STS 09 023
Examensarbete 30 hp
Juni 2009

Managing quantitative requirements in system safety

A generalization based on three application domains

Andreas Kristensson

UPPSALA
UNIVERSITET

Teknisk- naturvetenskaplig fakultet
UTH-enheten

Besöksadress:
Ångströmlaboratoriet
Lägerhyddsvägen 1
Hus 4, Plan 0

Postadress:
Box 536
751 21 Uppsala

Telefon:
018 – 471 30 03

Telefax:
018 – 471 30 00

Hemsida:
http://www.teknat.uu.se/student

Abstract

Managing quantitative requirements - A generalization based on three application domains

Andreas Kristensson

Combitech is an independent service company providing technical consultancy in system safety and the part commissioning this project. Dealing with system safety is often an issue of providing requirements in order to prevent the system from constituting danger. System safety also handles the issue of defining requirements to ensure that a pre-defined risk level is satisfied. The risk level is often set by legislative organs with the purpose to ensure that the system is safe enough. When the risk level is communicated in numbers i.e. quantitative requirements, a consequential issue is to provide a logic and consistent methodology. The objective of this thesis is to find an adequate and general approach for the management of quantitative requirements in three different domains.

This study involves a multiple case study, in which three domains have been taken into account; railway signaling industry, the air traffic management industry and the defense industry. The used material primarily consists of documents, investigations and standards although a small series of interviews is performed.

The study resulted in a model partly conveyed in an UML activity diagram. It was also found that most methodologies require substantial data input, which is what seems to be the main problem in the process of managing quantitative requirements.

Keywords: system safety, quantitative requirements, UML, Air Traffic Management, Railway signaling, defense industry.

Handledare: Christian Martinsson & Jan Espen Presteng
Ämnesgranskare: Anders Jansson
Examinator: Elísabet Andrésdóttir
ISSN: 1650-8319, STS 09 023
Sponsor: Combitech AB, Växjö

Populärvetenskaplig beskrivning

Sen tiden från andra världskriget har människan byggt alltmer avancerade system som idag ofta är att beteckna som stora och komplexa. Att hantera ett komplext system är, som namnet antyder, ofta svårt och det finns ofta inte någon som har en total överblick över ett sådant system. Då många komplexa system ofta är helt integrerade i samhället påverkar de också människorna som använder det och ibland på ett sätt som kan vara farligt för dessa användare men också för miljön det verkar i. Disciplinen som hanterar denna problematik brukar kallas systemsäkerhet och är ett av sju affärsområden som Combitech i Växjö inriktar sig på.

Det är inte ovanligt att myndigheter försöker ställa krav på att system inte ska utgöra större fara än vad som kan anses brukligt. För att säkerhetsställa att en viss risknivå har uppnåtts i ett system använder sig myndigheter och liknande organ sig ibland av numeriska krav. Såväl metod som krav kan se olika ut beroende på vilken bransch som studeras. Vidare har många stora system olika instanser som är anvariga för systemets olika delar, nivåer eller stadier i dess livscykel. Att alla dessa instanser samarbetar och delar uppfattningen och synen på vad som bör uträttas för att en acceptabel risknivå ska uppnås är därför av största vikt. Idag skiljer sig metoder och standarder, vari detta ofta regleras, mellan olika branscher vilket i sin tur utgör en stor utmaning för de personer som arbetar med numeriska krav.

Arbetet med denna uppsats har utgått från problematiken som Combitech i Växjö ställs inför när kvantiativa krav ska hanteras. Området som studerats är tre industrier; försvarsindustrin, flygledningsindustrin samt tågsignalleringsindustrin. Inom dessa har matrial främst erhållits genom att studera standarder och utredningar men också från intervjuer och korrespondens via mail. Det primära syftet har varit att undersöka möjligheten att bygga en generell modell för hur arbetet med numeriska krav bör genomföras. Sekundära syften har varit att tydliggöra skillnader mellan metoder för hanteringen av numeriska krav men också att undersöka metoderna som hanterar numeriska krav närmare.

För att kunna generalisera de olika angreppssätten från de tre studieområderna har det visat sig nödvändigt att använda en större mängd teori ur böcker och artiklar. Som utgångspunkt har teori för hur systemsäkerhetsarbetet bör genomföras tagits i beaktande. Vidare har det visat sig nödvändigt att utvidga det teoretiska ramverket med modeller och teorier för intilliggande discipliner såsom kravhantering samt systemutvecklingsprocessen. Dock har nyutvecklade systemteorier visat sig extra värdefulla och är i sin tur proijicerade på riskhanteringsprocessen för numeriska krav. Tillsammans utgör dessa det teorietiska ramverket som byggt grunden till den modell som arbetet med denna uppsats resulterat i.

Eftersom de tre branscherna hanterar krav olika har det delvis varit svårt att samanföra dessa i en generell modell. Den främsta anledningen till detta är att möjligheten för olika instanser att fritt välja angreppssätt skiljer sig mellan de studerade områdena. Att det förhåller sig såhär anses vara att de olika branscherna hanterar teknologier som i grunden ger olika förutsättningar för reglerande organ. Eftersom hanteringen av numeriska krav bygger på god tillgång av olycksstatistik blir det ett problem när sådan inte finns att tillgå. Att bättre utnyttja felrapporteringssystem, simuleringar och statisktiska metoder anses därför vara ett sätt för att förbättra precisionen i hanteringen av numeriska krav.

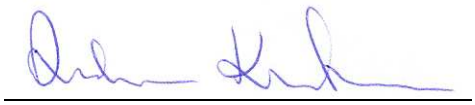
Preface and Acknowledgments

This project is my final course to my master degree in *Sociotechnical systems engineering* at Uppsala University in Sweden. This project was performed at Combitech in Växjö during the spring of 2009. This project was primarily performed for personnel working with system safety at Combitech.

This thesis has partly been written in collaboration with Johan Eklund at Växjo University in Sweden. This co-project is named *A Process for Hazard Identification – An approach to effectively improve inputs to safety requirements*. The result from this cooperation is found only in the first part of this thesis, namely Chapter 1.1, 1.8, 2, 4.1, 4.5, 4.6, 4.7 and 6.1.

I especially want to give my appreciations to the two of my supervisors, Christian Martinsson and Jan Espen Presteng for their superior guidance through the jungle of system safety and for using their extensive network within the field.

I further must highlight the graciousness of Ragnar Ekholm and Arne Börtmark (FMV) for letting me attend the armed forces education in system safety 2009 (67A). This was a first class opportunity to learn about system safety and it became immensely valuable to this project. Finally I would like to thank every one else that have participated in my study by giving me a piece of their time.



Växjö 2009-05-19

Andreas Kristensson
kristensson.andreas@gmail.com

Table of contents

Table of figures

Terminology

The field of system safety exploits an extensive terminology and differs greatly between different fields. In order to make it easier for the reader to follow this thesis the most vital terms will be described. The terminology used in this project is based on different frameworks and is therefore partly customized in order to make it fit together.

To understand what system safety tries to achieve it is important to first understand what it tries to avoid. In brief, system safety tries to prevent injury to personnel and damage to property and the environment, here captured in the term *accident*. What is then an accident and what is its' vital "components"?

The rise of an accident is dependent upon two factors; the probability of a hazard to cause an accident and the exposure to it (Ekholm & Börtemark, 2009). Conversely, an incident is when a hazard occurs and no one is exposed. The risk is the combination of the probability for an accident or hazard to happen and the consequence once it has occurred, sometimes named as the likelihood and the severity. (Leveson, 1995, Swedish Defense Forces, 1996) The terminology is illustrated by Figure 1.

Subsequently, the manageable part is hazards, yielding accidents or incidents. Hence, to a great extent the system safety effort attempts to prevent hazards and hazardous events occurring (Swedish Defense Forces, 1996). Basically, a hazard is a state or situation that could, but not necessarily do, lead to an accident (CENELEC, 1999b, Martinsson, 2007). However, the interpretation valid in this thesis is that a hazard is treated equally to a hazardous event in terms of interpretation.

What causes a hazard is a subject of disagreement among authors. The accident model displayed in Figure 1 is based on a framework from Ekholm & Börtemark (2009) although it has partly been customized. Generally a hazard occurs when a system and its context compose a danger resulting from a risk source combined with a dangerous state and a triggering event (Ekholm & Börtemark, 2009). A dangerous state or triggering event can, in turn, result from a failure. According to Leveson (1995) a failure is defined as:

> *"…the nonperformance on inability of the system or component to perform its intended function"* (Leveson, 1995, page 172)

The SS EN 50129 standard from The European Committee for Electrotechnical Standardization (CENELEC) further states:

> *"…A failure is the consequence of a fault or error in the system."* (CENELEC, 1999b, page 9)

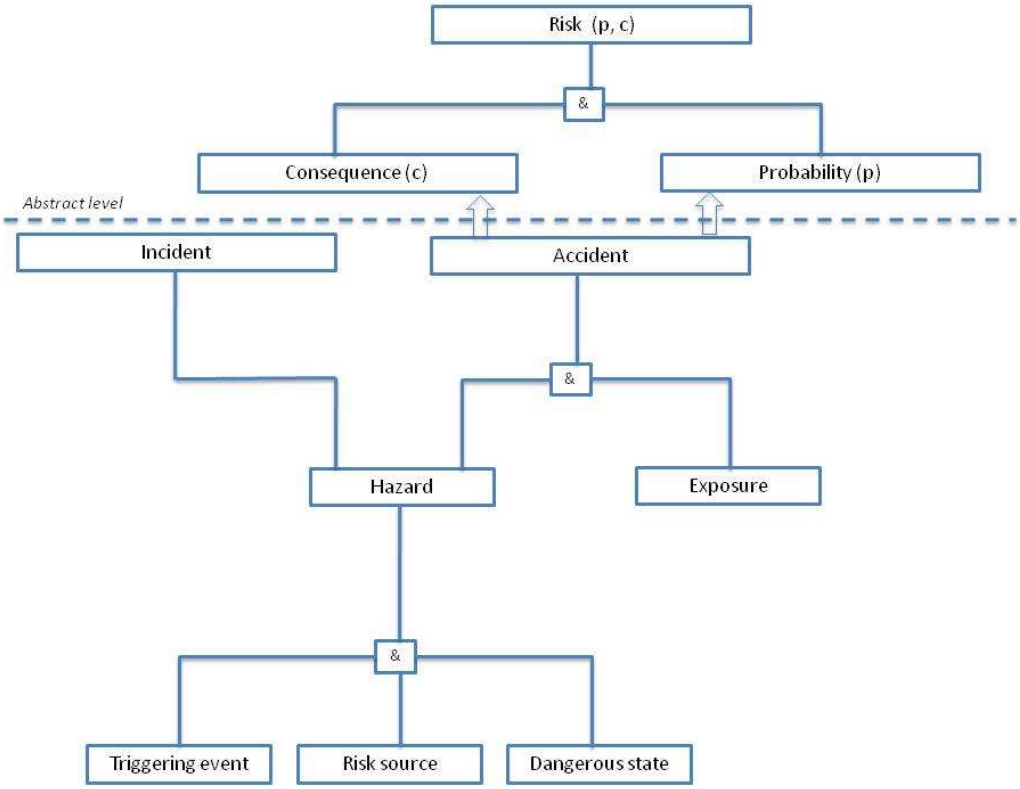


Figure 1 Accident model (Inspired by Ekholm & Börtemark, 2009b)

Abbreviations

Standards and organizations

AFS	The Work Environment Authority's Statute Book
DAU	Defense Acquisition University
DoD	Department of Defense (US)
CENELEC	European Committee for Electrotechnical Standardization
EATMP	European Air Traffic Management Program
EIA	Energy Information Administration
ERA	European Railway Agency
ESARR	EUROCONTROL Safety Regulatory Requirement
EUROCAE	European Organization for Civil Aviation Equipment
EUROCONTROL	European Organization for the Safety of Air Navigation
FM	Swedish Armed Forces
FMV	Swedish Defense Materiel Administration
GEIA Group	group within ITAA
H FordonSäk	Automotive Safety Manual (Own translation)
H SystSäkEE	System Safety Manual of the Swedish Armed Forces
H VAS	Weapons and Ammunition Safety Manual
IEEE	Institute of Electrical and Electronics Engineers
IEC	International Electrotechnical Commission
ISA	Industry Standard Architecture
ITAA	Information Technology Association of America
MIL-STD – 882	DoD Standard Practice for System Safety
SAM	Safety Assessment Methodology

Miscellaneous

ACC	Air Control Centre
AD	Aerodrome
AF	Ambition Factor
ALARP	As Low As Reasonably Practicable
ANS	Air Navigation System
ANSP	Air Navigation Service Provider
APP	APProach
ASM	Airspace Management
ATFM	Air Traffic Flow Management
ATM	Air Traffic Management
ATMSP	Air Traffic Management Service Provider
BPMN	Business Process Modeling Notation
CST	Common Safety Targets
CSM	Common Safety Methods
ETA	Event Tree Analysis
FHA	Functional Hazard Analysis
FMECA	Failure Mode and Effect Criticality Analysis
FR	Functional Requirements
FRACAS	Failure Reporting, Analysis and Corrective Action System
FTA	Fault Tree Analysis
GAMAB	Globalement Au Moins Aussi Bon
HR	Hazard Rate
IRF	Individual Risk of Fatality per hour
I-RILL	Individual Risk In Loss of Lives

MEM	Minimum Endogenous Mortality
MORT	Management Oversight and Risk Tree
NFR	Non Functional Requirements
OHA	Operating Hazard Analysis
O&SHA	Operating and Support Hazard Analysis
PAL	Procedure Assurance Level
PHL	Preliminary Hazard List
PHA	Preliminary Hazard Analysis
PET	Project Evaluation Tree
PSSA	Preliminary System Safety Assessment
QRA	Quantitative Risk Assessment
RAC	Risk Assessment Code
RCS	Risk Classification Scheme
RFP	Request For Proposal
SAR	Safety Assessment Report
SC	Severity Class
SCR	Safety Case Report
SHA	System Hazard Analysis
SIL	Safety Integrity Level
SO	Safety Objective
SOCS	Safety Objective Classification Scheme
SR	Safety Release
SRCA	Safety Requirements/Criteria Analysis
SRP	Safety Requirements Proposed
SRS	Software Requirement Specification
SS	Safety Statement
SSA	System Safety Assessment
SSHA	Sub-system hazard analysis
SSPP	System Safety Program Plan
SSWG	System Safety Working Group
ST	Safety Target
SV	Safety Verification
SWAL	Software Assurance Level
THR	Tolerable Hazard Rate
TIR	Target Individual Risk
TSI	Technical Specification of Interoperability
TSR	Total System Risk
TTFO	Technical Tactical Financial Objective
T-RILL	Total Risk In Loss of Lives
I-RILL	Individual Risk In Loss of Lives
UML	Unified Modeling Language

1 Introduction

This chapter introduce the background and outline for the master thesis. It begins by describing the field of system safety and its interrelated disciplines. Furthermore the purpose and research questions are presented, followed by necessary information when continuing to read the thesis.

1.1 Background

Everything we do is associated with risks and throughout the centuries risks have been controlled and managed by generations of experiences and accumulated knowledge. The last century brought new ways of living and working as a result of the industrialization. The industrialization also introduced ground-breaking technology, which enabled new ways of working and interacting. However, the technology also constituted new, until now, unexpected dangers. New technologies gradually evolved into new, sometimes large-scale, system constructions, such as the railway system. This new socio-technological development often followed an inherent course of events; first, a rather unexploited technology was built into a system and after a few accidents, new regulatory demands and requirements evolved. Typical at that time was the reactive way of eliminating risks rather than the proactive, meaning that an accident first had to happen before safety was considered. (Grimvall, Jacobsson & Thedéen, 2003)

The scientific field of system safety has its roots in industrial safety engineering, referring to the early stages of industrialization, but experienced a fundamental change after World War II. At that time a few new scientific disciplines arose, systems engineering and systems theory, in order to manage new and more complex engineering problems. Prior to those new scientific disciplines advances in systems theory had been made, which constituted the fundament for the new scientific disciplines. One of the first theoretical frameworks, which specifically relates to the field of system safety, was provided by W.H Heinrich when introducing the “domino theory”. This first accident model says that an accident invariably results from a completed sequence of factors caused by an unsafe act or hazard – analogous to a line of dominoes. (Leveson, 1995)

The time after the World War II the majority of business and industry learned that safety at many levels also were good business. At this point several grand-scale projects and systems started which involved higher complexity. Those projects could also cause a serious amount of harm to the society, environment, property, mission and humans in case of an accident. Some apt examples of large-scale projects are the nuclear power, high-pressure systems, the aviation industry and the national defense systems. This development further urged the need for proactive safety methods and analyses in systems engineering. (Leveson, 1995)

System safety is tightly connected to, as mentioned previously, systems engineering and system theory. According to Valerdi & Wheaton (2005), the scope of systems engineering could be summarized as follows:

> *“Systems engineering is concerned with creating and executing an interdisciplinary process to ensure that the customer and stakeholder needs are satisfied in a high quality, trustworthy, cost efficient and schedule compliant manner throughout a system's entire life cycle.”* (Valerdi & Wheaton, 2005, pp 2)

Systems engineering is, in practice, an often comprehensive process involving iterative and recursive problem solving methods. When developing a new system the systems engineering process consequently sets the framework for how to conduct the system safety process as well (Department of Defense, 2001). In other words, the perspective of system safety is closely related to the process of systems engineering but instead it focuses on preventing foreseeable accidents and to minimize the result of unforeseen accidents. Thus, system safety analyses primarily concern the management of hazards, which involves identification, evaluation and hopefully elimination of them (Leveson, 1995).

At the initial state of a system development effort, requirements are defined in order to specify what should be implemented. This action could be called requirements engineering. Requirements serve as the map of how to guide and channel the efforts made by engineers and developers. Hence, analysis of requirements is a crucial part in the commencement of systems engineering and is from that point an integrated part of the system safety process as well (Department of Defense, 2001). The cost of engineering requirements varies from 10 to 15 % of the whole system development cost. (Kotonya & Sommerville, 1997)

Requirements can formulate both what the system should do and how it should be done. In essence there are two types of requirements, functional (FR) and non-functional (NFR), where safety is related to the latter. NFRs give restrictions on the system development, the actual product and specify external constraints. (Kotonya and Sommerville, 1997) The quality of the requirements has a great impact on the rate of success of the development effort, since they affect almost all of the performed activities within system development (Nuseibeh and Easterbrook, 2000, Tsai, Mojdehbakhsh & Rayadurgam, 1997). In order to avoid costly design changes at a later stage, the requirements should be as complete as possible by the start of the development process. However, there are only a limited number of methods that enforce such an approach (Appukkutty, Ammar & Popstajanova, 2005). Instead, requirements are being refined during work iterations of system development, to eventually be verified during the later stages of life cycle development. (Kotonya & Sommerville, 1998).

1.2 Problem discussion

System safety analyses are often part of a system development and deal with requirements, in theory often described as three processes; the system safety process, system development process and the requirements engineering process. In brief, it is important to understand that system safety is not a work separated from its wider context. The larger context of a system development is central in several aspects and implications for the system safety analyses. In addition, constructions of large systems often require several stakeholders to contribute to system safety requirements. Typical stakeholders in one particular industry are: managing authority, customer and system developer/contractor. Due to this interdisciplinary structure there are a wide range of requirements and actors to consider. What also adds to the complexity of the system safety effort is the diversity among different industries when it comes to development techniques, processes and ways to write requirements. Relevant to this study are the defense industry, Air Traffic Management (ATM) industry and railway signaling industry.

Contemplating the background of how to build a safe system a certain complexity of the work structure is easily acknowledged. The process to first define an appropriate risk

level on a system and further refine this requirement or risk level down to specific parts of a system is complex and often lacks logical and measurable means. Nevertheless, from the systems safety engineer's point of view, the approach is to pragmatically achieve this by best effort. How can one then assert a certain risk level over a system? In brief, different domains have attacked the issue differently and in time obtained methodologies or techniques to manifest the safety of a system. Many safety assessment techniques are considered to be bottom-up approaches. However, a top-down approach dealing with how tools and concepts will work together is desirable in order to first settle the overall target level of the risk and further requirements consistent to the requirement on total system level (Drogoul, Kinnersly, Roelen & Kirwan, 2007).

1.3 Problem presentation

Standards describing techniques and methods are tailored to each industry, claiming differences in the effort on system safety engineers. Despite the apparent differences in methods and standards the ways to handle system safety have many common aspects. Therefore, it is interesting to identify such similarities and to explore the methods best suited to match a particular set of circumstances.

There are several different ways to state requirements, and eventually verify them. Those are often divided into quantitative and qualitative methods. The structure of defining, refining and allocating an appropriate risk level is most straight-forward when a quantitative methodology is used but are indeed incorrect due to the fact that numbers do not fully capture a behavior of a system. Furthermore, the behavior of complex system can never be modeled since the dynamics of a system and its parts can never be apprehended within a fully-fledged model (Leveson, 1995, Zio, 2009). Despite the several inconsistencies of a numerical model, the approach has gained a widespread recognition. Although system safety is not a unified methodology the question arises if it is possible to generalize and propose a work structure to manage quantitative requirements in system safety.

1.4 Problem formulation

In accordance to previously presented material the problem formulations for this study are:

- What different methodologies are available today to elicit, refine and allocate quantitative requirements relevant to system safety?
- Is it possible to suggest a general approach, guiding the work on quantitative requirements in system safety and if so, what would such an approach look like?
- What differs among the three industries and what could be learned in order to improve the situation of today?

1.5 Purpose

Today there is no general approach on how to apply, relate to and work with quantitative safety requirements. This is partly due to the fact that different industries follow different standards adjusted to the particular characteristics of their industry. Yet, the methods to handle requirement allocation and refinement are thought to be commensurable on at least a set of different characteristics. Synergy effects from industries and standards are therefore subject to analysis and can presumably be handled cross-sectional, and add to accumulated knowledge and experience on how to handle the problem.

The ambition of this project is to develop, test and validate a model, which structures the process of quantitative requirement formulation and refinement.

1.6 Relevance

The quantitative approach towards risk analysis has during the last centuries gained a widespread credibility not only amongst the high-risk and mature technologies, such as the nuclear industry and the avionics systems, but has lately also interested other areas (Abrahamsson, 2002). Surmising risk numerically is often an arduous task and is always done by best effort (Leveson, 1995). The continuous but cross-sectional development within this area requests the profession to handle different approaches.

Even within a certain industry the problem is sometimes clearly formulated. In the railway industry a manifested deficiency is the process of deriving and allocating a high-level quantitative requirement to system entities. (CENELEC, 2007, European Railway Agency, 2007) The same goes for the armed forces industry. According to Ekholm (2005, 2006) new methods are needed to develop and decide risk budgets, distribute these to underlying sub-systems, and monitor the designers' achievements keeping the TSR (Total System Risk) within these borders. A more general formulation is given by TechAmerica in one of its latest press releases:

> *"ANSI/GEIA-STD-0010, Standard Best Practices for System Safety Program Development and Execution, establishes a consensus definition of system safety and related best practices. The new standard addresses a perceived lack of guidance in how to best meet system safety requirements while also ensuring that any residual risk has been communicated to the end user and procuring authority. This is the next generation standard derived from MIL-STD 882."* (TechAmerica, 2009, page 1)

The focus of this project is primarily to highlight questions relevant to practical work in system safety. High-level quantitative requirements, i.e. by legislative organs, sometimes result in considerable challenges to system safety analysis in the sense of handling and relating to them (Martinsson, 2009).

1.7 Delimitations

The scopes of this thesis will not fully cover the field of system safety but instead it will briefly describe the background of conducting system safety analyses. Furthermore, there are an extensive amount of different methods available when to perform system safety analyses. The meaning of these methods is for this thesis only relevant when it comes to how these methods derive quantitative requirements.

This thesis will be based upon a multiple case study focusing on system safety requirements within three different industries, ATM, defense and railway signaling. Although a suggested process to handle quantitative requirements could indicate possibilities of generalizations (Merriam, 1994), it should be noted that Kotonya and Sommerville (1997) state that a requirement engineering process as a whole, has to be specifically developed to suit a certain company. The viewpoint for this study has been Combitech and their interests. Combitech is active primarily in the aviation industry and the defense industry but has earlier worked with the railway signaling industry. Each of these industries has a well-developed safety culture and in comparison having both similarities and differences. To choose these industries as sources to cover the viewpoint

of Combitech was therefore natural. The possibilities to gather facts and to be able to contact knowledgeable persons thereby increased considerably.

Moreover, this thesis will exclusively handle quantitative requirements, i.e. requirements stated numerically. Further delimitations involve the exclusion of requirements verification and validation. Instead attention is primarily given to issues concerning the requirement elicitation, refinement and allocation process. As a consequence the development life-cycle is not fully covered. Safety methods to discover potential hazardous events will not be covered either.

1.8 Disposition

This thesis has partly been written in collaboration with Johan Eklund at Växjö University in Sweden, whose master thesis is named *A Process for Hazard Identification – An approach to effectively improve inputs to safety requirements.* The result from this collaboration is found only in the first part in this thesis, namely chapter 1.1, 1.8, 2, 4.1, 4.5, 4.6, 4.7 and 6.1. It has been a clear distinction between the projects since this thesis solely considers quantitative methods and requirements.

