Armed Forces' Handbook on System Safety 2011
Part 1 – Common

H SystSäk E

Armed Forces Headquarter | 2011-10-31 | 14 910:66344

The Armed Forces Handbook on System Safety 2011 English edition (H SystSäk E 2011) M7739-352031 H SystSäkE 2011 Part 1 and M7739-352032 Part 2 are hereby approved for application from January 01 2012.

At the same time the 1996 edition of H SystSäkE, M7740-784861, as established with HKV April 20, 1998 14 910:72214, is withdrawn.

This English edition is a translation of the Swedish edition. In case of difficulties with regard to interpretation, the Swedish version applies.

This decision has been taken by Colonel Anders Emanuelson. It has been prepared by Arne Börtemark, Swedish Defence Materiel Administration.

Anders Emanuelson
Head of Swedish Armed Forces
Safety Inspectorate

Arne Börtemark

The handbook is published in cooperation with **Sörman Information AB**

Division: The Armed Forces' Security Inspectorate and Swedish Defence Materiel Administration

Editor: Mats Lundgren

M7739-352031 H SYSTSÄK E D1

Central storage: Armed Forces book and form store
Print: Elanders Fälth & Hässler, Värnamo, 2011

Table of Content

5 Description of System Safety Activities

6 The Armed Forces' System Safety Activities

Preface

Instruction – the Armed Forces' handbook on system safety

The instruction regarding the Armed Forces' handbook on system safety 2011 *[26]* specifies, among other things:

- The Armed Forces' working procedures stipulate that safety operations must counteract accident risks and injuries/damage to persons, materiel, or the environment. For matters relating to operational safety: the manager in charge of the safety inspection will decide on directives and instructions and will submit these to the operator concerned.
- System safety forms a part of operational safety activities.
- The Armed Forces' system safety activities are designed to not cause society any increased risks. They also aim to systematically reduce risks to a tolerable level for the Armed Forces.

The instruction includes:

- **Guidance:** Guidance and instructions for the application of this instruction can be found in H SystSäk E.
- **Decision:** For all procurement, modification, renovation and decommissioning of materiel (from 1 January 2011), a decision must be taken as to whether and to what extent system safety activities should be conducted in accordance with H SystSäkE.

Scope

H SystSäk E 2011 Part 1 – Common defines the grounds for the Armed Forces' system safety activities by specifying the principles for basic risk management and the defining of requirements; it also specifies the appropriate roles, responsibilities and tasks from a lifespan perspective, and their interaction. Certain organizations/roles are mentioned specifically; for example Owner Representative (ÄF), the organization with design responsibility (DesignA) and the supplier.

H SystSäk E 2011 Part 2 – Methods describes methods for reporting the activities (system safety tools) that form a part of the Armed Forces' system safety methodology. In several cases, reference is made to MIL-STD-882C *[46]* where the basic text for the activities can be found. Furthermore, general system safety requirements for development, manufacture and maintenance are specified.

Parts 1 and 2 of Armed Forces' handbook on System Safety are both in Swedish and English and are available at the Armed Forces' book and form stores (FBF).

H SystSäk CDR contains: H SystSäk E Parts 1 and 2, MIL-STD-882C as well as some supporting documents such as the Risk Logs, examples and templates.

H SystSäk CDR will be updated as necessary. It is included as an appendix in H SystSäk E Part 1.

Reading Instructions

a. The assessed needs for the use of components for the various roles are described below (this refers to personnel with system safety assignments within their specified roles).

Role Example of organization	User Unit	ÄF HKV	Design A FMV, FORTV and FömedC	Supplier Industry
Part 1 Common	×	×	×	×
Part 2 Methods		(×) Individual	×	×
MIL-STD-882C			×	×

b. The person who reads H SystSäk E for the first time should, in order to understand it fully, read all of Chapter 1. Note in particular that H SystSäk E is not a requirement document that must be followed strictly, but a handbook with both explanations and advice.

c. If ÄF at HQ needs a direct method of instruction for the production of requirements for system safety, in for example the TTEM, study the section below, including direct references in the text. The sections specified are written with others in order to provide support when determining requirements.

Section	Content
2.4 Laws	The link between the specified law/regulation and H SystSäkE
Chapter 5, (all)	Basic description of the Armed Forces' system safety activities. Decision-making and product documents for technical systems. Specific aspects of certain types of technical systems
6.5 Procurement	Requirements that may be considered on the procurement of different types of technical systems

d. User representatives who need a direct method of instruction for system safety activities during use should read *chapter 8* and supplement if necessary with parts from other chapters.

e. Anyone who needs a detailed account of system safety activities, including content and overall system safety requirements should read H SystSäkE Part 2 – Methods.

f. Those who need a general report of the basics of the system safety methods and how they are applied by the Armed Forces must read everything.

News

New structure – H SystSäk E 2011 is made up of two parts - unlike the edition from 1996 - and refers to a specified standard for the description of several of the activities of H SystSäk E Part 2. For a number of activities, a description of the designated standard is lacking. Complete descriptions are presented in part 2.

New approaches have been established, among other things, by including the concept of risk perception. The concept implies an effective work method that focuses on the user's attitude to accident risks occurring and his/her participation in the ongoing work efforts aimed at the technical system which should continuously include the requirements that are established at a specific risk level.

The need to establish specific system safety requirements early on in the requirements formulation process are described and examples of possible requirements are provided.

An extended description of the system safety documentation is included in the handbook.

The risk management methodology according to H SystSäkE 1996 has been further developed. Each individual accident risk and the different outcomes in particular, have been identified. Previous methodology only took into account the individual accident risk's most significant aspects.

A description and detailed instructions have been added for the management of system safety activities such as that exercised by the Armed Forces and DesignA.

Examples of requirements the Armed Forces may address to DesignA in the TTEM and the customer order have been formulated. These requirements are numbered.

A special CD has been produced. It is included as an appendix in part 1 of the handbook.

Design of Text

Indented blue text are translated quotes of the regulations.

References are linked to electronic editions, and are indicated through the use of italics.

There are three types of listings in H SystSäk E, numbered, as bullets and as an option list as below.

1. The measures contained in the numbered list should be taken in the order specified.

- The measures in the bulleted list can be implemented in any order.

a. The options list specifies a number of relevant alternatives.

Text in yellow boxes are of special importance.

Numbered requirements are presented in blue boxes. Mandatory requirements are written in a dark blue box and the number is of bold type. Requirements that are optional are written in a light blue box and the number in normal type.

Thank You

With the development of this part of H SystSäk E, some ideas, structures, images and text passages have been taken from An Introduction to System Safety Management and Assurance *[3]*, developed by the UK Ministry of Defence. Through a separate written decision, the MOD has kindly made this available to the Swedish Armed Forces.

For this we would like to thank the UK Ministry of Defence.

Improvement Suggestions

Proposals to improve the H SystSäk E should be sent to: The Armed Forces Headquarters, Safety Inspectorate, 107 85 Stockholm, Sweden.

1 The Focus of the Handbook

1.1 Background

In connection with the overall risk investigation which was commissioned by the government and conducted by the Headquarters of the Swedish Armed Forces (HKV) 1994/95, the Supreme Commander assumed a position on the Armed Forces' (FM) requirements regarding system safety activities.

The Handbook on System Safety (H SystSäk E 2011) is a development of an earlier edition (H SystSäkE 1996) and includes the Armed Forces' guidelines for the implementation of system safety activities relating to the Armed Forces' technical systems.

The Armed Forces will, in accordance with its working programme (FM ArbO), carry out activities aimed at reducing the risks associated with the use of technical systems so that they do not cause injury to people or damage to property or the external environment.

Weapons and weaponry systems are important prerequisites for Armed Forces' activities. New materiel is procured in order to produce a better effect. At the same time, the equipment used is often more complex, which may lead to new accident risks occurring.

Low accident rates (and the risks associated with them) are achieved through design and other active measures. Design measures are carried out mainly during the early development of technical systems. During the maintenance phase, the follow-up and management of both residual and emerging risks are ensured.

1.2 Purpose

Swedish laws and regulations govern the safety features which different types of implements, supplies, work premises, equipment etc., must have in order to be marketed and used. A number of these laws/regulations provide exemptions for military equipment and military use. However, these laws are continuously changing.

Notwithstanding these exceptions, the Work Environment (AML) *[5]* describes, among other things, the employer's responsibility to ensure that: “The employer shall take all necessary measures to prevent the worker from exposure to ill health or accident.”.

The instruction about the Armed Forces’ System Safety handbook *[26]* indicates that the handbook describes procedures and provides guidelines to the Armed Forces for the implementation of system safety activities during the procurement, modification, overhaul and decommissioning of technical systems.

H SystSäk E was created by the Armed Forces in order to cover the gap arising due to the exception described above. H SystSäk E therefore represents the Armed Forces' methodology to ensure the development of safe materiel/safe technical systems for the Armed Forces which will remain safe for all the activities in which the Armed Forces may handle equipment/technical systems, such as in its use during training, storage, transportation, maintenance and when being decommissioned.

H SystSäkE:

- Describes the responsibilities and role play to deal with risks during the procurement and use of military equipment/technical systems.
- Describes the Armed Forces' system safety methodology to be used to ensure that risks in the Armed Forces' materiel/technical systems *are and will remain so low that they meet the standards of a tolerable level of risk* throughout their service life.
- Constitutes the basic documents for the development of safety-related design rules for a specific technology area at DesignA (*section 3.8*).

1.3 Application

The Armed Forces regulates the scope of system safety activities conducted at FMV, FORTV, FOI and FRA. This is generalized in the coordination agreement with each organization.

Activities at FömedC and FMLOG are regulated by the HKV.

The Armed Forces regulates system safety activities via procurement and ordering via PPP partners and DesignA.

An instruction about the Armed Forces' System Safety handbook 2011 *[26]* specifies that for all procurement, modification, renovation and decommissioning of materiel (from 1 January 2011) a decision must be taken as to whether, and to what extent, the system safety activities should be conducted in accordance with H SystSäkE.

H SystSäkE is designed to be used at all times/phases when system safety features for technical systems are affected, which mainly occurs when studying, determining requirements, during development, manufacturing, procurement, testing, inspection, maintenance and during decommissioning. This handbook describes and provides specific instructions for the Armed Forces and DesignA's management of system safety activities.

The handbook can be applied to technical systems or technical subsystems at any level, i.e. also a specific technical device.

The Armed Forces' system safety requirements for a certain technical system are listed in Tactical-Technical-Financial Objectives (TTEM) and each customer order (KB) to DesignA. This is detailed in *section 6.5*.

