UPTEC STS 07 005
Examensarbete 20 p
Februari 2007

Summation of risk

Assessment of total system risk for complex systems

Vegar Lie Arntsen

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

Summation of risk - Assessment of total system risk for complex systems

Vegar Lie Arntsen

Material that is produced or modified by FMV for the Swedish military passes through a process of ensuring the system safety. This system risk assessment focuses today on the maximum risk level that each risk is allowed to contain. No focus is given to the total amount of risks that is put into a system. A drawback with this method is problems to control the actual risk value of a system, to compare different risks against each other. The literature study shows that the concept "Total System Risk" (TSR) introduces limitation to the quantity of risks in a system. The "Summation method" is a quantitative risk assessment tool under development for handling the TSR in a resource efficient way. The study, further development and analysis of the method suggest that FMV will gain benefits from implementing the summation method in their system risk assessment. The summation method reduces the costs for improvement and increases the control of the system safety in complex systems without adding any complex calculations

Handledare: Arne Börtemark & Ragnar Ekholm
Ämnesgranskare: Dag Jonson
Examinator: Elisabet Andrésdóttir
ISSN: 1650-8319, UPTEC STS 07 005

Populärvetenskaplig beskrivning

Summering av risker – Värdering av total systemrisk i komplexa system

Försvarsmakten arbetar metodiskt för att hantera och begränsa risker i nytt materiel som framställs eller i gammalt materiel som förändras. Ett samlingsbegrepp för denna metodik kallas systemsäkerhet. Det omfattar arbete och analys av materialet från förstudier till avvecklingstadiet. Som kriterium för vad som är en acceptabel säkerhetsnivå för ett system använder försvarsmaktens materialverk sig av förhandsdefinierade gränsvärden för risknivåer som gäller för alla risker som identifieras i systemet.

Med nuvarande metod uppstår problem då den inte tar hänsyn till antalet risker som tillåts i systemet. En följd av detta är även att de system som har de strängaste riskkriterierna blir mycket osäkra om man tillåt tillräckligt många risker. På grund av detta är försvarsmakten i behov av en metodik som hanterar både storleken på enskilda risker och antalet risker i systemen för att kunna hantera den totala systemrisken.

För att initiera en övergång till en analys baserad på total systemrisk måste riskerna hanteras kvantitativt så de kan jämföras med varandra. Detta sker genom att beräkna produkten av den förväntade sannolikheten och den förväntade konsekvensen, för att sedan kunna använda denna som ett väntevärde för varje risk. Om man gör ett antagande om att alla olyckor sker oberoende av varandra kan den totala systemrisken skattas av summan av väntevärden för varje risk i systemet. Detta innebär dock inte nödvändigtvis någon precision av skattningen, då systemet i fråga kan vara mycket komplext och ha beroenden mellan olyckor. Metoden kan trots detta anses göra en mycket bättre skattning och beskrivning av verkligheten än den befintliga ger ett definitivt tak på den risknivå som accepteras i ett system och möjliggör jämförelse mellan olika risker i systemet. Jämförelse mellan olika risker bättrar möjligheten att på ett effektivt sätt maximera riskreduktionen i ett system. Riskreduktionen kan optimeras genom att välja att åtgärda de risker som ger mest reduktion per krona. Försvarsmakten kan, med en sådan optimering mer effektivt och ekonomiskt skapa ett säkrare system.

Det finns dock frågor som måste utredas för att optimering ska kunna användas. Exempelvis spörsmål kring hantering av riskoptimeringen om resultatet exponerar en liten grupp personer med en mycket hög risk eller exponerar en grupp med liten eller ingen direkt nytta av systemet med hög risk.

Preface

This paper is my final project in the study programme *Systems in Technology and Society* at Uppsala University, which leads to the professional degree *Civilingenjör*. The project was done for the Swedish Defence Material Administration (FMV) during the last semester 2006. The findings are planned to be used in the development of the new Swedish armed forces system safety manual replacing the old one from 1997.

This paper was primary written for personnel handling system safety at FMV. I tried to keep the theory and examples on a generic level such that other persons handling system safety issues would benefit from reading it.

I want to thank Ragnar Ekholm and Arne Börtemark, my supervisors at FMV, for support, providing me with literature, feedback and many interesting discussions during the project work. I also want thank Professor Dag Jonsson at Uppsala University for his feedback, ideas and support on mathematical issues throughout my project work.

Uppsala, January 2007

Vegar Lie Arntsen

Tables

Table of content

Table of figures

Table of Tables

Abbreviations

c	Consequence of a risk
c_{sys}	Consequence, expected value, if an accident occur in a system
FM	Swedish Armed Forces (Försvarsmakten)
FMV	Swedish Defence Materiel Administration (Försvarets materielverk)
IT risk	Intolerable risk
LT risk	Limited tolerable risk
p	Probability for a risk
p_{sys}	Probability for any risk to occur in a system
r	Risk value for a hazardous event
RFP	Request for proposal
SHK	Swedish Accident Investigation Board (Statens haverikommission)
T risk	Tolerable risk
TSR	Total System Risk
VFM	Operative instructions for the Armed Forces (Verksamhetsordning för Försvarsmakten)

1 The problem and its context

1.1 Background information

In the decades after the Second World War up to the 1970's, the growing use of military and civil airplane caused an increase in numbers of aircraft accidents and mishaps (Hammer 1972 p. 3-7). Around the middle of the 1950s the US Air Force experienced 10 mishaps for every 100 000 flight hour (Air Force Safety Centre 2000 p. 2). The number was also high in Swedish Air Force during this period, in 1978 the Swedish Accident Investigation Board (SHK) was instated specifically to investigate all of these aircraft incidents and accidents (SHK 2000).

The idea of system safety was introduced in the mid forties, developed and got foothold in military and civil industry during the fifties and sixties. In 1965 System Safety became a university subject, and one could say that it had become an established practice. Parallel to the increase in popularity the amount of resources put into system safety for system development increased in the period after the war. Data from the end of the 1980s show that the rate of mishaps in the US Air Force was reduced from 10 to 2 mishaps for every 100 000 flight hours. (Air Force System Safety Centre 2000).

In the Swedish military focus on System Safety increased after the introduction of SHK (Ekholm 2006b). Today System Safety is implemented on all system and material development used by FM, this is done based on the following decision by Supreme Commander at FM.

> *The Operations Commander shall conduct and lead activities which have the objective of minimizing the hazards in a system so as to avoid injury to personnel and damage to property or to the environment (system safety) (VFM).* (FM 1996b p. 19)

At FMV the system safety is managed by operating with risk level limitations that all risks in a system must comply to. Improvements in the system safety are done until all risks fall under this limitation. When this requirement is met the system at question is classed as safe. (FM 1996b passim)

A weakness of the present method of assessing system safety is the lack of consideration for the amount of risks remaining in the system. In the extreme case a system with infinitely amount of risks with a tolerable risk level will be classed as safe. FMV is working to deal with the limitations within today's system of managing system safety. A new method is being developed, called the Summation method. It is planned to become a part of the new handbook for system safety, replacing the manual ensuring system safety in new and rebuilt systems today (FMV 2006a p. 3).

1.2 Object of study

A main objective of this study is to see how an introduction of a quantitative approach for approximating the total system risk will affect the assessment of system safety. The approach in focus will be the summation method (Ekholm 2005, Ekholm 2006a) and improvements of this method. Another main objective will be

to develop and present the method in a generic direction intended for various uses at FM and FMV.

It is will be necessary to study the ideas behind system safety and how system safety is handled at FMV today. It will further be important to understand the theory behind the summation method and its limitations. Emphasis will be put on the relations between the processes described in words by Ekholm (2005, 2006a) and mathematical theory. Another necessity will be to identify limitations in the method. These limitations should be the base on further development of the method, but without increasing the calculation complexity and demand for resources in the assessment work dramatically.

1.3 Limitations

The work of this paper is limited by the workload of 20 university study points, in time approximately 20 weeks of work.

All information is gathered from public sources, meaning that no sensitive or classified information will be included into the study.

This paper will only cover the calculation of system risks based on top events. The assessment work on a top event will not be dealt with, even if the correctness of assessing the system risk is dependent on the accuracy of the ingoing data. A reason for this is that the single risk assessment is not a generic methodology and varies between systems.

The paper will not cover special case implementations, but focus on generic use of methods and models.

FMV treat their risks in a discrete manner hence all model descriptions and mathematics will be discrete, even if it should be possible to use linear descriptions.

1.4 The structure of the paper

The first part, chapter 3, will present the ideas and principles behind system safety and risk handling that exists today. Chapter *4, The present system safety system at FMV,* handles the ideas and methodology that is practiced today by FMV. It also points out problems with the used methodology and point to areas that are in need of improvements.

Chapter 5, *The new system with Total System Risk*, describes the new idea of total system risk and how the summation method is intended to work. The theory behind this method is presented together with benefits and drawbacks of using it. The principle of risk budgeting is also described together with a method to calculate the effect of change in consequence and probability a single risk will have on the total system risk.

The following, Chapter 0, puts focus on error sources that will impact the system safety work when using the ideas of total system risk and the summation method.

The last part of this paper is a suggestion on how the summation method can be used in for calculating Total System Risk and the effect of changes in risk or consequence. The methodology suggested is based on the findings in earlier parts of the paper.

2 Material and method

The research for this paper is based on a combination of literature studies and mathematical investigation of the existing ideas of working with total system risk.

The first descriptive part of the paper, chapter 3, has mainly been based on information gathered from generic system safety literature such as the books "Handbook of System and Product Safety" (Hammer 1972), "System Safety Engineering and Management" (Roland & Moriarty 1990). The general description of risk evaluation is to a large extent gathered from a report done by the Swedish Rescue Services Agency (Räddningsverket 1997).

The second descriptive part, chapter 4, which deals with the present system at FMV is based on a mix of literature studies, conversation with system safety personnel at FMV and information I gained from participating in a one week course in system safety for system developers, Kurs 55A, held at Rimforsa, September 2006. An important source of information in this part has been the system safety handbook used by FM and FMV (FM 1996a,b), which describes the process of how the system safety work is to be done.

The descriptive part of chapter 5 is based on two articles written by Ragnar Ekholm (2005, 2006a). The parts of mathematical character are created from analyses and development of the ideas in Ekholm's papers. The analysis is based on mathematical principles such as stochastic variables. The last part of chapter 5 concerning risk budgets is developed from the theory around stochastic dependency. The last chapters are mainly analyses and work based on these analyses and information from the earlier chapters.

3 Risk and System Safety

3.1 Risk

Working with system safety indirectly means working to reduce risks or more literary, reduce the amount of unwanted events or accidents in systems (FM 1996 p 36). In order for an accident to happen inside the concept of system safety, two criteria are required, first a hazardous event have to take place and second damage to person, object or environment is needed (Ibid). If a hazardous event occurs and there is no damage, the event is called an incident (Ibid).