The structure of this thesis follows general academic principles, where the scope and intentions of the project is declared in chapter 1. Chapter 2 intends to give a thorough description of how to relate to fundamental scientific methodologies and place this project in relation to acknowledged philosophies of science. Chapter 3 aims to give a brief description of systems but also the relation to system safety. This chapter is to be seen as the first part of the theory. Chapter 4 further exploits the systems safety effort and explains the relation to, for example, the requirements process. Chapter 5 extracts relevant theoretical frameworks from Chapter 3 and 4 and further aims to build the theoretical foundation of the model.

Chapter 6 and 7 are the chapters where all the gathered material is presented. Chapter 6 intends to give a description of each domain separately but also to give a description of the methods found, relating to quantitative requirements management. Chapter 7, on the other hand, aspires to evaluate the methods found and described, in chapter 6 by unfolding their pros and cons.

Chapter 8 analyzes the gathered material and put it in relation to the theoretical framework. The chapter highlights the most important characteristics of the industries and discusses their importance in order to extend the theoretical model described in chapter 5 by the collected methods found in chapter 6 and 7. Chapter 9 describes the model and how it could be used which are part of the conclusions made in chapter 10 along with brief answers to the research questions posed in chapter 1.

1.9 Time frame

This table describes the time frame for this study and the sequential distribution of the different activities.

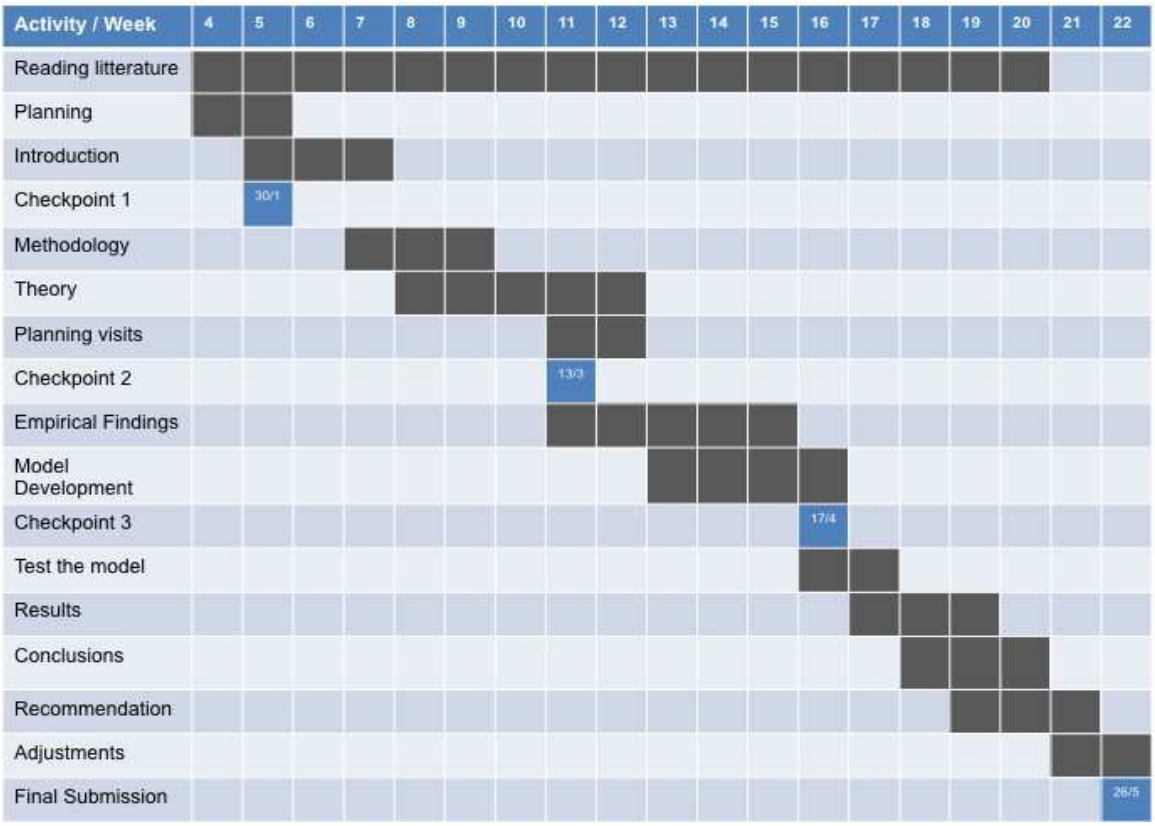


Figure 2 Time frame

2 Method

The following chapter provides a description of the studies' practical approach in relation to available theoretical frameworks. Research design and information about data collection will be treated along with the criteria to achieve a higher level of validity and reliability.

2.1 Scientific approach

The research approach refers to available methodological approaches on how to relate theory and reality in order to draw scientific conclusions. Deduction and induction are the two contrasting and recognized methods (Thurén, 2007). According to Björklund and Paulsson (2003) deduction starts from the theoretical framework and continues to draw conclusions about the empirical findings which are to be verified by collected data. On the other hand, induction first endeavors to discover patterns in reality that can be formulated in theories and models. According to Andersson (1998) the research process sometimes take the form of circular iterations with no distinctive end or beginning from a given research method. The research evolves from questions which are answered by existing theories, to argumentations in empirical findings, which in turn leads to new questions both for theories and empirical findings etc. Oscillating in this way between scientific approaches is captured in the third and additional methodological perspective; the abductive (Björklund and Paulssen, 2003). There is also a fourth method available based on deduction, called hypothetic deduction. (Patel & Davidsson, 2003) The method draws conclusions from theories, which in turn are tested to see if they correspond to the reality. This thesis gathers relevant facts to the model development both from established theories and empirical findings. That approach indicated the use of an abductive method, because it neither starts from a thorough theoretical view nor starts with collecting empirical data in order to relate to acknowledged research, but instead circles between different perspectives. However the model is intended to be tested in reality and that indicates a hypothesis deductive method with an information basis collected through abduction.

2.2 Research design

According to Yin (2003) predominantly four types of case study design alternatives exist. The first distinction to be made is weather to perform a single-case - or a multiple-case study. The multiple-case study can require extensive resources and time and in addition each case should serve a specific purpose within the overall scope of inquiry. Secondly, a case study can be either holistic or embedded. The holistic design of a study examines the global nature of an organization or program while an embedded design give attention to subunits or subsystems, (Yin, 2003). The embedded design may include the collection and analysis of highly quantitative data, including the use of surveys. Salient for the multiple-case study is the attempt to enable replication in order to see if the findings could be reproduced, this in order to see if the original finding could be considered as robust. This logic should also inflict upon the choice of studied cases Yin (2003). Either the studied case predicts contrasting results or similar results. A readily developed theoretical framework is therefore important in order to generalize amongst the cases studied.

Since this thesis study three different industries from one case company's perspective it could be described as a multiple case study. Within each industry only the generic process of requirements is of interest, which suggests the character of a holistic design. Due to this choice of method a rich theoretical framework is needed.

2.3 Data Collection

This section aims to briefly explain how data has been collected and triangulate this over the scientific field of qualitative investigations and case studies. The qualitative method aims at generating a deeper understanding of the problem area through different types of data collection, (Anderson, 1998). Suitable methods to use are e.g. semi-structured interviews, interpreted analyses and different forms of observations. The mentioned methods are all methods to gather primary data i.e. data collected by the researcher himself, while data compiled by others are called secondary data (Anderson, 1998).

To enable transparency and placing this study in a broader scientific context literature studies are preferable. Reviewing literature is needed to deepen the knowledge within the research area and to eventually formulate the problem specific to the study. To achieve this it is important to first understand; previous research (1), existing theory and knowledge (2), relevance of knowledge within the problem area (3), and for selecting research strategy (4) (DePoy and Gitlin, 1998).

2.4 Literature review

According to Merriam (1994) all research should have its' foundation in previously performed research within the area. Merriam (1994) states that the value of a research is to a great existent based upon how it fits into and relates to previous research. It is also important to discuss how a research distinguishes itself from others. A literature study can be divided upon three categories; integrated studies that sum up past research, theoretical reviews focusing on relevant theories and methodological studies that focus on research methods and definitions. However, in practice these methods are often combined (Merriam, 1994). Literature consists of printed material such as books, articles, reports, essays and handbooks etc, (Ejvegård, 2003, Merriam, 1994). It is also important to note that literature is secondary data and to be aware of its eventual biases (Björklund & Paulsson, 2003). This study provides a discussion of how it relates to and distinguishes itself from other studies in section 1.6 Relevance. Data from the literature study will be chosen with consideration to its origins and eventual agenda. The frame of reference for this project will be based on information collected from relevant articles, literature, manuals and standards which are all classified as secondary data.

2.4.1 Observations

When performing case studies multiple data collection methods are often needed. This project is conducted one case company with several cases, which imply observations of the daily work of safety engineers. This environment of social elements could also possibly affect the outcome whereas it is preferable to support the data collections by other methods e.g. cross-checking and interviews. (Yin, 2003)

Observations can be further categorized in direct observations and participating observations. Direct observations can involve observations of meetings and discussion and are often useful in providing additional information about the topic being studied (Yin, 2003).

Participating observations indicate that one take an active role in the events being studied (Yin, 2003). This way of collecting data could involve major problems; when interacting with the environment being studied, in terms of the potential biases produced. In this position, a common phenomenon is to become a supporter of the organization being studied. In addition, participating observations sometimes require too much attention relative to the role as an observer (Yin, 2003). On the other hand, participating

observations also provide opportunities in the ability to gain access to events or groups that are otherwise inaccessible. The usage of direct and participating observations is suitable for this case study due to daily interactions at the workplace. Practicing these methods will be good for the contextual understanding of the studied problem.

2.4.2 Interviews

According to Yin (2003) interviews require the ability to work on two levels at the same time; satisfying the line of inquiry and simultaneously create an open and friendly atmosphere. The more the respondent assists in the above stated efforts the more of an informant he becomes. An informant distances himself from being a respondent by providing insights and to suggest further sources of corroboratory or contradictory evidence (Yin, 2003). Informants are indeed acknowledged to be one of the primary sources of information for this study. During the latter steps of this study a series of semi-structured interviews are held. The semi-structured interview is appropriate when certain empirical and theoretical knowledge exists within the area of research. There often exist a few topics and circumstances for the interview to evolve around which most often are in printed form (Anderson, 1998).

2.5 Scientific credibility in case studies

Scientific researches including qualitative case studies strive for valid and reliable results. These concepts could be achieved by close attention on the method for gathering, analyzing and interpretation of the information. Validity and reliability in case studies could be summed up in this sort of question – to what degree could the researcher trust the results from a qualitative case study? (Merriam, 1994)

2.5.1 Internal and External Validity

In the case of internal validity the question is if the results of a study are coherent with reality and if the scientific researcher measure what is intended (Merriam, 1994). Within qualitative research there are six fundamental strategies that can be used to achieve high internal validity; triangulation, participant control, observation, horizontal review and criticism, participant approach and clarification of reference point (Merriam, 1994). Internal validity will be met by applying following strategies. Triangulation, both theoretical facts and empiric data will come from different sources. Company representatives will read and comment the study throughout the writing process and participate during model testing, which is equivalent to participant control. There will be some observations but not extensive enough to call that strategy fulfilled. Horizontal review will be achieved through continuous discussions with a tutor.

External validity is according to Merriam (1994) realized when a study could be applicable in another context than the original, i.e. how well suited it is for generalization. Merriam (1994) states that it is a prerequisite to first have achieved internal validity in order to make generalizations. On the other hand, internal validity is often achievable in qualitative case studies. A method to increase the possibility of generalization is to include several cases that concern the same issue (Merriam, 1994). The ability to generalize the outcome of this study is increased by the fact that it is a case study and it will examine similar cases in different industries. The execution will be documented and structured to further improve generalization opportunities.

2.5.2 Reliability

The reliability of a study defines to which extent the content could be reproduced (Merriam, 1994). To be able to reproduce a study the authors have to describe the plan of

examination as thorough as possible (Yin, 2003). Further the purpose of reliability is to minimize the number of faults and biases that could evolve. Yin (2003) also states that a good method to meet the reliability goal is to perform the study in a way that enables an opponent to follow the methods and reach the same conclusions.

2.6 Method summary

The scientific approach for this study could be described as a mix between abduction and hypothesis deduction. Due to the consideration of three different cases within the case study the thesis could be described as a multiple case study. Measures taken to improve validity include the use of triangulation and the use of multiple cases within the case study. The gathered data mainly comes from observations, interviews and literature studies which imply that this study is to be described as a pure qualitative. In order to attain a satisfactory reliability and validity the method has been explicitly discussed in chapter 8.6 Method discussion.

3 Introduction to systems and system safety

To understand the basic concepts of the system safety effort the fundamental terminology has to be clarified and explained. The aim of this chapter is to briefly examine the most fundamental terms and put those into the scientific context of system safety and system theory.

3.1 Systems fundamentals

In our everyday life we all interact with and use numerous systems. Systems are a part of our society and are therefore fundamentally integrated even down to a personal level. Some of these systems are rather easy to comprehend but to a greater extent used without any deeper understanding. The word systems are a common word which therefore calls for a definition:

> *"A system is a set of components that act together to achieve some common goals or objectives… The concept of a system relies on the assumptions that the system goals can be defined and that systems are atomistic, that is, capable of being separated into component entities such that their interactive behavior mechanisms can be described…"* (Leveson, 1995, page 137)

According to Zio (2009) modern systems has four basic components: hardware, software, organizational and human. Leveson (1995) further states that the system may have internal subsystems but could also be a part of a larger system. The components that are not part of the systems but whose behavior can affect the system state are defined as the *environment*. The interactions between the system and its sub-system are defined as inputs and outputs which also implicitly define the system boundary. (Leveson, 1995) See Figure 3.

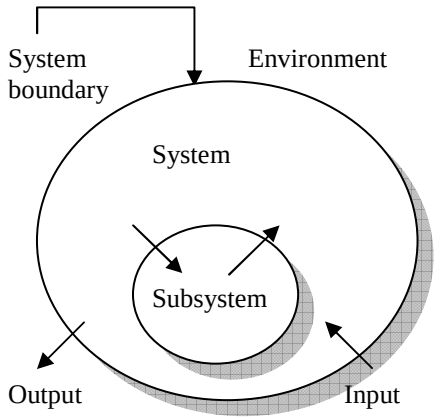


Figure 3 Definition of a system, (Leveson, 1995 Page, 137)

In this thesis the term *system* will be constantly recurring and often in the meaning of *complex systems*. According to Martinsson (2004) complex systems are multi-functional, exhibit an increasing complexity over time and are difficult to survey. An organization exercising several rather complex systems is the Swedish Armed Forces (FM). Future systems operable at FM have to be able to handle several unpredictable tasks in a complex world. According to Ahlin *et al* (2005) complex systems do not only embrace technical artifacts but also organizational aspects such as competence, processes and

information. FM will in the future be regarded as a system, compounded of several integrated sub-systems, with the purpose to meet a specific need or solve a certain task. (Hagström *et al*, 2005)

3.2 Systems theory

The scientific method builds upon the idea of reduction, repeatability and refutation which systems theory is a reaction to, or a complementary approach to. The concept of reduction, considering systems, makes the assumption that systems can be separated into subsystems for analysis purposes without distorting the result. Doing this will not affect the overall system analysis which also imply that the exact number of interacting parts are known and limited. Systems fulfilling this may be described as exhibiting *organized simplicity.* (Leveson, 1995)

On the contrary, systems can also display what theorists have labeled *unorganized complexity*. This means that the idea of reduction do not apply but are instead described as complex but regular. They are also random enough to be described by statistical means. (Leveson, 1995)

A third type of systems has been categorized as exhibiting *organized complexity* which means that a system is too complex for complete analysis and too organized for statistics. System theory specifically provides a means of studying systems exhibiting *organized complexity*. Social systems, biological systems, complex software and complex engineered systems are all examples of systems that exhibit *organized complexity.* (Leveson, 1995) See Figure 4.

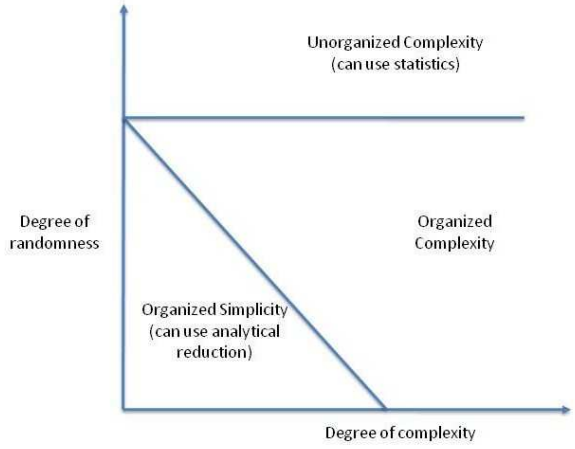


Figure 4 Complex system (Leveson, 2002, p 44)

To understand and anticipate the behavior of a complex system, several models or theories are developed. According to Zio (2009) some systems are best explained in terms of distributed systems, constituted by networks of components which is often referred to as infrastructures e.g. computer and communication systems, rail and road transportation systems etc. A number of these systems are critical to society and it seems that classical methods of reliability and risk analysis fail to provide proper instruments for analysis. Innovative and promising approaches is given by findings in complexity science where advances have indicated that many complex systems, technological, natural and even social are hierarchies of networks and components interacting through links or

connections. It is from the interactions of the components in such systems or networks that the behavior of the system emerges as a whole. (Zio, 2009)

Levesson (1995, 2002) gives a thorought description of the system theory based on complexity science and how it is relevant to system safety. According to Leveson (1995, 2002) systems exhibiting *organized complexity* can further be expressed in terms of *emergence and hierarchy* and *communication and control.* The first model can be expressed in terms of a hierarchy of levels of organization. The levels below are less complex than the levels above and on the first levels *emergent* properties does not exist (Leveson, 1995). Emergence is here a concept saying that complex systems can have qualities not directly traceable to the systems components but is the result of the complexity itself. The concept of emergence is the idea that at a given level of complexity, some properties characteristic of that level are irreducible. (Leveson, 2002). The latter model partly refers to the first by the terminology of hierarchies meaning that hierarchies are characterized by control processes operating at the interfaces between levels and that the control process yield activity meaningful at a higher level. The activities on each level can be captured by its own dynamics which does not apply to associate levels only that upper levels compose constraints on lower levels. Furthermore, each level is captured by its own control activities which imply the need for communication with its environment in form of inputs and outputs. (Leveson, 2002)

According to Leveson (2002) safety is an emergent property of systems due to the fact that it is the context of a system or sub-system and its interactions to the environment that determine the degree of safety. The emergent properties are controlled by sets of constraints (control laws) related to the behavior of the system and accidents stem from lack of appropriate constraints on the system components interactions.

3.3 System safety

The discipline of system safety is tightly coupled with other disciplines and therefore it is hard to give a sharp definition on system safety. Consequently, it is interesting to also describe parallel and similar disciplines in order to get a better grasp on what system safety is.

Definitions on system safety are found both in industry standards as well as in literature. In the railway signaling industry Reliability, Availability, Maintainability and Safety (RAMS) are treated together and also have aspects in common (CENELEC, 1999a). System safety in practice places protection barriers as safeguards from hazards posed by the system operation. Hence, the discipline reliability engineering is relevant to system safety whereas reliability engineering aims at quantification of the probability of the system and its protective barriers (Zio, 2009). According to Zio (2009) the availability of system could be treated by modeling techniques such as multi-state systems (MSS) and could be relevant to a system safety effort if the loss of functions constitute a danger.

Furthermore, to obtain the best results from methods and practice, system safety involve the entire life cycle of system development referring to its design, production, testing, operational use, and disposal, (Leveson, 1995, Ekholm & Börtemark, 2009) which calls for life-cycle analysis. Dependent on the phases in the system life cycle different types of dangers or possible accidents are to be considered (Derelöv, 2009).

The last decades has also shown that organizational and human factors are becoming increasingly important throughout the entire life cycle of a system. The reason is that, especially in highly critical systems such as aerospace and nuclear applications, the

reliability of hardware components has significantly improved. Instead the relative importance of organizations and operators has increased calling for Organizational and Human Reliability Analysis (HRA). (Zio, 2009) This further widens the scope of the system definition to socio-technical systems by considering factors such as safety culture, social processes, regulations, market pressures and political pressures etc. of an organization as well. (Leveson 1995, Zio, 2009)

There is also a weak distinction between system safety and the term *security*. Both qualities deal with threats or risks but actually handle risk to different properties. Security predominantly handles risks or threats to privacy and national security whereas system safety handles threats to life or property. System safety primarily focuses on the early identification and classification of hazards in order to take corrective actions before the final design is made. This often causes a tradeoff between safety and design goals such as operational effectiveness, performance, ease of use, time and cost.

However, there are plenty of available definitions on system safety and below only two are given, the first from theory and the latter from the armed forces industry:

> System safety is the discipline to: *"…prevent foreseeable accidents and to minimize the result of unforeseen ones…The primary concern of system safety is the management of hazards: their identification, evaluation, elimination and control through analysis, design and management procedures"* (Leveson, 1995, page 150)

> System safety is defined as: *"characteristics of a system that prevents injury to personnel and damage to property and the environment"* (Swedish Defense Forces, 1996, page 21)

4 Requirements management

The following section will describe the approach and theory that has acted as support as well as analytical tools during the project. It aims to provide the necessary frame of reference in order to define the system safety process as well as analyzing it with the system safety requirements process context in mind.

4.1 Classification of stakeholder requirements

Identifying, and controlling hazards that could lead to an accident are the core activities within system safety (Stephans, 2004). The identification of hazards is also the first essential step of developing system safety requirements according to Sommerville and Sawyer (1997). But all requirements are not derived from identified hazards, Kotonya and Sommerville (1997) and Stephans (2004) states that external certification and regulatory bodies as well as customers and procurement organizations also places requirements on system safety.

Kotonya and Sommerville (1997) further argue that safety requirements are a type of Non-Functional Requirements (NFRs). Other features that belong to the mentioned requirement class are security, usability, reliability and performance. However, it is important to note that the distinction between NFR and Functional Requirements (FR) can be vague (Kotonya & Sommerville, 1997). Sommerville and Sawyer (1998) give an example; a safety requirement may demand that an operator shall not have access to the machine components if the machine is running (a NFR). This requirement may result in a FR that forces the system to shut down operations if the casing is opened.

Certification and regulatory bodies as well as customers and procurement organizations often place NFRs on the system. Sommerville and Sawyer (1998) state that these requirements generally place restrictions on the system as a whole and that they may arise because the end user of a system needs to see to that their safety goals are met.

In general NFRs places restrictions on the product in development (product requirements), on the development processes (process requirements) and specify external restriction (external requirements) that the product or process must meet (Kotonya & Sommerville, 1997). Kotonya and Sommerville (1997) state that product requirements specify which characteristics a system or subsystems must have. Most of these requirements place constraints on the systems behavior in turn given to system designers. Specific NFRs constrain the development process of a system instead of the system itself (Kotonya & Sommerville, 1997). This sort of requirement is often based on development methods and standards. External requirements may relate to both the process and the product and could be derived from laws, regulations and the systems environment (Kotonya and Sommerville, 1997).

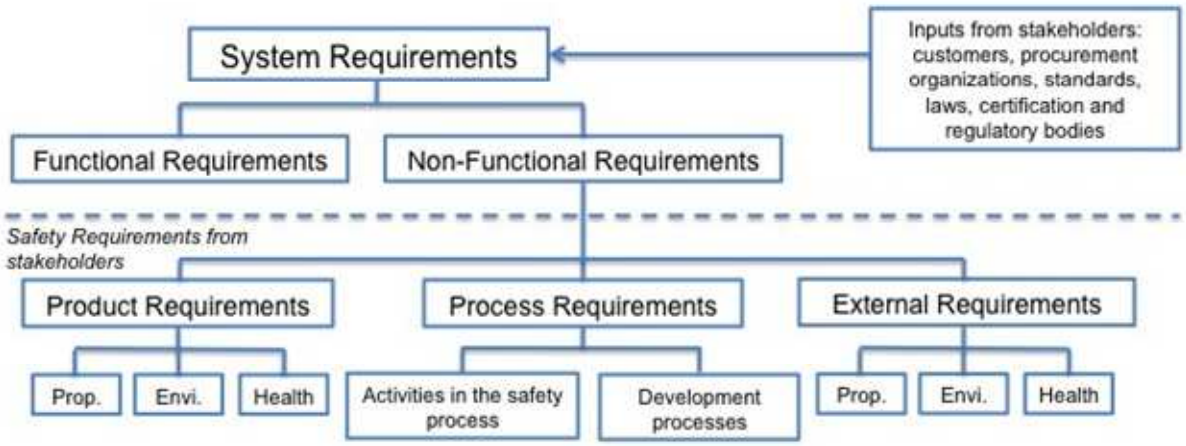


Figure 5 Classification of stakeholder requirements

Firesmith (2004) presents a further breakdown of safety requirements. The author derives safety form the quality term *defensibility*, where after he divides safety into; health, property and environment. Health is defined as to which extent illness, injury and death are avoided, found and reacted upon. Similarly, property and environment refer to the avoidance of accidental damage and destruction of property and environment, respectively. The synthesis of the gathered theories is further illustrated in Figure 5.

