for different levels of "hardness" in area attributes

Claims vary from each other in terms of which attributes they consist of. The attributes varies from being technical aspects dealing with installment of machinery to "softer" attributes for example operator education or maintenance routines. To be able to cope with this broad spectrum of attributes it is necessary to either choose multiple methods specialized in different attributes or to choose one method that may be less thorough but that can cope with the whole range of different attributes.

4.4 Potential risk analysis methods

To be able to choose which method to integrate into SQAD a wide selection of risk analysis methods available will first be chosen and shortly introduced below. Methods dealing with both technical aspects of risk and methods for analysis of human factors will be included but only methods that can be used with a strictly qualitative input are of interest and therefore any other method will not be mentioned. The number of methods available is quite immense and can of course not be evaluated in its completeness and must therefore be delimited. The methods presented below have been chosen as they are relatively known and well documented.

4.4.1 Methods for general technical and sociotechnical applications

4.4.1.1 Checklists

Checklists is a method that is based on previous experiences and is primarily used to indentify known sources of risk and to ensure that recognized codes and standards are being followed. The method required experienced analysts that know the system well and can predict usual sources of risk. The analysis results in a list with notes declaring if requirements are satisfied or not. A checklist can be of different grade of detail depending on scope of use and if good praxis is available and the system is well known, a checklist can be very quick and cost efficient method (Nystedt, 2000).

4.4.1.2 Preliminary Hazard Analysis

A preliminary hazard analysis is usually conducted during the planning stage of a project or during a preliminary analysis of an existing object. The purpose is often to give a coarse picture of which parts of a system that can induce risk. The method results in qualitative list of risk sources without numerical values or ability to prioritize between risk sources. However it is possible to achieve a numerical estimation of risk values by grading the probability of different risk sources after a predetermined scale. This requires experienced personnel with good knowledge of the system that can estimate the probability intuitively and thereby achieve an experience based estimation of risk (Nystedt, 2000).

4.4.1.3 What-if

The purpose of a "what if"-analysis is to evaluate the consequence of different scenarios occurring in a system. The analysis is carried out by choosing specific functions in a system and asking questions of the type "What if?" about that specific part. The part could for example be a pump and the questions "What if the pump stops?" or "What if the flow to the pump ceases?". The output from the analysis is strictly qualitative and ranking or prioritizing between risk sources is not possible (Nystedt, 2000).

4.4.1.4 FMEA/FMECA

Failure Mode, Effect (and Criticality) Analysis is a method used for identifying and eliminating possible sources of risk by systematically analyzing what can go wrong in a system, how the fault would affect the system and how often the fault could occur. How the problem should be mitigated is also addressed in the method (Davidsson, 2003).

FMECA is not effective at detecting combinations of faults that together leads to a hazardous event but it allows for risks to be graded, ranked and prioritized (Nystedt, 2000). And even if the methods main purpose is to analyze material and equipment failures it can in a broad sense also handle human error and performance and software errors (Dyadem, 2004).

4.4.1.5 Event tree analysis

An event tree analysis is used to identify which possible hazardous events can occur in a system as a result from an initiating event. The method can be applied on the output from an FMECA-analysis (Nystedt, 2000).

An event tree has its base in an initiating event, e g “High pressure in a tank”. Based on this event different following events are identified and presented in a tree structure. The method can handle both technical faults and human errors but require that the probability for an event to happen is known.

4.4.1.6 Hierarchical Holographic Modeling

Hierarchical Holographic Modeling (HHM) is a framework for identification of events that can affect a system in a negative manner. The events can be both external, for example natural hazards or world events and internal such as changes in management or technical failure (Malmkvist, 2008).

The core of HHM is a particular diagram that describes the crucial parts of the system and what needs to work for the system to work, see Figure 5.

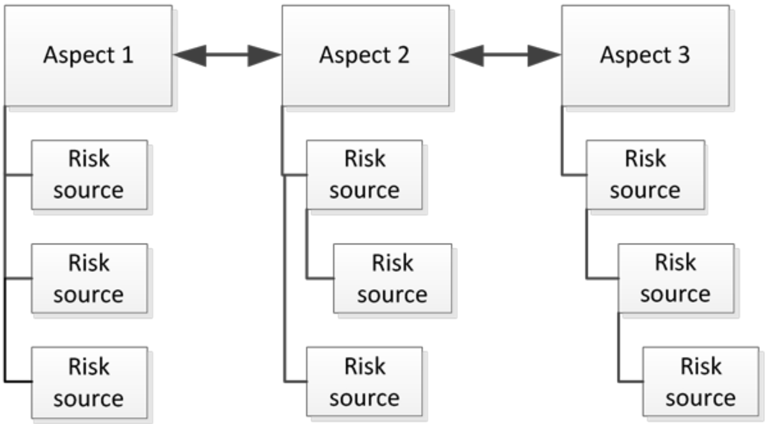


Figure 5 - The HHM-diagram.

The top row in the diagram is the *head topics* describe the “perspectives of success” (Kaplan, Haimes, & Lambert, 2002). They are basically the crucial parts of the system that all need to work for the system to work. The tree structures emerging from each head topic are the *sub topics*. They aim at providing more detailed classification requirements, i.e. requirements that need to be fulfilled for the head topics to be functional. HHM doesn’t provide any methods for quantifying or grading risks; its sole purpose is to provide a synoptic method for identifying risk sources.

4.4.2 Methods for analysis of human and organizational risks

4.4.2.1 HRA

Human Reliability Analysis is the name of a group of analysis methods that is used to evaluate human reliability in different work conditions. How humans perform in different working conditions is one of the hardest variables to estimate in a risk analysis. This doesn’t make it less important though. Human interaction with technical interfaces is an important part of the safety in any system as it often is human operators that in the end are in control of the system.

The methods aim at doing a systematical evaluation of circumstances that affect the performance of human operators, maintenance staff and technicians in their work tasks. The analysis identifies decisions or measures that can lead to an increased chance for a hazardous event to occur.

Well known HRA-methods are TESEO (Technica Empirica Stima Errori Operati), THERP (Technique for Human Error Rare Prediction), HEART (Human Error Assessment and Reduction Technique), etc. What many methods related to HRA has in common is that they require highly experienced analysts and they take a large amount of time and human effort (Malmkvist, 2008).

4.4.2.2 AEA

The Action Error Analysis is a method that is used to identify possibility of human errors in critical operations. It is basically the equivalent to the HAZOP-method modified to analyze human error. In an analysis a list of activities that should be performed by e.g. an operator is produced. Each activity is then evaluated with the help from a predefined set of possible events e.g.

- No action. *What happens if the action is not carried out?*
- Wrong action. *What happens if the wrong action is carried out?*
- Right action, wrong object. *Is it possible for the operator to e.g. shut the wrong valve?*
- To early, too late. *Can the action be carried out to early or too late?*
- Wrong sequence. *What happens if the actions are done in the wrong order?*

(Davidsson, 2003)

The Method can be of use when designing new equipment but also when new operation procedures are evaluated.

4.5 Which methods could be applicable?

To determine which methods could be applicable to integrate in the SQAD-methodology a list with pros and cons for each method listed above will be made presupposing from the requirements stated earlier. The applicability for each method will also be briefly discussed.

4.5.1 Checklist

Pros

- Easy to carry out
- Allows for different types of risk

Cons

- Require high grade of expertise
- The system needs to be somewhat standardized
- Non gradable output

Using only checklists in SQAD are not enough to meet the expectations of an evolved SQAD-methodology. Checklists don't in itself produce an output that is quantifiable and gradable and can't therefore work by itself as a method to integrate into SQAD. Checklists can however be of support to analyst to help asking the right questions when doing a SQAD-analysis.

4.5.2 Preliminary Hazard Analysis

Pros

- Able to produce a gradable output
- Allows for different types of risk
- Easy to carry out

Cons

- Require high grade of expertise
- May be hard to produce a comprehensive analysis as the method lacks systematicity
- Chances are that a graded output would be inconsistent

A Preliminary Hazard Analysis could be done at almost any system given that expertise are available that knows the system well enough to identify enough risk sources and also being able to grade them in a realistic manner. In the case of SQAD the identifying of risk sources in the form of claims have already been done so what's left of the PHA is to grade the claims. The backside of PHA is that the method is lacking systematicity and therefore it depends a lot on the analysts what the quality of the result will be. The pros are probably weighing up the cons though and the method is likely to be one of the most promising for SQAD-integration.

4.5.3 What-if

Pros

- Very systematic

Cons

- Strictly qualitative output, no risk ranking possible.

The What-If analysis produces a strictly qualitative output that in itself is not gradable. For certain, the output could be intuitively graded as with the Preliminary Hazard Analysis but even so, there are other aspects that make What-If unsuitable for integration with SQAD.