DesignA's requirements for system safety activities in the Request for proposal (RFP) are based on the requirements of TTEM and in *chapter 7*. In the selection and adaptation (tailoring) of the activities from part 2 that are intended to be carried out by the supplier, *H SystSäk E Part 2, chapter 3* applies.

Facilities are not included in the definition of the technical system, but make up the environment in which the technical system is installed and operated. A facility can also provide protection in addition to certain basic technical resources, such as electricity, power, heating, cooling, ventilation, water and sewage. The development of this type of resource is managed through an order from the Armed Forces to FORTV.

1.4 Requirements

1.4.1 Meaning

The Armed Forces, as the client, is also the standards authority. The handbook's requirements are divided into mandatory and optional requirements. The concepts of mandatory/optional selection form an instruction for the client when determining requirements in KB/TTEM. The same applies when DesignA stipulates requirements in the RFP.

The mandatory requirements are essential for system safety. To comply with laws, regulations and ordinances with an emphasis on system safety activities, all mandatory requirements must be met. However, conditions can arise which mean that certain mandatory requirements are not applicable to a certain order.

The selection of requirements to be implemented for a technical system must be adapted by the client based on the complexity of the system.

1.4.2 Numbering

H SystSäk E requirements are numbered according to the following principle.

The starting number for a specific requirement specifies where the requirement is derived from, for example, 2 indicates that the requirement is from H SystSäk E Part 1.

The digits that follow indicate the chapter and section, for example, 632 indicates that the requirement is from chapter 6, section 3.2. Finally, there is a serial number that corresponds to each section. For example, the numbers 2.632.01 relate to the first requirement in chapter 6, section 3.2 of H SystSäk E Part 1.

The initial numbers are distributed to the existing handbook's design regulations (for information concerning the hierarchy and the relationship between these documents, see *section 2.4*)

0	H SystSäk E 2011 Part 2
1	H VAS-E (FMV's Weapons and Ammunition Safety Manual) *[11]*
2	H SystSäk E 2011 Part 1
3	H FordonSäk (FMV's Handbook on Vehicle Safety) *[10]*
6	H ProgSäkE (FM's Handbook for Software in Safety-Critical Applications) *[20]*

1.5 Adaptation

H SystSäkE part 1 is primarily intended to inform readers about the facts, provide context and in-depth explanations (mostly regarding accident risk) and directly provide support to certain designated roles. The support consists of a description of the appropriate system safety activity to implement and an account of a number of formulated requirements, some of which are considered mandatory (marked with the code requirements in bold and with a dark-blue background) and others which are optional.

H SystSäkE part 2 contains a detailed description of all the activities that constitute the system safety activity's "tools". Part 2 also contains a number of requirements, divided into mandatory and optional, and these are numbered in the same manner as described above.

> H SystSäk E should not be construed as a requirements document that will be applied literally, but as a handbook describing the methods, activities, documents etc., to be used in the individual procurement and must always be adapted to the current system's technical nature, complexity and estimated risk content.

If there is a conflict with the regulations governing, for example, land, sea and air safety when applying the system safety methodology in accordance with this handbook, the regulations take precedence and *the relationship should be notified immediately in writing to the Armed Forces HQ SÄKINSP*.

2 Basics

2.1 Safety

The Armed Forces works with both short- and long-term risks. In order to create an understanding of the basics and context, a brief overview is provided below of the relationship between safety and risk. The text in *section 2.1–2.3* is taken from An Introduction to System Safety Management and Assurance *[3]*.

Man's instinct for self-preservation naturally leads to a constant effort to try to avoid injury and loss irrespective of cause - flooding, airplane crash, exposure to environmental toxins, accidents at work, financial loss in business, theft, fire, delay and more. Nevertheless, complete safety is rare since almost all activities involve risks. Tolerating certain risks, however, is a prerequisite to be able to obtain financial advantage or other benefits, excitement or otherwise. An evaluation of a perceived benefit and a tolerated risk is the form of risk control that is part of human life and can be referred to as the instinct of self-preservation.

The term risk is used in many contexts, and generally relates to a certain *outcome/consequence* (unwanted option/result) and the *likelihood* that there will be a consequence. There are a variety of risk concepts, and the most common are:

- **Business risk**, such as a financial risk - that cash flow may be inadequate or the risk of being sued for an infringement of the law.
- **Insurance risk**, such as risk of theft, property damage or unexpected medical bills on holiday.
- **Investment risk**, such as the risk of losing capital by investing in shares which then have a fall in value below the level of investment.

- **Project risk**, such as the risk of delay, the risk of exceeding the budget or a technical risk of not achieving the required objective. Even the risk of an accident occurring (see below) that may prove impossible or very costly to manage is a project risk.
- **Accident risk**, which relates to the risk of injury/damage to an individual, property and/or the external environment.

An accident risk can often lead to other types of risk; an accident can affect insurance and business risk.

The word risk can be used in so many different contexts that it is a good idea to use the words accident risk if misunderstandings are likely.

> In this handbook, the term safety relates to the absence of accident risk that can lead to accidental injury/damage

Safety has become increasingly important as it is now considered possible to avoid a disaster and a disaster is now no longer seen as a random event. Society's reluctance to accept accidents along with the realization that all human beings have an equal value has, among other things, led to the introduction of the Work Environment Act (Arbetsmiljölagen – AML). Its purpose is to promote a healthy work environment for all employees.

Knowledge of what causes injury is growing continuously. Several substances and working methods previously considered safe are now considered harmful. Examples include asbestos, a noisy environment and CFCs (chloroflourocarbons). Where a substance or work method provides a profit/benefit at the same time as it causes harm, it is necessary to have some objective way of balancing out the two. An example is the use of a particular drug to treat a very serious illness, where the drug used to cure the illness may, at the same time, also give rise to more or less serious side effects.

Safety is an area that is rather subjective and the understanding of this word may vary from one individual to the next. Many people would prefer that all risks that may affect them personally are eliminated. However, not all risks can be removed because a benefit may be removed at the same time, which may prove costly. The resources that are available must then be prioritized to those areas where they provide the greatest benefit.

A balanced approach must be applied, where safety is neither neglected nor allowed to dominate, so that the implementation of efficient operations is made possible in a sufficiently safe manner.

2.2 The Need for Activities to be Designed to Continuously Develop Safety

Modern systems are complex and often incorporate many dangers; this explains why accidents can be difficult to predict. Some accidents can have catastrophic consequences. Technological advancement creates a need for the replacement of proven technology with new technology, which means that structures and methods that used to have a high level of safety are no longer regarded as being safe.

Many accident investigations show that the same general weaknesses often recur. Examples include:

- Known issues that have previously led to minor incidents but that have never been fully investigated and have therefore not been addressed. (See the bow ramps that lifted on several of the Swedish Armed Forces' combat boats before Combat boat 848 sank in 2006.)
- The estimated probability for a certain accident has been underestimated, as no one could have imagined the circumstances that led to the accident actually happening. (See the Estonia disaster 1994.)
- People believe that someone else is responsible for dealing with safety.

- Existing safety routines are "watered down" or are not being applied and simplified routines are gradually being introduced over time (if no accident occurs) because they make operations easier and cheaper. (See the incident at the nuclear power station Forsmark, in 2006, which even prompted an inspection by the IAEA, and the disaster in 1967 on the aircraft carrier Forrestal, where approximately 140 people died as a direct result of procedures being simplified.)
- Equipment changes or equipment being used in ways it was not designed to be used. (See the fire disaster in Kaprun, 2000, in which a modified mountain train caught fire inside a tunnel and cost 170 people their lives. The modification consisted of an electric interior heater that was fitted under a newly fitted hydraulic pipe, which began to leak.)
- Incidents are not always reported. The reason may be, for example, that the person affected by the incident is afraid to report the incident because he/she has made a mistake and does not want to be punished or that the reporting system is too complicated.

Dealing with deviations must be carried out in a proactive manner by the appropriate people (*foreseeing problems*). The aim should be to prevent accidents instead of reacting only when an accident or incident has occurred or, worse still, looking for scapegoats.

Accidents are often indications of failures by management. A clear example of such a failure can be found in the official investigation report of the capsized vessel Herald of Free Enterprise, in which approximately 190 people died. The report included the following observations:

- The shipping company did not assume responsibility for safety on its ships. This was considered the basic and primary reason for the accident.
- All those involved with management responsibilities, from the board down to senior staff on board the ship, were partly to blame for the accident because they had not assumed their responsibilities for the allocated assignment.

Until very recently, blame for an accident was usually attributed to those people who were directly involved. Nowadays, it is stated that safety concerns everyone. Naturally, individual employees are accountable for their actions, but it is mainly the commanding officers who have the authority and the resources to ensure that any shortcomings with regard to materiel, attitudes and the organization, are dealt with – factors that often cause accidents.

Safety management is an applied form of quality control and is defined as all actions intended to influence the safety of an establishment and which encompass the following:

- safety policy (setting targets for safety, for example, specifying what should be protected and what must not happen)
- safety requirements
- safety organization, the authorities/rights various individuals have, and their work assignments
- engineering design
- configuration management and document management
- risk management (including the identification and assessment of risk and risk reduction)
- appropriate measures to determine what type of training is required
- the requisite measures to tighten up on safety during use (operators)
- the requisite measures to tighten up on safety in connection with maintenance (technical staff)
- the requisite measures needed to tighten up on safety in connection with practical measures when implementing the decommissioning phase (technical and supply personnel).

The Armed Forces' safety management system relates to safety activities and is presented in *section 2.7*.

2.3 How Safe is Safe?

Is this technical system safe? It is an easy question to ask, but difficult to answer simply and clearly. One way to begin is to study the statistics from a number of everyday activities. *Table 2:1* below, provides examples of the probability of death related to different activities.

Table 2:1 Average Probability of Death for a Number of Different Activities

Probability of death per exposed person and year (approx.)	Activity
1 in 100	Five hours of rock climbing alone every weekend
1 in 200	Smoking 20 cigarettes per day
1 in 5 000	Working in a risk-intensive industry
1 in 50 000	The use of oral contraceptives
1 in 100 000	Working in the safest area of industry
1 in 500 000	Being a passenger on a scheduled aircraft
1 in 1 million	Being at home, being killed by electrocution
1 in 10 millions	Being outdoors, being killed by lightning

These figures are taken from "The Tolerability of Risk from Nuclear Power Stations", HMSO 1992 *[47]* and Reliability, Maintainability and Risk, David J Smith and Butterworth Heinemann, paperback 2005 *[37]*. They can be used for comparison when assessing accident risks in own operations.