4.2 System safety process

The process of how to conduct system safety is not universally agreed. Different levels of elaborate efforts are found which are different in details but similar in essence. According to APT Research Inc (2007) and ITAA (2008) the design process could be extended to five major elements; program initiation, hazard identification, risk assessment, risk reduction and risk acceptance. According to IEC (1995) the system safety process is described by three major elements; risk analysis (scope definition, hazard identification, risk estimation), risk evaluation, (risk tolerability decision, analysis of options), risk reduction/control (decision making, implementation, monitoring). These tasks must be performed throughout the life cycle of any project i.e. the concept phase, design phase, production phase, operations phase and disposal phase. (Stephans, 2004)

The life-cycle of the system starts by a technical specification conveying the contextual environment where the system is meant to operate. From this document aspects solely referring to system safety requirements are derived, if not stated explicitly. The overall description of the system initiates the phase of hazard identification. The hazard identification process is concentrated in the concept and design phases but continues throughout the life-cycle. Once the hazards are identified they could also be assessed and analyzed. The goal is often to quantify risk from either actuarial data, handbook values or subjectively by judgment-based estimation. (Clemens & Pfitzer, 2006)

Identifying and controlling hazards that could lead to a potential accident are the core activity of the system safety effort (Stephans, 2004). The craft to avoid accidents resulting from hazards are often restricted and limited by the inherent composition of the system but there are actions more powerful than others. The precedence to reduce the identified and assessed hazards has a widely accepted order (Leveson, 1995, Stephans, 2004);

1. Hazard elimination, (alter the design)
2. Hazard reduction, (introducing barriers)
3. Hazard control, (warning devises or isolate the system from population centers)
4. Damage reduction, (provide training and education)

Figure 6 is a schematic picture showing the concept of hazard causes and their effects which are to be controlled by the system safety process. Barriers are to be seen as mitigators of a hazard, reducing the severity or the probability of a hazard. Suppose Accident 1 (from Figure 6) is considered the most severe accident, a barrier can then decrease the possibility of it to occur. The barrier could result form a requirement imposed by safety engineers. By adding barriers to prevent Accdent 1 from happening, the probability for other effects from this hazard would increase i.e Accident 2, 3 and the Incident (from Figure 6). An Event Tree Analysis ETA is often used to identify the effects of a given event (Swedish Defense Forces, 1996). The mitigations are then captured in the forks of an ETA. The Fault Tree Analysis (FTA), on the other hand, is an analysis method which investigates a hazardous event in order to identify the combination of subordinate events which could cause the top event. (Swedish Defense Forces, 1996)

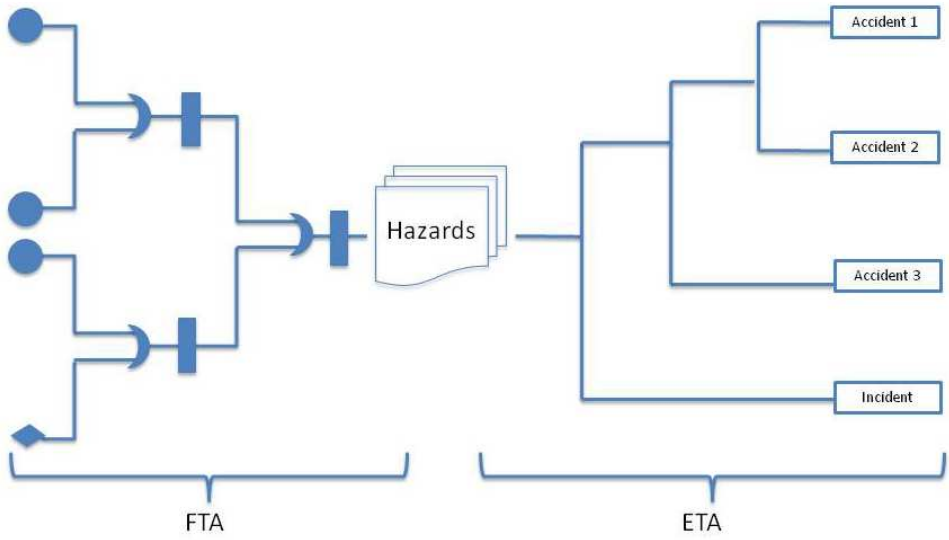


Figure 6 Hazard Concept

When design and development phase are complete, the system could also be evaluated and tested. This is often called an acceptance analysis and the goal is not to guide the design process of the system but to evaluate the product. This occupation should therefore not include just estimates of probability and consequences of hazards and accidents. Yet systems must be designed while knowledge of risks is incomplete or even nonexistent. The risk assessment of hazards and accidents attempts to solve this dilemma (Leveson, 1995).

Since this study focuses on quantitative requirements and how these are elicited and allocated from authorities and such this whole process are important. Especially the risk assessment of single hazards is interesting in order to quantify those and enable suitable risk reduction measures.

4.3 Quantitative Risk Analysis (QRA)

To quantitatively regulate potentially hazardous technologies, a calculation of risk has to be made. First to be able to pose a quantitative safety requirement, then to analyze and to assure that the system meet ends with this requirement. (Hardwick, Pfitzer, B & Pfitzer, T, 2004) QRA is performed by three reasons (www.anticlue.net/archives/000819.htm, 2009)

- To access the probability of achieving specific project objectives.
- To quantify the affect of the risk on the overall project objective.
- To prioritize the risk based on significance to overall project risk.

QRA methods originated in the early 1960s and were first employed in the nuclear industry and the aerospace industry. With continuing use, the assessment methods were refined and have ever since become more formal and scientific. (Hardwick *et al*, 2004) In Sweden, the QRA methods have proven useful and it is possible to discern a considerable use of QRA methods. Though, the analyses often lack in homogeneity due to the lack of consensus concerning which methods, models and inputs should be used. Especially when it comes to analyze the inaccuracy of a QRA, which are inevitable introduced when using QRA methods. Abrahamsson (2002). Without a discussion about inherent uncertainties of the results from an analysis the actual outcome are severely limited. (Abrahamsson, 2002) A part of the QRA trend is shown by the increased use of risk based standards and regulations which in turn call for use of QRA methods. (Hardwick *et al*, 2004)

4.4 Critique towards the QRA approach

A quantitative approach towards system safety is within the community of system safety subject for extensive criticism. The debate brings about issues and reasons why it is impossible to make use of numbers and calculations of risks. Although arguments are not completely rejected by persons who advocate such an approach they emphasize the need of quantification means, primarily by pragmatic reasons i.e. to enable a framework to prioritize hazards and thereby provide input for decision making. An intermediate critique is that it can be difficulties in assessing a design against a quantitative risk criterion at an early design stage where the knowledge of the system behavior is limited (Drogoul *et al*, 2007).

According to Leveson (1995) the quantitative approach lacks credibility by reason of several unrealistic assumptions; failures are random, testing is perfect, failures and errors are independent etc. Additionally, a probabilistic history of failures is often non-existent due to the fact that high technology systems often contain new components and sub-systems. Taken together the quantitative approach is bound to contain errors and if the heart of the system engineering effort is to quantify risks simpler and more meaningful engineering processes could be neglected and overlooked. (Leveson, 1995)

System safety is closely related to reliability engineering and the two disciplines and overlaps in one aspect; how to deal with uncertainty. However, in spite of the effort put into improving understanding of complex systems and processes, the fundamental issue of how to represent and interpret uncertainty remains. (Zio, 2009) Generally, the uncertainty can be of two different types: randomness due to inherent variability in the system (aleatory), and randomness due to lack of knowledge and information of the system (epistemic). In current reliability assessment and risk assessment both types of uncertainty are represented by means of probability distributions. This way to handle

uncertainty has come under criticism when questioned if uncertainty is best represented by a single probability or if intervals are needed. It is further suggested that probability should solely refer to binary or more precisely defined events. Suggested alternatives for addressing the problems include concepts as possibility theory, evidence theory and fuzzy probability. (Zio, 2009)

4.5 System safety requirements process

When trying to place the system safety process in a wider perspective it becomes obvious that risk management is a natural part of other activities e.g. the requirement engineering process. Safety requirements are derived from safety goals and policies as well as from hazard analyses (Firesmith, 2004, Sommerville & Sawyer, 1997). How these activities, risk management and requirement engineering, are connected is presented in Figure 7 and further based on the literature from Kotonya & Sommerville (1997). The arrows that are pointing backwards in the model indicate that the activities are of iterative nature (Kotonya & Sommerville, 1997). As seen in Figure 7 the overall requirements process of a system has a slightly different notation in comparison to the risk management process, partly due to the scientific origins, yet the processes are deeply interwoven. Relevant when embarking on risk management is often a set of abstract requirements. Those could be thought of as the input to the system safety process. The output, on the other hand, is the set of suggestions and improvements that are fed back to the main requirement process, which is further discussed in the next section. (Kotonya & Sommerville, 1997)

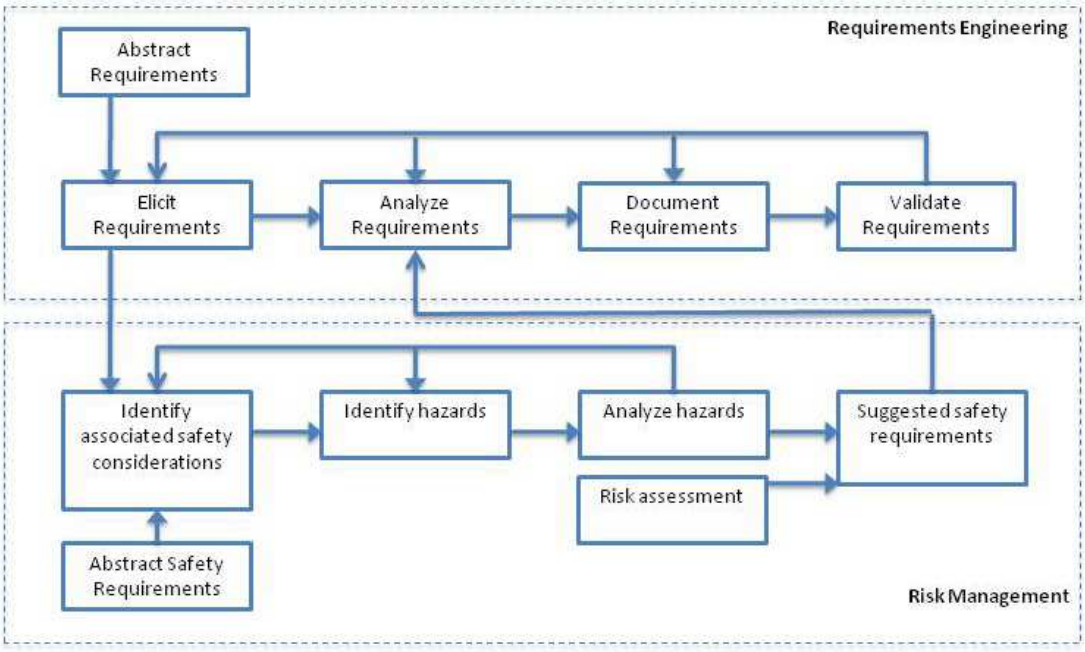


Figure 7 Integration of risk management and requirements engineering (Kotonya & Sommerville, 1997, page 208)

4.6 The requirements engineering process

In the previous section the relationship between the system safety process and the overall requirement process is discussed. It is important to bear in mind that the system safety is a part of the overall requirements process which also concerns, for example, functional requirements. Kavakli & Loucopoulos (2005) state that there is no common definition on how the requirements engineering process should be handled. However, the notation from Figure 7 is discussed below.

4.6.1 Requirements elicitation

The process of eliciting requirements involves many activities where the main output is the identified goals, which provides the objectives that the system as a whole must conform to. In a nutshell, they could be seen as a draft of the system requirements. (Nuseibeh & Easterbrook, 2000, Kotonya & Sommerville, 1997)

Identification of system boundaries is an important contributor to the elicitation of requirements. The boundaries are meant to describe where the considered system fits into the operational environment. (Nuseibeh & Easterbrook, 2000) Kotonya & Sommerville (1997) adds that system boundaries should be complemented with organizational information, domain information and information about previous systems. In addition, requirements are also discovered through stakeholder consultation, where a stakeholder is the one who is affected by the success or failure of a system. Common types of stakeholders could be customers and clients, developers and users (Nuseibeh & Easterbrook, 2000).

4.6.2 Requirements analysis

The output of the elicitation processes is analyzed in order to discover problems and conflicts. It is common that requirements are in conflict with each other and such conflicts should be handled in negations with the systems stakeholders. Typical aspects to consider performed during requirements analyses are; necessity checking, consistency and completeness (no requirements should be contradictory and no services or constraints should have been omitted) and feasibility (feasible to the context and the budget). (Kotonya & Sommerville, 1997).

4.6.3 Requirements documentation

The document of requirements may have different names such as functional specification, requirements definition and software requirements specification (SRS). The requirements documents shall be formulated in such manner that it is understandable to all stakeholders involved. Requirements can be complemented with diagrams and system models. Kotonya and Sommerville (1997) and Nuseibeh and Easterbrook (2000) state that it is important to be able to communicate what is considered a requirement among the different stakeholders. The way they are documented also plays an important role in order to be properly read, analyzed, written, rewritten and validated. Therefore the procurement of traceability is an important factor when communicating and documenting requirements. According to Nuseibeh and Easterbrook (2000) traceability is defined as the ability to describe and follow the life of a requirement both in forwards and backwards direction.

4.6.4 Requirements validation

Validation of requirements is the process of ensuring that the requirements elicited are in accordance with stakeholders' opinions about the system (Nuseibeh & Easterbrook, 2000, Kotonya & Sommerville, 1997). System stakeholders, requirements engineers and system designers, should analyze the requirements together to find problems, omissions and ambiguities. Generally speaking, when validating requirements the final draft are scrutinized and especially concerns the matter of how the requirements are written. By and large, validating requirements is fairly similar to requirements analysis (Kotonya & Sommerville (1997).

4.7 Requirements specifications

The aim of this chapter is to highlight aspects of processes and how the processes fit together. First, a categorization is made of potential system safety requirements, and then the process of how to work system safety is described. This process is further linked to the overall system requirements process which in essence are similar but has ha larger scope. But what is then a high-quality requirement? According to the IEEE (1998) a good requirement possesses the qualities captured in the 8 parameters described below. Although the parameters described predominantly concern software requirements specifications (SRS) those are deemed to apply to the requirements of the system safety effort as well. Subsequently, the characteristics of a good SRS can be summarized in the following:

- *Correct.* The SRS should be compared by superior specifications, other project documentation, standards to ensure it agrees to those.
- *Unambiguous.* An SRS is unambiguous if the requirement has only one interpretation and remains so to both developers and users.
- *Complete*. References to all figures, tables, and diagrams as well as the inputs and outputs to objects should be correctly specified. All in all, requirements regarding functionality, performance, design constraints, attributes and external interfaces should be acknowledged and treated.
- *Consistent.* If an SRS does not agree with some higher-level document, such as system requirements specification, then it is not correct. The SRS should also be internally consistent; specified characteristics of real-world objects are not to conflict, no logical conflicts between actions or differences in terminology.
- *Ranked for importance.* If each requirement has an identifier to indicate the importance or stability then the SRS is ranked for importance. Typically, requirements are not equally important and could be ranked by the degree of stability or necessity. The degree of stability can be expressed in terms of the number of expected changes that affect the organization, functions and people supported by the system. Another way to rank requirements is to distinguish classes of requirements as essential, conditional, and optional.
- *Verifiability.* A requirement is verifiable if there exists some finite cost-effective process with which a person or machine can check that the product meet the requirements. To verify a requirement the terminology is important. Choices of words as “works well”, “good” and “usually” are non-verifiable. Therefore the requirement should use concrete terms and measureable quantities.

4.8 Summary

In the first section of this chapter the requirements relevant to system safety are described. Those requirements can be seen as overall requirements coming from stakeholders constituting the context of a system. Then the process of system safety is briefly described and how it is interlinked to the general system requirement process. Systems engineers are dependent on well-formulated safety requirements engineered by the system safety effort. In order to produce high-quality requirements theory of how to give a high-quality requirement is given. Emphasis has further been put on the use of quantitative requirements. Together the frameworks give an accurate description of how requirements are handled within systems development and how this is connected to systems safety. Figure 8 serves as an illustration of the theoretical framework for this study.

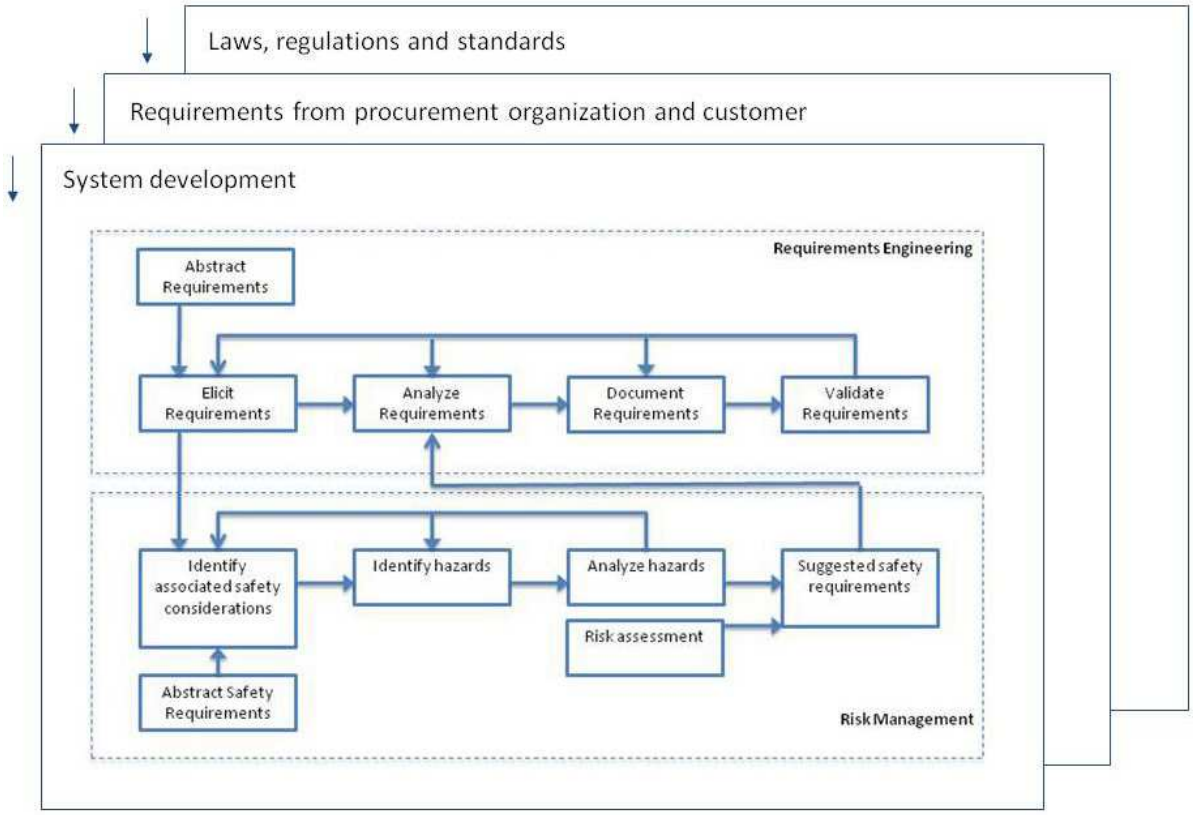


Figure 8 Illustration of theoretical framework

5 Model development

This section attempts to describe how relevant theories are used in order to build the theoretical framework employed when modeling the proposed work structure that describes the relationship among different quantitative requirements methods. This section will make use of relevant theory, accompanied by opinions from the author regarding the matter. In other words, the general purpose of this chapter is to synthesize the gathered and relevant theories and logically put them together.

5.1 Scope of the model

The main scope of this project is to give an illustrative relationship among methods concerning quantitative safety requirements. To order the methods found and put them into relation urges a thorough theoretical foundation. Although several theories are found they often concern different matters that in its entirety do not support the scope of this thesis. The modeling part is assisted by a modeling language called Unified Modeling Language (UML) using activity diagrams. Different UML representations bring forward different characteristics and the activity diagrams exhibit, as the name suggests, the performed activities and their relations.

5.2 Choice of theoretical framework

The reason why to rely heavily on theory from Leveson (1995, 2002) is that no other approach is found which combines ideas from systems theory and system safety and the fact that Leveson is an internationally acknowledged author in the system safety community. To integrate system theory and system safety are thought to be innovative and intuitively correct. The approach suggested by system theory gives explanatory value of the socio-technical aspects by enabling a system to be described in layers or hierarchies. The nature of complex systems is proved hard to model and does not only incorporate pure technical aspects. Handling system safety aspects is hardly pure technical and therefore a theoretical frame of reference allowing for a broader definition of technology is essential.

5.3 Hierarchies of control

From Leveson (1995, 2002) the usage of systems theory is also applicable to system safety. The general thought is that the concerns of systems safety is captured at different levels of hierarchy. The hierarchies are captured by the emergent properties rising from different levels of the systems concept. The hierarchies are described, in theory, in diametrically opposed terms, from the hierarchies in an apple (the molecules to emergent properties such as the shape of the apple) to the organizational hierarchies handling constraints and feedback (Leveson, 2002). One of the first problems is to define those hierarchies; what do they concern, what links and separates them?

According to Leveson (2002) accidents result from inadequate safety constraints on the behavior of the system components, i.e. the control loops between the various levels of hierarchical control. The term *constraint* is central to avoid accidents and in essence thought to be similar to the term *requirement*. In other words, the requirements or constraints serve as input and output to the different hierarchical levels which in turn are formed by the control processes (Leveson, 2002).

The first step for any safety program is to identify the hazards and in order to do this the accidents must be defined for the particular system. The accidents, from a requirements perspective, will also involve the entire socio-technical system which could potentially

have an effect (Leveson, 2002). This work will result in a small set of high-level hazards from an initiated system safety effort (Leveson, 2002) which comply with a high level of hierarchy. This structure suggests a generic system safety process starting at a high level of hierarchy considering accidents and the identification of hazards. All in all, the result from control processes is constraints which should be treated at the level of hierarchy over which the system, subsystem or component designer has control.

5.4 The communication and the control processes

According to Kotonya and Sommerville (1997) the system safety process and the requirement process are interlinked. The descriptions of the two processes from Kotonya and Sommerville (1997) are rather unsophisticated and are more profoundly described by other authors. The system safety process, for example, are described in several other articles, standards and books and contain several extensions but are in essence the same. The systems safety design process is further described in accordance to Leveson (1995) and Stephans (2004). Also, the requirement process is extended by a few steps by Nuseibeh and Easterbrook (2000). Those processes are thought of as control processes operating generically at different hierarchies of control. The processes described in this thesis are general and in real world partly extended by different methods. The aim of this project is to identify those methods and place them in relation to each other. Therefore it is important to bear in mind that those methods are parts of the more theoretical descriptions of the control processes, i.e. the system safety design process and the requirement process.

According to Leveson (1995, 2002) the communication between the different levels of hierarchy aims to place constraints or requirements to avoid or prohibit accidents coming from lower levels. From above it is explained that those requirements are the output at a specific level and therefore it is crucial that those communicated requirements serve the system development well. In order to do so a high-quality requirement specification is needed which is elaborated by the IEEE (1998) standard concerning SRS. Fulfilling the characteristics of high-quality requirements are also thought relevant when it comes to the methods eliciting them. If a method has several weaknesses they are thought to be traceable to the lack of those characteristics.

This communication is not only aimed at lower levels of system safety process but also to be communicated to the system design engineers. Often the system safety effort is active in relation the overall system engineering process and it is therefore crucial that the requirements are communicated in an understandable and correct way and in accordance to higher levels of hierarchy. It is also important that those requirements are not delayed or communicated late in the systems design phase (Leveson, 2002). Quantitative requirements concerning systems safety are only thought to be relevant to the system development process when it comes to allocating the requirements to parts of the system. The work before the allocation of requirements are thought to primarily concern the elicitation of quantitative risk levels and the refinement which then has no impact on the system development process. The theoretical framework are compiled and illustrated in Figure 9.