4.5.4 FMEA/FMECA

Pros

- Allowing for gradable output

Cons

- Most suitable for strictly technical systems where component failure is to be analyzed

The FMEA/FMECA methods are quite complex and also very specific in their area of use. It does offer possibility for grading of risks but because of its complexity, the method is deemed not suitable for SQAD-integration.

4.5.5 Event Tree Analysis

Pros

- Allowing for gradable output
- Highly quantitative output

Cons

- Most suitable for strictly technical systems where component failure is to be analyzed
- Require statistical values or the failure frequency for critical events

The Event Tree Analysis is a comprehensive method for mapping of risk structures in a complex system but the methods demand for detailed statistical values for each component makes the ETA unsuitable for SQAD-integration.

4.5.6 Hierarchical Holographic Modeling

Pros

- May allow for gradable output
- Allows for different types of risk

Cons

- Does not have specified method for displaying output

HHM is not totally unlike SQAD in its way to organize different risk aspects into different areas. The system is divided into groups and sub-groups to create a visual structure of the parameters that affect a system. Integrating HHM into SQAD is an interesting thought but the need for it is unclear as SQAD and Safety Case themselves offers a hierarchical structure that can be relatively easy to review.

4.5.7 HRA and AEA

Assessing human induced risks are important and an essential part of most risk reducing activities. However it is deemed to be outside the reach of this thesis to integrate methods specific for this purpose in the SQAD-methodology. The goal of this thesis must be to integrate a general methodology that works satisfactory for risks induced both by human and technical failure and therefore methods specifically used for assessing human induced risks will not be covered in this thesis.

4.5.8 The method of choice

From the listing of possible methods it is decided that the Preliminary Hazard Analysis is the best choice for integration with SQAD. Even if other methods possess certain elements that could be useful in SQAD no other method supply the same possibilities as a whole as PHA.

Usually a PHA consist of three steps: Hazard identification, consequence & frequency estimation and risk ranking & follow-up actions (Rausand, 2005). In SQAD the Hazard identification could be compared to building the safety case and formulating the claims and the Risk ranking & follow-up actions could be translated to the measures taken if a claim is failed to be fulfilled. The part that is of most interest to integrate into SQAD is way the consequence & frequency estimation is done in a PHA.

Other common artifacts related to PHA e.g. “Preliminary Hazard List” (Roland & Moriarty, 2009), “Hazard checklists” (Rausand, 2005) will not be integrated into SQAD at this point. What will be integrated are the methods for quantifying risk using frequency- and severity classes and different methods for ranking risk using e.g. risk matrices.

To be able to integrate the desired components from PHA into SQAD the difficulties of translating consequence and probability to fit the methodology must first be overcome.

Other methods of interests

Both Hierarchical Holographic Modeling and checklists offer interesting possibilities that could very well fit in the evolved SQAD-methodology. HHA offers an interesting approach to visualizing and organizing the risk identification process and even if this is not of the main concern in the process of evolving SQAD it could be of interest to take this aspect into consideration. What checklists are concerned, they could offer a good possibility to support the analysts in the process of conducting a SQAD-analysis and help asking the right questions etcetera. Using checklists is a way to further evolve the methodology by updating the checklists as new SQAD-analyses are made and new lessons are learned. However due to the tight time frame of this thesis the possibility to integrate HHA and checklists will not be further investigated in this thesis.

In the next chapter the outlines of an evolved SQAD-methodology will be drawn. The goal will be to integrate preliminary hazard analysis in the SQAD-methodology.

4.6 A proposal for an evolved SQAD-methodology

In this chapter a proposal for an evolved SQAD-methodology with integrated tools for producing a “risk” or – “claim significance” will be made. The method that has been chosen for integration is preliminary hazard analysis. As discussed in chapter 4.1 the way probability and consequence are traditionally used have to be adjusted, how this is supposed to be done is detailed in this chapter.

4.6.1 Prerequisites and delimitations

As described earlier the claims in a SQAD-analysis can be structured in a hierarchically manner with a top claim and several sub claims. In this thesis only the bottom claims in the hierarchy will be considered. This means that importance and urgency will only be assigned to the bottom level claims and that it are these bottom claims that are to be plotted and compared in the visualization phase described chapter 5. This is a simplification that eliminates the claim-levels between the bottom and top claims in the claim hierarchy. This might sound like an easy way of disregarding a problem but it might actually not be so. It is believed that looking at each lowest level-claim is fully satisfactory to reach the goal of this thesis. There doesn't really exist a need of following the claim-chain from bottom to top and look at how importance and urgency propagate through the chain as the goal and this would really be the only reason to take all claims in the chain into consideration.

4.6.2 Preliminary Hazard Analysis as the method of ranking

The method chosen to integrate into SQAD is Preliminary Hazard Analysis (PHA). Of the methods listed as possible candidates in chapter 4.5, PHA is believed to be the best method of choice as it is the only one that enables handling both qualitative and quantitative input and can produce a gradable output. PHA is believed to offer great flexibility and is possible to mold after the user's needs, this makes it a good choice for SQAD-integration.

To be able to integrate PHA into SQAD the following aspects have to be considered:

- How the urgency and importance -factors are to be formulated needs to be clarified.
- The scale after which the urgency- and importance-factors are to be rated needs to be established.
- How are the scaled urgency- and importance-factors to be weighted together?

The following chapters will aim at clarifying the aspects listed above.

4.6.3 Formulation of importance- and urgency-factors

The importance- and urgency factors are to be used as input for determining the total significance for the claims. In the following sub-chapters the two factors will be described in detail.

4.6.3.1 Importance factor

The importance factor is supposed to substitute the consequence used in traditional risk management, as the concept of consequence is believed not to be applicable to SQAD. The reason for this is that consequence when dealing with traditional risk management refers to a negative outcome of an unwanted event and this is not how SQAD works. The unwanted event when referring to SQAD would be the unfulfillment itself, not a certain claim. The proposed solution to this is to replace consequence with the importance factor. The idea is to grade each claim after how important they are for the total safety/quality of the system. As described in 4.6.1 only the bottom level claims will be considered in this thesis and which means that only the bottom claims will be given an importance and

The importance factor is not influenced by whether the system is under construction or taken into operation and can thereby be established for all claims during the construction phase of a project. The importance factor will then be valid throughout the systems lifespan unless the components function in the system is changed in such a way that the importance of that component isn't the same.

In Table 1 below a proposed scale for estimating importance is presented. The scale has been inspired by *Solvina's* internal manual for estimating consequence while conducting PHA which consists of five steps and can be seen in Appendix 3. The consequence classes described in the manual are not directly applicable to the importance factor as some of the consequences are not relevant for SQAD and have therefore been modified to fit the SQAD purpose. The descriptions are supposed to be a support for analysts when estimating the importance factor by choosing the description that fit the current claim best and then selecting the correspondent importance factor. The classes below are very similar to its consequence counterparts used in traditional risk management and as discussed in 4.1.1 a relationship do exist between consequence and importance. Because of this it is believed that it is possible to emanate from classes inspired by consequence and from that estimate claim importance. Table 1 is just an example of how importance could be estimated but it is believed to give a good picture of how importance could be assigned to a claim after how it affects total system safety.

Table 1 - Proposal for importance classes inspired by Solvina's PHA manual.

Importance	Description
1	System/function concerned by claim is a support function. Requirements exist for function concerned by claim, but safe operation is possible with claim unfulfilled.
2	System/function concerned by claim: - Is not required during normal operation, but could be required during startup or similar. - Can be replaced with costly technical repair/replacement. Failure in system/function concerned by claim could result in: - In downtime/disturbance <4 hours. - Economic impact of <1million SEK.
3	Failure in system/function concerned by claim could result in: -Situation that is required to be reported to authorities. -Requires high maintenance, complex, long troubleshooting. -Some production reduction as a result from loss of function. -Downtime/disturbance 4 hours - 1 day. -Economic Impact> 1million SEK.
4	Failure in system/function concerned by claim could result in: - Event in the magnitude of INES 1. -Reduced operation as a result of system malfunction. -Downtime / disruption 1-5 days. -Economic impact of> 5 million SEK.
5	Failure in system/function concerned by claim could result in: −Event in the magnitude of INES 2 - 7 - Serious security/production disruption - Economic impacts> 15 million SEK.

The descriptions in Table 1 above are just meant as a general example and have to be adjusted for the activity in question. The specific descriptions above are inspired by the nuclear power industry and there are two descriptions that are very specific for this. The first is found on level 3; Situation that is required to be reported to authorities arise. This represents an accident of a certain magnitude that must be reported to the regulatory authority. The other is INES, which stands for International Nuclear Event Scale, and is scale describing the magnitude of accidents in nuclear power plants (IAEA, 2008).

4.6.3.2 Urgency factor

While the importance factor is pretty straightforward the urgency factor is a bit more complicated. The purpose of the urgency factor is to replace probability as it is used in traditional risk analysis.