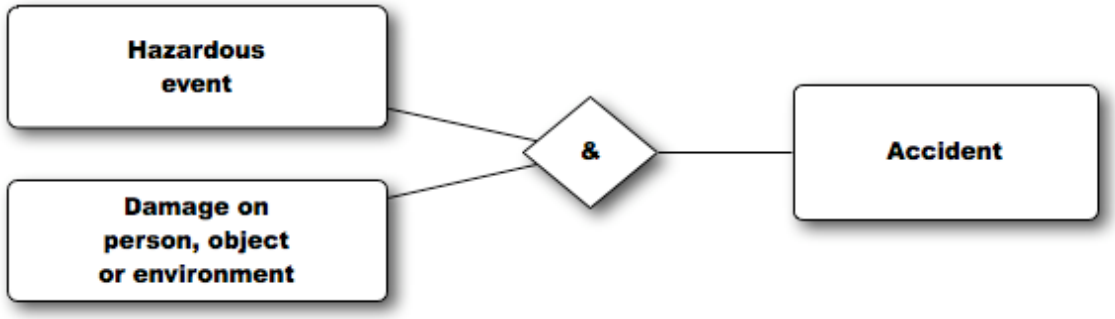

Figure 1 - A graphical representation of the building blocks for an accident.

Monitoring risks is the main activity when working with system safety. Risks are in literature and practice a frequently used unit for monitoring the chance and effect of an accident. It is often defined as a function of the probability of an accident to occur and the consequence of the accident if it does occur (NE 2006).

Risk = *f* (P (accident occurs), consequence of the accident) (3.1)

3.2 Systems and complex systems

There is no strict definition that distinguishes between "regular" systems and complex systems (Wikipedia, 2006). The amount of interaction between different parts of a system with different character seems to be the factor that distinguishes between the two (Berner 1999 p.130). FM (1996b p. 22) defines its use of a system as a combination of one or several of the following keywords: necessities, plant and equipment, personnel and instructions and regulations. This shows that it is impossible to isolate a system by a physical unit or an institution, but that different parts of the military organisation are included.

The systems that FMV handles are armed units and military materiel (FM 1996 p. 15). These materials are to be used in the military operations in peace and war. Charles Perrow (1984) analyses "military adventures" in terms of interactive complexity and loose and tight coupling. He defines the military adventures which all FMV provided material is a part of, as a loosely coupled complex system (Berner 1999 p. 131). If something happens to a component in a loosely coupled system it will not necessary affect other components, because of the loose coupling between components (Sharit 2000).

Based on the definition of FMV (1996a) and analysis of Perrow (1984) this paper will interpret the word system in relation to FMV and military materiel as a complex system. The use of the word "system" in this paper will also have the meaning "complex system".

3.3 System safety

The basic underlying idea of system safety is to prevent accidents in a system to ever happen (Roland & Moriarty 1990). This should be done by identification and control of potential hazards in the system throughout the whole system life cycle (Ibid). The term project life cycle includes storage, transportation, maintenance and termination in addition to the prime use of the system (Gunnerhed 1994 p.5). The goal of the system safety approach is to avoid/minimise the need for "fixing", instead a so-called *identify-analyze-control* methodology is used (Roland & Moriarty 1990 p. 9). The focus of control is put on system safety levels, which are defined for system during the high level design. To meet a system safety level the hazards in a system need to be identified and controlled.

Pre "system safety" safety systems were often based on a *fly-fix-fly* principle (Roland & Moriarty 1990 p 8). Fly the aircraft until something goes wrong – investigate the accident and find a solution to the problem – implement the solution into the new "better" aircraft. Rebuilding and constantly improving a system such as an aircraft can be costly and even in conflict with earlier investments and improvements (Roland and Moriarty, 1990 p 9).

There are several reasons for evaluating system risk before building. If the safety level in a system is low compared to the expected gain the system would give, it might not be motivated to build it. In other systems it might be possible to identify risk-reducing actions to increase the safety such that the gain overcomes the safety issues. The system safety approach is also gainful in the cases when there exist more than one different solutions to solve a system task. The least expensive solution, in form of risks, can be chosen before others. (Räddningsverket 1997 ch. 2 p. 3)

3.4 Handling risks

There are basically two main approaches of handling system risks, deterministic and probabilistic handling. Deterministic handling of risks identifies and analyses risk from the viewpoint, if an accident can occur what is the *worst case* or *dimensioned case* of damage. Worst case damage is the theoretical largest possible amount of damage that can be expected from an accident. Dimensioned case is defined as the largest possible amount of damage an accident can give rise to, given that basic precautions of the situation are done. (Räddningsverket, 1997 ch. 3 p. 5)

The deterministic handling of system risk has a disadvantage, it brings an ineffective utilisation of resources. A deterministic handling distribute lots of resources on improvements of risks that are not so likely to occur, but has large consequences in their worst case scenario. It is therefore argued that a probabilistic view of risks can give a more resource effective handling of system risk. In probabilistic handling the probabilities for accidents are included into the risks evaluation. The probabilities or distribution of consequences are also taken into

consideration. By comparing a risk against a pre defined tolerable risk level it is possible to set a risk as acceptable or not. (Räddningsverket 1997 ch. 3 pp. 6-8)

FMV uses a mix of a probabilistic and a deterministic approach when managing system risk, details on their handling will be presented later in this paper, in chapter 4 on page 14.

3.4.1 Quantitative and qualitative risk handling

There are two main approaches, qualitative and quantitative, within the probabilistic school of handling system safety Räddningsverket 1997 ch. 2, p.2). Qualitative handling is an intuitive direct approach of describing a risk allowing both risks and consequences to be described, for the risk, in an individual way. The result of this approach is a good description of what to expect from each specific risk (Räddningsverket 1997 ch. 3, p. 6). A drawback with this approach is that the differences between the risk descriptions may decrease the possibility to compare and collect global information from a system (Ibid).

A system where the risks are described with different structures and units of measures seems hard for a system safety team to handle. Risks that are defined in a qualitative manner are problematic to compare compared to a quantitative risk. The result from a comparison between qualitative risks is bound to be entirely based on the team's cognitive ability to process the information and their objective evaluation.

The problem of comparison is an incitement that favours the use of a quantitative approach for risk handling. In a quantitative approach it is necessary to identify risks into one common unit. By defining risks in such a manner it enables the possibility to evaluate and compare two risks. How this common unit should be set differ between systems. For risks where the consequence is damage on property it is possible to transform the consequence into a monetary value, reflecting the costs to rebuild. Environmental damages that are reversible can in a similar way be transformed into a monetary value, reflecting the cost of restoring the damages from an accident. Irreversible environmental consequences should not be included in the handling as other risks when looking at system safety. If there exist risks for irreversible environmental consequences the decision needs to be handled separately. The decision on such risks should not be handed to single persons or committees, but should be based on an organisational policy. (Ekholm 2006a)

A problem with the use of a quantitative unit in risk evaluation arises when handling risks with consequences for personnel injury and human life. It is hard to define a monetary value on a human life or a serious injury. A solution for this problem is to use separate risk evaluations for the different kinds of risks. FMV have chosen to distinguish between personnel injuries, property damage and environmental damage in their evaluation (Ekholm & Wallentin 2003).

Different kinds of personal injuries are handled inside the same system of safety analysis. To enable this it must be possible to compare different kinds of accidents against each other. A used method for differentiating personnel injuries is to use the terms *death*, *serious injury* and *limited injury* (Ibid). These three levels of injury are valued in relation to each other.

The U.S. Department of Defence (2005 p. 45) has evaluated the relationship between the levels as shown in the table beneath. It is not obvious that this is a correct relation for all systems. Ekholm and Wallentin (2003) states that the relations should be defined independently for each system in consideration to the scenario it is in.

Table 1 - Table for conversion of personnel accidents used by the U.S. Department of Defence.

1 death	⇔	10 serious injuries
1 serious injury	⇔	10 limited injuries

3.4.2 Defining system risk level

It is a challenge to define acceptable levels for risks, because systems can cause damage to people's life and well being. Only a zero-risk risk level will pass as a general accepted rule. The problem is that zero risk is only possible to achieve in theory, and only if an infinite amount of resources are put into reducing risks. It is therefore necessary to accept a certain amount of risk. Räddningsverket defines the following principles when dealing with system risk (Räddningsverket 1989).

- There exists no general level for tolerable risks.
- The fact that accidents have been on a low level under several years does not automatically impose that the risk level should be accepted.
- It is not acceptable that several people die
- It is not acceptable to create any kind of border limits on tolerable risk levels.

3.5 Principles for acceptable risk levels

A general understanding is that the risk level should be based on an "objective" evaluation where both the societal attitudes and the interests of affected groups are taken into consideration. Four evaluation principles exist to promote an objective handling; the principles of *reasonability*, *proportionality* and *distribution* and last the principle of *avoiding catastrophes*. The four principles are to be seen as a guiding framework for defining risk levels, because the principles cannot be met to one hundred percent in practice. In real life limited amounts of resources will put a limitation on the execution of the principles. It is also possible to end up in a deadlock where the principles are in conflict with each other. (Räddningsverket 1997 ch. 3 pp. 3ff.)

- **Principle of reasonability** means that all risks that can be reduced with a reasonable amount of resources should be reduced, irrespective of the existing levels.
- **Principle of proportionality** means that the risks in a system should not be disproportionately large compared to the benefits of the system.
- **Principle of distribution** implies that no group or individual should be exposed to a disproportionately large risk compared to the benefits they gain from the system.

- **Principle of avoiding catastrophes** states that risks with limited consequences that can be handled by alert resources is to be preferred before risks with catastrophically consequences.

All of these four principles are based on the probabilistic idea of risk handling. They are function of frequency, consequence and the amount of exposure for individuals in the risk environment.

4 The present system safety system at FMV

FMV is responsible for the procurement, maintenance and windup of all military materiel on the behalf of FM (SOU 2002 p. 123). In the work of fulfilling this responsibility FMV is obliged to work with activities that have the objective of "minimizing the hazards of the system" (FM 1996b p. 19). FMV works with *system safety* in three aspects which is to (FM 1996b p. 21):

- Prevent injury to personnel
- Prevent damage to property
- Prevent damage to the environment

FM sets the tolerable system safety level for new systems and for modifications of existing systems together with functional requirements (FM 1996b p. 33). These levels are handed over to FMV, which process them into a request for proposal (RFP) (FM 1996b p. 79). It is in the RFP that the system safety demands are put into explicit demands on the system in terms of functional requirements and requirements on integration toward other existing systems (FM 1996b p. 79). It is in this phase of the planning process where FMV gets the best effect on risk reduction in economical terms, since all ad hoc configurations will be outside of the contract with a developer (FMV 2006b).

The developer creates a *system safety activities plan* describing how they will handle the system safety requirements, which is included into the final contract for building the system (FMV 2006b). This plan and individual risks are handled in interaction with FMV during the process of developing and building the system (FMV 2006b). When the developer considers the system as ready for use it writes a *safety compliance assessment* (FM 1996b, p. 34). This is the assessment of the system safety work done in the project and contains a statement from the producer that the system safety is on a satisfactory level. FMV writes a *safety statement,* when they find the *safety compliance assessment* satisfactory, that they hand over to FM (FM 1996 p. 34). This statement is a part of what the FM commander base the decision, the *safety release*, if the system can be put for use (FM 1996, p. 34).