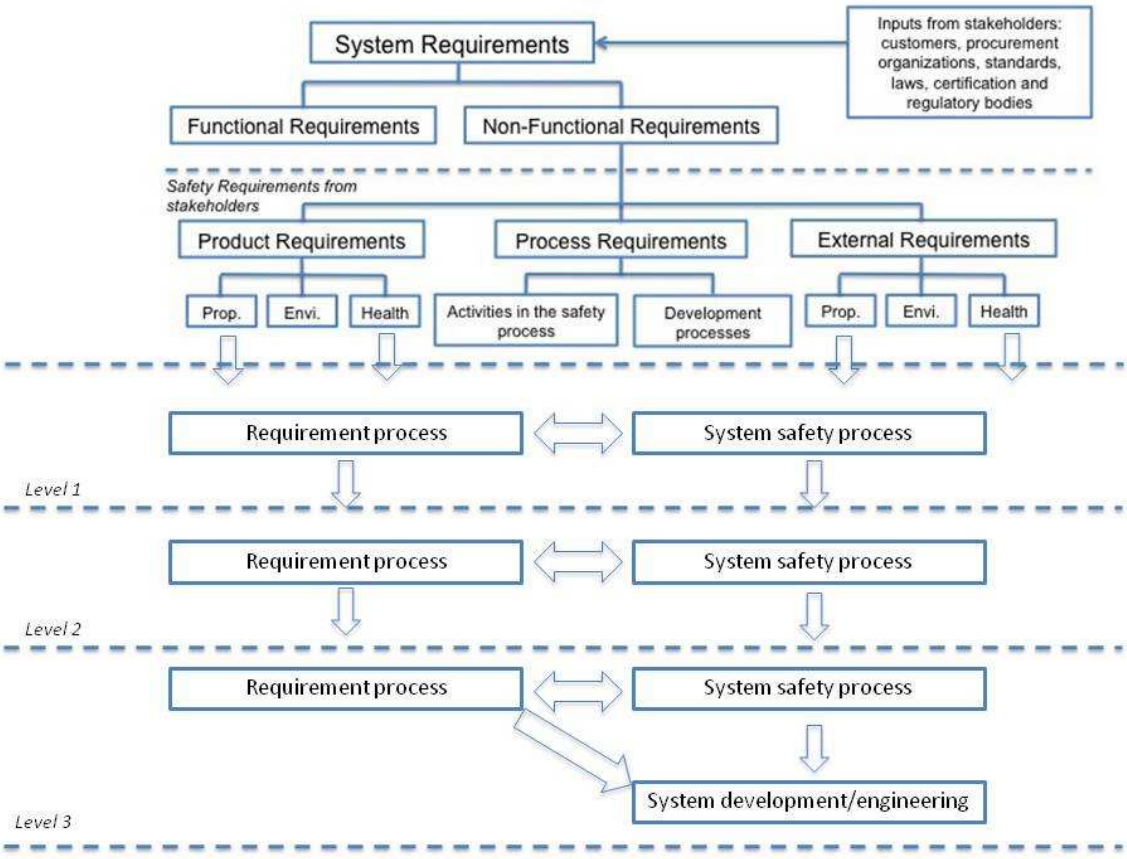


Figure 9 Illustration of model framework

5.5 Modeling using UML

From theory a framework is outlined of how to describe the environment where to elicit, refine and allocate quantitative system safety requirements. The modeling concerns a description of how to work quantitative requirements. There are numerous modeling tools applicable to such an effort. The main difficulty is to enable a description not constrained by the differences among the studied industries and their diverse conditions. First to consider was decision diagrams but those also reflected the freedom of choice of methods. Due to the fact that the freedom of choice of how to conduct quantitative requirement are different among industries this was not an appropriate way to illustrate the context of system safety. Instead two other techniques were given attention by reason of their ability to capture activities or processes; UML activity diagrams and the Business Process Modeling Notation (BPMN). The primary goal for BPMN is to provide a notation understandable to all business users, from business analysts to development engineers and managers (White, 2004). The BPMN technique is based on a flowcharting technique tailored for creating graphical models of business process operations (White, 2004). In comparison the two techniques use similar notation and both are also fairly uncomplicated. Although BPMN seems to better suit the purpose of this project the choice fell on UML simply due to path dependence; the BPMN was found late, and the fact that UML has a wider recognition.

According to Kratochvil and McGibbon (2003) the usage of UML activity diagrams show:

> *"…the complete chain of activities for a single process. When there are many processes, we recommend that the activity diagrams be completed by some kind of graphical index of processes, for example, a simple, top-down process hierarchy chart or a simple use case diagram."* (Kratochvil & McGibbon, 2003, page 15)

Long/complex back-office process chains, in where other systems could be involved but also interleaved with manual activities, are advantageously modeled by UML activity diagrams. However, weaknesses of such an approach are less suited for knowledge-intensive activities and front office activities where the user jumps more freely across processes. (Kratochvil & McGibbon, 2003)

The process tried to be modeled is the quantitative requirement process and is thought to be a rather long back-office activity process. Therefore, UML activity diagrams appears to be an appropriate choice of modeling technique. The recommendation to incorporate a top-down hierarchy also fits well with the previously described theoretical framework.

6 Three industries and their methods

This chapter aims to give a thorough description of each industry and their regulatory framework. To a great extent regulations are in the form of standards in turn derived from laws and regulations. The actual system safety effort is then performed in relation to those and methods of system safety requirements refinement and allocation are often found and described within each standard. Thereby it is necessary to first give the context of each method in order to fully comprehend the boundaries for the system safety management. The first industry described; the industry of defense, serves as a first introduction to the field of system safety work, its actors and products. The following industries incorporate the same dynamics but this thesis only describes the differences from the first, referencing, industry – the industry of defense.

6.1 Presentation of case company – Combitech

Combitech is an independent service company providing technical consultancy within information security, systems security, logistics, systems integration, systems development, environment and mechanics. The company works as a third party contractor during the product lifetime. The range of services embrace all phases of the product life-cycle; pre-studies and analyses, construction, process support, training, verification, validation and testing etc. (www.combitech.se, 2009)

Combitech has approximately 800 employees and an annual turnover of about SEK 950 M. In Sweden the company is represented in 20 different cities but is also found in Norway and Germany (www.combitech.se, 2009). Due to the substantial organizational restructuring the history of the company is hard do briefly describe. However, Combitech is owned by the Saab Group – a high technological company with its main operations within defense, aviation and space. The organizational structure of Combitech is divided in two divisions; systems engineering and security solutions. The latter has four departments where AO IL (Command and Control) incorporates the segment of system safety (System safety & ILS). (www.saabgroup.com, 2009)

The many years working with system safety analyses, has resulted in an in-house handbook for system safety work called Safety1st. This handbook serves as unified methodological mean to be used during all projects involving system safety. Activities proposed are only recommendations and not absolute and are further deemed to be tailored to each specific task performed in order to deliver an as effective and high-qualitative analysis as possible. (Martinsson, 2007)

6.2 The industry of defense

6.2.1 Introduction

The Swedish Armed forces has developed a manual based on the American MIL-STD-882C standard called H SystSäkE and describes the internal instructions and directives for system safety activities regarding the Armed Forces' systems. The British philosophy of ALARP (As Low As Reasonably Practicable) has also served as a major source of inspiration when developing H SystSäkE. (Swedish Defense Forces, 1996) Related to H SystSäkE are also "Weapons and Ammunition Safety Manual" (H VAS) and "Automotive Safety Manual" (H FordonSäk). Systems development in conjunction to the Swedish defense industry is excepted to follow the regulatory demands from the European Union first stated in 89/392/EEG, 91/368/EEG, 93/68/EEG and 2006/42/EG called "Safety of Machinery" which has been incorporated in Swedish law by AFS

1998:3 and AFS 1994:48 (www.av.se, 2009). The reason is to enable the military force to stay competitive in relation to international counterparts and not to be comprised by massive regulatory frameworks. Instead systems development has to follow the H SystSäkEE manual. (Swedish Defense Forces, 2009-02-24)

6.2.2 Actors and documents in system safety work

According to Stephans (2004) most system safety programs are involved in governmental acquisitions. This raises the question about relevant actors and their liabilities. The main actors are the government agency and the contractor. However, this structure is not always identical among industries and sometimes other constellations appear. One example is in the defense industry, where a third actor in the form of a procurement unit is involved. (Swedish Defense Forces, 1996) Due to this fact all major components of an organization are involved in system safety. Specific to the system safety engineer in particular and the system safety effort in general are the responsibility to integrate all relevant competencies to a well functioning unit; the system safety working group (SSWG). (Stephans, 2004)

The government agency or its procurement organization determines the specifications for the project including standards of safety performance and define the levels of acceptable risk. The request for proposal (RFP) is the document communicating the system specifications to different contractors, which serve as the overall requirements on the system being developed. Interested contractors then take part in prebid conferences. To ensure that requirements are met the government must also develop a plan to evaluate and monitor the program conducted by the contractor, often by implementing “milestones” to which certain advances should be reached. Additionally, a plan should also be developed by the contractor to meet the requirements stated in the RFP; often called the system safety program plan (SSPP). This plan is often the first in a row of system safety products and contains detailed information about system safety personnel, procedures and products. (Stephans, 2004)

Dependent on the size of a system being developed the extensiveness of system safety effort is reflected by the amount of system safety procedures and products as well. This is captured in the concept of tailoring which means that the size of a project also should reflected by the comprehensiveness of system safety documents and activities. (Ekholm & Börtemark, 2009) Figure 10 briefly describe the actors and the communicated documents. Whereas this study mainly focuses on a top-down approach and not so much on validating the stated requirements merely the left side of the figure is described. The dotted rectangle illustrates the system safety requirements process and is further discussed in next section.

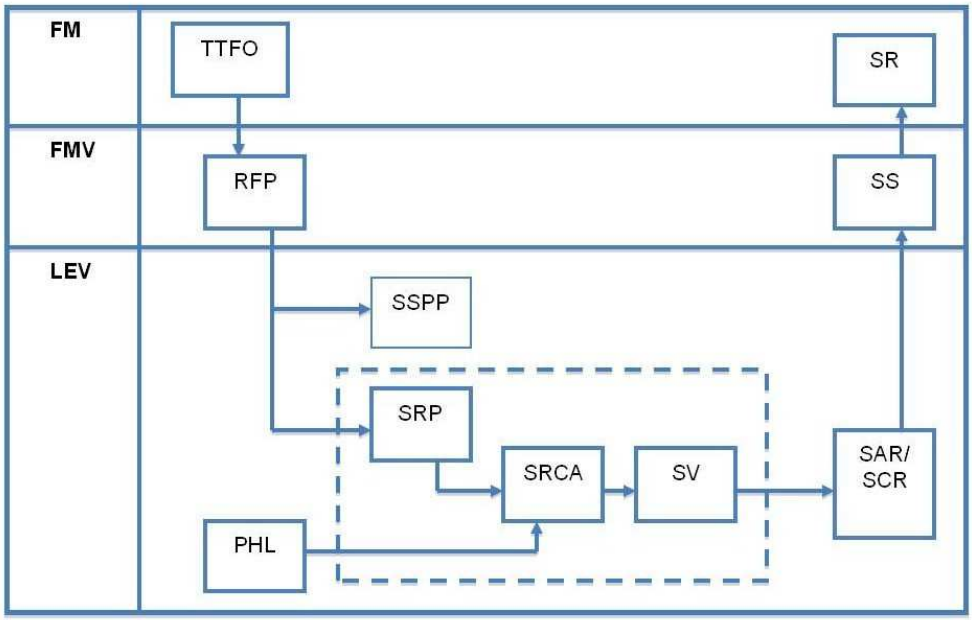


Figure 10 Actors and documents in system safety work

6.2.3 System safety products

Since the primary objective of the system safety effort is to identify, analyze and control hazards, a Preliminary Hazard List (PHL) is created relatively early in the system development process. The PHL document only aims to identify hazards by different methods. Reviewing lessons learned and accidents reports, informal conferences, energy trace and checklists are all feasible techniques to use. (Stephans, 2004)

The second and slightly more sophisticated task commonly used is the Preliminary Hazard Analysis (PHA). A PHA is a document containing identified hazards in the early life cycle stages. The PHA starts at the concept formation stage of a system and are therefore qualitative and limited. This document is updated iteratively during the early hazard identification process. The outcome of PHA serves as a baseline for later analyses and may be used in developing system safety requirements and thus affecting the design process as well. (Leveson, 1995) If a PHL has not been established, the PHA serves as the PHL as well (Stephans, 2004).

Next tasks often performed are System Hazard Analysis (SHA) and the Sub-System Hazard Analyses (SSHA) (Stephans, 2004). The SHA begins as the design matures and ends when no updates to the system design are being made. The analysis mainly focuses on examining the interfaces between subsystems. The main purpose is to recommend changes to meet with safety requirements. When the design of subsystems starts to mature the SSHA analysis starts and, as the name suggests, focuses on hazards associated with the design of subsystems. The SHA is a type of SSHA. The difference between SHA and SSHA lies in their disparate ambitions although they are accomplished in similar ways. The SSHA examines how an individual failure of components affects the overall system whereas the SHA analyses the effects of functioning and non-functioning components operating together on the overall system. (Leveson, 1995) Those tasks are often performed as more detailed design data are available to provide a more detailed and profound risk assessment. (Stephans, 2004)

The last performed safety programs are the Operating Hazard Analysis (OHA) and the Operating and Support Hazard Analysis (O&SHA) and take place rather late in the system development life cycle. The former analyses mainly focus on hardware whilst the OHA and the O&SHA integrates the people and the procedures into the system. (Stephans, 2004) Figure 11 attempts to demonstrate the main inputs from system safety work to the requirements process.

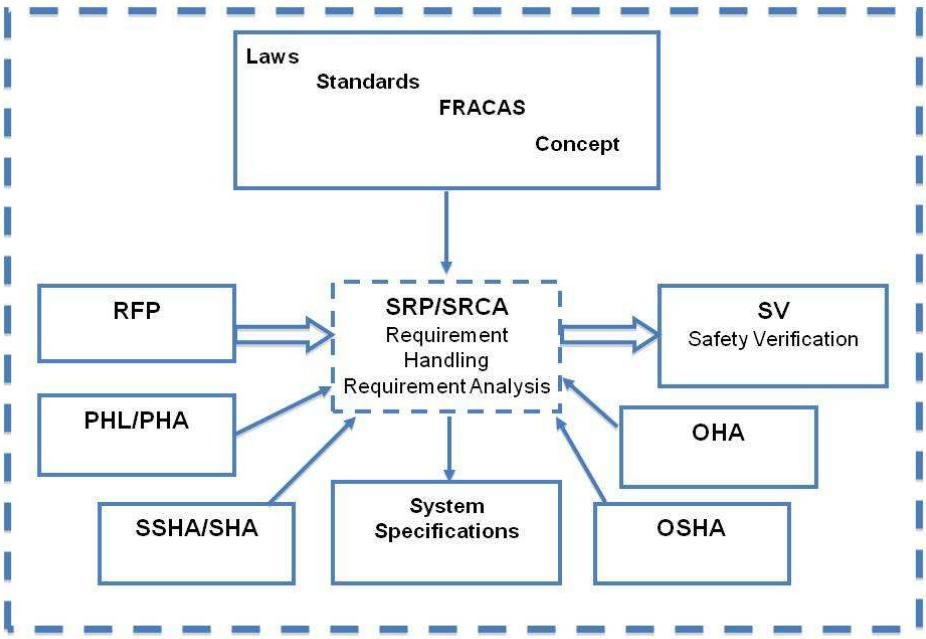


Figure 11 System safety products and the requirements process

6.2.4 System safety techniques

In order to create system safety products different techniques are used. This is an ever-growing list and their substance is partly outside the scope of this thesis. Although, when eliciting system safety requirements some techniques could be utilized as for example the ETA. All techniques have in common to bring forward the inherent hazards of the system being studied. An extract of available techniques are: (Stephans, 2004)

- Energy trace and barrier analysis
- Failure Mode and Effect Criticality Analysis (FMECA)
- Fault Tree Analysis (FTA)
- Project Evaluation Tree (PET)
- Change analysis
- Management Oversight and Risk Tree (MORT)

6.2.5 Risk matrix

The risk matrix, also called Risk Assessment Code (RAC), is a widely used tool to provide a valid base to illustrate risks. There are dozens of slightly different risk matrixes, but they all have one axis displaying the severity component of a risk and the other axis displaying the probability of a risk. The risk matrix serves as a type of requirement that is easily interpreted and can function as a basis for determining acceptability, prioritizing risks and allocating resources to reduce risks. (Stephans, 2004) The matrix was introduced, in the semi-quantitative form often seen today, 1984 when incorporated as a tool in the promulgated American defense standard – MIL-STD-882D (Clemens, Pfitzer, Simmons, Dwyer, Frost & Olson, 2005). Measuring the severity component of a risk has been, and still are, a particularly troublesome task, especially when embarking upon the challenge of estimating the consequences of human lives (Stephans, 2004 & Ekholm & Wallentin, 2003). Often the severity variable is divided into three types; personnel, property and environment (Swedish Defense Forces, 1996, Ekholm & Wallentin, 2003) which are further illustrated by Figure 12 above. Compartments in the matrix can be assigned different requirements of acceptance and therefore serve as zoning guides for acceptance or rejection of a single risk. (Clemens & Pfitzer, 2006)

Befarade dödsfall/ Estimated number of deaths.	Befarade allvarligt/ Estimated number of severe injuries.	Befarade mindre allvarligt skadade/ Estimated minor injuries	14	13	12	11	10	9	8	7	6	5	4	3	2	1
1000-3000																
300-1000																
100-300	1000-3000															
30-100	300-1000															
10-30	100-300	1000-3000														
3-10	30-100	300-1000														
1-3	10-30	100-300														
0,3-1	3-10	30-100														
0,1-0,3	1-3	10-30														
0,03-0,1	0,3-1	3-10														
0,01-0,03	0,1-0,3	1-3														
0,003-0,01	0,03-0,1	0,3-1														
0,001-0,003	0,01-0,03	0,1-0,3														
0,0003-0,001	0,003-0,01	0,03-0,1														
Sannolikhet för skada under ett (1) år (P) Likelihood for an injury during one (1) year (P)			1E-7-3E-7	3E-7-1E-6	1E-6-3E-6	3E-6-1E-5	1E-5-3E-5	3E-5-1E-4	1E-4-3E-4	3E-4-1E-3	1E-3-3E-3	3E-3-1E-2	1E-2-3E-2	3E-2-0,1	0,1-0,3	0,3-1

Figure 12 Risk matrix (Swedish Defense Materiel Administration, SOW, Medical care systems, 2009)

According to Ekholm (2009) the system safety effort today only encompasses single risk assessment which is assessed against a single risk matrix that none fully understand. Using one risk matrix as a high-level requirement to pertain to all risks has a few methodological deficiencies. Firstly, a risk categorized as intolerable has to be managed to a tolerable level otherwise the entire development are adventured. Furthermore, this model does not incorporate any economical aspects of how to prioritize risks. Thirdly, according to Ekholm (2009) the risk matrix is seldom tailored to a particular system development which then, to a great extent, becomes useless. In general models of today have several deficiencies and there is a need to increase the use and understanding of new models.

6.2.6 Crash risk factor

The System Safety Manual contains the Swedish Armed Forces' internal instructions and directives for system safety activities. In chapter 6 a full description of the defense industry's system safety effort are provided through an example. A project are suggested to be divided in sub-assemblies; a subdivision of a complex system in its smaller parts. There are often 30 to 40 sub-assemblies. The system safety requirements are then further allocated to each sub-assembly, and its corresponding, work group. The PHA is then carried out as early as possible by the system safety function. (Swedish Defense Forces, 1996)

Each sub-assembly is allocated a more concrete system safety objective from the overall objective. The numerical allocation is made without any theoretically sophisticated methods only by thorough studies of the sub-system concepts, results from previous projects, predictions of failure rates, assessments of the crash risk in the event of a failure and with the aid of a the PHA.(Swedish Defense Forces, 1996) The crash risk factor is defined as:

> *"… the product of the failure of probability for a specific event and the probability of crash if this event takes place."* (Swedish Defense Forces, 1996, page 176)

The crash risk factor was mainly pursued by the aviation industry and within Saab technology. Basically, this was a mean to calculate the size of an order to enable the government to estimate the number of airplanes still operable after a certain time. This method did not consider any harm to the pilot or environmental aspects but merely the probability of an airplane to crash. (Ekholm & Börtemark, 2009) Whilst this method only considers the probability, not the consequence, of an event leading to a crash, not an accident, the method falls outside to scope and framework of system safety exploited in this thesis. Therefore, this method is to be seen as a predecessor to more developed methods exercised today.

6.2.7 Risk summations and total system risk (TSR)

Through analytical approaches (e.g. FMECA) and activities (e.g. PHA) a hazard inventory is built up. Each hazard is usually described by the consequence and the probability which also could be done quantitatively and analyzed in accordance to a risk matrix. Matrix zoning indicates risk acceptability. Here risks or hazards are assessed singly, item-by-item, and their acceptability is judged individually (Swedish Defense Forces, 2006). According to Clemens & Pfitzer (2006) this insidious way of gaining hazard acceptance should be replaced by a risk summation, measuring the summed risk for the whole-system. From MIL-STD-882D it is suggested to tailor a matrix to conform to particular settings although this is rarely done in reality. Applying the risk summation method, it is therefore suggested to tailor a requirement for each hazard and one for total system outage in order to analyze both partial risks and the whole-system risk. In order to achieve this summation both the probability and consequences of risk need to be quantified. (Clemens & Pfitzer, 2006, Arntsen, 2007)

In GEIA-STD - 0010 the concept of Total System Risk (TSR) is introduced which assumes that the summed hazards are totally independent (ITAA, 2008). Furthermore, suggested measures of total system risk is:

- *Expected loss rate* computes the severity component as the average loss per system exposure interval. Estimates the level of loss that, on average, will happen every time the system is operated for the specified exposure interval.
- *Maximum loss assigns* the severity component to be plotted as the level of loss corresponding to the most severe single hazard. The probability of maximum loss is computed by dividing the expected loss rate by the maximum loss level.
- *Most probable loss*. Sum the probabilities of hazards at each level of severity. The severity level with the highest probability is the most probable loss. Plot this severity level with a probability computed by dividing the expected loss rate by the most probable loss level.

- *Conditional loss rate*. The probability value is the sum of the probabilities for all hazards. The severity value is the conditional expected loss and is computed by dividing the expected loss rate by the value of the summed probabilities. The result displays the probability that a mishap will occur, and the expected amount of the loss, given that a mishap does occur.

Next generation of H SystSäkE will be introduced in 2010. The authors, Ekholm and Börtemark, aspire to introduce the new model called risk summation. Whereas the new H SystSäkE serves as a standard to contractors and persons involved in system safety, the introduction of risk summation will alter the ways of working. It is suggested that risk summation will not fundamentally alter a sufficient risk analysis, but only add previously unknown measures. (Ekholm & Börtemark, 2009b)

The theory is based upon the thought that the number of comparable risks matters when to consider a system as whole. If the system encompasses 1, 10 or 100 equal risks must be of great significance to system safety. The risk summation model enables to sum the risks and then match with a requirement on total system level. Unique to this model is the work of quantifying the consequences which further always apply only to accidents affecting personnel. The measure is I-RILL (Individual Risk In Loss of Lives) and T-RILL (Total Risk In Loss of Lives). The occurrence of one death corresponds to 10 heavily wounded and further to 100 minor wounded. (Ekholm, 2006)

What is then a risk summation? First to do is to derive numeric probability or frequency values on each hazard occurrence. Then the consequences are assessed in order to find a distribution of possible outcomes from a hazard occurrence. To fall off a ladder can for example result in one out of hundred cases in fatality (according to RILL this gives a contribution of 1), in 10 out of hundred cases this may lead to a major injury (0.1 fatalities) and in 30 cases this could lead to a minor accident (0.01) fatalities. The risk in terms of I-RILL then becomes 0.01*1+0.1*0.1+0.3*0.01 = 0,0031 fatalities. The probability of this hazard to occur may be three times in a year which would result in 0.0031*3 = 0.00933 fatalities/year. Pose that the system then has two more hazards assessed similarly (0.11 and 0.15 fatalities/year). The T-RILL is then achieved by simply adding the numbers which is done by risk summation.

This way of quantifying risk is never to be related to economical means of measurements which have severe ethical problems and issues. However, by enabling consequence quantification and by assessing a risk by the product of consequence and probability a way of comparing the relative risk size is constructed. Connecting all risks i.e. the risk summation, a number on the total system risk is achieved. If this number is higher than the allocated risk budget the model further makes it possible to prioritize risk. If to compartmentalize risks into budgets to, for example sub-systems, a risk allocation from a high-level requirement is achieved. A major drawback of this method is that it builds upon the assumption that all hazards are independent i.e. they do not have any common cause. (Ekholm, 2006)

6.3 The Air Traffic Management industry

6.3.1 Introduction

ATM could be defined as the control of flights performed by air traffic controllers through commercial airspace, and is a part of the general aviations picture. (Drogoul *et al*, 2007). For ATM, manufacturers must comply with strict regulatory requirements. The

requirements are slightly more detailed and specific than what is usually presented in other industries. (Drogoul *et al*, 2007) From EUROCONTROL a manual has been developed by the EATMP Safety Assessment Methodology Task Force (SAMTF) called ANS Safety Assessment Methodology (SAM) to reflect best practices from safety assessment of Air Navigation Systems (ANS). (EUROCONTROL, 2004) SAM describes a generic process of three major steps (Drogoul *et al*, 2007):

- Functional Hazard Assessment (FHA)
- Preliminary System Safety Assessment (PSSA)
- System Safety Assessment (SSA)

The methodology primarily describes the underlying principle of the safety assessment process and leaves the detailed customization to each specific project (Drogoul *et al*, 2007). Figure 13 shows the relationships between these steps and the overall System Life Cycle.