Numerical values are calculated in safety analysis and should be regarded with caution, since most data is based solely on models. An accident investigation is of course also an attempt to assess how the accident happened. Facts related to an accident are limited to an accident having happened and having led to a specific injury outcome.

All accidents are unwanted and costly. Military accidents are special insomuch as the accidents caused by equipment deficiencies can have demoralizing effects on military personnel, especially in combat. System safety creates confidence in the equipment, which is one of the prerequisites of a good fighting spirit.

It is therefore necessary to invest actively in order to prevent accidents from happening or that try to minimize any serious consequences. However, the resources that are available within each individual project are limited. It is therefore important that we have good tools to identify WHERE efforts should be made and HOW LONG you need to have risk-reducing activities in place.

2.4 Legislation

Laws and regulations help to ensure that the systems that are in place prevent injury/damage to people, property or the external environment. The following section describes some of the most important laws. This section also includes some instructions as to how system safety methodology should be applied when particular legal aspects (laws, regulations etc.) apply at the same time. A technical system can consist of several subsystems. The challenge is to identify the rules that apply to their respective technical areas. It must be ensured that integration between the various subsystems is completely analysed in terms of risk. Examples of considerations and the application of standards are submitted at the end of *section 2.5*.

The specified document names etc., are the ones that were current when the handbook was compiled. In the event that a certain reference needs to be applied, it is recommended that you check to see if a later version has been produced.

2.4.1 The Work Environment Act

The objective underlying the Work Environment Act (AML) *[5]* is to prevent ill health and accidents at work, and to otherwise achieve a healthy work environment. AML regulates both the employer and the employee's obligations. Employees in the Armed Forces include all personnel, i.e. employees of the Armed Forces and the Home Guard personnel and staff from the voluntary defence organizations where staff participate in activities within the Armed Forces.

AML is a framework that is supplemented by regulations that are issued with the support of AML. AML assumes that the employer is responsible for ensuring that staff safety is satisfactory. The supervisory authority for AML is the Swedish Working Environment Authority (AV), with the exception of the working environment on board a warship, where the Swedish Transport Agency (Transportstyrelsen) is the supervisory authority.

According to AML the work environment must be working satisfactorily with due regard to the nature of the work and the social and technological developments in society. The working conditions should be adapted to man's differing physical and mental aptitudes.

In situations when a heightened alert is justified, the government may issue separate regulations.

The employer's responsibilities are specified in AML chapter 3, sections 2 and 2a:

> "The employer shall take all the precautions necessary to prevent the employee from being exposed to health hazards or accident risks.
>
> …

> The employer shall systematically plan, direct and control activities in a manner which leads to the working environment meeting the prescribed requirements for a good working environment. They shall investigate work injuries, continuously investigate the hazards of the activity shall take the measures necessary."
>
> ..."

The employer's responsibility is also clear from section 8 of the AV regulations on systematic working environment work *[2]*:

> "...
>
> "When changes to the activity are being planned, the employer shall assess whether the changes entail risks of ill-health or accidents which may need to be remedied."

It is important to identify risks before they are "built into the system".

General requirements for the nature of the work environment are described in AML chapter 2, section 1:

> "...
>
> Technology, work organisation and job content shall be designed in such a way that the employee is not subjected to physical or mental strains which can lead to ill-health or accidents. Forms of remuneration and the distribution of working hours shall also be taken into account in this connection. Closely controlled or restricted work shall be avoided or limited.
>
> ..."

AML chapter 2, section 5:

> "Machinery, implements and other technical devices shall be designed, positioned and used in such a way as to afford adequate safeguards against ill-health and accidents."

DesignA and the supplier's responsibilities are clear, as described in AML chapter 3, sections 1, 8–10:

Section 1

> "The stipulations of this Chapter shall be applied with due regard for the demands made in Chap. 2 concerning the nature of the working environment."

Section 8

> "Any person manufacturing, importing, delivering or providing a machine, implement, protective equipment or other technical device shall ensure that the device affords adequate security against ill-health and accidents when it is placed on the market, delivered to be used or displayed for sale.
>
> ...
>
> Directions for the device's assembly, installation, usage and operation as well as other information about the apparatus which is of significance to prevent ill-health and accidents (product information) shall be enclosed upon delivery through clear marking, in form of documentation or in other manner. Information of particular significance for the work environment shall be submitted in the event of marketing of the devices."

Section 9

> "Any person manufacturing, importing or delivering a substance capable of causing ill-health or accidents shall take the measures necessary in order to prevent or counteract any safety hazards entailed by the substance when used as intended.
>
> The stipulations of Section 8 (3), concerning product information and information in connection with marketing shall also apply with regard to substances capable of causing ill-health or accidents."

Section 10

> "Any person delivering or making available a packaged product shall ensure that the packaging does not entail any risk of ill-health or accidents."

Regulations According to AML

AML is a skeleton law that gives government the right to assign a specific authority, in this case the Work Environment Authority (Arbetsmiljöverket – AV), to provide supplementary regulations to the Act if necessary, something which is carried out on a continuous basis.

Regulations Regarding Machinery

AV's regulations regarding machinery (AFS 2008:3, which is based on the EU Directive 2006/42 on machinery) **exempts** "machinery that is specially designed and constructed for *military* or *police* purposes".

Machinery for military purposes is defined here as the technical system intended to carry out organized, armed combat.

AV's special provision for machinery (AFS 2008:3) specifies a long list of safety requirements to be used for various applications. The principle is that, for a particular mentioned application with generally known risks, these risks can be reduced by employing the prescribed safety requirements.

The background to this exemption for military equipment is that military operations require advanced materiel, often based on new technology and specific applications, which should not be communicated to potential adversaries. The technology and applications are treated confidentially, therefore preventing the development of harmonized safety standards that are required when producing "civilian" equipment.

AV's specific provision for machinery therefore does **not** apply to military equipment.

The Need for Special Rules and Regulations for Military Equipment

To ensure access to a work methodology that can manage risk when producing and using military equipment, the Supreme Commander of the Swedish Armed Forces permits the establishment of a system safety methodology, the details of which are regulated in this handbook on System Safety.

> The system safety methodology is designed to identify and manage risks.

AV Regulations with Limit Values etc.

AV has issued a number of regulations with detailed requirements and rules. The majority of these are general and always apply (with some exceptions, as described below). Regulations should be well known and carefully applied by those who receive assignments for the production of materiel for the Armed Forces. In some of the AFS (the AV's instructions on Systematic Environment Work) issued by AV, there are specified limit values that relate, for example, to air pollution (exposure limits), noise and vibration. These limit values must be given special consideration.

This means that, in addition to the application of system safety methodology for specified military technical systems, there may also be requirements that must be applied in accordance with specific regulations from AV. These requirements relate to the technical system in question or should be incorporated into this technical application, i.e. that special certificates or equivalent must be produced which certify that these requirements have been met.

Military Exemptions from Limit Values etc., in AV Regulations

Some of AV's regulations include specially expressed exceptions for military use. Examples of these provisions include the AFS that relates to the design of a workplace, the EU Directive 1999/5 (Radio Equipment and Telecommunications Terminal Equipment) and the AFS that deals with the use of machinery. Through the exemption for military use, the legislator intends to give the Armed Forces the necessary flexibility to devise a technical system

as “war demands”, but with the continued withholding of the basic requirement imposed on the employer in AML, see above. In order to use the intended freedom of action in a responsible manner, the Armed Forces is required to produce its own application instructions with guidelines, limit values etc., which the Armed Forces defines as tolerable for Swedish military personnel.

Certain civil law related to occupational health explicitly describes exceptions for military materiel and military use (see 1.2). If a law such as this specifies requirements on limit values, the Armed Forces needs to provide a detailed specification of the requirements that must be applied for a similar purpose in the Armed Forces. This is necessary in order to satisfy the protection of military personnel that will be using the technical system (this relates, for example, to an AFS that governs the design of a workplace).

Since laws are continuously changing, it is a great deal of work to continuously identify laws where the military is exempt. The identification of laws with a military exemption are suitably dealt with by giving each supplier the responsibility of identifying such laws. The assignment is formulated as a requirement in the invitation to tender so that, during the bidding period, the supplier will notify DesignA of such laws and seek instruction as to which requirements should be applied to the Armed Forces' technical systems that relate to the matter in question. DesignA will get back to the Armed Forces with the request for additional instructions that relate to the matter in question.

2.4.2 Product Liability Act and System Safety

The Product Liability Act (PAL - Produktansvarslagen) regulates the conditions for compensation for injury/damage that a product has caused an individual or private property, PAL is therefore a law for consumer protection. Section 1 specifies:

> "Damages in accordance with this law shall be paid for personnel injury which a product causes due to deficient safety. Damages in accordance with this law shall also be paid for damage which a product, due to insufficient safety, causes to property, which is usually intended for specific purposes, provided the product at the time of the damage was used mainly for the purposes intended. No reimbursement is paid, however, for any damage to the product itself."

Moreover, a legal definition of the concept of safety deficiency is provided in section 3:

> "A product is deficient in terms of safety if the product is not as safe as can reasonably be expected. Safety shall be judged with regard to how the product can be expected to be used and how it has been marketed and with consideration to work operation instructions, the time when the product is put into circulation and other circumstances."

This description of the Product Liability Act is provided first to give general information and second to show that there are no connections to H SystSäk E.

A product used by a person when at work which is covered primarily by AML – chapter 3, section 2 and other paragraphs. The employer is also responsible for ensuring that the working environment is appropriate and safe.

2.4.3 The Environmental Code and System Safety

The Environmental Code intends to promote sustainable development so that present and future generations can enjoy a healthy and satisfactory environment. The Environmental Code applies to all activities that have, or that may have, an impact on the environment. The operator responsible for an activity is obliged to have some knowledge of the environmental impact caused by an activity. The operator is obliged to carry out protective measures, observe the limitations and take the necessary precautions to prevent or compensate for the activity that causes damage or inconvenience to another person's health or the environment. The best available technology should be used and products should be selected that have the least environmental impact. Operators of an activity should use raw materials and energy sparingly and look for opportunities to reuse and recycle. Detailed rules and regulations are available in subsequent legislation to the Environmental Code.

These safeguards, precautions and so on must be taken whenever there is reason to believe that an activity or action may result in harm or inconvenience.