The main purpose of evolving SQAD is to enable a possibility to rank claims after how significant they are and how great the "risk" is for certain claims not being fulfilled. To manage this it is necessary to add a time aspect. This is especially interesting when using SQAD on systems under construction as it then could be of interest to know when in time claims needs to be fulfilled to ensure the project is on schedule. To be able to comply with this, the concept of probability is replaced with the urgency factor.

The urgency factor is an estimation of how well fulfilled the claim is based on how strong the evidence are considered to be, compensated by a time factor. The urgency factor thereby consists of two parts: "Strength of evidence" (here from SoE) and a time related compensation factor, the "exigency factor". To compile the urgency factor the SoE are first established by estimating how much of the evidence needed for fulfilling the claim are in place and what the quality of this evidence is. This should be done in the same manner as importance where a scale of a predetermined number of classes exists; the SoE should thereby be presented as a number between 1 and 5(How many classes there is in the scale could of course vary but in this thesis a scale of five classes will be used). The SoE are then compensated with the exigency factor regarding to how soon the claim needs to be fulfilled. This is done by simply lowering or increasing the SoE-number depending on if there is little or much time before the claim needs to be fulfilled. Thus a claim can receive a high SoE-class (low evidence strength) but adjusted to low urgency if there is enough time to fulfill the claim. Reasons for this could e.g. be that competence is secured; tools and material are available etc.

By introducing the urgency factor that takes into account how soon a claim needs to be fulfilled it is made possible to compare fulfilled and unfulfilled claims towards each other in the same analysis. A claim that is in essence fulfilled but is deemed as very important for total system safety could receive a higher significance than an unfulfilled claim with low importance. The purpose is not to highlight fulfilled claims and leaving them behind but instead giving them a low urgency and thereby a lower significance so that focus could be directed at claims that at the moment has a high urgency factor and thereby higher significance. Evaluating claim importance and urgency is an ongoing process though and the significance for a claim could therefore go from lower to higher (or vice versa) during the system life cycle.

Table 2 lists a proposal for a scale helping to choose the right SoE-class. Because of urgency being less related to probability than importance is to consequence the values are of a much more qualitative nature than its importance counterpart. Note that the table lists SoE and not urgency as urgency is SoE that has been compensated by exigency.

Table 2 - Proposal for Strength of evidence-classes.

SoE-class	Description
1	Very strong evidence -The evidence is considered strong enough to hold throughout the project and won't be affected by other claims.
2	Strong evidence -The evidence is considered strong but may be affected by other claims.
3	Good evidence -Evidence is good at this point but will most likely be affected by other claims during the project.
4	Weak evidence -Evidence is weak and will have to be strengthened soon.
5	Very weak evidence -Evidence is very weak and have to be strengthened as soon as possible.

4.6.3.3 Combining the importance- and urgency factors to produce the significance

The importance and urgency estimated in the PHA is to be combined to a factor called significance. The significance is a measurement of how significant a certain claim is for the entire system at the time of the analysis. When conducting the PHA the urgency- and importance factors are to be divided into classes ranging from 1 to X, where 1 is lowest class of urgency/importance and X the highest. Each class is associated with a specific set of demands representing that class's level of importance/urgency. The entire process can be compared with how consequence and probability are combined to communicate a level of risk. Two alternative methods for accomplishing this have been identified and evaluated: multiplication of class values and the risk matrix.

Multiplication of class values

Multiplication of the values received after grading urgency and importance are a straight forward process that quickly delivers a result. For a scale ranging from 1 to X the output would be in the range of $[1: X^2]$. For example a scale with classes ranging from 1 to 4 the output would range from 1 to 16 where 1 represent the lowest combination of urgency and importance and 16 the highest where both importance and urgency are assigned high values. The main benefits with this method are that it is quick, easy and produces a result that is directly comparable. The disadvantage however is that it doesn't offer any nuance between two claims with the same class values. Two claims where the first received 2 on urgency and 4 on importance and the second 4 on urgency and 2 on importance will both receive 8 as their significance. This could make it difficult to prioritize between multiple claims with the same significance factor.

Risk matrix

A risk matrix is a table that traditionally has several categories of likelihood and consequence in its respective rows and columns. See Table 3.

Table 3 - Example of a Risk Matrix with five likelihood classes and four consequence classes. The matrix below is for exemplification only and is not related to any actual data presented in the thesis.

likelihood/ consequence	1 Very unlikely	2 Remote	3 Occasional	4 Probable	5 Frequent
Catastrophic	🟨	🟥	🟥	🟥	🟥
Critical	🟩	🟨	🟨	🟥	🟥
Major	🟩	🟩	🟨	🟨	🟥
Minor	🟩	🟩	🟩	🟩	🟨

When conducting an analysis each error event identified in an event analysis is assigned likelihood and a consequence. The event is then placed in the cell of the matrix representing the assigned likelihood- and consequence class. In the example above color coding is used to identify which events needs to be prioritized were green are the least and red the most imminent dangers.

How many columns and rows used in a risk matrix are not in any way regulated and is entirely up to the analysts to determine. More cells give a finer resolution but as the grading of hazards is done intuitively a resolution too high could lead to inconsistent results.

The risk matrix is believed to be a better choice than multiplication of values as it offers greater possibility to give a nuanced output where multiple claims with the same significance but different class values are differentiated. If applied to SQAD however the likelihood and consequence would be replaced with importance and urgency factors.

4.6.3.4 Applying the urgency factor on systems taken into operation

The hopes with the evolved SQAD methodology are that it could be applied to a system during its entire lifespan, from planning and construction to decommissioning. The idea is to utilize SQAD to improve safety and quality to systems in operation by grading claim significance and further improve those that are least fulfilled or has the highest combined significance factor. Unlike the importance factor though, the urgency factor depends on if the system in question is under construction or taken into operation. The reason for this is as mentioned in chapter 4.2 that the time horizons from which the urgency factor is determined are different for a system under construction than for a system taken into operation. For a system under construction the time frame could be the time before the system are finalized and ready for operational status. When the system is taken into operation however there is no obvious time frame to work with. The solution to this is to establish a time frame that stretches over a for the current analysis relevant time horizon. This time horizon could stretch for any span of time, ranging from just this current year to in principle unlimited time ahead. The idea is easiest pictured with an example:

A claim handling competence assurance states that operators have sufficient education and training to perform their job. If operator competence is deemed satisfactory and this is sufficiently documented, the urgency factor would be low. But if suddenly new criterions regarding operator training is announced by regulatory authorities and it is deemed that new training procedures must be established, this could result in an escalation of the urgency factor. How much it is escalated would depend on when the new rules begin to apply and how long the revision of training procedures will take.

The analysis could also be done for more than one time frame at a time. For example if it is known that a number of events affecting the operation will occur in the future, but spread out over a wide time horizon. This scenario is described in chapter 6.

4.7 The resulting evolved methodology

This sub-chapter aims at concluding what is discussed in earlier chapters and presenting a formulated methodology in detail that will be demonstrated for integrated into SQAD in chapter 6. The suggested methodology for integration in SQAD consists of three stages:

1. The claim significance analysis part that involves the modified preliminary hazard analysis
2. The quantification of claim significance using a risk matrix
3. Evaluating and visualizing the data from the risk matrix

This chapter will describe stage one and two. The method suggested for integration is a modified preliminary hazard analysis where the consequence- and probability classes have been replaced with importance and urgency factors that together aim at determining the safety significance of claims within a SQAD; the significance factor. The urgency and importance will be graded on a scale from 1-X. The output will be plotted in a risk matrix from which the result will be further processed and visualized for easier communication, how this communication and visualization will be done are discussed in chapter 5. The process of doing an evolved SQAD is described in Figure 6 below.