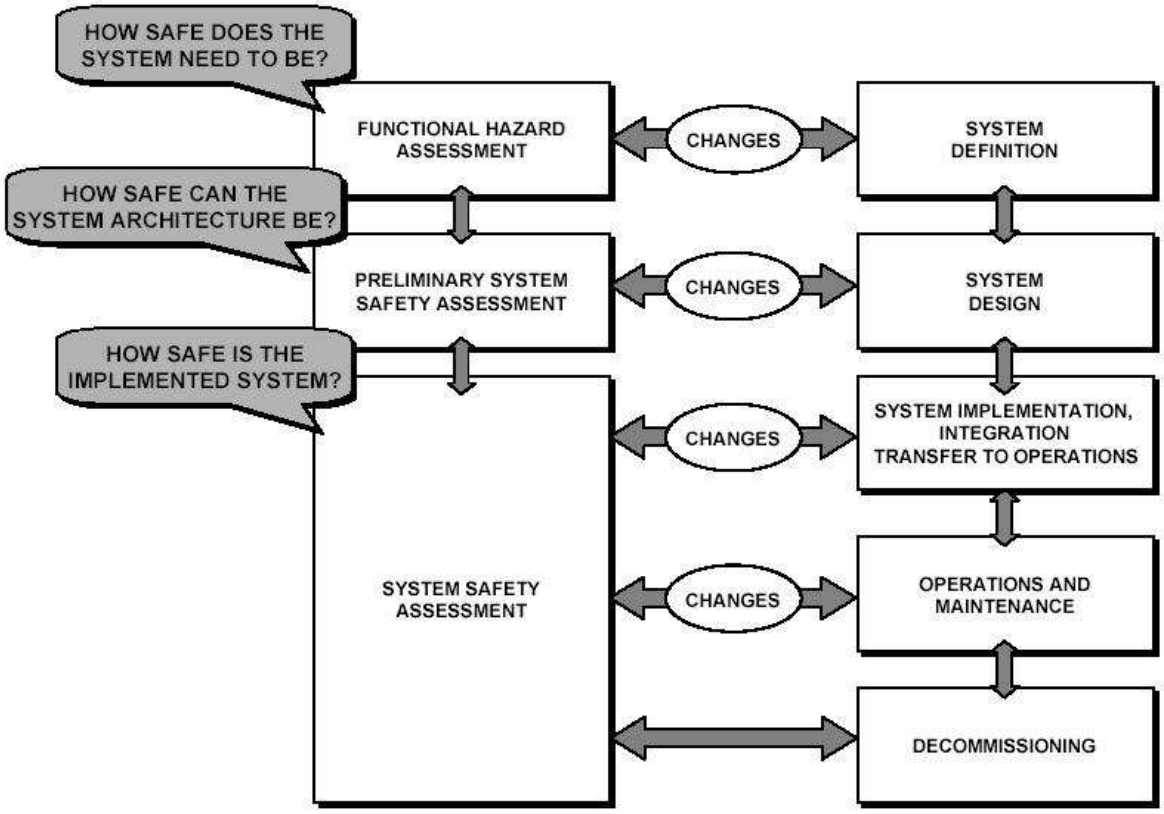


Figure 13 Relationships between the safety assessment process and the overall system life cycle (EUROCONTROL SAF.ET1.ST03.1000-MAN-01-00, 2004)

SAM aims to support ANS Service Providers to achieve an acceptable level of risk and intends to be a means of compliance to ESARR4. (Drogoul *et al*, 2007) SAM provides guidance material providing further detailed information of various techniques to achieve some parts of the three steps. The objective of FHA is:

> *"Functional Hazard Assessment (FHA) is a top-down iterative process, initiated at the beginning of the development or modification of an ANS.*

> *The objective of the FHA process is to determine: how safe does the system need to be.*
>
> *The process identifies potential functional failures modes and hazards. It assesses the consequences of their occurrences on the safety of operations, including aircraft operations, within a specified operational environment.*
>
> *The FHA process specifies overall Safety Objectives of the system, i.e. specifies the safety level to be achieved by the system."* (EUROCONTROL, SAF.ET1.ST03.1000-MAN-01, page 6)

The FHA is further divided in five steps: initiation, safety planning, safety objectives specification, evaluation and completion. Applicable to this study is the third step which has the following objectives (EUROCONTROL, 2004):

1. Identify Potential Hazards: What could go wrong with the system and what could happen if it did?
2. Identify Hazard Effects: How does it affect the safety of operations, including the safety of aircraft operations?
3. Assess Severity of Hazard Effects: How severe would those effects be?
4. Specify Safety Objectives: How often can we accept hazards to occur?
5. Additionally, Assesses the intended aggregated risk: What is the foreseen safety level aimed at?

SAM also provides guidance material to achieve the described objectives; severity classification scheme, risk classification scheme, safety objective classification scheme and methods for setting safety objectives.

The guidance material on severity classification gives complementary material to ESARR4 of how to classify each hazard also on sub-system level. The severity classification scheme suggests 3 sets of severity indicators of hazard's effect; effects on Air Navigation Service (ATM, Air Traffic Flow Management (ATFM) and Airspace design (ASM)), exposure and recovery. In each set, the different effects of hazards are ranked, in order to ease the assessment of the consequences. The aim is to assign each hazard to one of the five Severity Classes (SC). The use of an ETA is suggested as an analytical aid to the classification. (EUROCONTROL, 2004)

The Risk Classification Scheme (RCS) specifies the maximum acceptable and tolerable frequencies of occurrence of a hazard effect of a certain severity class i.e. define a safety target (ST). In other words, within each SC regions for what is acceptable and what is not, is basically defined by constructing a risk matrix. It is the ANS provider's responsibility to define the RCS and it should relate to the national RCS but also to the overall ATM risk. This is done by introducing an ambition factor that tightens the national safety requirements. After the allocation to overall system risk the RCS should also consider each individual risk. The individual risk can be achieved by applying a distribution over risks, either by an even or an uneven distribution. In the case of an uneven distribution, data from a system in use is needed and could for example be per phase of flight or per function of the ATM system. The requirements are often stated in maximal acceptable frequency of a hazard per reference unit (operational hour, per sector, flight hour etc.). (EUROCONTROL, 2004)

The Safety Objective Classification Scheme (SOCS) define the maximum frequency at which hazard can be tolerated to occur. SOCS are developed either at ANS/ATM

Organisation level or at Programme or Functional level. A SOCS correspond to a specific system or sub-system. The ANSP/ATMSP is responsible to ensure that the SOCS are consistent with the RCS. (EUROCONTROL, 2004)

The second step according to the SAM methodology is work of PSSA. The major task, important to quantitative requirements, is to derive requirements for each individual system element (people, procedure and equipment). Specifically, this is achieved by refining the functional breakdown, evaluating the architecture, applying risk mitigations, apportioning safety objectives to safety requirements and eventually balancing the safety requirements. (EUROCONTROL, 2004) The safety requirements are either intended to directly contribute to the reduction of the hazard risk or represent safety evidence demands. The safety requirements are divided upon people, procedures (PAL) and equipment. The equipment is further partitioned into hardware safety requirements and software assurance levels (SWAL). To assign PAL or SWAL a risk matrix is used whereas hardware requirements can be directly assigned through FTA. (EUROCONTROL, 2004)

The third step, the SSA, is a process initiated at the beginning of the implementation, thus a bit later in the system life-cycle. The main objective of the SSA is to demonstrate that the implemented system achieves an acceptable risk level i.e. meet the requirements from the FHA and PSSA. (EUROCONTROL, 2004)

6.3.2 ED - 125

ED – 125 contains guidelines jointly accomplished by the European Organization for Civil Aviation Equipment (EUROCAE) which is an international not-for-profit making organization. ED -125 is a document containing four approaches to risk assessment and mitigation in ATM. ED – 125 relies on a quantitative description of hazard identification, effects identification and mitigation means identification. The scope is to provide quantitative safety objectives for technical hazards; the maximum frequency or probability at which a hazard can be accepted to occur. The safety objectives are to be used in the specification and design of ATM systems. (EUROCAE, 2006)

In ED – 125 identified hazards shall adopt the Severity Classification Scheme which aligns with ESARR4 and imply five, qualitatively described, severity classes. ESARR4 also provides a maximum tolerable frequency, Safety Target (ST), of occurrence within ATM directly contributing to the first, and most severe, Severity Class (SC1). The four following severity classes are not assigned a maximum tolerable frequency from ESARR4 whereas estimates are used. Those estimates can be further refined by Ambition Factors (AFs) and set by the ATM service provider (ATMSP). All STs are described in occurrences per year or occurrences per operational hour, of a given severity class. (EUROCAE, 2006)

If a safety assessment is performed at a lower scope (sub-function or sub-system) the ED-125 does not apply. In order to apply ED-125 to such a scope the link between SO of the ATM service Provision and the SO of the hazards at the system boundary needs to be specified. (EUROCAE, 2006)

All external mitigation means between a hazard and its associated effects used to modify the safety objective shall be stated as a requirement at the operational level. Although, all hazards cannot be found but the determination of safety objectives is thought to be sufficiently conservative to compensate for these uncertainties. (EUROCAE, 2006)

The four models to derive SOs and STs, consider different variables which is also reflected by the variety of required effort. Unique to model three and four is the introduction of a complexity variable and the way to generalize the amount of hazards. If to give a brief introduction to the differences among the four models they could be described as (EUROCAE, 2006):

- Quantitative model; unique SOs are identified and assigned to each specific hazard which takes the probability that a hazard leads to an effect into account.
- Semi-quantitative model; unique SOs are identified and assigned to each specific hazard which take the probability that a hazard leads worst credible effect into account.
- Semi-prescriptive model; the risk is compartmentalized between different types of ANS units (Air Control Centre (ACC), Aerodrome (AD), APProach (APP)). Consideration is taken to the complexity of the airspace so as to different geographical parts of the airspace. The parameters are adjusted to the ANSP concerned.
- Fixed-prescriptive model; the risk is compartmentalized between different types of ANS units. Consideration is taken to the complexity of the airspace so as to different geographical parts of the airspace.

6.4 The railway industry

6.4.1 Introduction

In the railway industry there are mainly three standards and one report from CENELEC which discuss the field of system safety. The three standards, SS EN 50126, 50128 and 50129, are an interpretation of the civil standard IEC 61508 (Wigger, 2001, Hövel & Wigger, 2002) and represents the backbone of the system safety process (Hövel & Wigger, 2002).

Generally the Railway Authority, the Railway Department of the Swedish Transport Agency, derives the Tolerable Hazard Rate (THR) for a system, for example signaling systems. Signaling systems are a part of Swedish railroad administration's sectoral responsibility but has a wider sectoral responsibility for the railway sector in general and the railway's interaction with other forms of transport (www.banverket.se, 2009). Swedish railroad administration then becomes a customer or the operator. Usually the THR given by the Railway department are apportioned to sub-systems and specific functions by Swedish railroad administration (Kallman, 2009), which is input for the main contractor. The main contractor or supplier is then responsible to perform risk analysis i.e. to determine hazard rates and Safety Integrity Levels (SIL) for sub-systems and analyze the causes leading to a hazard. (CENELEC, 1999b) The risk analysis on supplier level sometimes use the risk matrix as a tool but also other assessment and hazard prioritizing methods (Uppegård, 2009) although the use of FTA is advocated (Sundvall, 2009, Norling, 2009)

Within the three CENELEC standards three different approaches to risk acceptance or a Tolerable Hazard Rate (THR) of a system are given. The methods to derive THR are based on three different principles (Wigger, 2001):

- Globalement Au Moins Aussi Bon (GAMAB), "All new guided transport systems must offer a level of risk globally at least as good as the one offered by any equivalent existing system."

- As Low As Reasonably Practicable (ALARP), “Societal risk has to be examined when there is a possibility of a catastrophe involving a large number of casualties.”
- Minimum Endogenous Mortality (MEM), "Hazard due to a new system of transport would not significantly augment the figure of the minimum endogenous mortality for an individual.”

6.4.2 ALARP

The ALARP method basically conjures up a risk matrix for the collective risks to all persons using the system and defines regions off acceptance within in it. Within each severity class hazard reduction has to take place if the Hazard Rate (HR) falls in the ALARP region of the risk matrix (Wigger, 2001). The ALARP principle implies that risk reducing measures have to be taken within this tolerable region as long as these do not result in economically unjustifiable effort (Hövel & Wigger, 2002).

6.4.3 MEM

The starting point of the MEM principle is from the discussion about the lowest rate of mortality for individuals. The idea is that a 15 year old person has the lowest individual mortality which read $2*10^{-4}$ per year. A high-level requirement is then introduced by saying that a technical system shall not contribute more than in 5 % of the fatalities. The tolerable individual risk is then down to 10^{-5} per year. This figure can be apportioned further to sub-systems. Subsequently, all hazards shall meet this requirement. (Wigger, 2001) According to CENELEC (2007) the value on the individual risk due to signaling would be less than 10^{-6} fatalities/(person * year).

6.4.4 GAMAB

The GAMAB principle does not apply to a single risk and implicitly requires progression to be made compared to older systems. The principle is general but presupposes a referencing system. When applied to railways systems a quantitative and one qualitative approach exists. The principle measures causalities caused by collisions between two trains and should be extracted from statistics. Only the quantitative approach is relevant to this thesis and is further described in Annex D of SS EN 50126. The quantitative approach can be translated in the following way: (CENELEC, 1999)

$$\lambda_c \leq \tau_{c.ref} * \frac{(r * C)}{n_c} * F$$

Data from existing system

$\tau_{c.ref}$ = the fraction (casualty/passenger) experienced for a certain number of transported passengers in the last years of operations. The fractions should be extracted from statistics for the existing system.

Data from replacement system

C = capacity of the train (passengers/hour)
F = frequency of trains (trains/hour)
r = mean occupation coefficient (train not completely full)
n_c = number of causalities per collision in this new system
D_m = throughput (passengers/hour) = r * C* F
λ_c = collision rate for the new system

6.4.5 Risk apportionment strategies

After the work on calculating the tolerable risk level for the entire systems this figure needs further apportionment to sub-systems or functions akin. The work on risk apportionment starts at the PHA which can demonstrate expected hazards and the corresponding consequences of each hazard. Deriving levels of tolerability of a system first requires a classification of all risks into various categories leading to an acceptable risk level of each category. To perform this apportionment Mihm & Eckel (2004) suggests five different approaches which are described in brief below:

- System breakdown approach; to decompose the whole railway system into its major constituent parts (organizational and/or physical parts). Giving a few examples; track, switch, signals, driver and wayside control.
- Breakdown by categories of hazard causes; relating the causes to four hazardous situations, technical faults, human errors, organizational failures and external causes.
- Functional breakdown approach; taking all the phases, functions and processes into account of a railways system either in a top-down approach or a bottom-up approach. Examples on functions and alike is: maintenance, load passengers, load freight, supply the train etc.
- Breakdown by hazard types; all possible generic system level hazards which can lead to accidents. E.g. over speed, wrong point setting, wrong signal transmission.
- Breakdown by accident types; taking a typical list of railway as input to the apportionment process. Examples on accidents are: derailment, front collision, rear collision, fire etc.

6.4.6 THR calculations and SILs

The CENELEC report, PD CLC/TR 50451:2007 - Systematic allocation of safety integrity requirements, presents a systematic methodology to determine safety integrity requirements for railway signaling equipment. According to CENELEC (2007) it is the task of the Railway Authority to define the requirements of the railway system, identify the hazards and derive tolerable hazard rates. The supplier, on the other hand, shall analyze the courses leading to each hazard, define the system architecture and then determine SIL for the subsystems. The scope of the CENELEC report is to define a method to determine the Safety integrity level of a system. (CENELEC, 2007)

Previous principles and apportionment strategies are used to set a tolerable risk level of systems and sub-systems. The CENELEC report further suggests two other methods to perform THR calculation; one quantitative and one qualitative. The terminology is not the same as in previous chapters. Both methods make use of numerical calculations but instead they refer to how the risk assessment is performed. The qualitative method relies on expert judgments and the quantitative on simulations of system behavior. To identify the relative significance of all identified hazards a hazard ranking matrix should be employed. The risk assessment should focus on the most significant hazards. (CENELEC, 2007)

Both methods first attempt to calculate a value on Individual Risk of fatality per hour (IRF) of the system. The qualitative method here uses a tailored three-dimensional risk matrix where each identified hazard is zoned and consequently given a numerical value. The first dimension is the frequency of occurrence of a hazardous event. The second is the severity levels of hazard consequence which is defined in accordance to the RILL

concept; 1 fatality equals 10 major injuries etc. The third dimension is a normalizing factor of individuals exposed. In case of 100 people exposed the normalizing factor corresponding to each individual is 10^{-2}. (CENELEC, 2007)

Conversely the qualitative method uses a formula:

$$IRF_i = \sum_{all\ hazards\ H_j} N_j \left(\left(HR_j \times D_j + HR_j \times E_{ij} \right) \sum_{accidents\ A_k} C_j^k \times F_j^k \right)$$

N_j	Number of users of hazard j
HR_j	Hazard rate
D_j	Duration of hazard j
E_{ij}	Exposure of individual i to hazard j
C_j^k	Consequence probability for hazard j leading to accident type k
F_j^k	Probability of fatality for individual i in accident type k

Next step is to match the IRF value to the Target Individual Risk (TIR) (thought to be calculated by any of the three principles above). If the IRF is larger than the TIR the railway authority may introduce barriers and recalculate or reduce the individual (or by some overall reduction factor) HR until the individual risk is tolerable. Then the HR is thought of as a Tolerable Hazard Rate (THR). (CENELEC, 2007)

From the methods briefly described above a figure of the calculated THR is obtained. This figure needs further apportionment to subsystems. The apportionment process involves the allocation of the THR to the key system functions to ensure that the total HR to the system arising from all system functions is equal to the THR. (CENELEC, 2007)

The apportionment process eventually gives a SIL to system elements. Safety integrity is basically specified for safety functions (Hövel & Wigger, 2002). According to CENELEC (2007), their standards as well as the IEC 61508 and ISA S84.01 standard provide an extensive framework of what has to be done to fulfill a certain SIL but lacks in descriptions of how to derive SILs for system elements from system safety targets or tolerable system risk. SIL tables are described in IEC 61508, SS EN 50128 and SS EN 50129. Wigger and Hövel (2002) describe this procedure as:

> *"…For the tolerable hazard rate, the coinciding class, i.e. the SIL, is searched up in the table. Then, design measures have to be applied during the design process. The standards EN 50128 and EN 50129 contain such design measures for hardware and software that should be used to fulfill a certain SIL…"* (Hövel & Wigger, 2002, page 3)

7 Methods of requirements refinement and allocation

This chapter will look deeper into the methods found in previous chapter. The methods are, as described earlier, part of a context and thereby not equivalent. This chapter retains the structure from previous chapter but describes the relevant methods found separately in each industry. This chapter aims to give a thorough description of the methods utilized in Sweden by documents and interviews.

7.1 Defense industry

From documents and interviews three methods are found that to handle system safety requirements within the Swedish Armed forces. The crash risk factor is here to be considered as a predecessor and not used in system safety work today. The two remaining methods; risk matrixes or risk summations are the two approaches used today which will be subject to more profound investigations.

7.1.1 Risk matrix

7.1.1.1 Strengths

The risk matrix is one of the most common risk methodologies used today and examples are found in numerous industries and in various forms. The Swedish Armed forces often use the matrix when posing system safety requirements both in RFP and TTFO. While the matrix is easy to understand it is particularly suitable for small size projects where no elaborate analysis is needed. The matrix is also a visual tool consequently favorable in collaborative projects where people, not skilled persons in system safety, participate. (Ekholm & Börtemark, 2009b, Clemens *et al* 2005)

The concept of a risk matrix also gives an unambiguous answer weather a hazard poses an intolerable risk. Within the defense industry the zoning of a risk into tolerable, intolerable or partly tolerable regions also connects to decision-making actors. If a hazard is calculated as intolerable, future proceedings are brought back to the customer i.e. FM, the partly tolerable to the procurement organization i.e. FMV etc. Routines like those are beneficial not only to the developer who immediately can refrain from problematical decisions but also to the customer who gains information about imminent and intolerable risks from the system being developed. In other words, the risk matrix provides a tool to rank the risks of importance and by doing so also the requirements or barriers (Ekholm & Börtemark, 2009b)

7.1.1.2 Weaknesses

The risk matrix only considers one hazard at the time. Taken together several tolerable risks may constitute an intolerable level of acceptance. This can further lead to sub-optimization of risks which assist to fatal miscalculations on the actual risk level for a system. (Ekholm & Börtemark, 2009, Clemens & Pfitzer, 2006)

Additionally, problems arise when a hazard results in several accidents or mishaps. (Ekholm, 2006) According to Martinsson (2007) the greatest risk in respect of severity and probability will be the “most credible” risk and the actual assessed mishap risk of the hazard. On the other hand the “worst credible” risk is the risk comprising the most severe consequence in terms of human lives. Both ways to deal with this dilemma of different resulting effects from a hazard is somehow incorrect and only tells us parts of the true risk. This can give the appearance of thoroughness while concealing whole-system risk if dealing poorly with the multiple scenarios scattering from a hazardous event. (Clemens *et al*, 2005)

All risks at the intolerable level must be mitigated to at least comply with region called limited tolerable or tolerable. An approach like this could possibly adventure the whole project if mitigations are expensive or impossible to implement. (Ekholm & Börtemark, 2009)

Although the risk matrix gives an unambiguous answer whether a risk is tolerable or not, the visual concept can in combination with the effortless approach make the risk matrix a demagogy. Additionally, the use of risk matrices seldom requires unquestionable proofs in order to categorize a hazard. Hence, the correctness and traceability of requirements are therefore often questionable. (Ekholm & Börtemark, 2009)

7.1.1.3 Opportunities

The matrix can display all three different facets of requirements in one single matrix by including constraints on personnel, property and external environment. (ITAA, 2008, Martinsson, 2007, Swedish Defense Forces, 1996) Harm to property are often measured in monetary terms or in objects (systems) lost (Martinsson, 2007). The external environment is also often measured in monetary terms or in time of recovery but is often more complicated to give an appropriate unit.

The concept of the risk matrix also complies with recently formulated requirements in GEIA – STD - 0010 by incorporating TSR. According to Clemens & Pfitzer (2006) the risk posed individually by each hazard could be of less importance compared to the risk of total system outage. Tailoring one matrix to represent risk tolerance for individual hazards and another to represent whole-system risk would allow the application of the TSR logic.

7.1.1.4 Threats

In case of a pure qualitatively tailored matrix, the many possible interpretations can easily lead to ambiguous requirements. The question of harm and probability easy lose its meaning discussed in qualitative contexts and eventually the requirement become useless while it is not possible to verify. (Ekholm & Börtemark, 2009b)

Although the matrix is often displayed it is seldom tailored to each specific project and even less often quantitatively equipped. From an industry perspective the matrix is often the only measureable indicator whether a risk is intolerable or acceptable and therefore it is immensely important that the matrix give relevant information about tolerable levels of each hazard. (Ekholm & Börtemark, 2009b, Clemens & Pfitzer, 2006, Clemens *et al*, 2005) The risk matrix also faces the possibility of being misinterpreted. If the axes are quantified (the probability is often stated in powers by the base of ten) the matrix can become misinterpreted by reason of a inconsistent scaling if omitting a few powers or simply by sizing compartments equal. (Ekholm & Börtemark, 2009, Clemens *et al*, 2005)

Defining the quantitative range of interest for which a risk matrix applies, the generic range of interest often has a huge variation. At one end of the scale are events which pose so little risk that they are of no consequence. The risk on the other end is more difficult to define clearly and is often huge and unthinkable. The risk here varies across such a large span that it is difficult to grasp. One can argue that it is impossible to fully comprehend the span of 12 or 15 orders of magnitude. (Pfitzer, Hardwick, Dwyer, 2001, Clemens *et al*, 2005)

7.1.2 Risk summation

7.1.2.1 Strengths

A major strength of the risk summation model is that it considers the amount of risks. The method enables to consider the TSR level and therefore have several advantages. The fundamental improvement is that the TSR now has a finite limit. The use of a risk matrix, in contrast, tolerates an infinite number of risks as long as the individual risk is below a certain level. In addition, the formulated risk quota can be handled dynamically in contrast to the use of a risk matrix. If, for example, a certain risk is considered high, the TSR quota could walk unaffected if several low risk hazards are controlled instead. (Ekholm & Börtemark, 2009b) This brings opportunities of how to prioritize risks. All the risks in a system can for example be evaluated economically in order to find the risks most justified to treat. (Arntsen, 2007)

When allocating requirements the risk summation model is a straight-forward work structure. The tolerable risk of a system is stated in a T-RILL number which are easy to handle and refine to sub-systems by creating risk budgets. It is also uncomplicated to relate to the fact that the system safety work is thought to find, at best, 50 percent of all risks in recently constructed systems. The alternative is the tentative work of tailoring risk matrixes to constitute acceptable risk levels to sub-systems. (Ekholm & Börtemark, 2009b)

The method further emphasizes modeling, simulations and testing which possibly allow for discerning the effects from mitigations and barriers. The reduction of a certain risk is clearly verifiable through simulations and testing before and after the insertion of a particular barrier whereas all parameters are held constant. (Ekholm & Börtemark, 2009)

7.1.2.2 Weaknesses

As most of methods described, the major flaw relates to lack of accuracy and correctness. Specific for risk summations is that it assumes statistical independence. However, the lack of correctness resulting from statistical independence can according to Arntsen (2009) often be neglected due to the superior importance of epistemic uncertainty (lack of knowledge and information of the system). Additionally, to investigate and calculate all dependencies among hazards are seldom economically justified in premature or developing systems (Ekholm & Börtemark, 2009)

Furthermore, when hazards are identified the potential accidents are thought to be cumbersome to investigate. This distribution could, in the best of worlds, be inductively tested or perfectly simulated but is instead often assessed on judgmental grounds. However, it will be problematic to find an accurate distribution when no guidelines exist on how to perform this exercise. (Ekholm & Börtemark, 2009b)

7.1.2.3 Opportunities

If using this method the opportunities are many to assess the risks and prioritize the control effort to hazards. (Arntsen, 2007) As mentioned above different methods could be used and not necessarily in terms of economical means. Any other measure is easy to apply if measureable. An example could be to use environmental pollution.