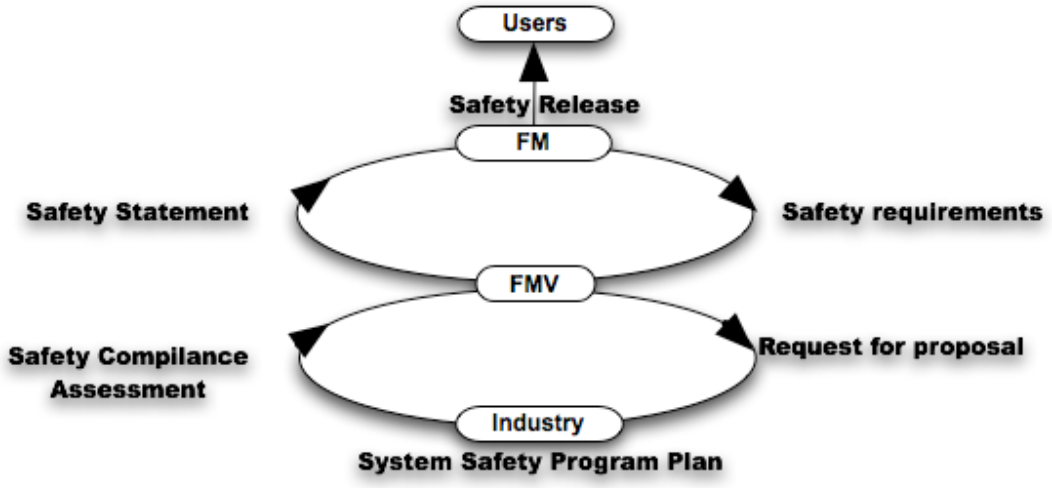

Figure 2 - A model of the activities related to system safety at FMV.

4.1 Risk list

All developed or modified systems under the supervision of FMV have a risk list. This list is one of the main tools in their risk assessment method. All identified risks are listed and broken down into a probability and a consequence. The definitions for the different classifications of the risk value are also included in the list. (FM 1996a p. 81)

An example of such a risk list and an entry is found in Figure 3 below. The categories c, p and Classification (Class) are described in the following chapter describing the risk matrix.

Risk no.	Risk Source	Identification of risk	Before			Analysis and action	After		
			c	p	Class		c	p	Class
001-1	Ladder	Personnel slip when climbing and get injured.	III	A	NT	Equip the ladder with a coating with slipping protection and make surface rougher.	III	D	T
001-2	Ladder	Fall caused by ladder falling over at a high altitude resulting in personnel injury.	II	C	LT	Reconstruction of ladder such that the possibility for fall of ladder is reduced.	II	D	LT

Figure 3 - Example of a risk list. Headers and content are based on *the risk list used for the UndE 23 serie (FMV 2003).*

The identification of the risks and the analysis is done by a special System Safety Working Group (FM 1996b p 97). This group consists of members from the final users of the system (FM), FMV and the Industry (FM 1996 p 78). They use information from organisational, historical and personal experience to identify, categorise and analyse risks into the system.

4.2 Risk matrix

The risk matrix is a tool for classifying system risk at FMV. Every risk identified in a project of creating a system is defined into this matrix. Below, Figure 4 is an example of such a matrix created by FMV for the system risk assessment of such a project.

Category of frequency	**Category of consequence**			
	I	II	III	IV
A	NT	NT	NT	LT
B	NT	LT	LT	T
C	NT	LT	LT	T
D	NT	LT	T	T
E	LT	T	T	T

IT Intolerable risk LT Limited tolerable risk. T Tolerable risk

Figure 4 - A risk valuation matrix used by FMV to evaluate the system risk for a system.

In the FMV organization the categorisation of frequency is done both qualitatively and quantitatively, depending on the projects (Börtemark & Ekholm 2006). Often, only qualitative sets of definitions exist, e.g. categories for the UndE 23 series, see Table 2 (FMV 2003 p. 2). The *middle* column of the following table is a short transcription, from Swedish, of the UndE23 series frequency classification. An example with quantitative descriptions is found in MIL-STD-882C (U.S. Department of Defence 1993 p. A-5), the standard that the system safety book used by FMV, H SystSäk 1996 (FM 1996a), is based upon. These quantitative descriptions are found in the *right* column of the following figure.

Table 2 - Example of definitions of frequencies.

Frequence category	**Description from UndE23**	**Values from MIL-STD882C**
A	*Frequently* to occur in a system's life cycle	$X > 10^{-1}$
B	*Probable* to occur in a system's life cycle	$10^{-1} > X > 10^{-2}$
C	*Occasionally* to occur in a system's life cycle	$10^{-2} > X > 10^{-3}$
D	*Remotely* to occur in a systems life cycle	$10^{-3} > X > 10^{-6}$
E	*Improbable* to occur in a system's life cycle	$10^{-6} > X$

The content of the categories of consequence is divided into the three types, personnel, property and environmental, as described in chapter 3.4.1. The following figure is an English transcription of the definitions of consequence levels for all categories in the UndE 23 serie (FMV 2003 p. 2). According to the FM manual of system safety are the consequence categories descriptions of "*the worst-case consequences for accidents* [that] *have been stated and the causes* [of the

accidents] *may be handling errors, environmental conditions, design deficiencies, procedural deficiencies, system failures, sub system failures, component failures and malfunctions*." (FM 1996b p 40). The content of the following definitions should therefore be seen as a worst case description of each risk.

Table 3 - Example of definitions of consequences (FMV 2003 p. 2).

Consequence category	**Injuries**	**Property damage** (SEK)	**Environmental damage**
I	Death or 100% invalidity	Loss larger than 10 M	Unchangeable, serious environmental damage, violation of law.
II	Partly invalidity, injuries that may result in hospital visits for at least three persons	Loss limited between 2M and 10M	Less serious environmental damage, violation of law.
III	Injuries or work related sickness that results in absence from the workplace.	Loss limited between 100k and 2M	Limited environmental damage without violation of law.
IV	Injuries or work related sickness that do not result in absence form the workplace.	Loss limited between 20k and 100k	Insignificant environmental damage without violation of law.

As seen in the risk matrix above, Figure 4, it is made up from a set of 20 risk value categories. The value of each category is defined from a qualitative evaluation of every single risk. The limits for intolerable (IT) risks are set by FM, the scaling of levels beneath IT are done by FMV for the purpose of avoiding conflicts with the producer if the risk is tolerable or not (Ekholm & Wallentin 2003). The category between the two, limited tolerable has floating limits of what is safe enough. In an argument on tolerability of a risk between the producer of a system and FMV on it is always FMV that has the final decision if a risk is tolerable or not (Ekholm & Wallentin 2003).

A system is not considered safe at a satisfactory level if a risk is defined into one of the IT categories. The same is true if a risk is defined into one of the LT categories in addition to that FMV is not willing to tolerate the risk level. In these cases further risk reducing action is needed. In the case of risks in the T-category no risk reducing actions need to be done. In order for FMV to write a safety statement on a system, the producer needs to provide information that all risks are defined as tolerable. (FM 1996 p. 37)

4.3 ALARP

The decision on approving a LT risk into a system is done by implementing the ALARP-principle (FM 1996b p 17). The main idea behind this method is to decrease a risk as low as reasonably practicable. ALARP was introduced by the British Health and Safety Executive (FMV2006a p. 20). A risk classed as ALARP

is on a level where further improvements in risk reduction actions cannot be justified because of the amount of resources needed to do the further reduction (U.S. Department of Defense 2005 p.4). This decision is based on subjective evaluations, but can get support from written standards and existing good practices (British Health and Safety Executive 2006).

A tolerable risk that normally does not need any further consideration for risk reduction can also be forced into the ALARP-principle. If the costs of reducing a tolerable risk are considered "low", then FMV have the possibility to require an implementation of the ALARP principle (Ekholm & Wallentin 2003). This can be seen as a parallel to the first principle acceptable risk levels, the principle of reasonability (Chapter 3.5).

4.4 Risk comparison

The matrix system used by FMV is a combination of both qualitative and quantitative handling. The use of the matrix makes it possible for a system safety working group to compare different risks with each other. For example, a risk in the IT category is a higher risk than one in the T category. This quantitative feature does not compile for comparison of all system risks. It is not obvious which one of two risks in the *same* category is the greatest risk just from reading the matrix, e.g. a risk classed in the probability category C and consequence category II compared to a risk classed in the categories B respectively C (Figure 6).

The qualitative categories that the matrix is created from do not endorse a total qualitative handling. For example, it is not obvious how often *frequent* is compared to *less frequent*. A consequence from this is an uncertainty of how much larger a risk with frequency category A is compared to a risk with frequency category B etc. Further it is not possible to compare the differences between two intervals frequencies such as A→ B and B→ C.

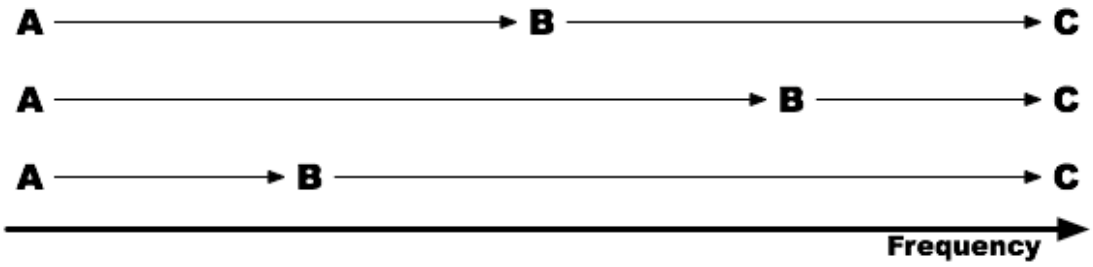

Figure 5 - The relationship between categories of frequency is unknown due to qualitative classification.

The injury and environmental damage categories under the consequence identification have the same problem as the identification of frequency. By studying the injuries and environmental damage columns in Table 3, it is not possible to read a quantitative relationship between the categories. Property damage is the only category where relations between consequence categories are known, because it is defined in terms of money, which is a quantitative scale by default.