The central regulator for the Environmental Code is the Environmental Protection Agency (Naturvårdsverket) and, at a regional level, the county councils also share this responsibility. The Surgeon General within the Swedish Ministry of Defence Department exercises supervisory rights over the Environmental Code for the Armed Forces, the FMV, FortV and FRA.

There are a number of other laws, rules and regulations in addition to the Environmental Code that impose specific requirements on the protection of the external environment.

The Environmental Code and other laws apply to all technical systems developed for the Armed Forces.

The application of H SystSäk E is designed to identify accident risks that a technical system may cause and where the consequences may also involve damage to the external environment.

2.4.4 The Electricity Act and System Safety

General

Good electrical safety is a prerequisite for the operational safety of the Armed Forces.

Technical systems and products must be designed for their intended purpose and the requirements imposed by climate and environments.

Technical systems that make use of an electric current greater than 50 volts must ensure electrical safety during development and procurement by taking into consideration the requirements of electrical safety and electrical design.

Following accession to the European Union (EU), Sweden's electricity legislation has changed significantly, from previously having a regulatory bearing to one of performance management. The overall objective is for systems and products to be safe. Increasing demands on the electrical performance of systems and equipment in terms of safety, especially for system safety work, must also be taken into consideration.

DesignA is responsible for ensuring that technical systems and products are safe and comply with the appropriate legislation and standards, or are carried out in another manner, as documented by DesignA.

The Electricity Act

The Electricity Act *[8]* deals with electrical safety and specifies in chapter 9, section 1:

> "Power installations, electrical equipment intended to be connected to such installations, electrical material and electrical facilities shall be of such a nature and placed and also used in such a way that sufficient safety is provided against personal injury or property damage or disruption of operations within their own installation or at other power installations."

The Electricity Act's requirements are clarified in regulations that also provide the Swedish Electrical Safety Board with the opportunity of issuing regulations. The regulations primarily affecting the design of technical systems containing electrical equipment include:

The Electrical Materiel Ordinance	SFS 1993:1068
High-voltage Current Ordinance	SFS 2009:22
The Electrical Contractor's Ordinance	SFS 1990:806
The Electromagnetic Compatibility Ordinance	SFS 1993:1067

Laws and ordinances in the electricity sector have a general structure and wording, with electrical safety as the objective. Authorities and organizations for standardization develop regulations and standards for application in the electricity sector – these are based on current laws and regulations.

Regulations

The Electrical Safety Board is the supervisory authority for electrical safety.

The Electricity Act states that electrical installations, electrical systems and their equivalent must be safe. What may be deemed to be safe in various situations and configurations are reported in the electrical safety field's regulations and standards, or by DesignA as specially documented and established guidelines, issued as technical orders (TO), or other forms of technical publication.

DesignA indicates to suppliers in the invitation to tender what the specific requirements are that the technical system must fulfil with regard to electrical safety, and this is done by reference to the standards that apply. This can also be done by reference to DesignA's specifically defined instruction or a combination thereof.

Technical systems and products for use by the Armed Forces may in some cases require designs that are not described in the standard, which always demands that DesignA describes and documents the design so that it can meet the requirement of being safe.

Electrical Safety Handbook

Electrical safety forms a natural part of operational safety in the Armed Forces. The Electrical Safety Handbook in the Armed Forces *[30]*, H Elsäk, is intended to support units, centres and schools in their efforts to implement and carry out systematic electrical safety work, prevent accidents and create a coordinated approach within the area of electrical safety in the Armed Forces.

System Safety

In addition to the above design requirements, system safety activities will be carried out in accordance with H SystSäk E methodology for the entire technical system – this includes a risk analysis conducted for the system, its interfaces and its use for its intended purpose.

This means that the technical system for which the Electricity Act is applicable, risk-reducing measures according to H SystSäk E must be taken as safety measures in accordance with specified design requirements.

2.4.5 The Ship Safety Act, RMS and System Safety

The ordinance on the safety of warships specifies which parts of the Ship Safety Act applies to warships. The Swedish Transport Agency issues regulations for the seaworthiness of warships and the Armed Forces has been instructed in consultation with the Swedish Transport Agency to draft rules for the control of the seaworthiness of vessels and how a vessel's seaworthiness should be checked. The Supreme Commander of the Armed Forces has given C SÄKINSP the authority to establish such rules and to exercise the supervision of warships. The set of rules and regulations is called Rules for Naval Operations (RMS).

RMS applies to military maritime operations, naval vessels and diving systems.

All vessels and boats belonging to the Armed Forces or those under military command are warships.

For every warship that is to be constructed, purchased, leased, rebuilt, assigned a new area of operation or new particulars, a start-up meeting with the Military Maritime Safety Inspectorate is required. At this start-up meeting the requirements that must be met are decided (see, among other things, RMS-F *[36]*).

So that warships can be used during peacetime, they must be seaworthy and equipped with a Seaworthiness Certificate and its equivalent for diving equipment. A Seaworthiness Certificate or equivalent will provide proof that current regulations are met.

A Seaworthiness Certificate does not normally apply to the command and control systems (C^2), weapon systems and interfaces to other systems that may imply other risks to the ship's system.

In addition to the Seaworthiness Certificate or equivalent, system safety activities will be carried out in accordance with H SystSäk E methodology for the entire system, whereby a risk analysis is carried out for the system, its interfaces and its use as a naval battle system.

This means that there should be risk-reducing measures taken in accordance with H SystSäk E and safety measures in accordance with RMS for warships and diving systems.

Military maritime safety aims to prevent the risk of accidents occurring that can cause death, ill health, damage to or loss of equipment, materiel and property or damage to property or to the external environment. Seaworthiness, like the working environment, manning, cargo/ballast and the external environmental are all aspects of ship safety. A vessel is said to be seaworthy when it, with regard to its purpose and the area in which it will be used, has been designed, built, equipped and maintained to provide adequate safety against maritime accidents.

In addition to the working environment, seaworthiness encompasses large areas relating to the technical requirements for the design and function of the vessel's structure and equipment, for example the hull, buoyancy, stability, steering, machinery, pipes and pumps, bilge and leak sealing devices, pressure vessels, lifting equipment, electrical installations, fire protection, life-saving

equipment, mooring, navigational and communication equipment and boat lashings. A ship or a boat is said to be seaworthy if requirements have been met.

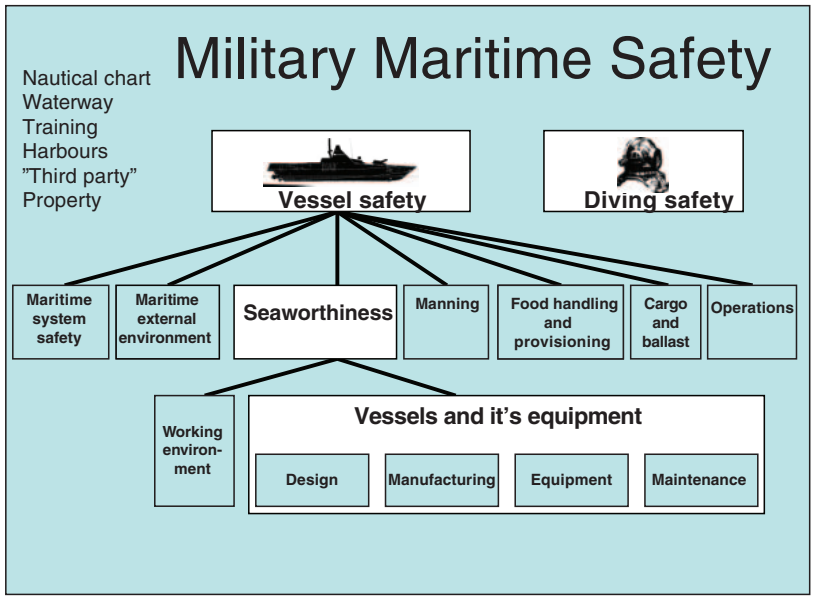


Figure 2:1 Military Maritime Safety

Regarding the seaworthiness of the Armed Forces' ships and boats, there is a regulation on the safety of warships, SFS 2003:440, which states that certain parts of the Maritime Safety Act, SFS 2003:364, also apply to warships.

Because of the special character and use of warships, the Swedish Transport Agency's constitutional manual cannot be directly applied to all areas. Consequently, naval implementation regulations have been prepared and compiled in the RMS.

2.4.6 RMM and System Safety

Rules for Military Ground Operations (RMM) *[35]* is the Armed Forces' governing document for the implementation of systematic ground safety work. Systematic ground safety work involves the design and review of the Armed Forces' operational management system and the design and review of specific requirement formulations for military units and materiel systems.

RMM is also the governing document for the design of the Armed Forces' ground safety handbook, military unit handbook and quota handbooks.

RMM will apply to all those operating within the Armed Forces or the Armed Forces' direction, nationally and internationally, where operations are not attributable to naval or military aviation.

Operational safety for the systems on the ground, or those managed from the ground, and that have a direct influence on naval safety or flight safety should refer to sea and air safety governed by the RMS and the Rules of Military Aviation (RML), and therefore do not appear in the RMM.

RMM consists of two parts, RMM Basics (G) and RMM Ground Safety Systems (M). The intention is to supplement RMM with additional parts, for instance RMM-T will contain the rules and requirements for technical system safety.

2.4.7 The Aviation Act, RML and System Safety

The Aviation Act

All activity that is considered to include aviation activities must be licensed under the Aviation Act. The government or the authority determined by the government specifies the terms and conditions governing the exercise of air operations in Sweden and for Swedish registered aircraft operating overseas.

For civil aviation and air traffic services for civil and military aviation the government has authorized the Swedish Transport Agency to adopt regulations and to act as a supervisory authority. Via the European Aviation Safety Agency (EASA), the EU has influence over civil aviation within the EU. This influence is exerted in particular through EU regulations and EU directives that are directly or indirectly applicable to civil aviation.

With regard to the military aviation system, the Armed Forces is the authority that issues regulations and has supervisory rights. This also applies to aeronautical services for military aircraft if this is to be exercised by an authorized operator within the military aviation system outside Sweden.

The Military Aviation System

The Supreme Commander is responsible for military aviation safety in the military aviation system.

Provisions for military aviation are described in the RML *[34]*. The manager of the Safety Inspectorate within the Armed Forces is authorized to determine the RML. The Armed Forces Flight Safety Inspector (FSI) is responsible for the exercise of all official authority and enforcement under the RML and is in charge of Military Aviation Safety (the Military Flight Safety Inspectorate (FLYGI)) at Headquarters.