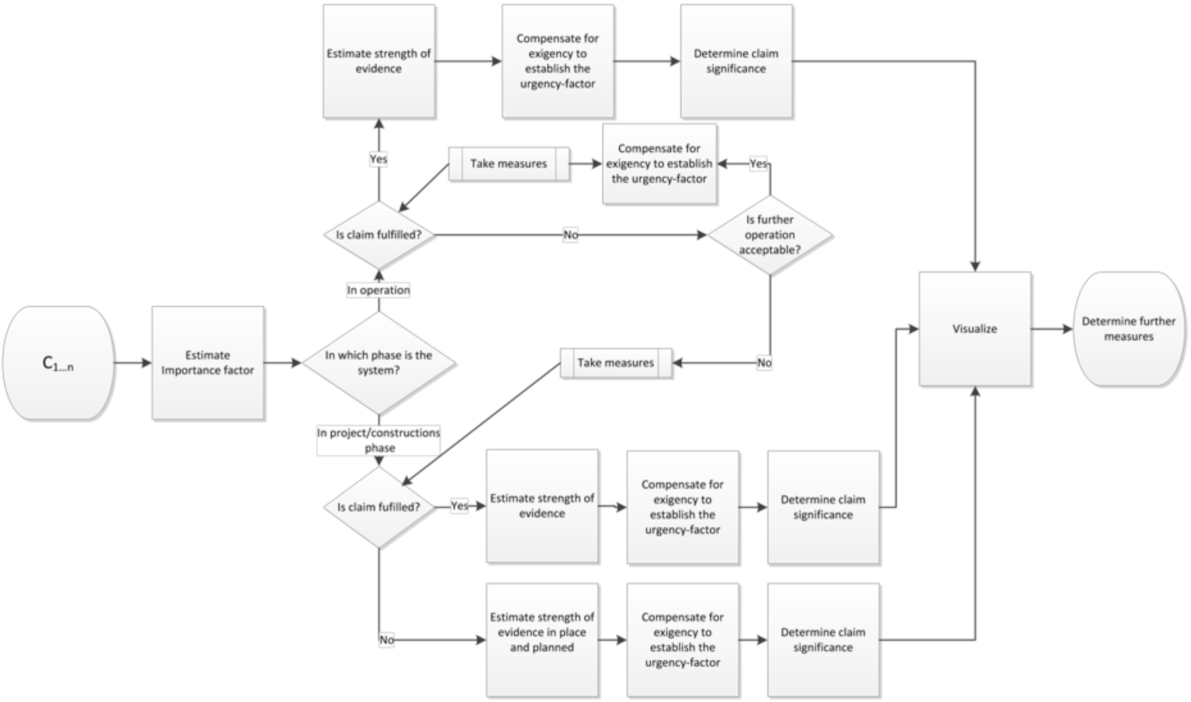

Estimate strength of evidence
Compensate for exigency to establish the urgency-factor
Determine claim significance
Yes
Take measures
Compensate for exigency to establish the urgency-factor
Yes
Is claim fulfilled?
No
Is further operation acceptable?
In operation
C1...n
Estimate Importance factor
In which phase is the system?
Visualize
Determine further measures
Take measures
No
In project/constructions phase
Is claim fufilled?
Yes
Estimate strength of evidence
Compensate for exigency to establish the urgency-factor
Determine claim significance
No
Estimate strength of evidence in place and planned
Compensate for exigency to establish the urgency-factor
Determine claim significance

Figure 6 - Work flow describing the process of conducting the modified SQAD analysis. The diagram includes the PHA and risk matrix parts of the analysis. A high resolution version is found in Appendix 2.

Note that there in the flow chart is a decision point asking if the claim is fulfilled or not. The evolved SQAD are not supposed to distinguish between claims that are fulfilled and the ones that are not as important claims that have low strength in evidence (or high urgency) should be prioritized higher than claims that are unfulfilled but unimportant. Though it is necessary to distinguish them in the flow chart because even if claims are not supposed to "pop out" as unfulfilled in the visualization process all claims has to be considered fulfilled to deem the system ready to e.g. be set into operation. When a claim could be considered fulfilled aren't covered in this thesis as it only focuses on the process that leads to the point where all claims could be considered fulfilled and the system deemed safe/good enough. The deciding in if a claim is fulfilled or not is thereby a necessary decision to make each time a claim is evaluated, which is an ongoing process that is repeated during a system whole lifespan.

4.7.1 The claim significance analysis using a modified preliminary hazard analysis

The modified PHA is the first step in the process of determining claim significance. The PHA is meant to be a tool for persons involved in the project that is conducting the SQAD analysis to intuitively grade claims after how important they are for the overall system and how urgent the claim needs to be attended to. The factors that are to be estimated are the importance- and urgency factors. How each factor are to be evaluated and what they include are described previously in 4.6.3.1 and 4.6.3.2. One thing that has to be taken into account while conducting the PHA-part of SQAD, is if the system is under construction or taken intro operation, as shown in Figure 6.

The importance factor of the modified PHA is relatively straightforward and aims at reflecting the importance to the overall system for an individual claim. As seen in Figure 6 the importance factor are not influenced by whether the system is under construction or taken into operation and can thereby be established at any time during a project or system life cycle. The importance factor will then be valid throughout the systems lifespan unless the components function in the system is changed in such a way that the importance of that component isn't the same.

The urgency factor however differs for systems under construction and systems taken into operation and must therefore be reevaluated regularly during the entire system life time.

4.7.2 The risk matrix

The output from the PHA is to be plotted in a risk matrix to produce the significance. The scale has been set to five steps on both the importance and urgency axis as seen in Table 4. If this is the best way to grade the scales are unclear but it is thought to be a good starting point that can be further evaluated in further work.

Table 4 - Example of a risk matrix

		Importance				
		1	2	3	4	5
Urgency	5	0,5	0,6	0,7	0,8	0,9
	4	0,4	0,5	0,6	0,7	0,8
	3	0,3	0,4	0,5	0,6	0,7
	2	0,2	0,3	0,4	0,5	0,6
	1	0,1	0,2	0,3	0,4	0,5

The numbering in the cells is the significance factors and is a substitute for the color grading traditionally used in risk matrices and are supposed help grading the claim significance. The benefit of using numerical factors is a finer resolution and the ability to use the values in further visualization purposes. The values are not to be seen as a way to illustrate claim significance in a fixed scale, but are just a way to compare claims toward each other regarding their significance.

4.7.3 How to interpret the output

After the estimation of the importance- and urgency factors have been established through the PHA, the results are to be plotted into the risk matrix. An example is shown in Table 6 below. Five claims numbered from 1 to 5 have been plotted in the matrix.

Table 5 - Example of output from a PHA.

Claim	Importance	Urgency
1	2	5
2	3	3
3	4	1
4	2	1
5	5	4

The values from Table 5 are plotted in the risk matrix below.

Table 6 - Example of how the output from the PHA is plotted in the risk matrix. Note that the plotted values are purely random and have nothing to do with other parts of this thesis.

		Importance				
		1	2	3	4	5
Urgency	5	0,5	1 0,6	0,7	0,8	0,9
	4	0,4	0,5	0,6	0,7	5 0,8
	3	0,3	0,4	2 0,5	0,6	0,7
	2	0,2	0,3	0,4	0,5	0,6
	1	0,1	4 0,2	0,3	3 0,4	0,5

The significance factor for each claim can now be read in the cells of each respective claim. The output from the risk matrix is summarized in Table 7. It is important to understand that the scale visualizing the claim significance is in no way absolute but rather relative. The idea is to rank claim significance by comparing claims toward each other. What this means is that what can be read from Table 7 is that claim 5 is the most and claim 4 is the least significant for overall system safety in relation to each other.

Table 7 - The claim significance output from the risk matrix summarized.

Claim	Claim significance
1	0,6
2	0,5
3	0,4
4	0,2
5	0,8

The next chapter will describe how visualization of the data produced through the risk matrix is to be done.

5 Communicating the result from the evolved SQAD methodology

The purpose of this chapter is to present a way to visualize and communicate the result from a SQAD analysis produced through the method presented in chapter 4.7. The purpose is to enable effective communication of the result for use as a basis for decisions regarding system safety and quality development.

5.1 What to communicate

The purpose is to communicate the result from a SQAD analysis for a certain system. The data sets communicated will be separated between when the system is under construction and when the system has been taken into operation. This shouldn't present any problems though as there is no need to compare the SQAD results of a system under construction with the same system when taken into operation.

5.2 Method requirements

To produce an effective way of communicating the SQAD results a number of requirements needs to be fulfilled. The goal is to allow for comparison between claims for an entire SQAD regardless of which area the claim belong to. It is thus favorable if the method could handle a large number of claims in the same data set.

The same methods will be applicable to both systems under construction and systems taken into operation, as the methods for conducting the analysis are the same even if the results aren't comparable. For both scenarios claims that are unfulfilled needs to be compared to claims that are already fulfilled and vice versa. If this could be solved without having to do two separate visualizations, one for fulfilled and one for unfulfilled, it would be preferable. The hope is that the concept of urgency will take care of this automatically, as an unfulfilled claim that needs to be fulfilled soon will receive a high urgency factor. The whole idea of introducing the time perspective into the urgency factor is to make it possible for claims of lower importance and high urgency factor to be prioritized over more important claims with low urgency.

5.3 Possible methods

In this sub chapter proposals of possible methods for visualization will be presented.

5.3.1 The risk matrix

The risk matrix used for plotting of the output from the PHA is in itself a method for visualization of claim significance. It offers a good overview of claim significance as long as the amount of claims is held to relatively small number. If too many claims are plotted in the same matrix it would probably become cluttered and hard to overview. The method could be a good way to visualize all claims within one area.