4.5 Inconsistent scaling of the risk matrix

Probability categories	Consequence categories				
	I	II	III	IV	10^{0}
A. Frequent	I-A	II-A	III-A	IV-A	10^{-1}
B. Probable	I-B	II-B	III-B	IV-B	10^{-2}
C. Occasional	I-C	II-C	III-C	IV-C	10^{-3}
D. Remote	I-D	II-D	III-D	IV-D	10^{-4}
					10^{-5}
					10^{-6}
E. Improbable	I-E	II-E	III-E	IV-E	10^{-7}
					10^{-8}
					10^{-9}
	100 MSEK	10 *MSEK*	*2 MSEK*	*100 kSEK*	*2 kSEK*

Figure 6 – Proportional correct risk matrix[†] created from Table 2 and Table 3

The current method for presenting the risk matrix has an inconsistent visual presentation. Qualitative definitions of the intervals in the axes of a matrix that later gets redefined in to numerical intervals may be of different sizes. An uncontrolled variation of the matrix intervals will result in that each cell covers an uncontrolled large part of the defined space for a risk. The present method of visualising is to keep all cells to the same size regardless of how much of the risk's space they cover. Equally sized cells can give the impression that all risk categories and all jumps between categories are equally large. The figure below (Figure 6) visualises a proportional correct matrix created for the risk matrix found in chapter 4.2. Notice that the risk categories have various sizes, e.g. when comparing III-C, III-D, IV-C and IV-D all are of different sizes while in Figure 4 they seem equally large.

4.6 Problem with the present system

The present system for managing system risk has no method for handling the total system risk of a system. FMV writes the safety statement for a system where all risks meets the tolerable risk criterion, there is no consideration made on the total amount of risk. A system of seven risks where all are classed as tolerable is visualised in Figure 7 below. This system will by today's standard of system safety be defined as safe.

[†] Notice that the lower border for category E, in the figure, is set to 10^{-9}. In a real system $p \rightarrow 0$ and E will become infinitely large.

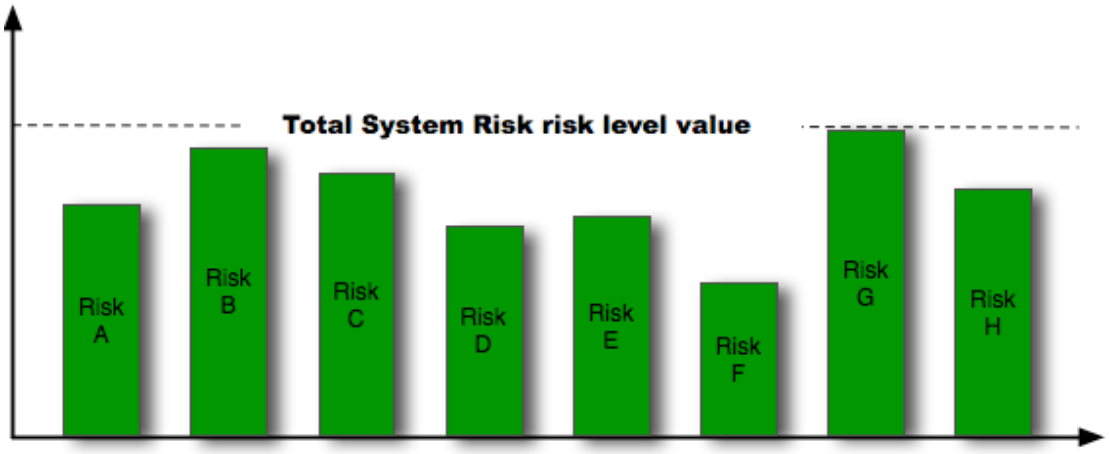

Figure 7 - Risk values for a "safe" system containing seven risks.

By applying today's methodology it is possible to extend a system with an infinite number of tolerable risks and it is still considered safe. An expansion of this system with 99 new risks will in reality make it increasingly unsafe. The chance for a system safety related accident to happen would in reality almost always increase when adding risks. If all the new risks are equal to the tolerable risk level value the new modified system is classed as tolerable by the present method.

The sum of two probabilities $P(A \cup B) = P(A)+P(B)-P(A \cap B)$ (Blom 1984 p. 24), this which leads to that P(an accident occur) $\rightarrow 1$ when the system expands with an infinite number of risks. The only exception to this increase is when all the risks at question are completely positively dependent, if A happens then B will also happen $P(A \cap B)=Min\{A,B\}$, in this case the probability will be equal to $Max\{P(A),P(B)\}$.

This conflict between the methodology and reality needs to be handled to get a better evaluation of the safety in a system. In recent time another dimension, quantity of risks, has entered into the risk analysis. A risk value where this new factor is included is known as *Total System Risk* (Ekholm 2006a).

5 The new system with Total System Risk

5.1 Total System Risk

The US Department of Defence (2005 p. 29) has made the observation that the quantities of risks are needed when looking at system risk. In the draft for a replacement of MIL-STD-882D it is called Total System Risk (TSR) (U.S. Department of Defence 2005). TSR is bound to become a part of the U.S. military system safety work since it is about to be included in this standard. The task of defining the methods for working with the unit is not yet standardised. The Department of Defence has not defined how such a unit should be calculated (Ekholm 2006 p. 1), but several system safety experts agree that TSR should, besides describing a total system risk, be easy to calculate and interpret (Clemens & Swallom 2005).

The new MIL-STD-882E is to become a part of the new FM system safety methodology when it is finished (FM 2006c p. 3). Ekholm at FMV presents a method for handling system risk with an implementation of TSR in a series of two papers, *Summation of risks* (2006) and *Risk Calculation for Complex Systems* (2005). These two papers are an attempt to meet the combined demand for including quantity of risk and usability.

5.2 The summation method

5.2.1 Quantitative approach

The summation method reuses parts of the present method of handling risks, but the greatest difference is that all risk handling is treated fully quantitative.

Both the frequency and consequence are defined as numerical values. The frequency is defined as a probability value for a risk to happen within a defined time frame. This timeframe can for example be per system and year or per system life cycle. The consequence is the estimated outcome of such an event in form of a death count or monetary value. A risk value is calculated from the product of the two, r=p*c. (FMV 2006a passim)

If defining the outcome of a single risk system as a stochastic variable X or X(u) it is possible to find a similarity between the risk value and the probabilistic estimated value E(X).

Let X be defined on the space Ω. The space defines and limits the possible consequences for the outcome, $\Omega = \{c_1, c_2, \ldots, c_n\}$, n=number of possible outcomes, $\sum_{k=1}^{n}\left(\mathrm{P}(X = c_k)\right) = 1$. The estimated value is defined as (5.1) below. (Blom 1984 p. 116)

$$E(X) = \sum_{k=1}^{n}\left(c_k * p_X(c_k)\right) \qquad (5.1)$$

Example
A simple example of this analogue to the summation method's formula r=p*c looks like the following. The space is defined into two outcomes, see Figure 8, an accident occurs with the consequence c_1=1, and no accident occurs with c_2 = 0.

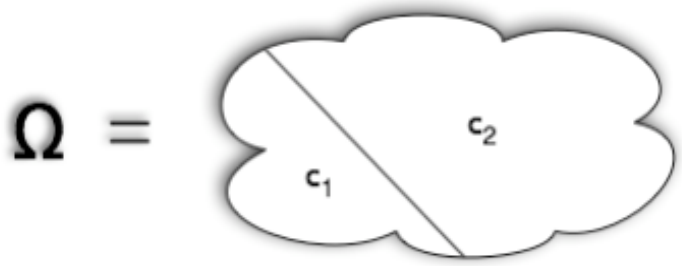

Figure 8 - Representation of the defined space Ω.

Ω={1, 0}

P(1) = p = 0.2

P(0) = q = 0.8

E(X)=0.2 * 1 + 0.8 * 0 = p * c + 0

The risk value presented in r and the risk value presented by E(X) are identical, $r \equiv E(X) = 0.2$.

5.2.2 Single risk breakdown structure/splitting of risk

In the present system safety system at FM a hazardous event is dedicated into a risk that has one outcome. This outcome is as described earlier the worst credible consequence of that hazardous event. Another approach in non-quantitative systems is to use the most credible consequence. Both definitions exclude a various amount of information from the calculation.

A single risk value calculation based on the worst credible consequence will always be estimated too high. This is because the consequence will be above what is to be expected on average. A calculation based on the most credible risk will lead to an error if the consequence has an uneven distribution, because the amount of consequences will not be equal above and underneath this credible level.

The previous chapter (5.2.1) described the analogue features to a stochastic variable. By utilizing this feature further it is possible to improve the handling of such events. The ability to control system risk will increase because the breakdown structures will explicitly state possible outcomes of a risk into the risk evaluation. Specific measures can be done to deal with each kind of consequence, not only measures to deal with the worst/most credible consequences.

Splitting a risk into a number of several smaller risks based on the defined space Ω allows the system risk management to get a more detailed picture of the system risks. Consider a risk with five different consequences. The space Ω of the

stochastic variable X will be divided into six (the five consequences plus one when the hazardous event does not occur = 0). Ω is visualised below in Figure 9.

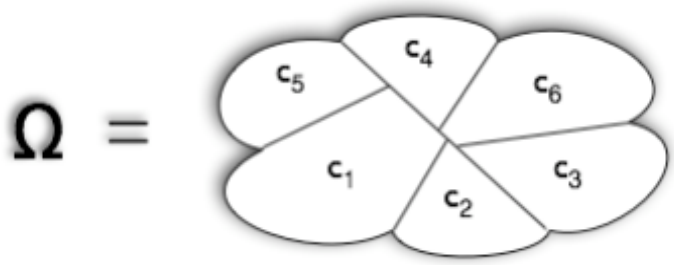

Figure 9 - Representation of the defined space into which X is defined, the partitions divided by lines represents the possible outcomes of this space.

The estimated value of the stochastic variable is $E(X)= p_1 * c_1 + \ldots + p_6 * c_6$. From this equation it is possible to split it into five disjunctive risks, which all are analogous to the risk value calculation formula in the summation method; r=p*c.

The new smaller risks made from a split can be included into the risk list of the summation method. All the risks get different consequences and probability values for the calculation of TSR.

It is important to keep track of risks that are the result of a splitting of a risk, for the purpose of handling their r-values. If an improvement in probability is done then the risk value for all the smaller risks with the same hazardous event are improved. Changes in consequence do not necessary change the risk value of other risks, but adjustments can have an effect and should be checked/considered before recalculating TSR.

An alternative to splitting of risks is to use one risk as in the present method. A more correct consequence, compared to the worst/most credible consequence, can be calculated from E(X). The "most likely consequence" = E(X)/p . An argument for not choosing this method is the loss in control and overview, information will be hidden inside the single estimated value for the consequence.

Example of splitting risk
Consider the risk of using a ladder and falling down from it.

Let the stochastic variable X describe the outcome of the use of a ladder.

The defined space of X is Ω={0 dead, 0.01 dead[†], 0.1 dead, 1 dead}

Let the probability for falling down the ladder and an injury to occur be estimated to $1^0/_{00}$. The outcome 0 dead will therefore be observed in 999 $^0/_{00}$ of the observations.

[†] 0.01 dead ⇔ 1 limited injury; 0.1 dead ⇔ 1 serious injury ⇔ 10 limited injuries. The rules used for transforming accidents into the unit *dead,* with levels <1 can be found in chapter 3.4.1 page 12.

The summation method splits the risk where injury is observed into three smaller risks where each outcome of falling from the latter is defined as one risk.