The definition of military aviation is based on the Armed Forces' definition in the RML. The definition states that military aviation is all aviation within the military aviation system. It also includes all development, acquisition, deployment, maintenance and decommissioning of units and materiel systems. It is also relevant for ground, premises, facilities and equipment in the military aviation system.

The concept of military aviation is therefore all flights etc., carried out for military purposes and also the activities that qualify as aviation-related services. This also includes the Armed Forces' own activities, activities within the Armed Forces' FMV and some areas of the defence industry, such as Saab AB, and in some civil maintenance facilities and suppliers of aviation products both within and outside Sweden. Military aviation can therefore also be conducted by a company.

Certified Design Organization

When the Armed Forces acquires new aviation products or parts and devices to these or orders changes to aeronautical products, it is required by the current supplier (a design organization) that the supplier has been authorized by the FSI as a member of the military aviation system. Authorization for a design organization, issued by another authorized authority (such as the Swedish Transport Agency, FAA, CAA, DGA) can be accepted by the FSI.

To put it simply, there must be:

- An authorized design organization (according to RML-V-5J) that assumes responsibility for the materiel system level (level 2 according to the RML), which is normally the FMV (Försvarets materielverk).
- An authorized design organization (according to RML-V 5JA) responsible at product level (level 3 according to the RML), which is typical in the industry, but also, for so-called "legacy" Aircraft, this may be the FMV.

  Note that RML-V-5N governs the import procedure.

At system level 2, the design organization is responsible for ensuring that the complete flight materiel system, aircraft, rescue systems, weapon systems, personal equipment etc., are safe for intended use.

Approval of Product and Materiel Systems

In general, a decision to use a Decision Regarding Use (BOA) must be issued before materiel can be put into service by the Armed Forces. This BOA intends to ensure that equipment is safe, primarily from a working environment perspective, and that other conditions exist.

For aeronautical products, there are additional RML which make demands on materiel and organizations within the Swedish military aviation system. Before an aircraft is put into service in the Swedish military aviation system it must be certified by the FSI, that is to say that a Material Type Certificate (MTC) must have been issued. The air materiel system, wherein the Aircraft Certificate is included, must also be approved by the FSI, which is done

by issuing a Materiel System Certificate (MSI). MTCs and MSIs are examples of aviation records. The holder (design organization) undertakes the responsibility in accordance with the RML (to monitor the aeronautical product during its operation and, if necessary, to introduce requisite improvements) for the entire product's respective service.

When the FSI has issued an MSI and/or MTC no further consultation is required from the Safety Inspectorate prior to a Central Safety Compliance Decision (CSSB) or BOA.

The design organizations (approved by the FSI) apply for an MTC or MSI, and then a set of requirements are agreed and formalized, called a "certification base". After verification etc., the design organizations issue a type or materiel system declaration, which, among other things, states that the requirements have been met (or, if they have not been met, how compensation has been made so that the same level of safety has been achieved) and that the type or materiel system is safe for its intended use. It is necessary to implement the system safety work in order to be able to verify this. When the FSI, after the FLYGI's review, then issues an MTC or an MSI, these can be seen as the FSI's "acknowledgement" of the declaration.

The requirements that apply for the application and for the issuance of MTC and MSI are found in RML-V-5B.

The equivalent process is used for any major changes to the type or air materiel system declaration. For minor changes, see RML-V-5D.

The standard to be applied for system safety work is proposed by the design organization and is accepted by the examining authority (FLYGI). An example of the standard is MIL-STD-882C, but there are several standards used by the aviation industry. In the case of software systems included in the aircraft, the process standard RTCA/DO-178B *[38]* is often applied.

Other standards and methods of reporting, other than those specified in H SystSäk E, may, with the FSI's acceptance, be used for system safety work for aviation products.

The above description is general and applies as a principle for all materiel systems that impact on flight safety. However, there may be exceptions that are either induced by an older materiel system that is designed and put into use when other rules applied or that the materiel system is regarded as having a lower ranking in terms of its impact on flight safety and is therefore judged as not requiring an MSI and/or MTC. The design requirement in RML V-5 will, however, be applied to new purchases and major changes to air material systems, including Unmanned Aerial Vehicle (UAV) systems.

Approval by a Simple Product or Simple Materiel System

If a product or materiel system within the military aviation system is to be taken into use and it has been decided that an MSI and/or MTC is not required, the system safety work is normally carried out in accordance with H SystSäkE and a consultation is requested from the Safety Inspectorate prior to the CSSB and the BOA. Following a proposal from the design organization, the FSI can even accept other established standards and reporting procedures in these cases.

2.4.8 Vehicle Safety, Equipment and System Safety

The Vehicle Act

The Vehicle Act *[13]* contains regulations about:

- The inspection of vehicles and relevant systems, components and separate technical devices.
- The inspection of the vehicle's load.
- The inspection of the recording and metering devices and the control of and use of these.
- The activities are operated by inspection bodies in the automotive field.

The Vehicle Act does not apply to:

- Vehicles owned by the state that are manufactured for specific military purposes.
- Powered vehicles designed to be operated by pedestrians or a trailer which has been linked to any such vehicle.
- Vehicles used exclusively within a fenced railway or industrial areas or within fenced competition areas or other similar enclosed areas.
- Toy vehicles.

The Vehicle Ordinance *[12]* includes regulations regarding:

- A vehicle's qualities and equipment.
- The inspection of vehicles and relevant systems, components and separate technical devices.
- The activities operated by inspection bodies in the automotive field.

The Vehicle Ordinance does not apply to:

- Vehicles owned by the state and which are manufactured for specific military purposes.
- Powered vehicles designed to be operated by pedestrians or a trailer which has been linked to any such vehicle.
- Vehicles used exclusively within a fenced railway or industrial areas or within fenced competition areas or other similar enclosed areas.
- Vehicles designed as toys.
- On- and off-road traffic during military operations and military exercises etc.

The Military Traffic Ordinance *[31]* contains specific provisions on:

- The characteristics and equipment for vehicles used by the Armed Forces, the FMV and the Defence Radio Establishment.
- The inspection of vehicles for registration in the military vehicle register (MIFOR).
- The registration of vehicles in the MIFOR.
- The right to drive vehicles used by the Armed Forces, the FMV and the Defence Radio Establishment.
- The training of drivers in the Armed Forces.
- The appointment of personnel to perform certain functions in the traffic area.

The Military Traffic Ordinance, chapter 3, contains provisions on vehicle characteristics and equipment.

The Armed Forces may provide regulations regarding vehicles owned by the state and which are manufactured for specific military purposes. Such vehicles may be operated in traffic only if they are reliable from a traffic safety point of view and are otherwise suitable for traffic.

For vehicles manufactured for specific military purposes, the Armed Forces will provide instructions regarding the registration inspection of vehicles. Registration inspection and testing for an individual approval may be performed by an accredited inspection authority or by a military motor vehicle examiner.

If a vehicle is approved following a registration inspection or by individual approval, the information to be entered into the MIFOR will be submitted to the Armed Forces.

In the National Road Administration's code of statutes (VVFS 2003:22), vehicles registered in the MIFOR and operated by the Armed Forces, the FMV and the Defence Radio Establishment are exempted from having certain equipment on vehicles.

On behalf of the Armed Forces, the FMV prepares support documentation for regulations, general advice and guidelines on the roadworthiness of vehicles registered in the MIFOR or that belong to or are used by the Armed Forces, the FMV and the Defence Radio Establishment.

Such support documentation may relate to:

- a vehicle's characteristics and equipment
- a vehicle's registration
- the regular inspections of a vehicle.

A vehicle is roadworthy if it is designed, built, verified, equipped and maintained in such a manner, and has such characteristics, that safety and environmental requirements are met.

The Military Traffic Ordinance, chapter 2, provides the Armed Forces with access to certain exemptions from civil traffic laws.

System Safety for Vehicle Equipment

Roadworthiness encompasses a vehicle's characteristics in traffic. Vehicle systems can be complex and, apart from vehicles, include C^2-systems, weapon systems and interfaces to other systems, for example. The complex technical system's accident risks may therefore have diverse origins.

In addition to measures to meet the requirements for roadworthiness, system safety activities must be implemented in accordance with H SystSäk E methodology with regard to the overall technical system, including interfaces, for use as a ground combat system.

The FMV has compiled a design rulebook: The FMV Handbook on Vehicle Safety, H FordonSäk *[10]*.

H FordonSäk aims to manage risks in the vehicle system containing known technology. In order to manage risks in newer technologies and the risks resulting from integration, H SystSäk E is applied at the same time as H FordonSäk.

2.4.9 Bridging Materiel and System Safety

General

The technical system bridging materiel is designed to create a link across watercourses and other obstacles in the terrain. The system must be grouped before the intended capacity can be delivered. For bridging materiel the capacity for stability must be looked at carefully with regard to GROUPED/MULTIPLE systems, to prevent the technical system from sinking into the ground, which may result in equipment tipping or falling over. It is important to continuously monitor ground stability when a bridge is being built.

Bridging devices are divided into solid and floating bridge materiel. With the materiel, bridges and ferries can be erected.

Requirements for bridging systems are divided into two parts: design and operational reliability requirements, the latter requirements are not described in H SystSäk E.

Design Requirements

Legal requirements for the dimensioning and use of bridging material are defined in the Planning and Building Act *[33]* and Maritime Law *[41]*.

For a definition and verification of military bridging systems, the regulations relating to Trilateral Design and Test Code for Military Bridging and Gap-Crossing Equipment from 2005 are applied.

System Safety

In addition to the above design requirements, system safety activities must be carried out in accordance with H SystSäk E methodology for the entire technical system; this includes a risk analysis conducted for the system, its interfaces and its use as a bridge-creating technical system.

This means that the bridge-creating technical system must be subject to risk-reducing measures in accordance with H SystSäk E as well as safety measures in accordance with specified design requirements.

2.4.10 Medical Equipment and System Safety

General

Medical equipment relates to technical systems with the ability to provide medical care and medical transportation. Due to the specific requirements regarding patient safety, medical equipment systems are rather specific with regard to their character.

Pharmaceuticals are not covered by this section as this area of responsibility is dealt with by the Defence Medical Centre.

Design Requirements

The Medical Devices Act *[29]* and the Medical Devices Ordinance *[15]* provides regulations for medical devices. In addition, there are regulations concerning such products in other legislation.