The risk matrix offers a feature that could be useful if more weight want to be put on one evaluation factor than the other. For example if it is decided that urgency plays a more important part than importance the weight can be shifted by either rearranging the claim significance values in the cells of the matrix. Or as shown in Table 8 introduce color grading that shift weight to urgency and makes it more influencing on the result. This is an interesting aspect that may be useful in some conditions but it won't be investigated further in this thesis as it falls outside the main assignment of the thesis.

Table 8 - Example of how the weight of urgency can be shifted so that it becomes more important than importance when determining claim significance.

		Importance				
		1	2	3	4	5
Urgency	5	0,5	1 0,6	0,7	0,8	0,9
	4	0,4	0,5	0,6	0,7	5 0,8
	3	0,3	0,4	2 0,5	0,6	0,7
	2	0,2	0,3	0,4	0,5	0,6
	1	0,1	4 0,2	0,3	3 0,4	0,5

5.3.2 Radar chart

A radar chart is a graphical presentation method for displaying several different factors relating to the same item. In this case different claims related to the same case or area. The benefit of a radar chart is that a large number of data points can be plotted without the chart being overwhelmingly cluttered. It is also effective if it is desirable to highlight certain data points that diverge much from the rest. Figure 7 shows an example of how visualization could be achieved with a radar chart. The data plotted is the same as in previous examples.

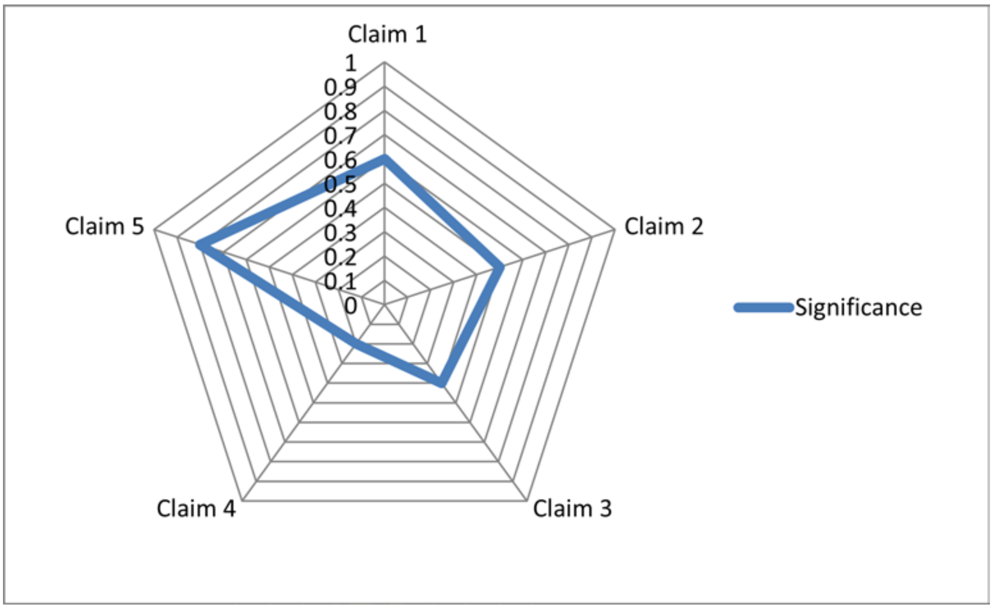


Figure 7 - Example of how a radar chart could visualize claim significance.

In the chart above it is clearly visible how claims can be compared to each other and it's easy to see that claim 5 stands out regarding its significance. This is the main benefit of a radar chart; it makes it possible to easy highlight claims with a higher significance grade than the rest so that effort can be put were it is needed.

The method developed are supposed to enable comparing of both fulfilled and unfulfilled claims in the same analysis and presented in the same visualization chart without explicitly specify which claims are fulfilled or not. The whole idea behind introducing claim significance as a variable depending on importance and urgency are that a fulfilled claim with high importance can be considered more significant than unfulfilled one with low importance and low urgency. Therefore no method for highlighting or separating fulfilled and unfulfilled claims will be introduced in the visualization.

5.4 Choice of method

Which method presented in 5.3 is best for integration in SQAD is hard to decide as both got potential and are suitable for different purposes. The risk matrix is suitable for small number of claims e.g. claims from the same area and when it is useful to be able to shift how importance and urgency are weighted together. However the method may not be suitable for large numbers of data points and are thus not good for visualizing many claims in the same chart. If this is to be done the radar chart is a better alternative. The radar chart also visualizes claims that protrude regarding claim significance in an over viewable manner.

The conclusion is that both the risk matrix and the radar chart are interesting methods for visualization and will both be suggested for integration in SQAD. They are believed useful for different purposes and how they are utilized may vary after demands. Their usability will both be demonstrated in chapter 6.

6 Demonstration of evolved methodology by conducting case test

This chapter aims at demonstration the evolved methodology by conducting a mini SQAD-analysis. The demonstration case was conducted with an engineer from *Solvina* with previous experience from SQAD and that were involved in the SQAD-analysis conducted in the TWICE-project at Ringhals power plant. The purpose is at first hand to demonstrate the evolved methodology but also to test the method and at the same time ask critical questions and raise a debate about the functionality of the method developed.

6.1 Demonstration target

As a target for demonstration and testing, four claims have been constructed. The claims originate from four actual claims from four different areas from the TWICE-project mentioned earlier. This also gives a good picture of how actual claims from an actual SQAD-analysis could look like.

The claims selected for this demonstration are the following:

1. Processes, strategies and plans have been defined that encompass the project scope and the complete life cycle
2. Design/V&V and change handling processes and plans, provide assurance that the Assumptions, Preconditions, Design Basis and Requirements (APDB&Rs) for all products will be completely and correctly implemented.
3. The Plant I&C (Instrumentation and Control) System in nuclear power plant has been qualified also from a HFE (Human Factors Engineering**)** aspect.
4. It has been assured that an organization with required competence to safely operate, maintain and modify R2 Plant is completely and correctly in place.

The following is a short description of what the claims mean:

Claim 1: This claim handles the aspect that a complete set of processes, strategies and plans have been defined to handle the complete scope of works over the whole project life cycle. When applied in this example to when the system is in operation (post project) it is estimated as if it was aiming at the normal processes, strategies and plans for the plant operation – this was not the case in reality; it is only for illustration here.

Claim 2: The purpose of this claim is to ensure that the design control process (design process, validation & verification plans and change handling) is specific and good enough to assure proper design and to maintain achieved qualification. This claim is only interesting during the project phase of a system but similar claims could be established for systems taken into operation as well

Claim 3: The purpose of the project was to replace all analogue plant control systems with digital systems, this included designing a complete new control room with control panels that the operators work with. The goal was to design the new control panels so that they resembled the original ones as much as possible including how they communicate with the operator (indication and controls). Claim 3 ensures that this is done correctly and also ensures that qualification of the control room ability to proper man/machine functionality and performance are maintained.

Claim 4: This claim states that proper measures have been taken to ensure that maintenance and engineering have received proper training and achieved the competence required to carry out their task.

6.2 Demonstration preconditions

The preconditions for the demonstration are that the example project is seen as an isolated project where no other projects or events can influence the claims stated. This is an assumption made to simplify the evaluation process. In reality certain claims would be affected by for example other ongoing projects or events in relation with the current or other projects. Furthermore, in reality a SQAD would be done by multiple persons with different expertise. The demonstration however is performed by a single person and only based on first estimates in order to demonstrate the method as such. The resulting "values" are thus not a valid representation of the real status – they are more for illustration purposes of the methodology.

The evaluation is done from two scenarios "project scenario" where the system is under construction and the "system in operation scenario".

6.3 How the demonstration was conducted

The evaluation was conducted in collaboration with an engineer from *Solvina* that conducted the SQAD in the TWICE-project. The work flow in 4.7 was used as a guide when doing the evaluation, in this way the work flow itself could be evaluated. Other factors evaluated were:

- The scaling of the urgency and importance factors
- How evaluating plausibility and exigency to establish the urgency factor was working

The demonstration was conducted for the two scenarios "system during project phase" and "system taken into operation". The scenario "system during project phase" was divided into three blocks or "project phases", each representing a different stage in the project. The three blocks are:

1. FAT – Factory Acceptance Test is the stage where parts and system components have been manufactured by the contractor and are claimed qualified through V&V (Verification & Validation) sufficiently for shipping to site by the manufacturer.
2. Installation phase – In this phase the system components tested during FAT are installed in the plant.
3. Complete "system in plant" test phase – In this phase the entire system has been built and is set into operation under controlled conditions. The system may be working but could have minor flaws that are to be resolved.

The urgency factor was estimated for each of the blocks above. The reason for dividing the timeframe as above was to demonstrate the methods potential to work as a tool for continuous safety/quality improvement throughout an entire project. In reality the analysis would probably have been performed several times more.

In the scenario "system taken into operation" the corresponding analysis was performed with three different timeframe perspectives. This was done to illustrate different possibilities where the method could be used (evaluating the present year of operation – "now" and evaluating for a few years forward). This may be the way the method will be applied when realized.