Using basic and acknowledged systems safety methods as FTA are also proved handy when allocating a RILL number to specific sub-systems and are easily converted to reliability measures. (Ekholm & Börtemark, 2009b)

7.1.2.4 Threats

According to Clemens (2009) there are multiple reasons why this method has not gained the before-hand assumed proliferation. Firstly, summing full-system risk nearly always requires placing a dollar value on human lives. Secondly, only a few of the standards governing system safety practice and require risk summation. Thirdly, risk summations by comparison to risk matrix zoning of individual hazards the latter method is more easily understood, though often improperly taught. (Clemens, 2009)

7.2 The Air Traffic Management industry

ED-125 is one of many documents fundamental to the system safety effort of the Swedish transport agency's aviation department. The agency is responsible to conform to international laws and regulation but also to adopt and customize those into a national legislative framework. According to Oberger (2009) the corresponding Swedish framework (ANS SMS) builds heavily upon the ED-125 standard. ANS SMS is a customized and augmented version of the fixed-prescriptive model (model four) in ED-125. (Oberger, 2006)

In Sweden the principles on ED-125 are customized to conform to the specific conditions in Swedish air space. The details on how this customization is performed are described in the document D-LFV 2006-18538 and are summarized below: (Oberger, 2009)

- The workgroup on ANS SMS has decided to merge requirements specific to AD, APP and ACC systems.
- Furthermore, ANS SMS take the two highest complexity parameters into account (C3 and C4) which are thought to address the conditions in Sweden. This gives a numerical value on the number of hazards but also on the probability that a hazard lead to an effect. The number of hazards has notably been multiplied by a factor of five due to the fact that further hazards are thought to be found in analyses on sub-systems and alike and the total sum are 510 hazards. Conceivably this leads to a more conservative requirement.
- Requirements in ANS SMS are stated in events per flight hour and in events per operative flight traffic management hour in accordance to the international RCS from EUROCONTROL.
- The system definition in ANS SMS differs from ED-125 whereas ANS SMS encapsulates ANS systems in which ATM systems only are a sub-part.
- The workgroup has chosen to follow the recommended level of AF and is set to 10 times stronger than the international.
- ANS SMS encompasses hazards related to technology but also assimilate human factors and organizational factors.
- Only worst credible effect is considered.

7.2.1 ED-125

The work on methods stated in ED-125 is transparent in respect of advantages, limitations and assumptions which are explicitly described.

7.2.1.1 Strengths

According to EUROCAE (2006) the fixed prescriptive model is easy to apply due to the fact that it only considers one parameter – the volume of traffic and complexity. This is thought to overcome reluctance to quantify SOs. It also does not require specification of the probabilities of the hazard generating certain effects. Since only the Worst Credible effect is considered only one probability leading to effects needs to be specified. Hence,

the model is easy to understand and help the system safety engineer to focus on the most important aspects; how the system works and could fail (de Rede, 2009).

Another advantage is that it avoids mis-evaluations e.g. the probability of a hazard leading to an effect, as values are already given. This lead to, on an average basis, correct SOs. It is further deemed that the use of this model eases harmonization and consistency of the safety assessment process when the model is applied to different systems within the same organization. (EUROCAE, 2006)

According to Oberger (2009) the choice to use the semi-prescriptive and the fixed-prescriptive model liberate resources more beneficial to system safety of ATM systems. If to follow the first two models in ED-125 this would lead to an extensive amount of calculations which require both money and human resources. If instead to rely on average numbers calculated beforehand attention could be drawn to system safety aspects as the human factor contributes to 90 percent of all accidents.

7.2.1.2 Weaknesses

Since it focuses only on one scenario i.e. the Worst Credible effect of the hazard it is put on risk to miss details leading to other scenarios. If, for example, rivalry amongst two potentially severe outcomes of a hazard exists only one of them is considered. In addition, whilst the probability of a hazard leading to an effect is calculated and averaged beforehand this number is evenly distributed among all hazards belonging to a severity class. To assume that all hazards have the same probability leading to a hazard may not be true (EUROCAE, 2006). This rough order of magnitude could further lead to an over- or under estimation of the SO for each hazard leading to a more or less demanding safety requirement (de Rede, 2009). Consequently, the use of this model may need further investigation in order to derive an appropriate Safety Target (ST). (EUROCAE, 2006)

7.2.1.3 Opportunities

In ANS SMS each SC are connected to ALARP regions defined to assist decision making activities. It is further suggested how to attack problems when they arise. If a hazard is non-tolerable and the requirement is thought not to capture current conditions further investigations are proposed. The requirement can then be re-assessed, if credible evidence exist, by applying calculations described in the first two models in ED-125 and see whether explicit calculations give tolerable results. (Oberger, 2009, de Rede, 2009)

In addition EUROCONTROL is now working on unifying different national interpretations and versions of the RCS. Whereas the latter classes (2-5) of SCs are not universal, this work will probably improve system safety procedures internationally. (Oberger, 2009)

7.2.1.4 Threats

The only input to the model is the choice of airspace complexity. When this parameter is incorrectly defined this may therefore lead to SOs being either over-engineered or under-engineered. Another threat is that time, money and effort spent on system safety are often limited. (de Rede, 2009)

When a system safety assessment is performed using the semi-prescriptive model knowledge about how the system interacts with the ATM system and the overall aviation system is not required. How hazards and their corresponding effects are interrelated to external mitigations does not need to be understood which could lead to unexpected hazard effects when the system operates in real world. Therefore, the method is not

blindly to be trusted in and a threat is that neither related methods nor tools are entirely mastered. (de Rede, 2009)

7.3 The Railway industry

The railway industry has several standards and international work to consider. Although several methods are found together they build the framework of how to conduct the system safety effort. Not to find any common strategy has partly been arduous when trying to apprehend the system safety effort. Apparently, development is made at different levels when writing this thesis. The European Railway Agency (ERA) is working on CST and Common Safety Methods (CSM) but is not adopted by member countries yet and, in addition, the standards from CENLEC are revised (Ericsson, 2009). In order to extract the most commonly used methods, reports and projects are examined and several interviews conducted and from them the most elaborated methods will be subject to deeper investigation.

7.3.1 GAMAB

To expound acceptable risk levels methods like GAMAB, ALARP and MEM could be exploited. The inherent assumption behind GAMAB is that the risk associated with existing systems is tolerable (CENELEC, 2007). According to Mihm & Eckel (2004) the railway system are being considered as a safe mode of transport and therefore taken as a basis criterion for Common Safety Targets (CST). Also in a report by AerotechTelub on the railway ERTMS regional the working group utilizes the GAMAB principle extensively described in SS EN 50126. All in all, this gives the idea that the GAMAB principle is important within the railway industry in Sweden.

7.3.1.1 Strengths

A strength of the GAMAB method is that by transformations and grouping variables together it is easier to find suitable data from reality (Martinsson, Smith & Svantesson, 2004). Due to this feature it is easier to apply when facing different situations. The principle is based on experiences with similar systems already in use which certainly is the case in the railway industry. In addition, the international railway in general and the Swedish railway in particular are considered a safe mode of transport (Eriksson, 2009, Mihm & Eckel, 2004). The method necessitates a large amount of accident data (Martinsson *et al*, 2004), and therefore a well functioning failure report system is needed. According to Kallman (2009) Ofelia is a well functioning failure report system collecting data suitable for analysis. The GAMAB method implicitly takes the probability of a hazard leading to an accident by the use of the fraction $\tau_{c.ref}$ which ought to improve the accuracy. Furthermore, GAMAB can be stated, by reorganizing the formula, in terms of individual risk which often is the case in the railway industry (Mihm & Eckel, 2004, CENELEC, 1999a).

7.3.1.2 Weaknesses

As mentioned above GAMAB analysis requires reliable system data to be able to compare an existing system to a replacement system. Poorly collected datasets would result in uncertainty and lead to risky assumptions. (Martinsson *et al*, 2004)

The method does not fully comply with the individual risk concept while GAMAB only takes the risk per passenger and journey into account and not the individual travelling profile. (Martinsson *et al*, 2004).

Moreover, when considering the individual risk it is not obvious what the harm consists of. The consequence is not fully defined and therefore it is not obvious what the following risk is; if an accident means fatality, major injury or minor injury.

7.3.1.3 Opportunities

According to Martinsson *et al* (2004) the GAMAB principle is used through linearity which proved useful for several reasons. All in all, using linearity does not require calculations of absolute values. Instead a comparison is made by using the fraction of the existing system and the replacements system. By doing this, less data and analysis is required but has to be compared to an already existing high-level requirement (THR) for the existing system and thereby using the fraction (difference) and calculate the acceptable risk level on the replacement system.

According to CENELEC (1999a) the designer/supplier is free to distribute λ_c (collision rate for the replacement system) between different risks but also different sub-systems components e.g. way-side equipment and on-board equipment.

The use of quantitative risk levels are becoming more and more critical whereas Swedish railroad administration is from the 1990s and forward having less and less close collaborations with their suppliers or contractors. Then it is becoming increasingly important to convey acceptable risk levels, and then quantitative measures are advantageous. (Ericsson, 2009)

7.3.1.4 Threats

The existing system could in several aspects not be comparable to the replacements system (CENELEC, 1999a). For example does the method build upon the assumption that the distribution of casualties among passengers in the same train is similar in the existing and the replacement system.

According to ERA (2007) deriving a high-level requirement from accident data and fatality rates could be misleading due to the high uncertainty and variability in intervening factors from technical failures which are not easy to quantify precisely and consistently i.e. it is hard to construct a proper fault tree.

7.3.2 THR allocation in Sweden

From a globally defined risk level the Swedish way to assign a risk portion to sub-systems and alike is by decomposing the whole railway system into its major constituents parts depending on the estimated contribution of each part to the global risk (Kallman, 2009, Eriksson, 2009, Kinneryd, 2009). The constituent parts could be both organizational and/or physical (Mihm & Eckel, 2004) but in Sweden they are mainly referring to physical parts (Sollander, 2009). In Sweden the high-level requirement for signaling railway systems says that a safety critical failure are not allowed to occur more than once in a hundred years (Sollander, 2009, Kallman 2009, Eriksson, 2006). Surfacing this requirement was not done by any elaborate analysis, instead this was, back in 1994, deemed to be a suitable level of risk. (Eriksson, 2006) Albeit, the level of acceptable risk has proved successful throughout the years and compared to the European risk levels satisfactory (Kinneryd, 2009, Eriksson, 2009). From the high-level requirement and by THR apportionment each constituent part is given a specific THR number. The corresponding SIL level is then straightforwardly assigned by a table. (Kallman, 2009, Kinneryd, 2009) Important to note is that systems not yet constructed in accordance to CENELEC-norms are not encompassed by safety requirements stated in internal regulatory documents at Swedish railroad administration (Eriksson, 2006).

From SS EN 50126, 50128 and 50129 and from the CENELEC report it is suggested to first assign THR to functions and then map functions to sub-systems. The reasons not working this way are several. Firstly, the railway industry is a mature industry which developed long before the era of system safety. Therefore risk acceptance norms and laws are consequently of pure ad hoc character while the safety are already built into the systems resulting from many years of experience. (Niklasson, 2009) Secondly, the system safety approach, described in SS EN 50126, 50128 and 50129, are merely used when developing new systems or when to implement major updates whereas otherwise an extensive work has to be performed, implicitly already done (Kinneryd, 2009, Eriksson, 2009). According to Kinneryd (2009) a pragmatic view has to lay the ground also for system safety when endless financial resources do not exist and because system safety by far has not been neglected before, only not strictly done in accordance to any, then nonexistent, standards.

7.3.2.1 Strengths

The Swedish numerical risk allocation is so far in compliance to corresponding European requirements. Elaborated CST and CSM at European level are also thought to be easily combined to procedures and risk levels in Sweden. (Ericsson, 2009) According to Mihm & Eckel (2004) defining common safety requirements at constituent level is by itself an advantage. They further states that this approach provides direct references for cross-acceptance of products and definition of Technical Specification of Interoperability (TSI) quantitative requirements (Mihm & Eckel, 2004).

By building the technological development on tested principles and not radically alter the system architecture current risk levels are to a great extent held constant and does not need constant updates. Working with tested knowledge, technology and collaborators are also thought of as an important system safety feature. (Eriksson, 2009, Kinneryd, 2009)

7.3.2.2 Weaknesses

Unambiguous apportionment is sometimes difficult due to interfaces and transverse safety functions (Mihm & Eckel, 2004) and are partly exemplified by difficulties shown in THR allocations in the ETCS system where many actors were to define appropriate boundaries of sub-systems. (Eriksson, 2004)

Definitions of risk in current railway signaling systems today do not consider the risk to the individual. The number on THR is not customized to apply neither to an individual risk nor to a societal risk. The definition only considers safety critical failures and therefore it is hard to interpret what this represent to the persons using it and the system environment. (Norling, 2009)

Partly outside the scope of how to refine quantitative risk levels is the allocation of SILs. However, according to Norling (2009) the effort to accomplish different SILs is slightly disproportionally distributed. The quality requirements in SIL 3 and 4 are similar in contrast to SIL 2 and 3. (Norling, 2009)

There is no criterion on risk levels universally accepted in Sweden. According to Martinsson *et al* (2004) the current risk level, referring to the requirement of no safety critical failure in 100 years, would benefit from a further analysis.

7.3.2.3 Opportunities

The Railway Department of the Swedish Transport Agency has started a work on compiling relevant documents, manuals and regulatory internal documents from Swedish

railroad administration, which may result in a more heterogeneous picture of safety requirements (Norling, 2009)

According to Mihm & Eckel (2004) a simple way for improvement of safety performance of railway signaling system could be to increase the requirement by a fixed percentage every year. Considering the vast disproportion of a function (read constituent parts) it seems appropriate to put forth an effort on sub-functions (read constituent parts) where cost-benefit-analysis shows the best results.

7.3.2.4 Threats

As interoperability becomes increasingly important this will, and does, affect systems and their requirements as well. By apportion risk levels to its constituent parts does not respect heterogeneity of EU railways (Mihm & Eckel, 2004). Another point is that a CST apportioned to constituent parts depends on current state of technology and therefore needs to be frequently updated as technology and parts develop. (Mihm & Eckel, 2004) According to ERA (2007) some studies of railway accidents suggests that the proportion of technical failures attributable to the overall risk is very low and is estimated to approximately 1%. This implies that it may be inappropriate to use a quantitative requirement to represent the overall risk when this overall risk is almost entirely determined by the impact of human errors and other non-technical factors.

8 Analysis

This chapter aims to structure the aggregated material and analyze it in accordance to the problem formulation of this thesis. The focus is to highlight methods describing quantitative requirements refinement and allocation, relevant to the system safety effort.

8.1 The fundamental differences among industries

Not surprisingly, differences of best effort, standards and state-of-the-art methods have shown throughout the work of this project. The main reason for the disparate working structures is thought to stem from the actual technology and the level of maturity of the system in focus. Crystal clear is however that system safety does not offer a universally agreed methodology.

As discussed before the penetration of system safety to different industries are to a great extent connected to what consequences potentially brought to the individual. Relevant to this project is the early safety related work in the aviation industry where it is reasonable that a safety culture have risen early. In aviation business the degree of interoperability are immensely important, and naturally international and amalgamated organizations have grown. The grave consequences following an accident and the need for interoperability in aviation industry brought together with the fact that aviation is a relatively young technology lay the ground for a highly developed system safety methodology.

The railway industry, on the other hand, makes use of a technology almost hundred years older, and are not commonly thought of as a high risk technology. Conversely, the armed forces industry develops and use high risk systems but not with the objective to safely transport people. The safety of a military person is often not primarily determined by the technology he uses but what technology the enemy uses. In addition, in order to outclass or defeat the enemy the operative technology is never to be obsolete. The armed forces industry focuses on innovative technology, does not need interoperability (until recently) and work in an environment with low risk aversion. All in all, the aviation has an international agreed framework to follow, the railway follows a national agreed framework and the defense industry has a rather flexible framework of how to conduct system safety.

8.2 The divergence of methods

To apply a limited, general and easy system safety requirement approach two aspects have proved important. The occurrence of a referencing system and the maturity of a system are thought to be highly relevant.

In the ATM/ANS industry a high-level quantitative requirement are set, the refinement are done by legislative organs, and a straight-forward methodology are suggested. Due to the fact that large datasets of failures and reliability values are available generalizations of the amount of intrinsic hazards and the probability that they lead to accidents are made. If accurate, such achievements are valuable to systems safety engineers and also liberate recourses enabling focus on other aspects of system safety such as human factors. This urges a referencing system which in turn collects facts from a mature system. This achievement is therefore not possible if a completely new system is being constructed. This is often what engineers in the defense industry face. Consequently, designing completely new system make top-down requirements refinement much harder. Requirements may not initially be correct until the architectural design moulds and take its ultimate form. This may lead to both inconsistency to a high-level requirement and

ambiguous requirements if not continuously updated. Working with new systems therefore necessitates higher degrees of freedom from methods and standards.

To apply a stringent framework of how to conduct analyses and who is responsible for what often eases the work and avoids costly and time-consuming discussions. The risk of such an approach is to miss or leave out areas needing analyzes just because the system safety framework has a blind spot in the area. This could for example be the case if a framework compartmentalizes too much and if areas needing further analyses are left out only because the responsibility is not properly regulated.

Furthermore, the concept of risk is handled differently among industries. The three domains have, maybe by natural reasons, interpreted the concept of consequences in their own unique way. The RCSs, from aviation industry, handle the consequence in form of one class of accidents (SC1) and the following classes handle incidents. The THR value, made use of in the railway signaling industry, does not incorporate any aspect of consequence and it is therefore hard to interpret the significance of different hazards on lower levels whereas only the probability of the hazards serves as a measure of the risk level. Working this way partly diverges from the risk concept and become more of reliability analysis due to the fact that it does not consider any consequence.

Crucial is also the concept of a hazard. The concept of a hazard can apply to functions, system parts, random failures, process failures, human factors etc or parts of interaction among them all. Not knowing what to incorporate in system safety analyses are therefore important. The ATMSP in ED-125 specifically handle technical hazards and the railway distinguishes between random and systemic failures. If treating risks coming from system parts and not incorporating human factors are thought to only give a limited understanding of the risks. How to handle this particular issue is proved to be handled differently among the industries studied. In the aviation industry this is sometimes described in regulatory documents which is not seen neither the railway signaling systems nor the industry of defense. To compartmentalize too much is, on the other hand, not always desirable whereas a hazard can incorporate technical, procedural and human factors.

Another issue is on what level a hazard is best described. A hazard can either be described at a high system level describing, for example, a mid-air collision and but it could also describe a sharp edge on a chair. The many implications of a hazard urge a definition of how to handle them all or if only to handle a fraction of hazards i.e. the technical hazards applicable to a specific level.

8.3 Deficiencies in methods and industries

It is important to have a structured and logic chain of requirement allocation in an industry. It is virtually meaningless to start deriving quantitative requirements at a low level of development when the figure do not map to any high-level requirement. It is further imperative that each industry follow an agreed logic of how to allocate quantitative requirements. If a high-level risk level of a system is apportioned to functions in one part of a system and to accident types in another, requirement consistency, ambiguousness and correctness becomes hard to advocate. Furthermore, inconsistency also becomes apparent when there is no agreed level of risk quantification in a project or system.

In the railway system the most apparent deficiency appears to be the heterogeneity at international level reflected in standards and legislative documents. This is partly a result

from the long life-cycle of the railway system. International harmonization in all industries will probably become increasingly important which is partly a political question and therefore making this even more difficult. In addition, the standards only consider a system safety effort only applicable to changes in prevailing systems or in fundamentally new systems. In almost all countries it seems more appropriate to suggest methods and work structures also applicable to old technology.

Crucial to derive risk levels is descriptive data. The railway industry has a well functioning failure report system accountable to set risk levels. To use a proper risk definition the industry need a common risk classification scheme which is not found. The Swedish ANS authority also has accessible data to support risk classification and an internationally agreed definition of consequences. The armed forces industry is thought to have data but it does not seem to be used to set risk levels and the risk definition is hard to set globally due to the large set of operating systems. Though, the industry is aware of this and proposes that the risk level should be customized to each project.

The definition on safety integrity suggests implications of interpretation. To cause an accident a safety critical failure has to occur plus the exposure of meeting another train has to occur. All in all, this means the only hazards on safety critical systems are valid as hazards, not the system itself. This is fundamentally different from other definitions in system safety and therefore it is crucial to fully comprehend before starting analyses.

8.4 Generalizing methods

This project generally concerns the matter of how to handle quantitative requirements within system safety work. This report so far brings about several aspects concerning system safety. Contemplating aspects of this matter raise several questions at different levels of abstraction. System safety concerns a socio-technical system, legislative organizations, risk models, risk methods, risk theory, requirement processes, system safety processes, several documents and standards. Keeping focus on what is important, the aim of this report is to answer the question – how do you work quantitative requirements? Several methods are found but all of them comply with different contexts. The question then becomes what those different contexts are?

The aim of this report is to make use of existing theory and UML activity diagrams such that different models could be compartmentalized. What will be described here is a best effort to structure the reality and how it looks like today by using theory, best practice and experience. The notation in Figure 15, Figure 16 and Figure 17 is described in Appendix 1.

8.4.1 Defining hierarchies

From system theory three different approaches to systems are described. Larger systems built today are often exhibiting characteristics of what is called *organized complexity*. Theory on such systems are elaborated and described in the chapter on system theory. First to consider is different hierarchies in system development. By using a hierarchy relations among objects or abstract objects are shown. This chapter aims to differentiate the levels of hierarchy and eventually define the levels relevant to this project.

The first type of hierarchy refers to the system. The main focus of all actors is the system in focus, in this thesis always containing technology. The system itself is often possible to reduce to sub-systems and in the end to their physical components. To model a system is proved to be an extremely hard task. If scientific advances eventually accomplish to model complex dynamical systems the area of system safety will have many problems

solved. A system is often displayed in terms of a system, its sub-systems and its components on the lowest level.

Another relevant hierarchy is the relation among actors. The actors are the organizations trying to control the risk. Reality is structured in a way such that different liabilities lie on different actors and contribute in different ways to eliminate the risk, which is often displayed in documents or products at different levels. The international legislative organ constitutes the absolute top level of such organizations. International organs always have, at least in Sweden, a national counterpart. Brought together they could be thought of as the top level of organizations regulating system safety. Next level is often a mid-level organization e.g. an operator or a procurement organization working on refining system safety liabilities. The third level is the organization or the group working hands on with system safety. As described earlier system safety is often one aspect in the development of new systems and has close collaborations with systems engineers i.e. a supplier or developer. The developer or contractor could also be any safety manager operational later in the system life cycle in contrast to the construction phase.

In the chapter on terminology the risk hierarchy is described and illustrated by the chain of events occurring to compose a risk to any object. Basically this chain of events are tried to be controlled somehow. This chain of events is however to be seen in relation to the previous defined levels of hierarchy. The top level; legislative bodies, and total system level, are primarily interested in accidents and to formulate what an acceptable risk is. The first mid-level, operators, procurement organizations and the sub-systems level are interested in refining a risk level to sub-systems and therefore also the hazards within. The third level, investigates and analyzes the failures and risk sources. It is often the responsibility of a contractor or developer to analyze a minor section or sub-system down to specific components of the system.

On the whole, empirical studies combined with the theoretical framework outline the hierarchies incorporating the hierarchy of the system, the actors and the accident model. This is further displayed in Figure 14.