A medical device is referred to in the law as a product, which according to the manufacturer will be used, separately or in combination with another device, in order to:

- detect, prevent, monitor, treat or alleviate a sickness or disease
- detect, monitor, treat, alleviate or compensate for injury or disability
- examine, modify or replace the anatomy or a physiological process
- control fertilization.

The Swedish Medical Products Agency (Läkemedelsverket – MPA) may prescribe that the law on medical devices will also apply to other products used in a medical device system or otherwise, in respect of use that is closely related to medical devices.

The MPA may also prescribe that the law on medical devices, completely or in part, will not apply with regard to certain medical devices.

System Safety

In addition to the above design requirements, system safety activities will be carried out in accordance with H SystSäk E methodology for medical device systems in order to identify the risk of accidents that can cause injury/damage to people (as patients), property or the external environment. In the event of conflicting requirements, patient safety takes priority over system safety.

2.4.11 Ammunition and System Safety

General

The Flammable and Explosive Goods Act (LBE) *[28]* applies to the handling and importation of flammable and explosive goods. The purpose of the law is to prevent such products causing unintentional fire or explosion and, in the handling of such products, to prevent and limit harm to life, health, the external environment or property by fire or explosion.

The Flammable and Explosive Goods Act (LBE) *[28]* specifies, in section 12, that:

> "In order for an explosive to be released onto the market it must have been judged to comply with what is acceptable under the regulations in force within the European Economic Area or, if there are no such regulations, have been approved by the authority determined by the Government."
>
> *Updated; deviates from the printed Swedish version.*

The Explosives Inspectorate's (SÄI)[1] regulations for the import and transfer of explosives (SÄIFS 1997:5) *[42]* highlight the European Council Directive 93/15/EEC on the harmonization of regulations concerning the release onto the market and the supervision of explosives for civil use (The Explosives Directive). The regulation says, in section 1.2, that:

- "Specific provisions apply for the approval of an explosive good that is imported and for assessment of conformity or approval of the explosive which is transferred.
- The approval referred to in section 10 of the Ordinance on Flammable and Explosive Goods is not required for the handling, import or transfer of ammunition under The Weapons Act (1996:67) if the ammunition has passed inspection in accordance with the Convention of 1 July 1969 on the mutual recognition of inspections stamps on hand-held weapons (CIP Convention) and has a CIP proof stamp."

Design and Review Requirements for Ammunition for Military Purposes ("Military Munitions")

The Ordinance on International Humanitarian Law for the Monitoring of Arms Projects *[16]* states that the review of projects from an international legal point of view should be made by the Delegation for International Humanitarian Law Monitoring of Arms Projects. The ordinance requires that the Armed Forces notifies the Delegation, as soon as possible, of any project relating to the study, development, purchase or modification of weapons or methods of warfare.

Over a long period of time the FMV, on behalf of the Armed Forces, has compiled and further developed a design rule book: Handbook on Arms and Ammunition Safety, H VAS-E *[11]*. H VAS-E covers ammunition intended for military purposes. H VAS-E reports on the requirements and safety characteristics of the functions used with military ammunition.

1. SÄI is now a part in the Agency for Civil Contingencies, MSB.

H VAS-E aims to deal with the risks associated with the use of ammunition that contains known technology. In order to manage risks in newer technologies and the risks resulting from integration, H SystSäkE is applied at the same time as H VAS-E. When procuring ammunition, this condition must be given particular consideration.

H VAS-E also includes specific requirements for military munitions that comply with international legal standards.

At the FMV there is a special organization for the independent review of military ammunition. This organization is managed by the Armed Forces. This organization can carry out reviews of military ammunition, also commissioned directly by the Armed Forces, or by another supplier/DesignA that carries out the assignment on behalf of the Armed Forces.

An independent review is generally applied when the technical system's accident risks are regarded as major/serious, see *section 5.12*.

2.5 System Safety Handbook

2.5.1 H SystSäk E

The purpose of the H SystSäk E has previously been described in *section 1.2*. The H SystSäk E covers:

- A description of the system safety methodology to be used to ensure that accident risks in the Armed Forces' technical systems are kept so low that they incorporate the established requirements throughout their service life.
- A report of activities describing system safety methodology (requirements, decisions, tools, methods and how they operate together) as a basis for an organization's formalization of responsibilities, organization, working methods, the development of own support processes and their adaptation to own phases - in order to facilitate the development of safe military technical systems.

- **A method of instructions** regarding the Armed Forces' system safety methodology to all those involved in Armed Forces' system safety activities; the Armed Forces as owner representative (ÄF), the Armed Forces as the client, the user, the Design manager (DesignA; collective designation at the FMV, FORTV, FOI, FRA, FömedC and PPP partner) and the supplier.

2.5.2 Definitions

To define system safety methodology using H SystSäk E, three basic definitions are used:

- **System safety** is defined as the property of a technical system that does not intentionally cause injury/damage to a person, property or the external environment. (Person: death, physical injury or illness. Property: damage to or loss of property or equipment. External environment: "superficial" damage - which can be entirely, or in part, reconstituted or permanent damage - such as the eradication of a species).
- **Technical system** is defined in the coordination agreement *[40]* in accordance with ISO/IEC 15 288 as: "An assembly of interacting elements organized to achieve one or more stated purposes."

  By system in H SystSäk E, it is always understood as the Technical system. (If another type of system is referred to, it must be stated clearly.)

  Ammunition is always a stand-alone technical system, at the same time as it often constitutes an integration product in one or several other technical systems.
- **System safety activities** can be described as the amount of work that is carried out on a particular technical system during its study, development, acquisition/procurement, renovation and modification, production, operation (including technical adaptation), maintenance and decommissioning in order to identify and quantify risks, eliminate them or reduce them in accordance with the requirements that have been established.

2.5.3 Application

H SystSäkE applies to all activities relating to the development, production, maintenance and decommissioning of technical systems. See Preface, Instruction on the Armed Forces' System Safety Handbook.

> The application of H SystSäk E does not remove the obligation to comply with applicable laws.

2.5.4 Comparison of Methods Used

The laws, the Armed Forces' rules and regulations (RMM, RML and RMS) and other established safety activities, as described above in *section 2.4*, are all of a regulatory nature. The regulations that have been developed are designed to prevent injury/damage and may either be dimensioned based on the outcome of the injury/damage or a worst possible outcome (based on consequence = *deterministic*). The regulations can, for example, specify rules for design, assign responsibility and outline requirements for both activities and system properties. The method aims to achieve an acceptable level of safety through compliance to the rules and regulations.

H SystSäk E is, on the other hand, mainly *probabilistic* (based on probability) *[27]*. This means that H SystSäk E is designed to identify and deal with accident risks inherent in the technical systems.

Accident risks in technical systems can generally arise as a result of new technologies being applied where previous experience is lacking or by using a known technology in new applications where previous experience is lacking. (In addition, accident risks may arise as a result of shortcomings in design or manufacturing, see *H SystSäk E Part 2, chapter 2*.)

A logical consequence is that the applied technology used at any time by DesignA will provide new knowledge of accident risks, their nature and the measures used to reduce them in the existing system.

DesignA should ensure that such experiences are “recycled”, see *section 3.8*.

2.5.5 Consideration of Rule Application when a Technical System Contains Several Subsystems

Below is an illustrative example of the considerations.

Example: Fuel-supply vehicles at a marine base.

Question: Through what sort of safety application is a refuelling vehicle safe, so it does not to cause accidental injury/damage to humans, property or the external environment during a refuelling procedure?

Alternative answers: Use RMS for the vessel, check the roadworthiness of the refuelling vehicle and follow the system safety methodology.

Correct answer: System safety methodology.

Considerations

Roadworthiness relates only to the vehicle's capacity to be operated safely in traffic.

RMS relates to military maritime operations, naval vessels and diving systems. A Seaworthiness Certificate is issued for technical systems that meet current regulations. A Seaworthiness Certificate does not normally apply to the C^2-systems, weapon systems and interfaces to other systems that may imply other risks to the technical system.

Another alternative could be the ADR rules and regulations *[1]*. This aims to ensure that hazardous goods that are transported with the fuel-supply vehicle should not cause injury/damage to humans, property or the external environment due to deficiencies in relation to the vehicle. However, it does not prevent the operator falling from the tank body while working on the top of the vehicle (during, for example, an inspection through a manhole or while performing camouflage work in the field). Such dangers are discovered only through system safety methodology.

2.6 Operational Safety and System Safety

2.6.1 Basics

People seeking employment in the Armed Forces realise that there are serious dangers in the work and that safety awareness is especially important.

The Supreme Commander, in his capacity as an employer, has a moral and legal responsibility to his employees. The Armed Forces is also responsible for other people who are exposed to possible shortcomings and deficiencies in the Armed Forces' operations.

The Armed Forces acts as a standards authority and is an end-user of all technical systems used in the Swedish Armed Forces, and therefore has an impact on the design, development, manufacture and maintenance of these technical systems. The safer the equipment that the Armed Forces acquires and uses, the easier it is for the Armed Forces to be able to fulfil its legal and moral responsibility.

In addition, the Armed Forces also has a significant responsibility to continuously ensure that it is generally competent to deal with all the risks that society entrusts it with.

In the business world, a company's good name and reputation is considered to be a major asset that can be protected with the support of system safety activities. A business that loses this is driven quickly out of the market. The Armed Forces' name and reputation should be regarded in a similar manner. The Armed Forces, in its new role on the international arena, is expected to be invited to participate in joint military assignments. A continuation of its good name and reputation to conduct armed combat is required for future missions. See also *section 3.2* what is written about military risk. System safety activities together with high-risk awareness can contribute to this.

The Armed Forces' task with regard to armed conflict must be resolved in compliance with applicable laws. The methodology for this has been formalized in an internal safety management system called the Armed Forces' safety activities and is defined as follows:

> Armed Forces' safety activities refer to the Armed Forces' ability to manage risk in all aspects of its operations so that the constitutional requirements in terms of the working environment and safety for Armed Forces' personnel and requirements with regard to safety for third parties, the external environment and property are met.

Operational safety within the Armed Forces is divided up into areas of activity that relate to: military territorial safety, military maritime safety and military aviation safety.

The Armed Forces' ultimate task is to be able to carry out effective armed combat and this makes special demands on good risk awareness during both training and exercises and when military forces are deployed.

The activities of the Armed Forces are becoming more technically advanced and complex. This fact, combined with increased international involvement and society's requirements for a general increase in safety, means that safety issues have also been revised and are much more diverse.

The level of operational safety that must be maintained is an effect of the operational safety work that is conducted within the Armed Forces and other relevant organizations working on behalf of the Armed Forces.