6.4 The demonstration

6.4.1 The method for estimating claim significance

The demonstration was conducted in two steps, one for the scenario "system under construction" and one for the scenario "system taken into operation".

Systems under construction

In Table 9 below the importance and urgency that were estimated have been noted. In the cells containing the urgency factors both the estimated Strength of Evidence and the urgency factor after adjustment are noted. The first value is the SoE and the second the urgency after adjustment by exigency.

While conducting the analysis a question was raised regarding how the grading is done. It was found that grading the claims after a fixed scale was hard and that the analyst intuitively rather wanted to grade the claims toward each other instead. As a result of this the values inside the brackets in Table 9 emerged. The value outside the brackets is the estimated importance/urgency factor. It was found however that certain claims could be considered as more important/urgent than others even if they fitted in the same description. The value inside the brackets is thus to be seen as a complementing value if it would show that multiple claims would receive the same significance. This isn't supported in the method as described earlier and cannot be visualized with the method presented. It is an important aspect though and needs to be investigated further.

Table 9 - The actual values evaluated for the scenario "system in project phase"

		Urgency		
Claim	**Importance**	**FAT**	**Installation phase**	**Complete system test phase**
1	1(-2)	4 → 3	3(-4) → 4(-5)	2(1) → 2(1)
2	3(-4)	3 → 4	1(-2) → 1(-2)	1 → 1
3	3	3 → 2	2 → 3	2 → 3
4	3	5 → 2	2 → 2	2 → 2

As seen in Table 9 the importance factor is set only once for the entire project but the urgency once for every project phase. The urgency is determined by first estimating the Strenght of Evidence (value left of the arrow) which is then adjusted by exigency into the urgency factor (value right of the arrow).

An example of how the urgency shifts: During FAT the SoE for claim 3 is estimated to a 3 but adjusted to 2 because it is believed that enough time exists to fulfill the claim in time. In the next phase the SoE is set to 2, the claim is closer to fulfillment but it upgraded to a 3 in urgency because even if the claim is near fulfillement it is near deadline and a possibility of delay exists.

Systems taken into operation

Table 10 below shows the values estimated for system in operation. The analysis was divided into three time intervals; "this year" "1-3 years" and "5 years and more". How these intervals were chosen have no connection to how an analysis would be done in reality, it was only selected to demonstrate the method. In reality the intervals would have been chosen with regards to conditions around each specific case or claim. During the analysis the same wish to compare claim urgency toward each other emerged.

Table 10 - The actual values evaluated for the scenario "system in operation phase"

		Urgency		
Claim	**Importance**	**This year**	**1-3 years**	**5 + years**
1	1(-2)	2 → 3	3 → 2	4 → 2
2	3(-4)	3 → 4	2 → 2	2 → 2
3	3	3(4) → 4	2 → 2	1(2) → 1(2)
4	3	1(2) → 1(2)	1 → 1	1 → 1

Just as with the "system under construction"-scenario importance is set once for the entire period and urgency for each time frame.

It's important to understand that the analysis for "system in operation" the analysis for all three time frames are done in the same time and the second and third time frames are forecasts made on information currently available.

6.4.2 The method for visualization

As mentioned above a tendency to compare claims toward each other when estimating importance and urgency emerged and as this is not supported by the method previously presented for visualization it has not been any attempt to integrate this in the evaluation. A discussion about the need to integrate this feature has been made though.

Systems under construction

The importance and urgency factors for the scenario "systems under construction" have been plotted in Table 11 - 13 below. The values plotted are the ones that are outside the brackets in Table 9. The values have then been plotted in a radar chart in Figure 8.

Table 11 - The importance and urgency estimated for FAT phase, plotted in a risk matrix for visualization of claim significance.

		Importance				
		1	2	3	4	5
Urgency	5	0,5	0,6	0,7	0,8	0,9
	4	0,4	0,5	2 0,6	0,7	0,8
	3	1 0,3	0,4	0,5	0,6	0,7
	2	0,2	0,3	3,4 0,4	0,5	0,6
	1	0,1	0,2	0,3	0,4	0,5

Table 12 - The importance and urgency estimated for installation phase, plotted in a risk matrix for visualization of claim significance.

		Importance				
		1	2	3	4	5
Urgency	5	0,5	0,6	0,7	0,8	0,9
	4	1 0,4	0,5	0,6	0,7	0,8
	3	0,3	0,4	3 0,5	0,6	0,7
	2	0,2	0,3	4 0,4	0,5	0,6
	1	0,1	0,2	2 0,3	0,4	0,5

Table 13 - The importance and urgency estimated for complete systems test phase, plotted in a risk matrix for visualization of claim significance.

		Importance				
		1	2	3	4	5
Urgency	5	0,5	0,6	0,7	0,8	0,9
	4	0,4	0,5	0,6	0,7	0,8
	3	0,3	0,4	3 0,5	0,6	0,7
	2	1 0,2	0,3	4 0,4	0,5	0,6
	1	0,1	0,2	2 0,3	0,4	0,5

In Figure 8 the significance factors from the three risk matrcices above have been plotted in the same radar chart. The chart gives a good view of how claim significance differs between claims, it is e.g. clear that claim 2 stands out during FAT. It is also evident how the signifiance transforms between project phases.

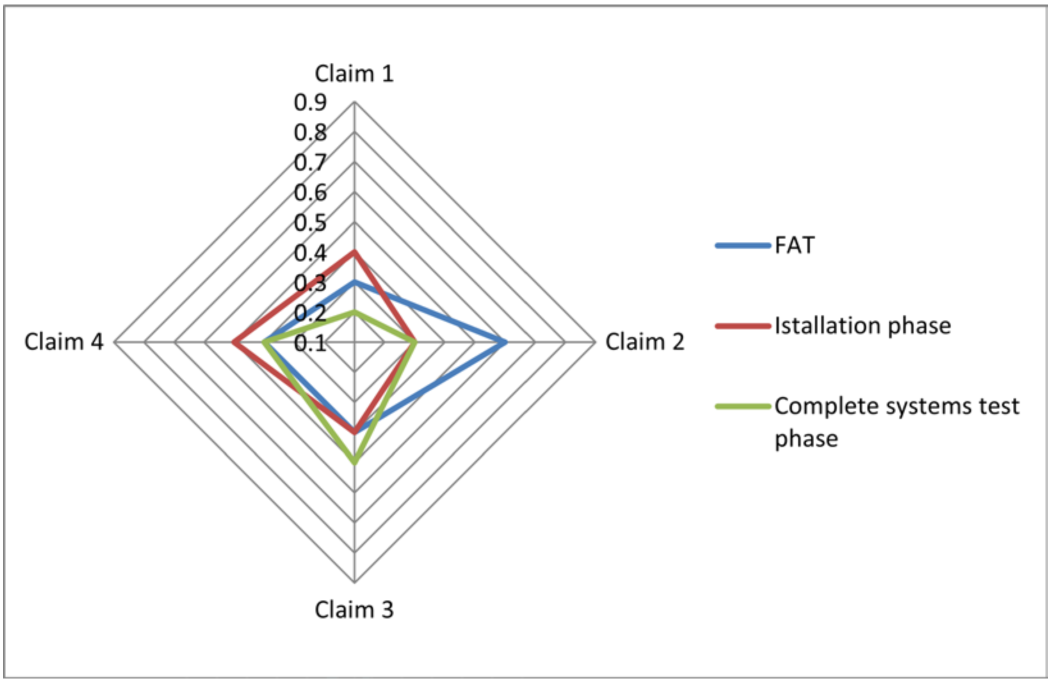


Figure 8 - The significance factors from all three analyses from scenario "system under construction" plotted in the same radar chart.

System taken into operation

The importance and urgency factors for the scenario “systems under construction” have been plotted in Table 14- 16 below. The values plotted are the ones that are outside the brackets in Table 10.

Table 14 - The importance and urgency estimated for "this year", plotted in a risk matrix for visualization of claim significance.

		Importance				
Urgency		1	2	3	4	5
	5	0,5	0,6	0,7	0,8	0,9
	4	0,4	0,5	2,3 0,6	0,7	0,8
	3	1 0,3	0,4	0,5	0,6	0,7
	2	0,2	0,3	0,4	0,5	0,6
	1	0,1	0,2	4 0,3	0,4	0,5

Table 15 - The importance and urgency estimated for 1-3 years, plotted in a risk matrix for visualization of claim significance.

		Importance				
Urgency		1	2	3	4	5
	5	0,5	0,6	0,7	0,8	0,9
	4	0,4	0,5	0,6	0,7	0,8
	3	0,3	0,4	0,5	0,6	0,7
	2	1 0,2	0,3	2,3 0,4	0,5	0,6
	1	0,1	0,2	4 0,3	0,4	0,5

Table 16 - The importance and urgency estimated for 5+ years, plotted in a risk matrix for visualization of claim significance.