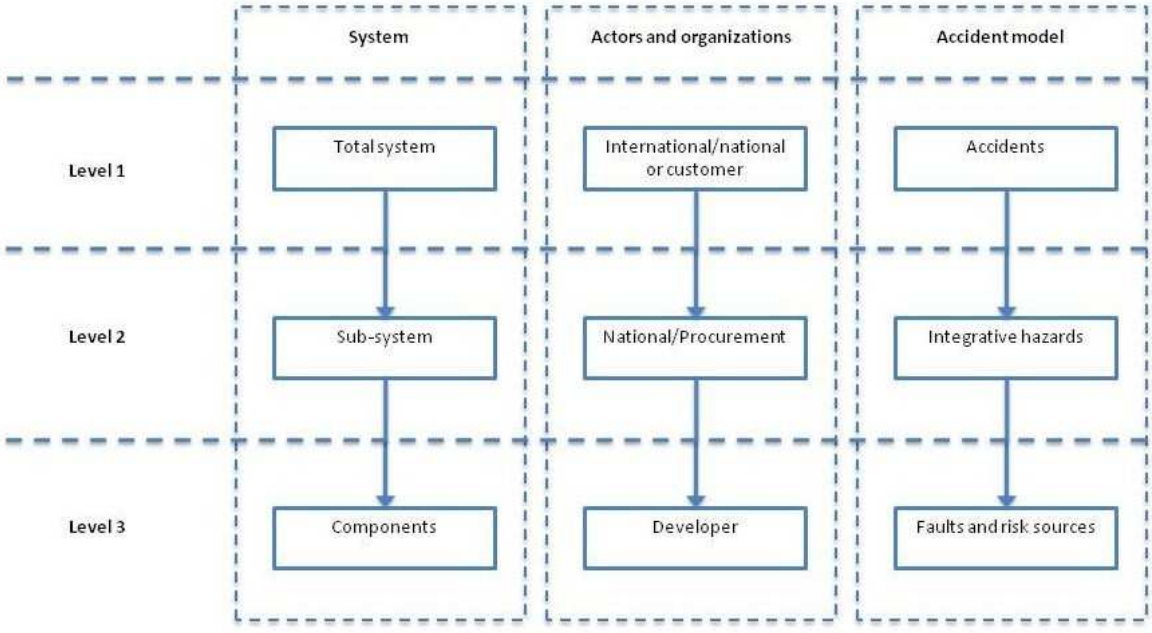


Figure 14 Hierarchies

8.4.2 Methods in processes

The model of communication and control partly refers to the terminology of hierarchies meaning that hierarchies are characterized by control processes operating at the interfaces between levels and that the control process yield activity meaningful at a higher level. The activities on each level can be captured by its own dynamics which does not apply to associate levels only that upper levels compose constraints on lower levels. Furthermore, each level is captured by its own control activities which imply the need for communication with its environment in form of inputs and outputs.

Stated above is basically a quotation of the systems theory chapter, and it yields an immediate mental association to the processes described in the chapter *5.4 The communication and the* control processes; the systems safety process as well as the requirements process. At each level of hierarchy the control process is analogous to the risk control process amongst several others. The control processes is parallel both on each level and between the levels. Take for example the continuous work on laws and standards from organizations at the top level. This work is one control process whose work is considered by control processes on the mid-level e.g. FMV or Swedish railroad administration who continuously work on improvements on their level. Apt examples of such improvements are manuals or work to refine the top-level requirements to comply with their specific interests.

Considering communication between different levels of hierarchy and the processes on each level, the system safety process emerges parallel to the system development and requirement process. It is important to remember that those processes seldom are properly defined but is instead an abstract pattern captured in the concept of a process. The distinction between the three processes is first and foremost made by theorists but this terminology is found to fit well with observations and the nature of standards and alike. The distinction is further relevant in order to distinguish how system safety requirements are treated and communicated. Taking this approach makes it easier to generally describe the patterns of how the work is conducted without taking only one industry into account. The result of this project is a description of how quantitative system safety requirement methods are interrelated and when to use them and it is therefore important to remember that this is one process embedded in the process of system safety. The system safety process in turn, is an integral process to the requirement and legislative process but also to the system development process. Those processes together can be differentiated to different levels etc.

The communication between the levels varies widely. The hierarchies defined in the previous chapter, described one system hierarchy, one organizational hierarchy and one hierarchy in the risk concept model. The communication between different levels in a technical system could be signals, physical transport etc which are to be controlled. In the hierarchy of organization the communications are often achieved by different documents controlling the system safety effort among actors. In the accident model the levels are tried to be controlled by mitigations operating on and between the different levels. The communication is here to be seen merely as the probability of a course of events.

Also important is that higher levels compose constraints on lower levels. The system safety process on, for example, the developer level has to comply with the requirements from the customer. The constraints from high levels also have a wider implication in the fact that the structure must follow a specific logic. If an acceptable risk level from FMV is demonstrated by a qualitative risk matrix there is no idea to start using, for example,

risk summations. If doing so there is no logic chain due to the fact that the control process on each level is not dependent on the level above.

8.4.3 Recursion

From the *1* Introduction chapter the system safety process is to be seen as a recursive process and this becomes evident when studying system safety effort at a top-level. Even though development often is seen in a top-down advancing process the results of a later phase in the system safety process could necessitate changes in previous phases. Take for example the example of completing the PHA. At a top level of hierarchy a PHA is often performed in order to be able to derive quantitative requirements but the PHA at this level is seldom complete. Instead the work on the PHA continues by other actors at a lower system level and eventually brought back to the customer or equivalent.

8.5 General model of work structure

The model is to be seen as a mixture of the theoretical framework and the methods found when investigating the area and could serve as a helpful tool when working quantitative safety requirements. Though, the context of each industry does not always allow for all of the suggested activities. The premises are then fixed by standards or other legislative organs. However, if no such directions exist and it is free to choose between the models the most important models are further investigated by its pros and cons in the chapter *7 Methods of requirements refinement and* allocation.

8.5.1 The risk concepts – Level 1

What almost all industries and standards acknowledge as true is that risk is a combination of probability and consequence. The combination is often approximated by the product. On the contrary, to whom and what the risk constitutes a threat is not an agreed subject. From the model of system requirements found in Figure 9 it is suggested that safety requirements concerns property, environment and health. From standards and reports it is suggested that risk focuses on airplane crashes, train collisions, the individual risk, the societal risk, risk to third person, risk in loss of lives etc. If trying to pigeon-hole this it is easily agreed that everything concerns an aspect of health of human lives and not property and environment. The differences lie in more or less sharp or distinct measures of the risk. To say that the risk is that the plane crashes is not a very precise measure of what the risk is to the individual health. By comparison, if to say that the risk is to face a major injury e.g. a broken leg, airplane crashes and train collisions mainly refers to blunt measures. However, how to define the risk is dependent upon the system being studied but also regulations in standards and other documents etc. The idea is that dependent on specific risk concept different models to calculate requirements are more or less suited.

Embarking upon the challenge to give a high-level requirement one of the first steps must be to analyze the context of a system and gather relevant information. Such information would be to analyze the risk definition; is it pre set by standards or is it free to define? Information about high-level hazards and giving a proper definition about the system boundaries are also information needed to facilitate further analyses.

Airplane crashes and signaling failures does not set a specific figure on lives and instead state a requirement in the form of a tolerability value on that particular accident e.g. the RCS in ATM systems. Dependent on how the GAMAB principle is used the principle could be appropriate to use if considering a risk definition in a number of accidents. The GAMAB principle is implicitly used to calculate requirements in ATM systems but also found in several other applications.

Slightly less demanding is the use of individual risk concept primarily found in the railway industry. The formulation is different from the GAMAB principle whereas the risk is formulated in the perspective of one individual. Both MEM calculations and THR calculations make use of this definition by using IRF. The two methods greatly differentiate in required effort. It is important to note that THR calculations, originally, take an IRF value as input but can also be applied, if instead the THR value is known beforehand, to calculate the IRF value. This is the case in the railway industry where a high-level THR requirement is set for all railway signaling systems.

If the risk definition allows for, or requires a sharp description of the risk, considerations can also be taken to conform to minor consequences of the risk. The assumption is in accordance to the RILL-concept where fatalities, major incidents and minor incidents are weighed and gives a figure on the consequence. This concept is also utilized in THR.

After the achievement of setting a risk level from an, for example, acceptable referencing system, other decisions must be made. It is often appropriate to tighten the requirement further by applying AFs or by tighten the risk level on severe accidents.

The case of a risk matrix is somewhat complicated and its usage is hard to fully comprehend. Sometimes it is merely an illustration of a particular risk. Sometimes it defines a tolerable risk level of a system and sometimes it serves as a method to estimate hazards. The confusion is therefore substantial of how to actually relate to the risk matrix. If used as a tool to set a tolerable risk level of a system the problem is often that it is seldom customized to actually mirror the actual risk level of the system but is instead only copied from other projects or theory books. Remembering conceptions from SRS, a requirement stated like this lacks correctness, consistency, verifiability and is often ambiguous to different actors. The risk matrix is a widely used tool to set a tolerable risk level on a system albeit not highly thought of lately. If to use a risk matrix or equivalent this is merely a tool to illustrate the risk. If the axis are continuous, exponentially described and the consequence is properly quantified, the tolerable risk resulting from THR, MEM, T-RILL calculations is easily illustrated. ALARP regions are exclusively used together with a risk matrix and serve both decision-making and displaying calculated uncertainty. Figure 15 displays the most important activities of Level 1. The lines out from the figure are further connected to the second level which will be discussed in next chapter. Figure 15 is a part of Figure 18.

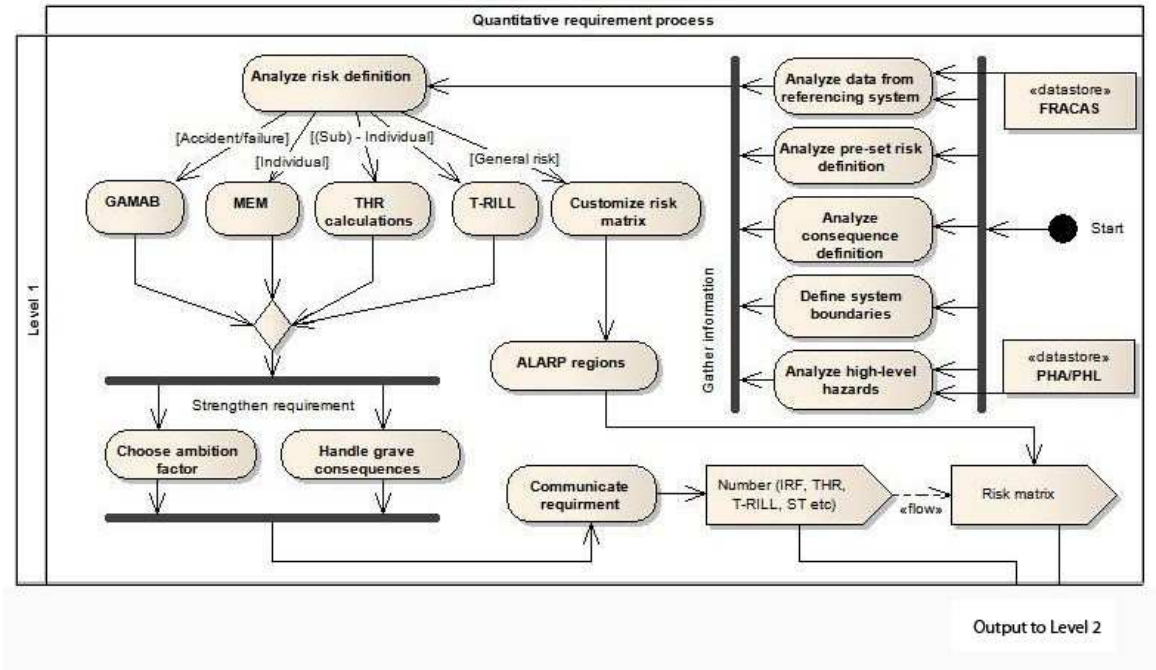


Figure 15 Level 1

The armed forces industry is the industry where the freedom of choice amongst methods is highest. Considering the first level, no model is fixed other than the general requirement that an appropriately defined risk level should be accomplished. The most usual way of working is by the use of a risk matrix although future development suggests starting working with T-RILL values instead.

The ATM industry has a completely different approach to quantitative requirements in comparison to the armed forces industry. International legislative organs have together agreed on an appropriate risk level for all air traffic. This figure is then apportioned to the different countries by the individual amount of flight ours. Then this requirement is tightened by the use of AFs often resolved by the national ATMSP.

The railway signaling industry is working its way through a new era of interoperability, not in a technical meaning but in procedural meaning. Different methods are suggested and harmonized on a European level and although the Swedish railway system is considerably safe it might have to take the new legislative demands into account over time. In Sweden a high-level requirement is set for signaling equipment; one safety critical failure per 100 years.

8.5.2 The refinement concepts - Level 2

Next level primarily concerns the matter of refining the high-level requirement from a legislative body on total system level to, for example, sub-systems. When working with quantitative requirements it is fairly easy to actually refine or apportion the requirement to sub-parts of the system. The hard question then becomes what those sub-parts are? At least five possible ways are found to distribute the high-level requirement on. The railway signaling industry in Sweden uses the constituent parts of the system and the ANS industry uses several ways. In the ANS industry, first the high-level requirement is recalculated to conform to the actual amount of flight hours in Sweden. Then the requirements are distributed over the systems e.g. ATM, ATFM, ASM etc. and thereafter on the number of hazards within each sub-system. The approach to refine the high-level

requirement on to sub-systems is also proposed by the armed forces industry. The following task then becomes to map the relevant hazards on to a particular sub-system. The approach suggested from CENLEC is to first distinguish the functions then map all functions to the constituent parts of the system and from them indentify all hazards rising from the particular functions. Nevertheless, when refining a requirement the analyst is not bound to follow only one way to refine the requirement but instead use several techniques as long as they logically fit the context of the system. Therefore the refinement must be preceded by an analysis of how the system is constructed, its interactions and boundaries determining which refinement methods that fits the inherent logic. When separating a system into sub-system it is also important to analyze the boundaries and interactions of sub-systems in order to find hazards rising from such integrations. Another aspect is to analyze the independence of sub-systems and its functions. When a requirement eventually is refined to sub-systems it often needs to be balanced. A suggestion is to spare a fraction of the overall portion which makes the requirement conservative. This "reserve" could be saved for future unexpected risks. The requirement is then further communicated to the stakeholder responsible for that sub-section of the system. The aspects of level 2 described above are summarized in Figure 16.

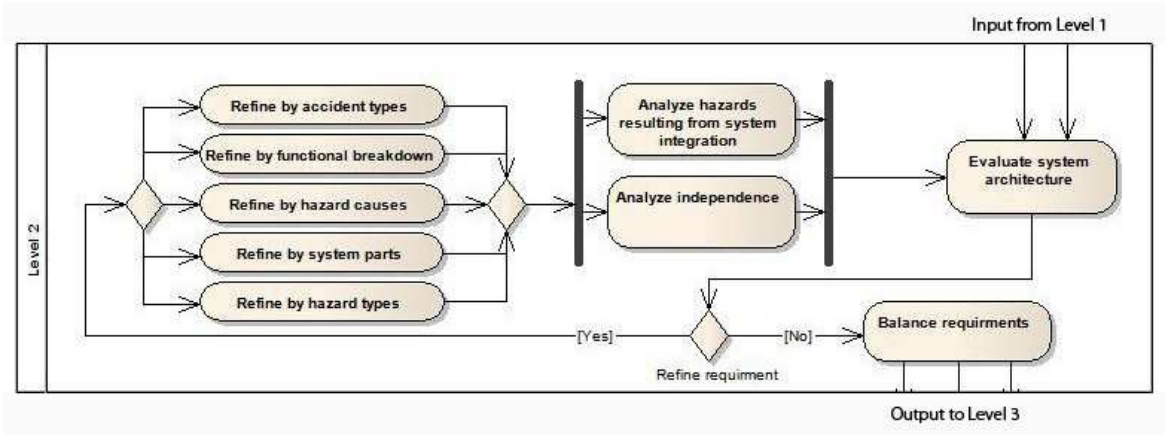


Figure 16 Level 2

The second level, in the defense industry, is the concern of the procurement organization; FMV, responsible for refining the requirement from FM, often by analyzing the system architecture and deciding an appropriate risk level. The outcome from FMV is often a strengthened requirement using ALARP regions.

In the ATM industry, the national ATMSP suggests a refinement of the high-level requirement. In Sweden the first refinement is made in accordance to the actual system components i.e. the constituent parts. Next step is chosen to be the use of ED – 125 in order to generalize the amount of hazards in relation to each severity class. The national ATMSP further suggest an appropriate level of airspace complexity and is from that given an averaged and conservative number of the hazards coming from each sub-system. Also the exposure of each hazard is suggested and from that a final restriction is given on each hazard found in the system.

In the railway signaling industry, the refinement process is achieved by dividing the requirement (THR number) on the constituent parts of the system. From this THR number, a SIL is allocated either by Swedish railroad administration or the supplier. External risk reduction facilities and the system risk reduction facilities should,

eventually, match the necessary minimum risk reduction required for the system to meet the target level of safety.

8.5.3 The allocation and verification concepts – Level 3

The process of hazard analysis can start at a high level. It is for example suggested by the CENELEC standards that the railway authority is responsible to perform hazard identification and hazards assessment. Although, from observations and interviews it is found that this is not the case and that hazards analysis is most often performed on a lower level and often by contractors. However, both the aviation industry and the railway signaling industry take a wider approach. They define processes as SIL, SWAL and PAL etc., which are to be seen as quality packages of how to meet and verify a quality level of system development. Depending on the risk level of a particular sub-system the development must then follow a particular set of quality activities and achievements incorporating hazard analysis. The process often also contains measurable aspects assisting the verification of the system safety effort.

Nevertheless, the hazard analysis is the heart of system safety and it is the assessment of hazards that incorporate QRA methods in order to give a logic chain and to estimate the level of risk in a particular sub-system. Basically, it is a choice if to assess every hazard to a particular risk level or sum the hazards and then match to the risk level. The assessment of risk also has a falling scale of ambition. The analysis that requires least effort is probably by assessing a hazard in a most credible scenario, taking the probability of occurrence and the consequence of the hazard into account. This is usually done by a using a risk matrix. On the contrary, a hazard can be estimated by performing more elaborate calculations, using both ETA and FTA, and thereby taking all hazards and all possible accidents (and incidents) into account. Examples of more elaborate calculations are ED-125 model 1 and 2 (and 3), I-RILL calculations or by calculating the IRF. The hazard analysis is an iterative process and is not a pure top-down approach.

The process of analyzing hazards eventually results in both an agreed level of each hazard but also requirements. The requirements are of various character e.g. reliability requirements on components, requirements on introducing barriers or other design changes but could also be referred to the functions (FRs) of the system. At the third level the focal point is the hazard analysis. A clear duality amongst the industries studied is if to consider total system risk or not, which is illustrated by the two iterative regions in Figure 17. When an agreed level of each hazard is achieved the total system risk could be analyzed by summing all the hazards found (or calculate that for instance only 50 percent of all hazards are found) and match to the high-level requirement.

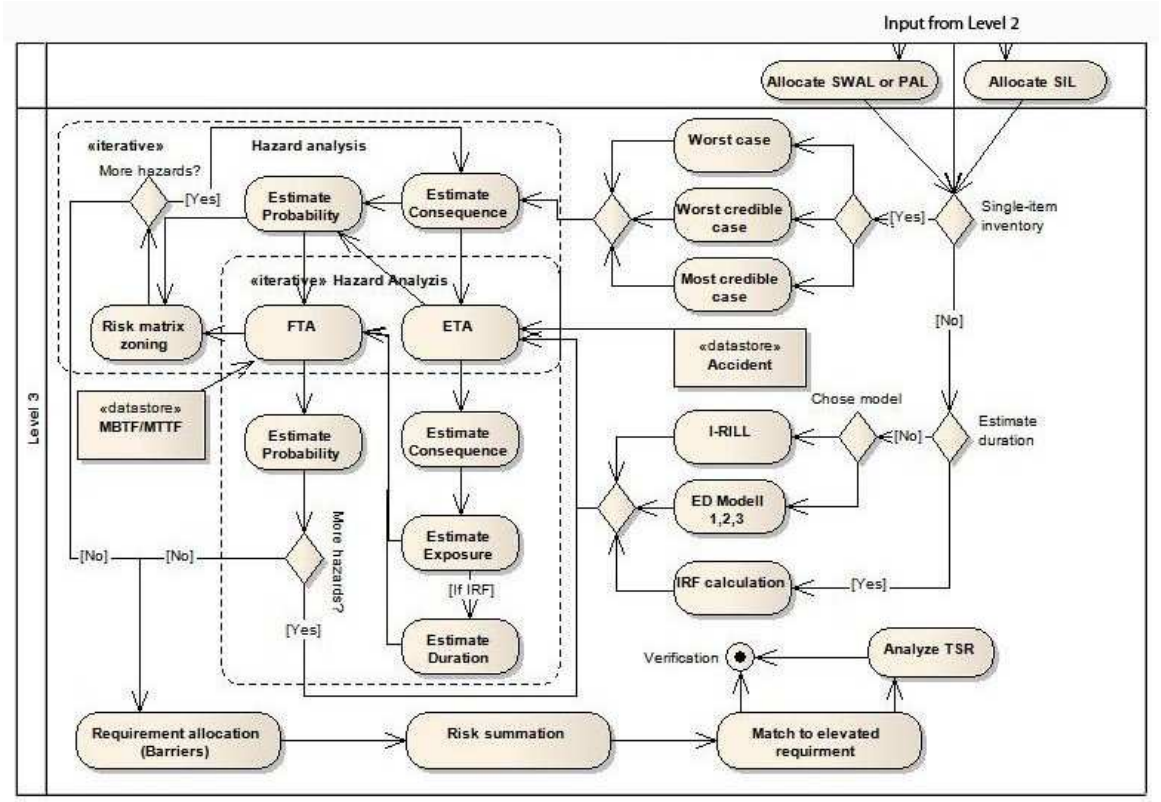


Figure 17 Level 3

In the defense industry, the actual system development often starts by contracting a supplier. Either the supplier handles the system safety process in-house or outsources on, for example, Combitech. Sometimes a PHA and a risk assessment exist already at this point, though the most common situation is that the system safety process starts when the supplier is contracted. Today a *single-item inventory* is often used, evaluating each single hazard against the high-level requirement i.e. a risk matrix. The risk summation is a suggested method where all hazards are taken together and then matched to the high-level requirement. This makes the process not a pure top-down approach and urges an iterative hazard analysis process. After the final agreement on an appropriate risk level for each system a further refinement is suggested and it is free to use any appropriate method.

If to develop a new system or upgrade an existing system, an elaborated description of how to conduct the system safety effort and how to handle each hazard separately, is given by the SAM framework. The hazard analysis is then performed by assessing each hazard against the high-level requirement, and dependent on the size and the art of the hazard, different quality processes is proposed. If the hazard has the art of a procedure a specific quality assurance level is given by the framework of PAL etc.

8.6 Method discussion

Since this study to a great extent is a descriptive or exploratory study heavily relying on printed material referring to multiple sources, the most severe biases are hopefully avoided. Another reason advocating reliability is that the field from where material is gathered is narrow. The methodologies are not profoundly described anywhere which in turn gives only a slim chance to find diametrically different information. One reason not to explicitly providing interview templates, although such were created, is that they were impossible to follow. This is partly due to the various experiences from respondents.

Another reason is that the methodologies were not possible to clearly define, enforcing open interviews rather than semi-structured.

The material has also proved harder to grasp in one particular domain. The field of railway signaling required much more effort than the other industries. The reason for this is first that almost no experience from that domain exists in-house at Combitech and the information had instead to be extracted from interviews and mail correspondence. Furthermore, the railway signaling industry has developed several methods applicable to this study but in reality merely uses a limited number.

It is further found during this holistic multiple case study that the three application domains have diametrically different methodologies to handle quantitative requirements. This is partly mirrored by the amount of standards to consider when entering the field. Hence, if only considering the actual methodologies external validity is not achieved. However, combined with the theoretical framework and the interpretation of methods the three application domains have many aspects in common and the result of this study could therefore be applicable in other contexts as well. The fundamental differences and divergence of methods has also been explicitly discussed.

The proposed model has been tested by a smaller amount of persons at Combitech. The test persons have different experience from the system safety field and have during the work conveyed suggestions of improvements which have been accounted for.

9 Results

In this chapter the topics from the analysis are put together to display the proposed work structure of how to handle quantitative requirements. The model is a suggestion of a pure top-down approach of how to deal with system safety requirements which is not always possible. The notation in Figure 18 is described in Appendix 1.

9.1 Quick reference guide

If to look closely at Figure 18 small numbers are placed on top of the activities which are explained briefly below:

1. Embarking on the challenge to handle quantitative requirements starts by analyzing the system, similar system, data from FRACAS and the system architecture.

2. When an overview of the system is achieved the question becomes how to handle the risk definition. This analysis is tightly coupled to the definition of consequences. Dependent on the system character more or less sharp measures of consequences is suitable which in turn is followed by appropriate methodologies eliciting appropriate risk levels.

3. After the acquisition of an appropriate risk level considerations must be taken if to strengthen the requirement on the system and if to handle accidents with grave consequences differently.

4. The tolerable risk must then be communicated in a proper manner understandable to all actors. The communication of requirements can be accomplished in several ways but are in general done by conveying a number or a risk matrix.

5. In order to refine the requirement and allocate the requirement on appropriate properties the refinement has to be preceded by an evaluation of the system architecture.

6. The requirements can either be refined on several properties or not distributed at all.

7. After the choice of a suitable property to refine the requirement on, integrative hazards, i.e. hazard resulting from systems of systems, must be analyzed. It is further important to analyze independence of the properties.

8. When a proper refinement is performed the requirements often benefit from being balanced and may save a certain budget for unexpected risks. From here some industries allocate safety packages such as SWAL, PAL and SIL.

9. Choose if to estimate each hazard by a single-item inventory i.e. not considering all hazards together.

10. Choose if to use a method explicitly estimating both duration and exposure of a hazard or only the exposure.

11. Determine how to analyze each hazard in the single-item inventory. Dependent on the choice of how to estimate the risk or the result of a hazard, different hazards are given certain priorities.

12. Chose if to apply I-RILL calculations (from the defense industry) or to utilize the framework described in the first two models in ED-125. In ED-125 the consequence is pre-defined by the RCS and cannot be given a figure to jointly compare the categories. This could be achieved by I-RILL calculations.