In this case we let the probabilities 0.01, 0.1 and 1 dead* be 3/6, 1/3 respective 1/6.

Giving the following:

r_1= P(Falling from ladder and get 0.01 dead)*0.01 dead
= (0.001 * 3/6) * 0.01 dead = $\underline{5*10^{-6} \text{ dead}}$

r_2= P(Falling from ladder and get 0.1 dead)*0.1 dead
= (0.001 * 1/3) * 0.1 dead = $\underline{3.333 * 10^{-5} \text{ dead}}$

r_3= P(Falling from ladder and get 1 dead)*1 dead
= (0.001 * 1/6) * 1 dead = $\underline{1.667 * 10^{-4} \text{ dead}}$

R= $r_3 + r_3 + r_3 = 2.05 * 10^{-4}$

5.2.3 Quantitative risk matrix

Quantifying risks enables the possibility to evaluate different risks against each other. This property is shown in the new quantitative risk matrix, which is developed from the present risk matrix (FMV 2006a). The new quantitative matrix has axes with numerical values. Another property of the matrix is that the product of probability and consequence is constant in a diagonal line. This is because the increase of value along the two axes is proportional to each other. An interval of one order of magnitude is marked out with equally large intervals in the matrix. A result of this property is that all *risks of the same size will be plotted into the same diagonal.* All risks above this line are greater than the risk at question and all risks below this line are smaller. This is an improvement for the task of comparing risks against each other.

By using intervals when calculating risk values one has to choose a representative value from inside each interval. In the case where the internal distribution is not known a worst case calculation could be done. This will prevent an underestimation of the single risk value and the TSR. By having this as a default value, FMV can guarantee a maximum system risk value against FM. If other numbers are to be used by a producer, FMV can demand a documentation proving the worst case calculation are to conservative.

In Figure 10 below the consequence deals with values of death <1. It is possible to have consequences of these dimensions because of transformation of different kinds of accidents into a common unit. When using the conversion table, Table 1, category I will cover 1–3 serious injuries, 11–30 limited injuries or a combination of these values. 1 serious injury + 10 limited injuries = 0.2 dead would fit into this category.

Categories of Frequency	Categories of Consequence†
A.]0.01, 0.03]	**I**.]0.1, 0.3]
B.]0.03, 0.1]	**II**.]0.3, 1]
C.]0.1, 0.3]	**III**.]1.1, 3]
D.]0.3, 1]	**IV**.]3.1, 10]

† Measured unit "dead"

Category of frequency	Category of consequence			
	I	**II**	**III**	**IV**
D	r=0.3	1	3	10
C	0.09	0.3	0.9	3
B	0.03	0.1	0.3	1
A	0.009	0.03	0.09	0.3

Figure 10 – An example of a risk matrix with quantitative axes. The diagonal line marks out a set of risks with the same risk value.

5.2.4 TSR value

It is possible to compare all risks that are plotted into a quantitative matrix against each other. A risk in the B-IV category above is larger than a risk in the D-I category. It is also possible to estimate how much larger or smaller a risk is compared to another. The r-values in the matrix are estimates of the expected outcome from one risk, the relationship between risks are therefore handled as the relation of their r-value. The summation method (Ekholm 2005) uses this feature and calculates a quantitative value for TSR from these values. The method calculates the TSR value as the sum of the r-values for all the single risks in the system.

$$TSR = \sum_{i=1}^{n} r_i \text{ , n= number of risks} \qquad (5.2)$$

Example

A system has two risks, a and b.

p_a = frequency category **A**. c_a = consequence category **III**

p_b = frequency category **C**. c_b = consequence category **IV**

The risk values for a and b are:

r_a=0.03 * 3 = 0.09 r_b= 0.3 * 10 = 3

The total system risk of this system of two risks are the sum of the single risks r-value.

$$\text{TSR} = \sum_{i=a,b} r_i = r_a + r_b = 3{,}09$$

TSR is a unit of measure that improves control over system risk. By using requirements of TSR values instead of the present requirements of tolerable risk levels values it is possible to prevent the actual risk of the system to increase uncontrolled by adding risks. In a system where the TSR quota is used and it is necessary to introduce another risk to the system, it will be necessary to sharpen the requirements of already existing risks that are in the system.

5.2.5 Assuming independency

The calculated TSR value is a rough and fast approximation of what to expect from a system. A reason for this is the assumption that all the hazardous events in the system risks are independent of each other. An increase of one risk will not affect the total system risk more than the local increase. In real life systems there will be dependencies of different kinds such that an increase in one risk may trigger an increase or decrease of another risk and thereby resulting in a larger change in the total system risk compared to the isolated change of the individual risk.

The estimated value of a system S containing several stochastic variables, $X_1, X_2, \ldots, X_n$, will without the assumption of independency have an estimated outcome defined by (5.3) below. The estimation is analogous to (5.1), here E(S) is the sum of the product for all combinations of all values of $g(X,X,\ldots,X)$ and $P(g(X,X,\ldots,X))$ (Blom 1984 p, 118).

$$\begin{cases} X_1 = x_{11}, x_{12}, \ldots, x_{1k} \\ X_2 = x_{21}, x_{22}, \ldots, x_{2k} \\ \vdots \\ X_n = x_{n1}, x_{n2}, \ldots, x_{nk} \end{cases} \tag{5.3}$$

$$E(S) = \sum_{j_1, j_2, \ldots, j_n} \left(\left(x_{1j_1}, x_{2j_2}, \ldots, x_{nj_n} \right) \times p_{X_1, X_2, \ldots, X_n} \left(x_{1j_1}, x_{2j_2}, \ldots, x_{nj_n} \right) \right)$$

The assumption of independent risks reduces the complexity of the equation and decreases the number of calculations to a large extent. Calculations without the assumption will have a calculation cost of $O(k^n)$ operations, when a calculation with the assumption will only have the cost of $O(kn) \approx O(n)$ operations. This improvement reduces the need for resources on calculations and data collection. A system of independent risks allows a simplification of (5.3), because it is possible to define $g() = X_1 + X_2 + \ldots + X_n$. The new formula (5.4) is equivalent with the TSR calculation and has a less calculation complexity.

$$E(S) = \sum_{j_1, j_2, \ldots, j_n} \left(\left(x_{1j_1} + x_{2j_2} + \ldots + x_{nj_n} \right) \times p_{X_1, X_2, \ldots, X_n} \left(x_{1j_1}, x_{2j_2}, \ldots, x_{nj_n} \right) \right) \tag{5.4}$$

A limitation in the method that arises from this assumption is its inability to discover correlating effects between risks. These correlations can drive the actual risk value to both above and below the estimated value, depending on if it is a positive or negative correlation.

It is stated by FMV (2006b) that although it is important to find a good risk calculation method, it is more important to find a method that is easy-to-use, even if the result is only an approximated value. The assumption of independent risks does simplify the calculation for an approximated risk value; it is shown when comparing (5.3) and (5.4). One measure to reduce the error is to cluster known dependent risks into a single risk before using it in the summation method.

5.2.6 System breakdown structure/ splitting of systems

For Technical systems in FM an aim is to create modules, such that it is possible mix and match units together to be able to meet different levels of military readiness (SOU 2002 p. 125). Creating a module based risk evaluating system would fit well into this aim, and ease work load for assessing the risk levels for many different kinds of technical combinations.

The summation method enables the implementation of the idea to reuse certain parts of a system into another systems without the need to redo the whole system safety evaluation process. The only additional system safety assessment needed is for the interaction risks.

A feature of the summation method is the possibility to break down a system risk into smaller systems or build larger systems from several smaller systems, also known as system of systems (Ekholm 2005 p. 5). This activity is similar to the activity of splitting single risks. By defining each risk into a sub system the result from a TSR calculation, will for each sub system be handled a statistical independent unit with a specified risk level. E.g. a radio system in a vehicle is a sub system of the whole vehicle, it can also be a sub system of another unit such as a military tank.

The sum of all sub system TSR can be used to define TSR for a larger system of systems. In addition to this sum there is a need to extend the TSR with integration risk values. Combining sub systems into a larger one leads to risks that is caused by the integration itself. It is therefore necessary to extend the TSR with an integration risk.

TSR for a system consisting of *n* sub systems can be calculated from the equation (5.5) below. The r-values are the single risk values of all k number of identified integration risks in the system.

$$TSR = TSR_{S1} + TSR_{S2} + ... + TSR_{Sn} + r_{i1} + r_{i2} + ... + r_{ik} \qquad (5.5)$$

5.3 Risk budget

A concept that has risen from the TSR handling is risk budgeting. It is based on the feature that a system is only allowed to contain a certain amount of risk. There are no constrains in regard to how the risks are distributed, compared to the present concept where a system is bound to a uniform distribution of risks.

In the present system, system developers who manage to push a risk down further than the tolerable risk level will get no effect on the future system safety work. The new system acknowledges this reduction of the system risk and allows the developer to keep another risk on a higher than average level.

By opening for the possibility to budget with risks it is possible for the developer to meet the TSR requirements of the customer at a lower cost compared to a flat risk level system. With risk budgeting the producer is able to distribute resources for risk reduction in areas where the effect is the best. Instead of using resources on a small risk reduction in a risk that is expensive the producer can may use the resources on other, easier to reduce, risks that have a larger effect on the system.

5.3.1 Working with risk budgets

To work effectively with risk budgets it is necessary to have control over the cost effectiveness of improving both p and c for all risks. An overview of this kind will enable a developer to create a ranking system where the most effective reductions are prioritised. This optimisation can be done both linearly and discretely over risk value intervals depending of the amount of information of the system risks and knowledge accuracy of the reductive actions.

5.3.2 Understanding the effect of p and c

When creating an overview of the effect from reducing p and c it is necessary to be aware of their relative change in effect compared to an initial risk list. The p value will have a less effect than stated in the risk list and c will have a larger effect.

The reason for these changes in effect is based by the initial summation of risks to get the TSR value. The summing of risks uses the theory of summing probabilities which is P(A∪B)=P(A)+P(B)-P(A∩B) in its simplest form (Blom 1984 p. 24). The process of adding two risks is visualised in the figure below, Figure 11. The area of the two colour circles represents the probability for A and the probability for B. The area of orange colour represents P(A), the area of blue colour represents P(B) and the area of mixed colour represents P(A∩B). The figure to the right is a representation of the global system risk probability, which equals to P(A∪B).

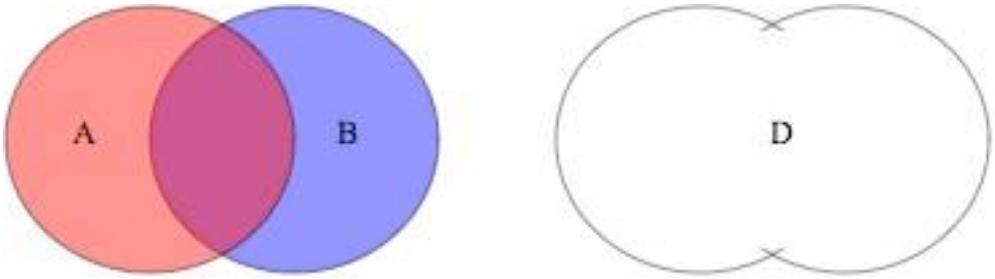

Figure 11 - Graphical representation of the sum of two risks.