The word "safety" is used to mean both "safety" and "security". Operational safety in this comparison primarily encompasses the concept of "safety", but it is also clear that any weaknesses in the safety that corresponds to the concept of "security" can, by extension, lead to a reduction in operational safety. There is no sharp distinction between "safety" and "security", so there is no point in drawing a line within the framework of operational safety. An operator (such as an operations manager) needs to continuously make sure that safety is good enough in both these respects.

The basis for efficient and safe operation is the user's knowledge of operations and materiel, and the ability to apply this knowledge in practical situations. Realistic exercises increase this knowledge. An open attitude and a willingness of management to continuously improve safety by reporting deviations is regarded as a natural part of operations and is a cornerstone of all operational safety activities.

2.6.2 Scope

Operational safety work includes regulating, the implementation of activities under these rules, and monitoring, to ensure that regulations are followed.

Regulating means the supplementing of laws, regulations and other rules of law with directives and internal stipulations, where and as required.

Laws, ordinances and instructions are applicable to the Armed Forces' operations and personnel in the same way as for society in general. However, there are rules that call attention to the Armed Forces' activities and provide the Armed Forces with the opportunity to design rules for such activities.

The implementation of operations in accordance with particular rules and regulations means that operational safety work is integral to the carrying out of an assignment or operation. The Armed Forces may assign a manager with the task of being the key operator with accompanying responsibilities in terms of operational safety. This means that there is an obligation within the area of responsibility concerned to create an operational safety system that guarantees that established regulations are followed and therefore makes it possible to achieve the objective of safe operations.

The follow-up of an activity that has been carried out in accordance with established regulations takes place partly by monitoring that the operator complies with their obligation to report shortcomings and partly through inspection, monitoring and review.

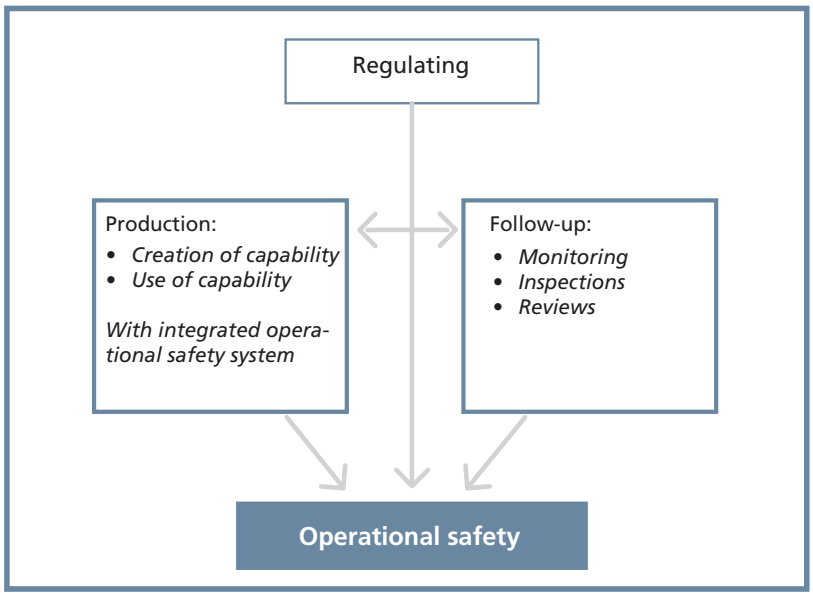


Figure 2:2 Operational Safety is Created through Production, Regulating and Monitoring

Regulating

The Armed Forces decides on regulations in the form of statutes promulgated in a Statutes Book (FFS) and the Armed Forces' internal stipulations (FIB). The FFS and FIB are decided by the Supreme Commander or authorized by him. The FFS is also used by the National Fortifications Administration (Fortifikationsverket), the Swedish Defence Research Agency (Totalförsvarets forskningsinstitut) and the FMV. In FIB, only the Armed Forces' internal stipulations are published.

Regulating is, and always will be, a continuous activity. New materiel and new types of activities make new demands and make old standards obsolete. Increasingly complex systems also make increasingly greater demands on personnel/units/materiel/systems so that all areas must work together to produce the required effect and provide acceptable levels of safety.

Regulating the activities within the area of operational safety takes the form of directives, issued as instructions and rules, such as the Armed Forces' Safety Instruction for Weapons and Ammunition etc. (SäkI), the RMM, the RMS and the RML.

Knowledge of the rules that apply is a necessary prerequisite for achieving good operational safety.

2.6.3 Follow up

In all operations, deviations from planned activities inevitably occur, from the established rules and from the expected behaviour of the equipment. The probability of deviations increases as the tensions and pressures brought about by a particular situation increase. The earlier a deviation is recognized and dealt with, the easier it is to fix and the lower the risk of serious consequences.

The Armed Forces must have a functional operational management system that incorporates systems that can recognize, document and analyse deviations and initiate corrective measures. This system should be well integrated in all activities within the Armed Forces and provide the basis for continuous improvement with regard to safety.

The operational management system is supplemented by independent inspections, audits etc. The results of these investigative activities are documented and integrated into the Armed Forces' improvement activities.

Observations from inspections and audits etc., should be used for the development of corrective action.

Follow-up work should be carried out as improvement operations provide the desired effect.

The Armed Forces' operational management system is based on self-inspection, which means a conflict between safety and production requirements.

Anyone who observes a deviation should report this, even if person reporting the deviation has caused it. The report is a good basis to discuss improvement proposals.

An open and confident attitude to all reported anomalies is a necessary prerequisite for the Armed Forces' safety activities.

2.6.4 Operational Safety from a Lifetime Perspective

Operational safety work starts when objectives have been formulated for a new unit or new technical system. Alternatively, it is initiated when new work assignments are formulated for an existing unit or an existing technical system. Even at this early stage, the system safety requirements are identified and requirements are specified regarding their level of risk. The requirements are established for the intended service life.

For operations in the future, when setting up a new unit or procuring new materiel or developing existing material, safety considerations must be included as an integral part of operations and must be continuously developed. The goal is that the new unit, with its new materiel, will be safe during the execution of all required activities, in all required environments and under all required conditions. The required activities always include training, exercise and combat during an operation.

2.6.5 The Armed Forces' System Safety activities

In the instruction concerning the Armed Forces' System Safety Hand-book 2011 *[26]* system safety is specified as a part of the Armed Forces' safety activities.

The Armed Forces is experienced in dealing with accident risks in both technical systems and in its activities. Historical data on accidents indicates that measures taken by the Armed Forces' operations have gradually led to lower accident rates. The system safety methodology allows the Armed Forces, when determining requirements for new systems, to transfer these experiences in order to continue to achieve a continuously reduced accident risk level.

The Armed Forces has adopted system safety activities that include methods to achieve and maintain the technical systems with a good level of safety. System safety methodology includes tools for governance as well as the implementation and monitoring of system safety activities during the Armed Forces' production of technical systems.

System safety methodology is a general conceptual model to describe how risks are identified (in new technologies and new applications of known technology). System safety activities will always form an integral part of a technical system's development, maintenance and decommissioning.

2.7 The Armed Forces' Joint Risk Management Model

The Armed Forces Joint Risk Management Model *[19]* deals with the risks that a commanding officer faces during an operation. These risks come from both hostile and non-hostile threats directed at a unit's assets worthy of protection (such as the health and life of personnel and operational capacity). The word used in this context is security. The risk management model aims to facilitate the commanding officer's decisions in the field on matters that relate to conscious risk taking and the use of protective measures in connection with the planning of combat action that has been planned or may occur.

This description of the Armed Forces' joint risk management model is provided partly as general information and partly to show that there are only peripheral associations to H SystSäk E which, of course, only deals with accident risks (not hostile threats, security) related to the technical system's characteristics.

3 Risk

3.1 Basics

Risk management is a general technique used in many different areas (see *section 2.1*). The text in this section is taken from An Introduction to System Safety Management and Assurance *[3]*.

The quest to identify all risks associated with the system is under development. In the international system safety world there is now widespread agreement that only approximately 50% of all hazards are found during development and manufacturing. It is therefore recognized that there is a high probability that residual risk will make itself apparent during the system's use. System safety methodology therefore needs to include tools for risk management with both a proactive and a reactive approach. Proactive risk management means the identification and management of risks in advance. Reactive risk management is carried out ("where warranted") when an accident or incident has occurred. The objective, in both cases, is to investigate and resolve the causes, identify what constitutes the basis of risk and to take appropriate measures to try to prevent an accident from occurring.

Risk and risk management are described using certain terms, even if they form a part of everyday language, they are used here with a specific meaning. Examples of such terms include: danger, hazard, hazardous condition, risk, incident and accident. The purpose of this chapter is to familiarise the reader with the basic terminology behind the methodology.

The functional safety of the system relates to access to the capability/function, or access to the service that the system will provide. The ability to perform the intended function as often as necessary is called **reliability** and will not be discussed further here. It must be noted that the reliability of certain military situations can be a vital prerequisite. For example, English commanding officers with combat experience from the two Gulf Wars claim that when the unit has fired the first shot, it has revealed its presence and its position.

Reliability of the effect in terms of hitting the target, achieved by weapons and ammunition, is therefore of extreme importance (that is, direct safety-critical).

Accident risk relates to the risk of injury/damage to an individual, property and/or the external environment.

Accident risk can often lead to other types of risk – an accident can affect insurance and business risk.

The word risk can be used in many different contexts, so it is a good idea to use the word "accident risk" to avoid confusion.

The concept of risk is based on the assumption that complete safety is not achievable. Risk management means, among other things, the comparison of different safety shortcomings, measured by how serious they are and by prioritising the risks that are deemed necessary to reduce. Risk management can be performed for all types of risks.

Even if it makes no difference to the individual victim of an accident, if a person is involved in an accident alone or together with 100 others, it is essential that, when conducting a risk analysis, the number of people exposed to a certain accident risk are identified.

This focus has led to the following two concepts:

- **Individual risk** is defined as the frequency at which an individual is likely to be exposed to a given level of injury caused by specified hazards. It is usually based on an average person in the group.
- **Societal risk** is defined as the relationship between frequency and the number of people affected by a specified level of injury in a given population exposed to specified risk. It expresses how many people may be involved in an accident.

3.2 Military Accident Risk

Military accident risk *[3]* is defined here as the risk of injury during military operations caused by deficiencies in the design and function of materiel. Especially crucial is the advantage the enemy could gain from this in a combat situation.