13. Estimate the consequence in accordance to the definition of consequences. This is often a part of the risk assessment process. Choose if to use ETA in order to estimate different outcomes of a hazard in order to assist the consequence estimation or to estimate the probability of each hazard.

14. When using more advanced methods the consequence analysis must be preceded by an ETA if to calculate several outcomes and effects resulting from a hazard. This analysis is often assisted by data from accidents or simulations.

15. The exposure to a hazard can take various forms and dependent on the logic also given different units.

16. If to use IRF calculation the duration of a hazard must be explicitly estimated and in accordance to the formula described in section *6.4.6 THR calculations and SILs.*

17. The probability of a hazard to occur can be calculated or estimated by a number of means. An FTA is often required when performing more elaborate analyses and is then often assisted by reliability data. Methods from reliability engineering and QRA then become paricularly useful.

18. When no more hazards exist and the inventory is complete, allocation of requirements is performed, if not done earlier. When the inventory is complete several methods allow for analysis of TSR through risk summation. The TSR could be matched to the high-level requirements on either a particular sub-system or the system in its entirety.

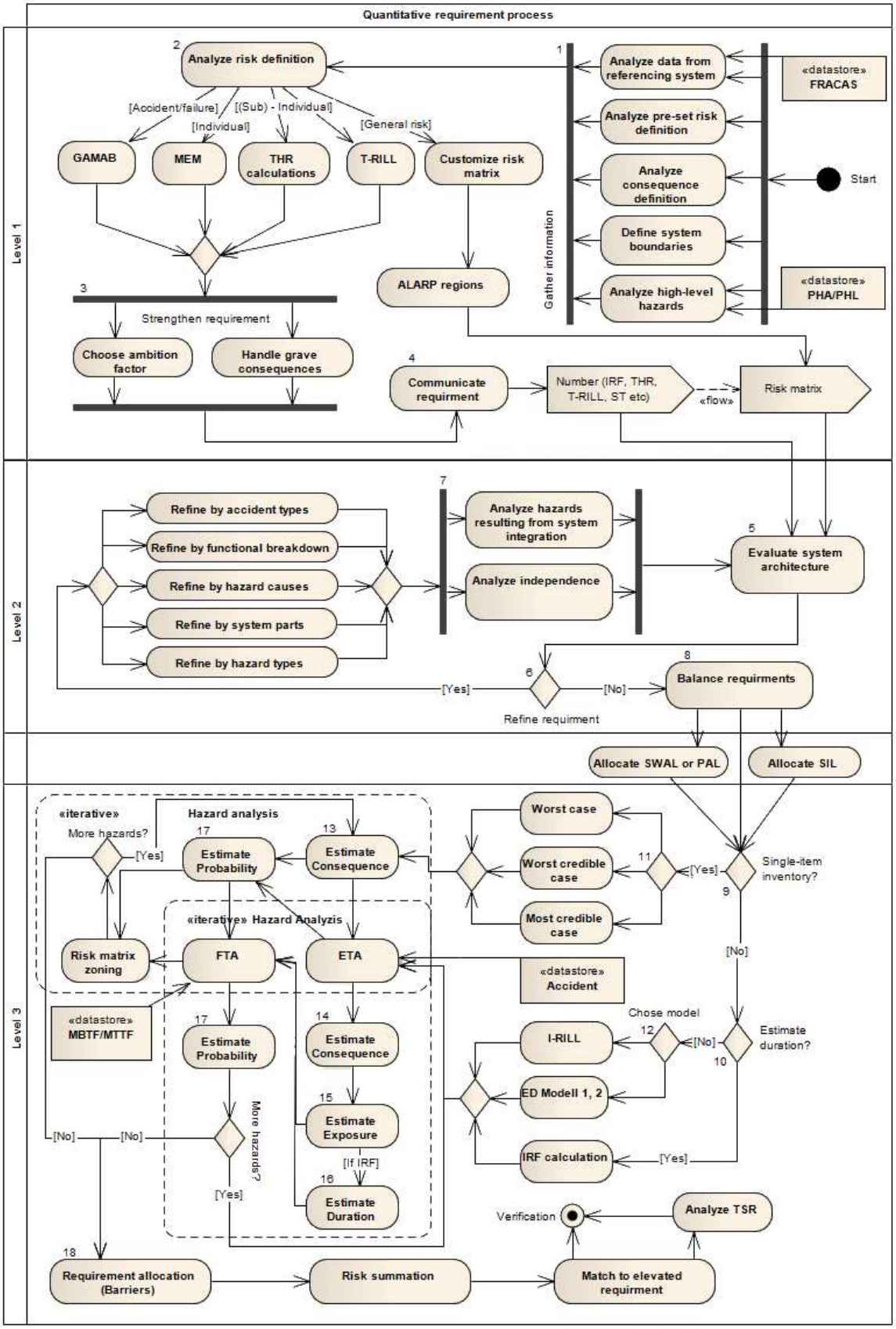


Figure 18 General model

10 Conclusions

In this chapter brief answers are given to the three research questions described in chapter 1.4 Problem formulation.

- What different methodologies are available today to elicit, refine and allocate quantitative requirements relevant to system safety?

From the empirical foundings it is clear that several methods are available which incorporate quantitative requirements. The methods are described in the context of each application domain issued in chapter *6 Three industries and their methods* and the method utilized in Sweden are further described in chapter *7 Methods of requirements refinement and allocation*. It is also obvious that there is no consensus amongst industries on how to handle the difficulties imposed by such an approach.

- Is it possible to suggest a general approach, guiding the work on quantitative requirements in system safety and if so what would such an approach look like?

Although it has proved hard to analyse the different methods relative each other, the gathered theory has proven to be useful when trying to put the gathered methodologies in relation. The suggested approach to guide the work on quantitative safety requirements are described in the previous chapter. The suggested approach is predominantly to be considered as a top-down refinement process of requirements considering three hierarchies. The approach further aims to structure the use of different methods found the application domains.

- What differs among the three industries and what could be learned in order to improve the situation of today?

In general, to be able to derive a tolerable risk data from failure report systems has proved crucial to almost all methodologies independent from intended use.

It is also proven to be difficult to assert one generic methodology to an arbitrary domain due to the fact of inherent fundamental differences, although general concepts have shown valuable.

Managing quantitative requirements in system safety are, by and large, a task of incorporating a logical chain of refinement and allocation mapped against a high-level and agreed risk definition which only a few methodologies facilitate. However, a certain freedom of choice is advantageous when to consider diverse systems architectures. On the contrary, mature and static architectures benefit from a more rigid legislative framework in respect of quantitative requirements management.

11 Further studies

The theory and model in this study is adjusted for the implementations at Combitech, and only generalized amongst the three applications domains. A natural development of the findings would be to take more domains into consideration. Different domains have different technologies to consider but if even more domains are included better generalizations could theoretically be achieved. The analysis would further benefit from the inclusions of more mature and relevant methodologies, supposedly found in e.g. the nuclear industry.

Another interesting and beneficial direction for further development is to reflect on the possibility of handling dependencies in the system. Functions can for example be excessively interlinked and therefore not entirely independent from each other. Such dependencies could be modeled and is not included in this thesis. The usage of such analyses are thought only to be relevant when the system are either highly critical or when evaluating extensive projects or systems.

In the work of managing quantitative requirements it is also important to discuss if it is possible to refine and allocate requirements in the form of numbers. Several authors have demonstrated their disapproval of measuring risks numerically and their refutations are valid arguments. A threat is to blindly focus on numbers and omit analyzes such as human factors and hazards resulting from procedures and alike. To fully capture the risk level of a system an interdisciplinary approach incorporating several aspects of a system are thought to be imperative. A suggested domain for further research is therefore if the inclusion of such questions also in the work on quantitative requirements is possible.

The models studied in this project almost solely consider one aspect of system safety namely the risk to human health. However, it might be possible to incorporate other aspects of risk as well. A methodology could also consider the property or external environment. Several methodologies would allow for integration of property. In contrast, merging also external environment into one methodology are thought to be hard to achieve. However, the contrasting and compartmentalized methodologies would benefit from integration amongst domains as well as over disciplines.

12 References

12.1 Literature

Abrahamsson, M, 2002, *Uncertainty in Quantitative Risk Analysis – Characterization and Methods of Treatment*, Department of Fire Safety Engineering, Lund University, Sweden

Ahlin, J, Elmlund, P, Enander, R, Hagström, M, Hallberg, J, Hallberg, N, Svensson, P, Timerdal, J, Yi, C-H, 2005, *VO StraMtrl 21121:57900/2005 Teknisk Prognos 2005 Bilaga 1 Komplexa System*, FMV, Stockolm

Anderson, I, 1998, *Den uppsenbara verkligheten – Val av samhällsvetenskaplig metod*, Lund, Studentlitteratur

Appukkutty, K, Ammar H, Popstajanova, K, 2005, *Software Requirements Risk Assessment Using UML*, Computer systems and applications, page 1-4

APT Research Inc, 2007, *Final Report: System Safety Performance Level Model*, Huntsville, Alabama

Arntsen, V, 2007, Summation of risk – Assessment of total system risk for complex systems, Uppsala University, Uppsala

Björklund, M & Paulsson, U, 2003, *Seminarieboken – Att skriva, presentera och opponera*, Lund, Studentlitteratur

CENELEC TC 9X, 1999a, *SS EN 50126 Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)*, Brussels

CENELEC TC 9X, 1999b, *SS EN 50129 Railway applications – Communication, signaling, and processing systems – Safety related electronic systems for signaling*, Brussels

CENELEC TC 9X, 2007, *CLC/TR 50451:2007 Railway applications – Systematic Allocation of Safety Integrity Requirements*, Brussels

Clemens, P & Tom Pfitzer, 2006, *Risk assessment & control – Is your system safety program wasting resources*, Professional safety, The American Society of Safety Engineers, January 2006, page 41.44

Clemens, P, Pfitzer, T, Simmons, R, Dwyer, S, Frost, J, Olson, E, 2005, *The RAC Matrix: A Universal Tool or a Toolkit?*, Journal System Safety, System Safety Society Inc.

Department of Defense, 2001, *Systems engineering fundamentals*, Fort Belvoir, Virginia, Defense Acquisition University Press

Depoy, E & Gitlin, L, 1998, *Introduction to research: understanding and applying multiple strategies*, St Louis, Mosby, cop

Drogoul, F, Kinnersly, S, Roelen, A, Kirwan, B, 2007, *Safety in design – Can one industry learn from another?*, Safety Science, vol 45, page 129-153

Ejvegård, R, 2003, *Vetenskaplig metod*, Lund, Studentlitteratur

Ekholm, R & Wallentin, P-A, 2003, *LectionsPM. Swedish Defense Materiel Administration, System safety course 54A,* Common part. Chapter 5, page 9, Version 0.11, 2003-01-23.

Ekholm, R, 2005, *Risk Calculation for Complex systems*, Stockholm, Sweden

Ekholm, R, 2006, *Summation of risk*, 24th ISSC in Albuquerque 2006

Eriksson, U, 2006, Bakgrund till RAMS-kav för signalsystem och komponenter, Swedish railroad administration

European Organization for Civil Aviation Equipment (EUROCAE), 2006, *ED – 125 – Process for specifying risk classification scheme and deriving safety objectives in ATM "in compliance" with ESARR 4*

European Organization for the Safety of Air Navigation (EUROCONTROL), 2004, Air Navigation Systems Safety Assessment Methodology – SAF.ET1.ST03.1000-MAN-01, Brussels, Belgium

European Railway Agency (ERA), 2007, *WP1.1 Assessment of the feasibility to apportion Common Safety Targets*, Valenciennes, France

Firesmith, D, 2004, *Engineering Safety Requirements, Safety Constraints*, and Safety-Critical Requirements, Journal of object technology, vol 3 no 3

Grimvall, G & Jacobsson, Per & Thedéen, T, 2003, *Risker i tekniska system*, Lund, Studenlitteratur

Hardwick, M, Pfitzer, B, Pfitzer, T, 2004, *A comparison of QRA Methods used by DoD for Explosives and Range Safety with Methods used by NRC and EPA*, Huntsville, Alabama, APT Research, Inc.

Hövel, R & Wigger, P, 2002, *Safety Assessment – Application of CENELEC Standards – Experience and Outlook*, Germany, Institute for Software, Electronics, Rail Technology (ISEB), Germany, TÜV InterTraffic GmbH, a company of the TÜV Rheinland / Berlin-Brandenburg Group

Institute of Electrical and Electronics Engineers (IEEE), 1998, *IEEE Recommended Practice for Software Requirements Specifications*, New York, IEEE, Inc.

Information Technology Association of America (ITAA), 2008, *GEIA-STD-0010*, ITAA Standards & Technology department, Arlington, U.S.A

International Electrotechnical Commission, (IEC), 1995, *IEC 60300-3-9, Dependability management – Part 3 – Application guide – Section 9 Risk analysis of technological systems*, Geneva, Switzerland, IEC

Kavakli, E & Loucopoulos P (2004) *Goal Driven Requirements Engineering: Analysis and Critique of Current Methods, in Information Modeling Methods and Methodologies* (Adv. topics of Database Research), John Krogstie, Terry Halpin and Keng Siau (eds), IDEA Group, page 102 - 124.

Kotonya, G & Sommerville, I, 1997, *Requirements Engineering – Processes and Techniques*, Chichester, John Wiley & Sons Ltd

Kratochvil, M & McGibbon B, 2003, *UML – Xtra – Light*, Cambridge, Cambridge University Press

Leveson, N, 1995, *Safeware: system safety and computers*, New York, Addison-Wesley Publishing Company Inc.

Martinsson, C, 2007, *Safety1st – Handbok för systemsäkerhet*, Combitech, Växjö

Martinsson, C, Smith, G, Svantesson, M, 2004, THR *för ERTMS Regional*, AerotechTelub, Växjö

Merriam, S, 1994, *Fallstudien som forskningsmetod*, Lund, Studentlitteratur

Mihm, P, Eckel, A, 2004, *European Commission Fifth Framework programme (SAMRAIL) WP 2.4 – Acceptable Risk Level*, SAMRAIL partners and EC

Nuseibeh, B & Easterbrook, S, 2000, *Requirements Engineering: A Roadmap, The Future of Software Engineering*, Companion volume to the proceedings of the 22nd International Conference on Software Engineering, (ICSE'00)

Oberger, L, 2006, *Bakgrund till ANS flygsäkerhetsmål vid systemförändringar*, Flygtrafiktjänsten ANS, Luftfartsverket

Patel, R & Davidsson, B, 1994, *Forskningsmetodikens grunder*, 2: a upplagan, Lund, Studentlitteratur

Pfitzer, T, Hardwick, M, Dwyer, S, 2001, Pascal and the Risk Assessment Code (RAC) Matrix, Apt Research, Huntsville Alabama

Sommerville, I Sawyer, P, 1997, *Requirements engineering: a good practice guide*, Chichester, Whiley Cop.

Stephans, R, 2004, *System safety for the 21st century – The updated and revised edition of system safety 2000*, John Wiley & Sons Inc.

Swedish Defense Forces, 1996, *System Safety Manual – H SystSäkE*. Edita Nordstedts Tryckeri.

TechAmerica, 2009, *TechAmerica Issues New System Safety Standard*, Washington DC, Immidiate release May 11th, 2009

Thurén, T, 2007, *Vetenskapsteori för nybörjare*, Malmö, Liber AB

Tsai, W-T, Mojdehbakhsh, R & Rayadurgam, S, 1997, *Experience in Capturing Requirements for Safety-Critical Devices in an Industrial Environment*, High assurance systems engineering workshop page 32-36

Valerdi, R, Wheaton, M, 2005, *ANSI/EIA 632 As a Standardized WBS for COSYSMO, AIAA 5h Aviation, Technology, Integration and Operations conference*, California, American Institute of Aeronautics and Astronautics, Inc.

Wigger, P, 2001, *Experience with Safety Integrity Level (SIL) Allocation in Railway Applications, Germany, Institute for Software, Electronics, Rail Technology (ISEB)*, TÜV InterTraffic GmbH,a company of the TÜV Rheinland / Berlin-Brandenburg Group

Yin, R, 2003, *Case study research – Design and methods*, Sage Publications Inc.

Zio, E, 2009, *Reliability engineering: Old problems and new challenges*, Reliability Engineering and System Safety, vol 94, page 125-141

12.2 Interviews

Derelöv, M, Saab Underwater Systems, 2009- 03-24

Ekholm, R & Börtemark, A, Swedish Defense Materiel Administration, 2009-02-24

Eriksson, U, Swedish railroad administration, 2009-04-06

Kallman, S, Swedish railroad administration, 2009-03-27

Niklasson, G, Swedish railroad administration, 2009-03-30

Norling, P, Railway department of the Swedish Transport Agency, 2009-03-27

Oberger, L, Aviation department of the Swedish Transport Agency, 2009-03-26

Kinneryd, C, Swedish railroad administration, 2009-03-30

Sundvall, K – E, 2009-03-27

Uppegård, J, Swedish railroad administration, 2009-04-06

12.3 Mail correspondence

Clemens, P, APT Research, Huntsville, Alabama, 2009-02-10

de Rede, EUROCONTROL, Brussels, 2009-05-06

Sollander, S, Railway department of the Swedish Transport Agency,
2009-04-01, 2009-02-19

12.4 Internet

Leveson, N, 2002, System *Safety Engineering: Back to the future*, Aeronautics and Astronautics Department, Cambridge, Massachusetts Institute of Technology, http://sunnyday.mit.edu/book2.pdf, (accessed 2009-04-22)

White, A, 2004, *Introduction to BPMN*, IBM Corporation,
http://www.zurich.ibm.com/~koe/teaching/ETH2009/White-BPMN-Intro.pdf, (accessed 2009-05-22)

www.av.se, 2009-03-17, Swedish Work Environment Authority

www.anticlue.net/archives/000819.htm, 2009-03-18

www.combitech.se, 2009-03-16, Combitech

www.banverket.se, 2009-03-27, Swedish railroad administration

www.saabgroup.com, 2009-03-16, Saab Technology

http://www.visual-paradigm.com/VPGallery/diagrams/Activity.html, 2009-05-25, Visual Paradigm

12.5 Courses

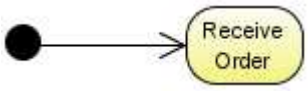
Ekholm, R & Börtemark, A, 2009b, System Safety Course 67A, Swedish Defense Materiel Administration, Rimforsa strand

Appendix 1

The aim of the information in this appendix is to give explanations to the symbols used in Figure 18, Figure 17,Figure 16 *and* Figure 15. *The symbols are collected from the OMG Unified Modeling Language Specification - UML 2.0. The material is downloaded from:* http://www.visual-paradigm.com/VPGallery/diagrams/Activity.html, 2009-05-25

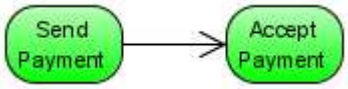
InitialNode

An activity may have more than one initial node.



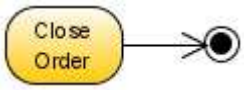
Action

An action may have sets of incoming and outgoing activity edges that specify control flow and data flow from and to other nodes. An action will not begin execution until all of its input conditions are satisfied. The completion of the execution of an action may enable the execution of a set of successor nodes and actions that take their inputs from the outputs of the action.



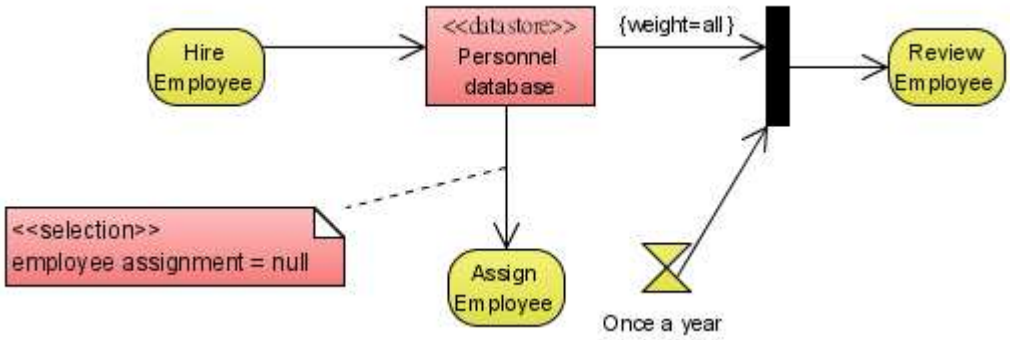
ActivityFinal

An activity may have more than one activity final node. The first one reached stops all flows in the activity.



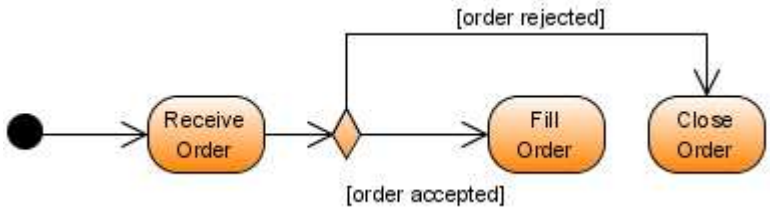
DataStore

A data store keeps all tokens that enter it, copying them when they are chosen to move downstream. Incoming tokens containing a particular object replace any tokens in the object node containing that object.



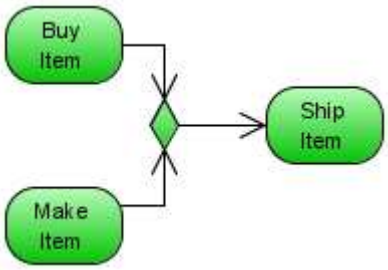
DecisionNode

A decision node is a control node that chooses between outgoing flows.



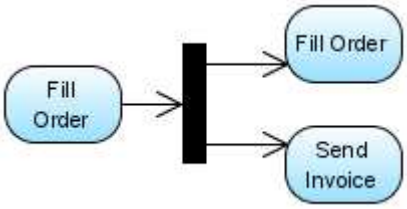
MergeNode

A merge node is a control node that brings together multiple alternate flows. It is not used to synchronize concurrent flows but to accept one among several alternate flows.



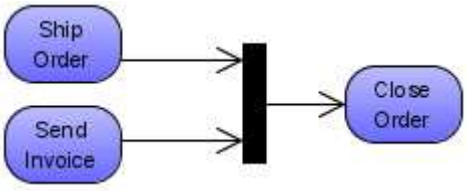
ForkNode

A fork node has one incoming edge and multiple outgoing edges.



JoinNode

A join node has multiple incoming edges and one outgoing edge.

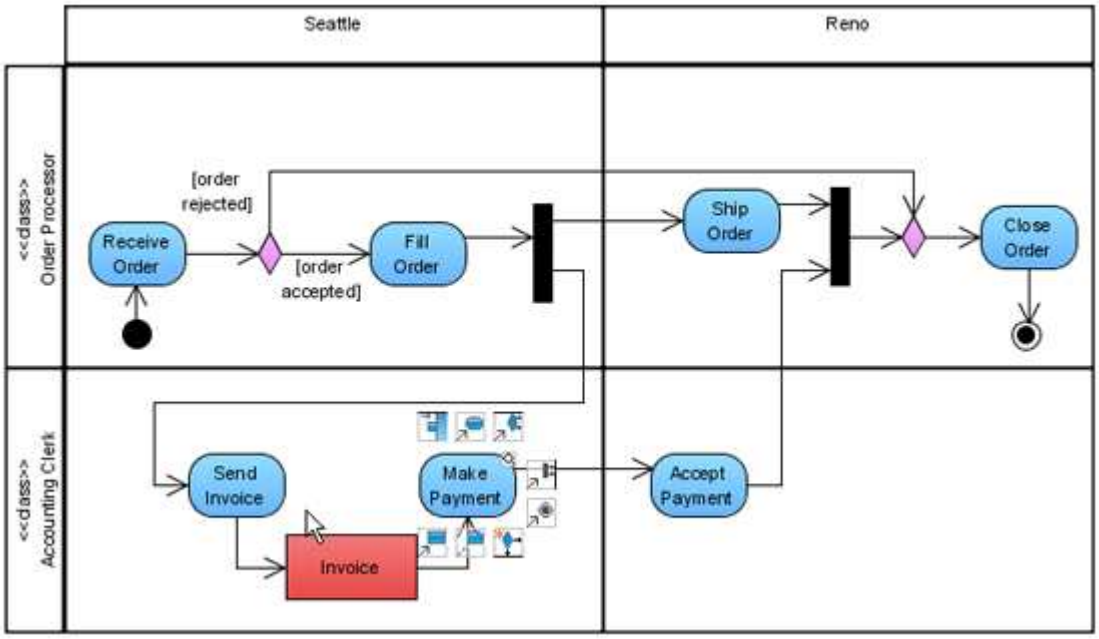


ObjectNode

An object node is an activity node that indicates an instance of a particular classifier, possibly in a particular state, may be available at a particular point in the activity. Object nodes can be used in a variety of ways, depending on where objects are flowing from and to, as described in the semantics section.

ActivityPartition

Partitions divide the nodes and edges to constrain and show a view of the contained nodes. Partitions can share contents. They often correspond to organizational units in a business model. They may be used to allocate characteristics or resources among the nodes of an activity.



InterruptibleActivityRegion

An interruptible region contains activity nodes. When a token leaves an interruptible region via edges designated by the region as interrupting edges, all tokens and behaviors in the region are terminated.