In a system with independent risks the following is true:

$$P(A \cap B) = P(A) * P(B) \tag{5.6}$$

Because of P(A∪B) > 0, the probability that a hazardous event should happen in the system, $p_{sys} < p_A + p_B$. Similarly it is possible to see that the estimated consequence if a hazardous event does occur, c_{sys} , is smaller than the weighted average of c_A and c_B.

$$c_{sys} > \frac{p_A * c_A}{p_A + p_B} + \frac{p_B * c_B}{p_A + p_B} = \frac{p_A * c_A + p_B * c_B}{p_A + p_B}$$

This is shown below.

$$\begin{aligned} & TSR = r_A + r_B = p_{sys} * c_{sys} = (p_A + p_B - p_A * p_B) * c_{sys} \\ & = p_A * c_A + p_B * c_B = p_A * c_{sys} + p_B * c_{sys} - p_A * p_B * c_{sys} \\ & \Leftrightarrow c_{sys} = \frac{p_A * c_A + p_B * c_B}{p_A + p_B - p_A * p_B} > \frac{p_A * c_A + p_B * c_B}{p_A + p_B} \end{aligned} \tag{5.7}$$

These features of c and p are of importance when recalculating risk values inside a system. Consider the system D found in Figure 11 above and let $p_A = p_B$. To identify the effect of the risk A and B in the system we know that A and B are equally large. By dividing D in two equal parts, p'_A and p'_B, we have distributed the total effect of the probability, p_D, according to the size of p_A and p_B. When calculating system safety reductions based on probability it is therefore possible to see that the effect will be lower than the initial set p-value.

The c_{sys} is in a similar way as p_{sys} differing from the initial values since a shortening of (5.7) gives $c_{sys} > (c_A + c_B)/2$. It is therefore possible to see that the effect of c will be higher than the initial set c-value. This is because $P(A \cap B)$ will increase when A and B increases.

The outcome of these two differing effects of p and c will vary depending on the size of $P(A \cap B)$, which depends on amount and size of the p-values in the system. Systems with few risks or risks of small probabilities will have a smaller effect than systems with many risks or risks with high probability.

This principle is even valid for systems with more than two risks, but the complexity of dividing according to the initial p and c values will increase. The main reason for this complexity is the problem of controlling the proportional effect of intersection between all risks against all other risks.

Because of the complexity of this calculation it is not of practical interest to include it into the risk budget. In systems that are subject to be affected by this in a larger extent it is possible to do a much less complex approximation of the effect. The approximation calculates p_{sys} and c_{sys} and distributes the values according to relative size of the p-value of each containing risk. This will result in a set of relative risk values, r'-values, that are proportional equal to the initial r-values, but the effect of change is distributed by the size of the risks. E.g. in a system where a risk r_1 that is twice as probable as the risk r_2 will the proportions still be the same, r'_1 twice as large as r'_2 , after the redistribution.

5.3.3 Approximating the effect of p and c

It is necessary to calculate the probability for any accident to happen in the system, p_{sys} to calculate the effect p and c has on the system. To do this one needs the values of all hazardous event probabilities, because $p_{sys} = P(r_1 \cup r_2 \cup \ldots \cup r_n)$.

The proportional distribution of p_{sys} is calculated from the proportions of all p-values. In a system of two risks r_1 and r_2 with the risks p_1 and p_2 and consequences c_1 and c_2 the p_{sys} is equal to $p_1 + p_2 - p_1 p_2$. The proportional distributed p-values, p'_1 and p'_2 , would be the following:

$$\begin{cases} p'_1 = p_{sys} \dfrac{p_1}{p_1 + p_2} \\ p'_2 = p_{sys} \dfrac{p_2}{p_1 + p_2} \end{cases} \qquad (5.8)$$

In a general form the calculation of p'_k is:

$$p'_k = p_{sys} \frac{p_k}{p_1 + p_2 + ... + p_n}, \text{ n= number of hazardous events, k} \leq \text{n.} \qquad (5.9)$$

Using p'_1 and p'_2 instead of p_1 and p_2 in the calculation of the effect on a risk reduction will only redistribute the different risk values and not affect the TSR value. The total probability will be the same, since the p'_k values are only a redistribution of p_{sys}, such that $\sum_{i=1}^{k} p'_i = p_{sys}$.

The effect of c, c' is calculated by the p' values, c, and TSR. In the case of a two risk system where r_1 is defined on $\Omega_1 = \{c_{11,}, c_{12}, ..., c_{1n_1}\}$ and r_2 on $\Omega_2 = \{c_{21,}, c_{22}, ..., c_{2n_2}\}$ one know that:

$$\begin{cases} c_1 = p_{11}c_{11} + p_{12}c_{12} + ... + p_{1n}c_{1n_1} \\ c_2 = p_{21}c_{21} + p_{22}c_{22} + ... + p_{2n}c_{2n_2} \end{cases} \qquad (5.10)$$

Since the relative effect of a risk is dependent on the probability the relation between c and c' is a variable x.

$$\begin{cases} c'_1 = c_1 x \\ c'_2 = c_2 x \end{cases} \qquad (5.11)$$

It is possible to calculate x since the TSR does not change with the use of relative risk values.

$$TSR = p_1 c_1 * p_2 c_2 = p'_1 c'_1 * p'_2 c'_2$$

$$\Rightarrow x = \frac{TSR}{p'_1 c_1 + p'_2 c_2}$$

In the general case the calculation would be done as the following:

$$\begin{cases} c'_1 = c_1 x \\ c'_2 = c_2 x \\ \vdots \quad \vdots \\ c'_n = c_n x \end{cases} \quad \text{n = number of hazardous events} \qquad (5.12)$$

$$x = \frac{TSR}{p'_1 c_1 + p'_2 c_2 + \ldots + p'_n c_n}$$

6 Error sources

Besides the sources for error described earlier such as the assumption of statistical independence there are other factors that affect the accuracy of the final result.

6.1 Human perception

The human perception of small numbers can become a source of error in the system safety work. Most persons do have an understanding of the qualitative words used today such as frequently, several times, some time, unlikely but possible. The problem can occur when the same persons are set to define the qualitative estimate into a quantitative scale. How frequent is "frequently"?

A method by transforming the old risk levels into numeric values can work for several of the risks, but it all depends on the evaluator's perception of probability. An example of such quantification is found in H SystSäkE (FM 1996 p.67) where the frequency levels are defined into the following intervals.

Table 4 - Example of a quantification of qualitative frequency categories

Frequency category	**Interval**
A) Very frequent	$\geq 10^{-1}$
B) Frequent	$< 10^{-1}$ $\geq 10^{-3}$
C) Less frequent	$< 10^{-3}$ $\geq 10^{-5}$
D) Improbable	$< 10^{-5}$ $\geq 10^{-7}$
E) Highly improbable	$< 10^{-7}$

Most humans do have a good perception of probabilities that are measured in percent and parts per million. When the orders of magnitude decrease for p, then a person's perception of the p-value decreases as well. It may not be quite as difficult for a person to distinguish between the first two categories compared to the last two. The error however will be proportional equally large.

Another concern for error is when handling even smaller frequencies. Using the definitions from the example above, all probabilities below 10^{-7} will be treated as the same probability. The category E, highly improbable, is here defined as $<10^{-7}$, in the new system it is necessary to differentiate between 10^{-7} and e.g. 10^{-9}, 10^{-11}. It will be necessary for those who are defining risks to define the order of magnitude for probabilities, which are outside of the systems borders of the present methodology and outside their personal conceptual envelope.

FMV have tried to deal with this problem by creating a TSR – protocol (appendix), which divides the estimation of a probability into several steps. By using quantitative factors such as number of exposed persons, exposure time and probabilities for an accident to occur given that personnel are exposed. This protocol reduces the need for estimations of very small probabilities and therefore increases the accuracy of the method.

6.2 Sensitive risks

Large risks with very large or small probabilities are the risks most sensitive to errors in a system. Large probability risks with relatively small errors in the consequence will have a large impact on the final r-value. Similarly low probability risks will be sensitive for errors in the consequence value c.

The system risk management should be aware of this feature of sensitivity, especially for the case of low probability and high consequence. There are two reasons why these are of importance. Commonly these risks will result in a "catastrophe" if it happens. The societal acceptances of such risks are much lower compared to similar high probability risks and one could expect a greater societal pressure if a miscalculated high consequence risk occurs. The second reason is related to the problems with human perception from the chapter above. Because the estimation of a precise low probability value is harder than high probabilities errors in low probabilities, attention to these should be given priority over low consequence risks.

6.3 50% identified

One of the largest sources for the uncertainty when working in system safety is the amount of risks not to be identified. In the ideal world of system safety all risks will be identified but in reality this is shown to be impossible. The experience made by FMV (2006b) and studies shows that a great amount of system risks does not get identified before building a system. The risks not identified can be split into two categories. The first contains risks that exist in the system from the beginning. Theoretically it is possible to identify all of these, but in practice it is not possible. The second category consists of risks impossible (not of immediate interest) to identify when building system. These will be risks created during the system's life cycle. New areas of use, shorter education, different maintenance than expected, different wears than expected and usage by unauthorised personnel are all examples of sources for such new risks (Försvarsmakten 2006, p 38). A rule of thumb for the amount of unidentified risks is said to be in average around 50% (Ekholm 2005 p. 4). This amount includes both risks that do and do not result in an accident during the system life cycle. For some systems this number is above in other below 50%.

To minimise the amount of new risks to evolve into the system one should describe the ideas behind the system and for what scenario it is created. Suggested topics for such a description are (Gunnerhed 1994 p. 5):

- Who is supposed to use the system
- Who is not supposed to use the system
- Which environments is the system created for
- In which environments is it possible to use the system

By keeping such information together with the system at all times, it is possible to reduce the possibility for new risks to occur.

If the variation around 50% is large one could argue that TSR will not be an effective correct tool to control risk in a single system. However, in a portfolio of

systems developed based on the TSR principle the error will stabilise on 50%. For FM that orders and modifies many systems, and if calculations which compensate for the missed half of the risks are done, the error from variation will be minimised. Consequently the total FM system will have a stable 50% risk identification, even if it is 40% or 60% for a single system.

It is the FM commander, with the overall responsibility of the FM safety, who should make this assessment of unidentified risks. In the limitations of TSR handed down to FMV the calculation of unidentified risks should have been done. The value, which FMV gets to handle, is the part of FM's risk budget dedicated for identified risks.

7 Implementation of a TSR method

This chapter will present a workflow of how to implement a risk summation method. It will be based on the summation method (Ekholm 2005), but changes and extensions will be made according to the findings in previous chapters. This workflow will look at risks affecting personnel injuries, but the principle of the workflow will be the same when working with other measures such as monetary risks.