		Importance				
Urgency		1	2	3	4	5
	5	0,5	0,6	0,7	0,8	0,9
	4	0,4	0,5	0,6	0,7	0,8
	3	0,3	0,4	0,5	0,6	0,7
	2	1 0,2	0,3	2 0,4	0,5	0,6
	1	0,1	0,2	3,4 0,3	0,4	0,5

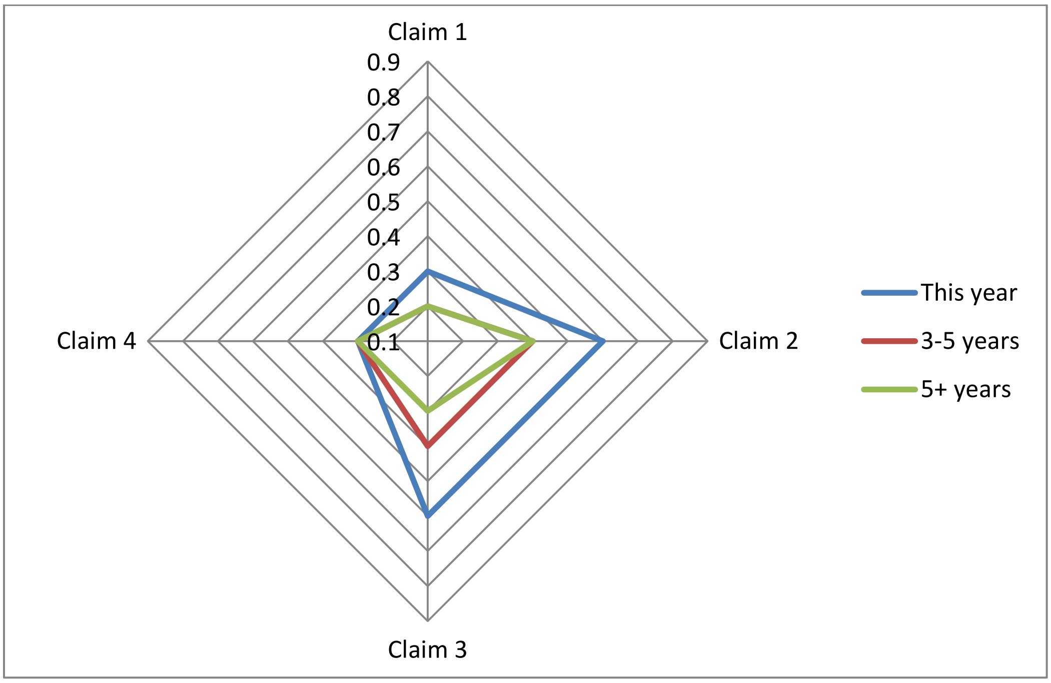


Figure 9 - The significance factors from all three analyses from scenario "system taken into" plotted in the same radar chart.

6.5 Conclusion of demonstration

The demonstration generally showed that the method manage to do what it is supposed to. The grading of the importance and urgency worked as intended apart from the fact that it in some cases were hard to determine which importance class to assign to claims that fitted in the same description but still were of different importance. The most obvious solution to this would be to introduce more classes or to refine the descriptions to each respective class. This is not believed to be the best solution though as the method is meant to be quick and easy and adding more classes and criterions may render in a more complex methodology. Another solution would be to introduce a possibility to rank claims towards each other instead of after a fixed scale but this would require a complete rethink of the entire methodology presented in this thesis and is therefore not an option at this point. The solution in the demonstration example was a variant to the second option; if several claims needed to be separated regarding to importance they were assigned a complementing value within brackets that give the possibility to prioritize between two claims with the same importance/urgency if needed. This value was not included in the visualizations however as it isn't supported by the method but it is still possible to make use of the complementing value. If multiple claims end up with the same significance and prioritizing is needed, it is possible to go back to the tables used when doing the analysis to see if any claim has a secondary value that can be used for prioritization.

Visualization by using the radar chart is also believed to be a good choice as it offers possibility to both compare claim significance between different claims but also a possibility to see how significance changes between project phases. The risk matrix also prooved to be useful as a method for visualization as it offers a quick way to give a good overview of which claims stands out regarding significance.

7 Conclusion and discussion

In the beginning of this thesis a goal and three problem formulations were formulated. The question is now: has the goal been reached and have the problems been solved? The answer is: In a broad sense, yes. This thesis has showed that it is possible to integrate recognized risk analysis methods into the SQAD methodology to produce a result that grades claims after significance. A major strength of the evolved SQAD is its applicability to both systems under construction and taken into operation. To enable this it is important to encourage analysis of claim significance in an ongoing process instead of just proving claims fulfilled or not, and when fulfilled leaving them at that. This is where the evolved SQAD differs from a traditional Safety Case and this make SQAD a potentially powerful tool for safety and quality improvement in systems taken into operation.

The method chosen for visualization of the result show satisfying results as they offer a fairly uncomplicated way of presenting the analysis and pinpointing claims that needs to be addressed. The visualization part of the thesis is quite uncomplicated though as the difficult part is to know if the analysis itself produce results that are usable and reliable enough. This is believed to have been accomplished in the evolved methodology suggested in this thesis. It has been showed in this report that basic risk assessment tools can be utilized to evolve SQAD in the desired direction. As a prerequisite for the thesis was to use established methods for risk analysis to solve the problem, no other possibilities for reaching the goal have been investigated. It is believed though that the chosen method inspired from the preliminary hazard analysis is a good choice for evolving SQAD and the results are satisfying. Of course the evolved methodology shows some shortages and further work need to be done to establish the evolved SQAD as a fully functional methodology. For example a real evaluation of the methodology would need to be done on an actual case. Also the problem of choosing which importance and urgency class to apply to different claims discussed in chapter 6 needs to be addressed. In chapter 4.3 one requirement listed is “Allowing for analysis of how risk propagates in the entire case”. This is an important feature that enables the analyst to foresee how a possible poorly proven claim made early in the process could affect the outcome of the entire case. This requirement has not been fulfilled in the proposed method but is seen as an important feature that should be further investigated.

Altogether the result of this thesis is believed to be a good starting point for further development of the SQAD-methodology into a method generally applicable to any industry where safety and quality are of great importance. Even if SQAD only have been used in nuclear power related projects this far, there aren’t any obvious reasons that the evolved methodology would not work in other applications. Safety Cases are used in broad array of industries and applications but the approach is the same so applying the evolved SQAD to any application shouldn’t be a problem.

8 Further work

During the work on this thesis ideas have emerged that could be of interest to SQAD but that hasn't been further investigated in this report. The purpose of this chapter is to give suggestions for ideas for further work.

During the evaluation of the method it became apparent that a need exists for comparing claims toward each other when estimating importance and urgency. A couple of methods have been identified that could be investigated to address this shortcoming. Fuzzy logic and value tree objective hierarchy are two interesting theories that may be applicable in SQAD. Fuzzy logic is an extension of logic theory that deals with approximations rather than accuracy. When classical logic theory only handles binaries (0 and 1), fuzzy logic handles values that ranges from 0 to 1. How this can be applied to preliminary hazard analysis is described in (Klim, 2004).

The value tree objective hierarchy is a method for ranking "risks" or unwanted events that is a part of a larger hierarchy by grading the events in the bottom of the hierarchy from 0-1 in such a way that the sum of the grading equals 1. The entire purpose of this is to rank events toward each other without using a fixed scale. The method is described in (Apostolakis & Lemon, 2005) and (Pöyhönen & Hämäläinen, 2000)

While determining what method to use for quantification of importance and urgency to use PHA was chosen but it was also established that checklists could be of interests for SQAD, mainly as a help for the analysts to ask the right questions during the analysis and to structure the work flow. An interesting paper was found during the project that addresses the same topic written by the Swedish Nuclear Power Inspectorate (Dahll, Liwång, & Wainwright, 2006)

9 Bibliography

Apostolakis, G. E., & Lemon, D. M. (2005). A screening Methodology for the Identification and Ranking of Infrastructure Vulnerabilities Due to Terrorism. *Risk analysis, VOL 25, No. 2*, 361-376.

Bishop, P., & Bloomfield, R. (1998). *A Methodology for Safety Case Development.* London: Adelard.

Bloomfield, R., & Bishop, P. (2010). Safety and Assurance Cases: Past, Present and Possible Future – an Adelard Perspective. *Making Systems Safer: Proceedings of the Eighteenth Safety-Critical Systems Symposium* (pp. 51-67). Bristol, UK: Springer.

Dahll, G., Liwång, B., & Wainwright, N. (2006). *Safety Justification of Software Systems, Software Based Safety Systems.* Stockholm: Swedish Nuclear Power Inspectorate.