7.1 Risk list

Identify all risks and define a probability for the hazardous event to happen. It is important to state what periodisation the probability value is based upon, it can be per year, unit and year, system and year, running hours, etc.

For each risk identify all possible consequences. Transform all consequences into a common unit. Create separate lists and calculations if it is not possible to transform all consequences into a common unit. See chapter 3.4.1.

Create a set of intervals, where the size of each interval in each set should be of equal logarithmic size. The total range of the intervals should cover the whole spectra of consequences in value and personnel injury.

Define a distribution, one per set of intervals, of the consequence intervals. The sum of the consequences should be equal to 1 for both sets. Notice that 0 (zero) is not included in any interval since a hazardous event with no consequence is not an accident and therefore outside of the definition of a risk. It is possible that an event will happen more than once in the defined period the risk list is created for and p should not be seen as a strict measure of probability, but a measure of frequency, hence $p \geq 0$.

Table 5 - Example of a risk list.

Risk number	Sub system	Risk source	Possible accident	p per system life cycle	c-interval	Distribution	p_i
1.1	Antenna	Pieces of ice, ice block	Personnel is hit by falling ice	20	]0.01, 0.03]	0.5	10
1.2					]0.03, 0.1]	0.44	8.8
1.3					]0.1, 0.3]	0.05	1
1.4					]0.3, 1]	0.01	0.2
2.1	RC	Fire	Personnel gets burning injury or injured from poisonous gas caused by gas in the system unit	0.5	]0.01, 0.03]	0.05	0.025
2.2					]0.03, 0.1]	0.39	0.195
2.3					]0.1, 0.3]	0.55	0.275
2.4					]0.3, 1]	0.01	0.005

7.2 Risk matrix

Create a risk matrix similar to Figure 12. The range of the axes of each matrix should cover values from the smallest to the largest consequences and risk probabilities found in the risk list. Each interval within the matrix, both consequence and frequency, should be of same size e.g. one order of magnitude (See chapter 5.2.3 on page 24).

Categories of Frequency	**Categories of Consequence (dead)**	**Category of frequency**	**Category of consequence**			
A.]0.01, 0.03]	**I**.]0.003, 0.01]		**I**	**II**	**III**	**IV**
B.]0.03, 0.1]	**II**.]0.01, 0.03]	**F**	r=0.3	0.9	3	9
C.]0.1, 0.3]	**III**.]0.03, 0.1]	**E**	0.1	0.3	1	3
D.]0.3, 1]	**IV**.]0.1, 0.3]	**D**	0.03	0.09	0.3	0.9
E.]1, 3]		**C**	0.01	0.03	0.1	0.3
F.]3, 10]		**B**	0.003	0.009	0.03	0.09
		A	0.001	0.003	0.01	0.03

Figure 12 - Example of a risk matrix based on the information found in the risk list of Table 5 above.

Make a conservative estimation of the r-value of each cell by using the highest interval values, the r-value of A-I will be equal to 0.03 * 0.01=0.001 .

Extend the risk list for Table 5 with three columns, *Frequency* category, *consequence* category and *r-value*, similar to

Table 6 below. Fill in values for each risk. The frequency category is found by looking in the column *Risk probability*. Read the r-value by combining the two categories into the risk matrix.

Table 6 - An extension of the risk list. Frequency and Consequence categories and risk values are added.

Risk number	**Frequency**	**Consequence**	**r**
1.1	F	I	0.3
1.2	F	II	0.9
1.3	D	III	0.3
1.4	C	IV	0.3
2.1	A	I	0.001
2.2	C	II	0.03
2.3	C	III	0.1
2.4	B	IV	0.09

7.3 Calculating TSR values

To calculate TSR of a system one needs information on the r-value for all risks in the system. TSR is the sum of all r-values for risks of same kind.

In the example used above the calculation of TSR is:

$$TSR = \sum r_i = r_{1.1} + r_{1.2} + r_{1.3} + r_{1.4} + r_{2.1} + r_{2.2} + r_{2.3} + r_{2.4} = 2.0021 \approx 2 .$$

Because of the inaccuracy of indata to the calculation of TSR, it is not justified to use all decimals of the calculation. The TSR is to be seen as a guiding approximate number, and it should be rounded off to no more than one decimal. In this case $2.0021 \approx 2$.

This value should be interpreted as that the identified risks for the system are estimated to result in injuries equivalent to 2 dead. See chapter 3.4.1.

7.4 Calculate the relative effect of c and p

To calculate the relative effect of p and c one needs, TSR, all p values for hazardous events, the estimated consequence for all hazardous events, p_{sys} . In the example used above the following is already calculated:

TSR≈2

p_1=20, p_2=0.5 (frequency)

To calculate p_{sys} use the rule of summing probabilities.

$p_{sys} = P(r_1)+P(r_2)-P(r_1 \cap r_2)= p_1 + p_2 - p_1 * p_2 = 20 + 0.5 - 10 = \underline{10.5}$.

The relative effect of p is calculated with (5.9) such that:

$$\begin{aligned} p'_1 &= p_{sys}\frac{p_1}{p_1 + p_2} = 10.5\frac{20}{20.5} = 10.24 \\ p'_2 &= p_{sys}\frac{p_2}{p_1 + p_2} = 10.5\frac{0.5}{20.5} = 0.26 \end{aligned} \qquad (7.1)$$

The estimated consequence for all hazardous events, c_1 and c_2, are found by multiplying all probabilities and consequences for each of the split fractions of the hazardous events. In this example the calculation based on *(5.10)* will look like the following.

$$\begin{cases} c_1 = p_{1.1}c_{1.1} + p_{1.2}c_{1.2} + p_{1.3}c_{1.3} + p_{1.4}c_{1.4} = 0.5*0.03 + 0.44*0.1 + 0.05*0.3 + 0.01*1 = 0.084 \\ c_{21} = p_{2.1}c_{2.1} + p_{2.2}c_{2.2} + p_{2.3}c_{2.3} + p_{2.4}c_{2.4} = 0.05*0.03 + 0.39*0.1 + 0.55*0.3 + 0.01*1 = 0.2155 \end{cases}$$

The relation between c and c' is known as

$$\begin{cases} c'_1 = c_1 x \\ c'_2 = c_2 x \end{cases}. \tag{7.2}$$

The calculation of x is done with (5.12) such that

$$x = \frac{TSR}{p'_1 c_1 + p'_2 c_2} = \frac{2}{0.86 + 0.056} \approx 2.2$$

further $\begin{cases} c'_1 = c_1 * 2.2 = 0.185 \\ c'_2 = c_2 * 2.2 = 0.474 \end{cases}$

Recalculate all risk values with the new relative values similar to what is done in the initial risk list. For the example used above the relative effect of c and p will look like in the table beneath. These numbers should be used when measuring the effect of using resources on reducing risk values.

Table 7 - List of the relative effect values for probability and consequence for all risks in the risk list of Table 5.

Risk number	**Risk probability** (relative effect)	**Risk consequence**(relative effect)
1.1	5.12	]0.022, 0.066]
1.2	4.5056	]0.066, 0.22]
1.3	0.512	]0.22, 0.66]
1.4	0.1024	]0.66, 22]
2.1	0.013	]0.022, 0.066]
2.2	0.1014	]0.066, 0.22]
2.3	0.143	]0.22, 0.66]
2.4	0.0026	]0.66, 22]

8 Discussion and conclusions

8.1 Summing risks

Risk estimation of complex systems is not and will not be an easy task to do, even with this new method. The interaction between different parts of a system will have a larger effect, for better or worse, on the system safety than what is possible to foresee with limited amounts of time and resources. This is because complex systems will always have interaction with parts of the world that lie outside the model limits. Changes of the system over time will also have an effect on the exactitude of an estimate.

Dependencies are another concern for the accuracy, since the summation method assumes statistical independence which might not be the case. But the alternative, not to assume independence, will bring costly calculations and a costly investigation to the assessment. In risk assessments of risks regarding money one can compare the cost of investigating against the gain from the more precise estimate. When the risks are personnel injuries as similar argument is harder to do, but one can argue that resources put into investigating risks could instead be used in risk reducing actions.

The model does only take input data from top events of a system as input parameters. By doing so the analyses of complexity and dependencies in each event assessment are already included. The only dependency issues that are excluded from the system are the dependency between top events. It is therefore important for the user of the summation method to be aware of this error. There exists no reason to believe that all such dependencies should be identified in the system safety work, when comparing it to the risk identification rate. A reasonable assumption is that the rate will be the same, 50%.

It is also possible to defend the choice of simplifying the calculations of the method based on the accuracy on the indata. As long as the indata is assessments made by humans based on information that is qualitative or not guaranteed precise there the values put into the summation method will not be totally precise either. Using a fine calibre algorithm on roughly accurate indata will not make outdata beneficial more precise than the summation method.

Regardless of the inaccuracy issues of the method there are benefits of this method. The new summation method will be an improvement to the system risk assessment if implemented at FMV. In the summation method a system has a limited quota of risk that can be used up, and when the quota is filled no additional risks can be added. This is a fundamental improvement compared to the present system where the amount of risk in a system can swell out without any limits as long as it is below the tolerable risk level.

8.2 Budgeting with risks

The possibility of prioritizing risks according to the price effect ratio will create a conflict with the accepted principles of risk handling of today. Managing risk through such a system will not necessarily follow the principles of Räddningsverket (Chapter 3.5). A strict focus on a maximised effect of the risk reductions in the

system safety work allows a certain risk or a group of risks to be at a high level. If no further criterion is set there is a possibility that all these high risks left "unattended" will be affecting a certain individual or group of people, who compared to the present system, may be exposed to a larger amount of risks from the system.

A solution to prevent a large part of "unattended" risk to affect a single group or person can be to create a variation of the risk budgeting. By keeping track of the amount of risk that each group is exposed to one could create limitations on how large part of the TSR a person can be exposed to. The amount should vary between different groups of persons, and an evaluation of how this should be calculated would have to be done. The result of this would not necessarily be an economical optimal risk reduction, but it would prevent a concentration of risk on one specific group or person.

Another problem that occurs is related to the third principle, concerning large accidents. People and society in general seem to have an aversion against high consequence risks, there is a larger societal acceptance of risks with small consequences even if the r-value is the same (Börtemark & Ekholm 2006). The accepted risk value for driving a car in traffic is much higher than the accepted risk value for a meltdown in a nuclear plant. When working strictly with the risk budget principle, no consideration is done on the size of the c-value, only the combined value is in focus.

A direction to handle this issue is to use a practice which favours the reduction of large c values. If the cost of reducing a high consequence risk and a high probability risk is about the same, then the high consequence should be preferred. One could also use a practice of preferring a reduction of c over the reduction of p when working with high consequence risks. This measure will not affect the efficiency of the risk budget as long as such practice is only done on equally large risks. It is however possible to imagine a method where risks within an interval get treated by a similar prioritising. The result from this would affect the efficiency of the method, but reduce the risks of the accidents that are the hardest to deal with. Improved accuracy is another benefit from a method of prioritising reduction of risks with large c and low p values, since these risks are associated with most uncertainty in the assessment.