Davidsson, G. (2003). *Handbok för riskanalys.* Karlstad: Statens räddningstjänst.

Dyadem. (2004). *Guidelines for failure mode and effects analysis for automotive, aerospace, and general manufacturing industries.* Ontario: Dyadem Press.

HM Nuclear Installations Inspectorate. (2008, 12 05). *Health and Safety Executive.* Retrieved 09 02, 2010, from Relicensing the Atomic Weapons Establishment Sites to AWE plc: http://www.hse.gov.uk/nuclear/awe/awe00-12.htm

IAEA. (2008). *International Atomic Energy Agency.* Retrieved 11 21, 2010, from http://www.iaea.org/Publications/Factsheets/English/ines.pdf

Kaplan, S., Haimes, Y. Y., & Lambert, J. H. (2002). Risk Filtering, Ranking and management Framework Using Hierarchical Holographic Modeling. *Risk Analysis Vol. 22, No. 2*, 383-397.

Kelly, T. P. (1998). *Arguing Safety - A Systematic Approach to Managing Safety Cases.* York: Department of Computer Science, University of York.

Klim, Z. H. (2004). Preliminary hazard analysis for the design alternatives based on fuzzy methodology. *NAFIPS 2004. 2004 Annual Meeting of the North American Fuzzy Information Processing Society*, (pp. 46-50).

Malmkvist, K. (2008). *Riskhanteringsprocessen på OKG AB.* Lund: Department of Fire Safety Engineering, Lund University.

Ministry of Defence. (2007). Safety Management Requirements for Defence Systems Part 2: Guidance on Establishing a Means of Complying with Part 1. *Defence Standard 00-56.*

Nystedt, F. (2000). *Riskanalysmetoder.* Lund: Department of Fire Safety Engineering, Lund University.

Pöyhönen, M., & Hämäläinen, R. P. (2000). There is Hope in Attribute Weighting. *Information Systems & Operational Research, Vol 38, No. 3,*, 272-283.

Rausand, M. (2005, oktober 7). *Norwegian University och Science and Technology.* Retrieved 03 11, 2011, from ROSS Gemini Centre NTNU/SINTEF: http://www.ntnu.no/ross/slides/pha.pdf

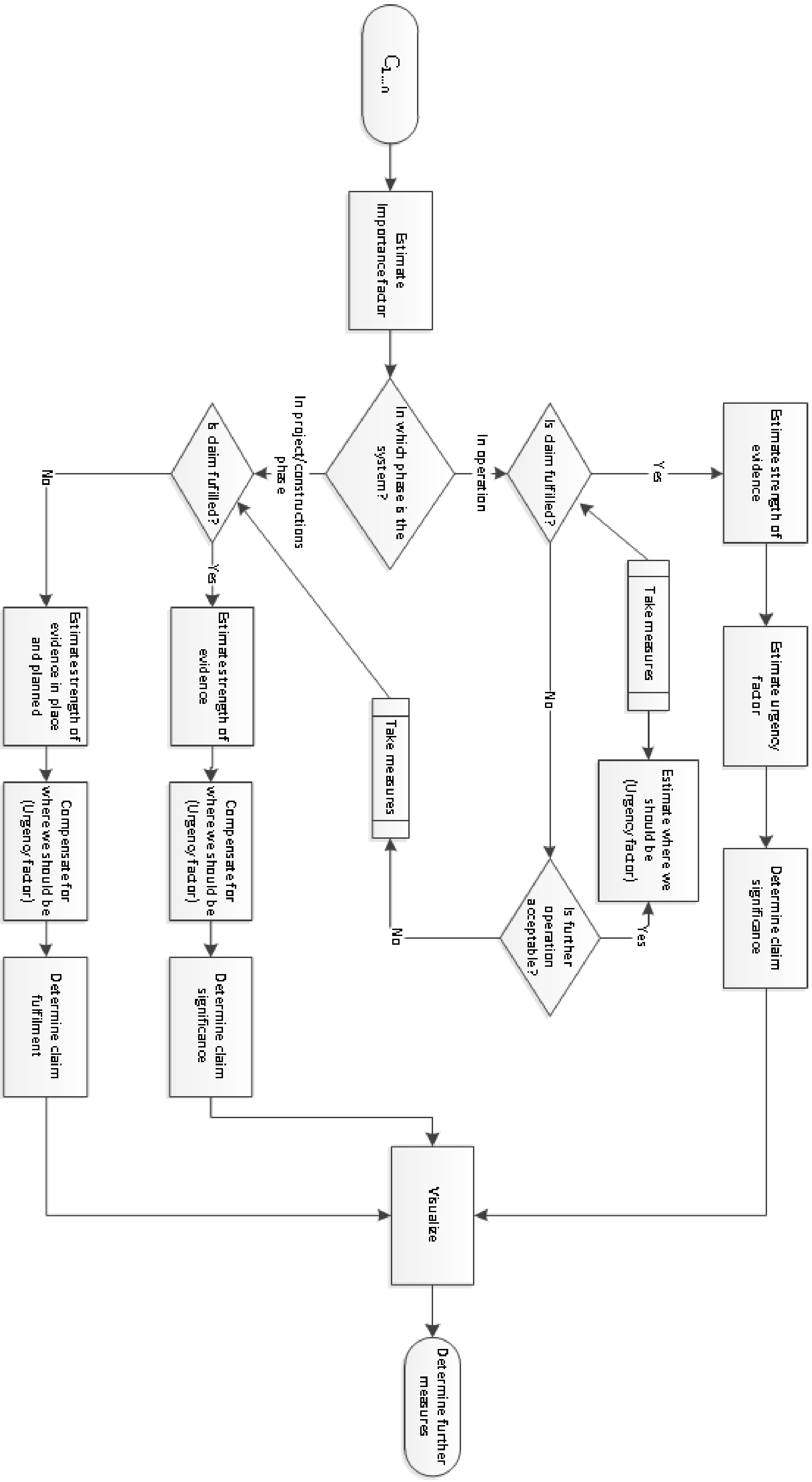
Roland, H. E., & Moriarty, B. (2009). *Preliminary Hazard Analysis, in System Safety Engineering and Management, Second Edition.* Hoboken, NJ, USA: John Wiley & Sons, Inc.

Ryd, P., & Knutsson, A. (2010 йил November). Concluding on Plant Safety and Functional Reliability based on Safety Case Assessments with Configuration Management and Requirements-Solution-Verification Evidence. *Nuclear Power Europe.* Amsterdam.

Zotov, D. (2007). *Moving From SMS to Safety Case.* Retrieved 03 11, 2011, from Australian Society of Air Safety Investigators: http://asasi.org/papers.htm

Appendix 1 – The Safety Subject Areas of the TWICE project SQAD

1. Scope capture, Safety Categorization and System Definitions
2. Quality Assurance (QA/QC/QI)
3. Processes, Strategies and Plans (TWICE Specific)
4. Assumptions, Preconditions, Design Basis & Requirements (APDB&Rs) Identification
5. Regulations, Codes, Standards & Guidelines (RCS&Gs)
6. Solution –System Architecture, Functional, System and Detailed Design
7. MCR/HSI/MMI/HFE
8. V&V (Validation and Verification) of Plant I&C (Instrumentation and Controls) System
9. Base Product Qualification
10. Plant Installation
11. Plant Documentation
12. Organization and Competence Assurance
13. Integration in Plant
14. Operation, Maintenance and Modifications


C1...n
Estimate Importance factor
In which phase is the system?
In project/constructions phase
In operation
Is claim fulfilled?
Yes
No
Estimate strength of evidence
Estimate urgency factor
Determine claim significance
Take measures
Estimate where we should be (Urgency factor)
Is further operation acceptable?
Yes
No
Take measures
Is claim fulfilled?
Yes
No
Estimate strength of evidence
Compensate for where we should be (Urgency factor)
Determine claim significance
Estimate strength of evidence in place and planned
Compensate for where we should be (Urgency factor)
Determine claim fulfilment
Visualize
Determine further measures

Appendix 2 – The SQAD workflow

Appendix 3 – Solvina's scale for establishing consequence in PHA

Consequence class	Description
1	System/function is a support function. Requirements exist for function, but repair or exchange under operation is possible.
2	System/function is only required during startup or similar. Can be replaced with costly technical repair/replacement. Important info/automatic function is lost. Downtime/disturbance <4 hours. Economic impact of <1million SEK.
3	Situation that is required to be reported to authorities arise. Requires high maintenance, complex, long troubleshooting. Some production reduction as a result from loss of function. Downtime/disturbance 4 hours - 1 day. Economic Impact> 1million SEK.
4	INES 1 Reduced operation as a result of system malfunction. Downtime / disruption 1-5 days. Economic impact of> 5 million SEK.
5	≥INES 2 Serious security/production disruption Economic impacts> 15 million SEK.