Despite the issues in relation to budgeting risks there are also great benefits. The features quantification and the possibility to go from a strict uniform to a free distribution of risk levels are very important. This allows a more controlled and effective reduction of risks, which is a gain for all who takes a part of the system, system builder, buyers and users. Users may gain a better understanding of the risks using a system. The possibility to optimise risk reductions in relation to resources gives a positive economical effect for both developer and buyer. The developer may reduce costs in fulfilling system safety demands, by reducing the amount of resources put into the reduction of hard-to-reduce risks. The buyer can obtain a lower price on a system since the economical benefits for the producer could affect the business offer they get from a request for proposal.

8.3 Future development

The theory in this study is adjusted for the implementation at FMV, FM and connected industry. A natural development of these findings would be to transform them into more generic terminology. For instance the mathematics used in this paper is based on discrete values on probabilities and consequences, analogous to how risk assessments are handled by FMV. Creating a general description including the linear case would be beneficial for the usability of the method by others and in other kinds of systems.

Another interesting and beneficial direction for further development is to look on the possibility to implement the calculations for effective p and c values (Chapter 5.3.2) into an economical prioritising method based on the cost effect ratio for reducing risks. Such a method could make it easier to see the benefits from working with system safety. A method connected to economical systems push forward system safety improvement in a system as a cost reducing measure. Improvements in the development phase can be shown to reduce future costs from accidents and parts of the system safety work can become a self financed activity.

In the work of handling risk budgets it is also important to discuss the ethical dilemmas that occur when choosing between a maximal risk reduction or making sure no that group or person gets exposed to an unfair share of the system risk. The issues about handling high consequence and high probability risk are important to discuss in relation to optimal risk reduction.

9 Summary

Modern system safety handling is in need of a tool to assess the total risk of a system. The only control mechanism for system safety in the present method is regulation on the allowed risk value for the individual risks, the total effect is not evaluated. A system is vulnerable to an uncontrolled increase in risk without an assessment method for the total risk. The summation method is a cost effective solution for monitoring the total system risk in a system.

The summation method is based on the present system safety method used at FMV. The main difference between the summation method and the present method is the change from a mixed, qualitative and quantitative, risk handling to a strict quantitative risk handling. It utilises the relationship between risks and probability and consequence to create a numerical expected value for all risks. This makes it possible to evaluate, compare and make risk calculations of the individual risk values.

A limitation of the new method is the need for assuming statistical independence between all risks, limiting the correctness of a risk calculation. A calculation without such an assumption is found to increase in complexity in an exponential rate and will by practical means be impossible to accomplish for large systems. The calculation with the assumption is however accomplishable by human force and still returns better information on the system risk than the present system. Another benefit from the assumption is the possibility to break down both individual risks and systems into smaller parts and vice versa, it enables a more effective calculation of risks in so called systems of systems.

The qualitative handling of the total system risk will also enable the possibility to create risk budgets, where it is to see and compare the effect a reduction of probability or consequence in a risk will have on the total system risk. The effect from the initial probability and consequence values changes with the size of the system and should be approximated. In general terms will always the effect of the probability be lower than the initial value and the effect from the consequence will be higher. The feature of risk budgeting is useful and has a positive effect when optimizing the risk reduction in a system where there are limited amounts of resources available for the reductions.

There are also issues that need to be solved before implementing the method of summing risks in an organisation such as FMV. Issues on how to deal with the risks that are left in the system because of their relatively expensive reduction costs, but disadvantageously in relation to the size of consequence or distribution on individuals or groups of individuals.

10 Sources

Air Force Safety Agency (2000). *Air Force System Safety Handbook - designing the safest possible systems consistent with mission requirements and cost effectiveness*. Air Force Safety Centre, Kirkland.

Berner, Boel, (1999). *Perpetum Mobile? Teknikens utmaningar och historiens gång*, Arkiv förlag, Lund.

Blom, Gunnar, (1984). *Sannolikhetsteori med tillämpningar*, 2nd ed. , Studentlitteratur, Lund.

British Health and Safety Executive (2006). *Risk Management – ALARP at a glance*. http://www.hse.gov.uk/risk/theory/alarpglance.htm (2006-10-11).

Börtemark, Arne & Ekholm, Ragnar (2006). *Project meeting at FMV* (2006-09-27).

Ekholm, Ragnar & Wallentin, Pär-Anders (2003). *LectionsPM*. FMV Systemsäkerhet Kurs 54A, Gemensam del. Chapter 5, p 9. Version 0.11, 2003-01-23.

Ekholm, Ragnar (2005). *Risk Calculations for Complex Systems*. 23rd ISSSC in San Diego 2005.

Ekholm, Ragnar (2006a). *Summation of Risk*. 24th ISSSC in Albuquerque 2006.

Ekholm, Ragnar (2006b). *Project meeting at FMV* (2006-05-04).

FM (1996a). Försvarsmaktens handbook för Systemsäkerhet. *H SystSäk 1996*. Stockholm. M7740-784851.

FM (1996b). System Safety Manual, *H SystSäkE 1996*. Stockholm. M7740-784861.

FMV (2003). Rapport. *Risklista UndE 23 serie*.

FMV (2006a). Försvarsmaktens handbook för Systemsäkerhet. *H SystSäk 2006 Del 1 Grunder*. Remissutgåva, remiss noll version 5.0, 2006-03-15.

FMV (2006b). Lecture. *Systemsäkerhet Kurs 54A*. Rimforsa 2006.09.11 – 2006.09.14 .

FMV (2006c). *Swedish defence forces - System Safety Manual Shortened*. H SystSäk E. Draft version July 2006.

Gunnerhed, Mats (1994). *VI Kvalitet – Produktsäkerhet*. Industrilitteratur AB, Stockholm. ISSN 1103-8195.

Hammer, Willie (1972) *Handbook of System and Product Safety*. Englewood Cliffs, New Jersey: Prentice-Hall.

International Association of Classification Societies (IACS), (2004) Formal Safety Assessment - Risk evaluation. *Maritime safety committee, 78th session, Agenda 19,* 2004-02-05.

Nationalencyklopedin (2006). *Risk i tekniska sammanhang*, http://ne.se/jsp/search/article.jsp?i_art_id=294214, retrieved (2006-11-16).

Perrow, Charles (1984) Normal Accidents. *Living with High-risk Tehnologies*. New York: Basic Books.

Roland, Harold E., & Moriarty, Brian (1990). *System Safety Engineering and Management*. 2nd edition. New York: John Wiley & Sons.

Räddningsverket (1989*). Befolkningsskyddet, räddningstjänsten och framtiden*. P20-47/89.

Räddningsverket (1997). R&D report. *Värdering av risk*. Karlstad. ISBN 91-88890-82-1.

Sharit, Joseph (2000). A Modeling Framework for Exposing Risks in Complex Systems. *Risk Analysis,* Vol. 20, No. 4, 2000. Pages 469-482. doi:10.1111/0272-4332.204045

SHK (2000) Information pamphlet from the Swedish Accident Investigation Board, *Haverikommissionen – vad gör den*?. Stockholm: LFV.

SOU (Statens Offentliga Utredningar) (2002) *STYROM – STYRning och Organisation av Materielförsörjning för Försvaret, SOU 2002:39*. Fritzes Offentliga Publikationer, Stockholm.

Swallom, Pat L. & Swallom, Donald W. (2005). *Summing Risk – An International Workshop and Its Results. Journal of System Safety*, November–December 2005. Pages 21-31.

U.S. Department of Defense (2005). *Standard Practice for System Safety*. MIL-STD-882E, Draft 30 Dec 2005.

Wikipedia (2006). *Complex System*, http://en.wikipedia.org/wiki/Complex_system (2006-11-07).

Appendix: Total system risk protocol

Materiel system:	**Radar facility**	**Version**	**10.0**

1	2	3	4	c	6	7	8	9	10	11	12	13	14	15
					RISK PRIOR TO CORRECTIVE ACTION									
Risk #	Sub-system	Risk source	Property	Possible accident	Assessment that condition creating factors exist with the following frequency	Assessment that triggering factor is present with the following frequency	What can be exposed	Exposure	Hit probability	Number of people involved in the accident during system lifecycle	Mishap-categories	Con-version number for fatalities	Assessed mishap distri-bution	Each mishap-category's share of the total outcome, expressed in fatalities
01-0001	Antenna	Pieces of ice , ice block	Potential energy	Personnel is hit by falling ice	Ice formation, 30 days/year	Is falls every other day during period	In average 2.5 persons	1/24	50 %	19,531250	Fatal	1	0,05	0,976563
01-0002											Serious injury	0,1	0,35	0,683594
01-0003											Minor injury	0,01	0,5	0,097656
01-0004											De minimis	0	0,1	0,000000
01-0001											Fatal			
01-0002											Serious injury			
01-0003											Minor injury			
01-0004											De minimis			
01-0001											Fatal			
01-0002											Serious injury			
01-0003											Minor injury			
01-0004											De minimis			
01-0001											Fatal			
01-0002											Serious injury			
01-0003											Minor injury			
01-0004											De minimis			

Basic data

System lifecycle	25	År
Frequency of usage	100	%

Date	06-04-07

16	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35
	Action							RISK FOLLOWING ACTION										
Number of equivalent fatalities during system lifecycle	D	S	W	I	T	(Used currency shall be marked below.) The cost per referenced action per consequence or for the entire accident. (Write on appropriate line. The entire accident on the de minimis line).	Intended action per consequence or for the entire accident (write on appropriate line. The entire accident on the de minimis line).	Assessment that condition creating factors exist with the following frequency	Assessment that triggering factor is present with the following frequency	What can be exposed	Exposure	Hit probability	Number of people involved in the accident during system lifecycle	Mishap-categories	Con-version number for fatalities	Assessed mishap distri-bution	Each mishap-category's share of the total outcome, expressed in fatalities	Number of equivalent fatalities during system lifecycle
1,757813							Reinforced tin roof	Ice formation, 30 days/year	Ice falls every other day during period	In average 2,5 persons	1/24	3 %	1,171875	Fatal	1	0,05	0,05859375	0,10546875
														Serious injury	0,1	0,35	0,041015625	
														Minor injury	0,01	0,5	0,005859375	
		X			X	500 000,00 kr								De minimis	0	0,1	0	
														Fatal				
														Serious injury				
														Minor injury				
														De minimis				
														Fatal				
														Serious injury				
														Minor injury				
														De minimis				
														Fatal				
														Serious injury				
														Minor injury				
														De minimis				

TSR before action	Total cost of action	TSR following action
1,76E+00	500 000,00 kr	1,05E-01

Actions

D = Design change	W = Warning device	T = Training
S = Safety device	I = Instruction/Warning sign	

Only one currency shall be used in a TSR Protocol	
Here is used:	Swedish Crowns, SEK