The background to this specific risk being identified, among other things, is that during the Gulf War and other recent conflicts, more injuries have occurred as a result of accidents occurring rather than from hostile action. Safe technical systems, good instructions on how to use the materiel and a secure operating environment are important contributory factors for the ability to maintain military capability.

It is of vital importance that soldiers have confidence in their equipment to ensure the effectiveness of a military unit. Maintaining a high level of system safety when employing technical systems is just as important in a combat situation as it is in peacetime training. System safety activities must provide the commanding officer with technical systems that are effective (and safe) for the intended military use and therefore enable the unit to conduct combat operations without (unnecessary) losses caused by shortcomings in their own technical systems. See also *section 2.3* above, on the demoralizing effects of military accidents.

3.3 Friendly Fire

System safety activities do not normally involve the risk of weapon effects against own weapons systems, personnel or the external environment. The evaluation of the risks associated with hostile detection, weapons used, the effects of engagement and consequential damage must be prepared for as part of the requirements analysis and requirements fulfilment with respect to performance, such as systems effectiveness, combat power and protection capabilities. Aims and requirements are described in TTEM and specifications, see *section 6.5*.

In the event of doubt, DesignA, in conjunction with HKV (ÄF), demonstrates which risks must be analysed. Uncertain cases may, for example, include ammunition disposal in peacetime (practice disposal of foreign live mines), towing firing targets (acting as a target) and participation in international operations. If the risks relating to weaponry effects are analysed, a careful specification of the weapons system it relates to is required, along with what sort of performance is acceptable/should be applied.

Accident risks caused by friendly fire should always be analysed as part of system safety activities. Accidental shooting with own weapons, the need for direction constraints to rule out firing from own platforms, flames that result from the firing of missiles, blowback from recoilless anti-tank weapons, ammunition safety, and so on, should always be covered by the system safety activities that are carried out for a new or modified technical system.

3.4 Relationship between Safety and Risk

The Armed Forces defines safety as freedom from accidental injury/damage to person/property and/or the external environment. Accidental damage/injury can be both immediate (e.g. a fence that has been driven into or a broken arm) and also an injury that takes a long time to develop (such as ill health/cellular changes caused by high-frequency radiation, ill health/hearing loss caused by noise, ill health/stress injury caused by incorrect posture or the extinction of certain species caused by toxic emissions).

3.5 Accident Risk

The concept of risk is central to system safety. Risk expresses a combination of severity of injury, ill health, musculoskeletal injury (the consequences, i.e. how bad it can get) and the probability (how often) an event/incident with this particular impact is expected to occur.

Each individual risk is based on a hazard. Danger is caused either by a hazard (risk source) or a hazardous condition.

A hazard is a phenomenon that has the potential to cause harm, given the circumstances in which a hazardous event can be triggered (for example, arsenic in a glass bottle that breaks as a result of the bottle falling to the floor).

A hazardous condition is characterized by the fact that its danger is directly present and unconditional (such as an unprotected rotating cross-cutting saw).

However, an incident or accident that leads to injury caused by hazards such as these cannot occur unless someone or something is exposed to the effects of the hazard.

Even a slow-acting hazard has an effect and causes injury only during the time when a person is exposed to the hazard. The point in time when the damaging effect actually manifests itself is dependent on the concentration of what is dangerous or the degree of poor ergonomics, and the person's resistance to the fatal or poor ergonomics. Examples of slow-acting processes may include ill health developed due to tobacco smoking (see *table 2:1*, which shows that the probability of getting lung cancer and dying for a person who smokes 20 cigarettes per day is 1 person out of every 200 smokers per year). Another example may be a musculoskeletal injury which develops over a long period of time by a soldier who has operated combat vehicles with low headroom in relation to the combat equipment he uses.

Sometimes, the expression hazard or risk of disease/ill health is used to increase transparency of the circumstances in question.

Risk relates as much to an accident (a serious incident where injury arises) as to a more slow-acting sequence of events which results in an injury – induced ill health.

In H SystSäk E, the term risk will continue to refer to the risk of an accident occurring (usually the word hazard is used), this is to clearly show what kind of risk it is.

3.6 Risk Model

A general risk model has been developed to facilitate understanding (for example among design engineers) of the technical system's various accident risks, their origin, the different possible sequences of events and the relevance of exposure for an accident to happen at all.

The risk model is suitable to use for a risk analysis to enable the identification of an accident risk caused by a hazard (which requires certain events to trigger a hazardous event) or an accident risk caused by a hazardous condition. In either case, the conditions for potential exposure are identified so that the risk of an accident occurring can be thoroughly evaluated.

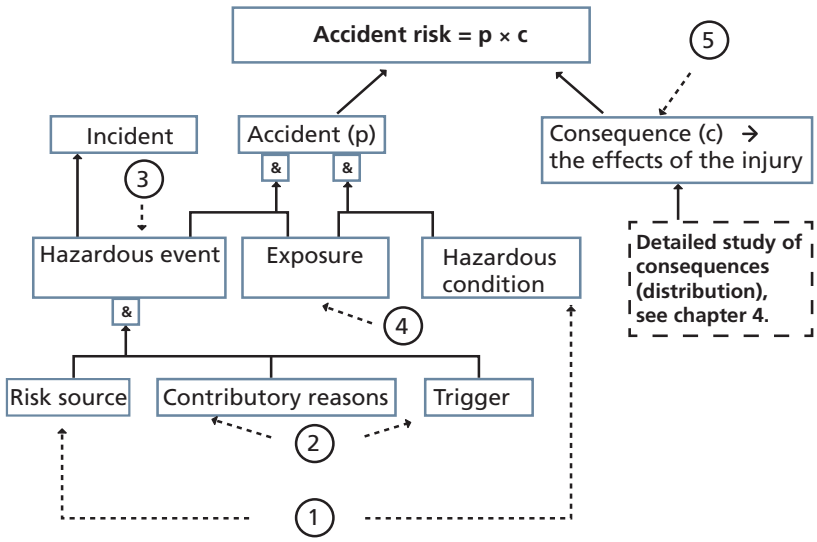


Figure 3:1 Risk Model

Comments about figure 3:1.

The model's two terms, **hazard** and **hazardous condition** are somewhat overlapping and not always perfectly exclusive. There is no need to create an unambiguous classification. However, we need both concepts to help risk analysts to identify and describe the dangers of a particular system. The model makes no claim that directly covers every possible risk situation.

Sometimes, therefore, a hazard that can be triggered is often regarded as a hazardous condition.

A hazardous condition that is equipped with a barrier can, on the other hand, be perceived as a hazard, where the failure of the barrier takes the form of a trigger.

The risk model in *figure 3:1* provides support for the idea of risk management. During the identification of accident risks the following questions below may be asked. The number of the question and the context is also evident from the figure.

1. Central to the risk of an accident occurring is that there is either a hazard or a hazardous condition (= danger). Here we must ask the question: "Where is the danger?"
2. The source of the risk can be triggered and cause a hazardous event. The triggering of the hazard can take place through any phenomenon in the manner of use or in the user environment. This poses the question: "What is the nature of its use and what does the user environment look like? Is there anything that can trigger the hazard in question?"
3. A hazardous event can be identified by asking the question – based on a certain hazard: "What must not happen?" To answer the question, all possible types of event must be identified.

   Note that when a hazardous event occurs, this does not always lead to an accident happening. When a hazardous event occurs without anyone/anything being exposed, "only" an incident occurs.
4. An accident occurs if someone/something is exposed to the hazardous event. In order to find what is exposed we must ask the question: "Who/what is exposed?" (That does not say anything about the actual outcome of the accident, the outcome can range from practically nothing happening to a disaster.)

   The danger may also be made up of a "hazardous condition". A hazardous condition is characterised by the fact that it always exists (assuming that the technical system is operational and performing in the location in question) and therefore its dangerous properties are fully developed.

A power line retains its constant danger, even when the power cable has fallen down, and it remains dangerous until the power is actively switched off. The tail rotor of a helicopter is always dangerous when the helicopter is in operation. People may be exposed to its danger when the helicopter "is operating" at ground level.

If someone or something is exposed to a hazardous condition, it is likely that an accident will occur.

5. An unfortunate consequence can be assessed by following the methodology outlined in *appendix 1, Risk Appraisal*, for each individual risk, financial risk and risk of damage to the external environment.

An **accident** is defined as an event in which any person, item of equipment or any part of the external environment are exposed to a hazardous incident or hazardous condition and an injury/damage occurs. The nature of the injury/damage can have an immediate effect, such as a broken bone, or it may take a long time to develop, for example, it may lead to ill health which can take decades to develop. An accident is always unplanned and is not the result of a hostile act, for example.

An **incident** is defined as a hazardous event in which no person, equipment/property or any part of the external environment are exposed to a hazardous event. There are usually many more incidents than accidents. From both types of event valuable information can be gathered to improve safety by reducing the number of possible hazardous events or restrict/regulate exposure to risk.

The full meaning of the concept of an incident in the handbook is more specific than what is normally found in common parlance. So, for example, the expression **near misses** means a type of accident where it is often due to chance that a more serious outcome did not arise. Therefore, this expression makes no difference between an accident with zero outcome and an incident (hazardous event without exposure).

Injuries from the release of hazardous substances, within the limits allowed, should not be regarded as system safety problems.

The likelihood of an accident occurring is caused by a hazard, consisting of a probability of a hazardous event combined (multiplied) by the probability of exposure. This fact is often misunderstood as to why it sometimes happens that the probability rate established for a certain accident risk really only refers to the hazardous event and not the accident. This way of handling probabilities leads to too high a value of the assessed risk of an accident occurring.

The relationships between the various elements that can lead to accidents are fairly complex. Therefore, the handbook's methodology for risk management should be used. It is based first and foremost on finding the dangers within the system. You must then identify what each hazard must not cause (= hazardous event). Subsequently, the uses (modes of application) and user environment are identified, and in these, all events that can cause a danger, and any possible triggering factor. To identify potential accidents, all objects in need of protection (people, property and the external environment) must also be identified which may be exposed to the effects of possible hazardous events.

3.7 Types of Risks at different System Levels

Dangers (hazards and hazardous conditions) are very different when they are compared with each other. Differences exist in a broad spectrum of physical areas. Often, the system level determines which of the safety risks can occur and which may therefore pose a threat. The concept of a system level may be an appropriate basis upon which a technical system's accident risks are identified. *Figure 3:2* aims to show the link between system level and type for most of the accident risks that may occur at a specified level of the technical system.

A detailed description of the different risk types are found in *section 4.2.2*.

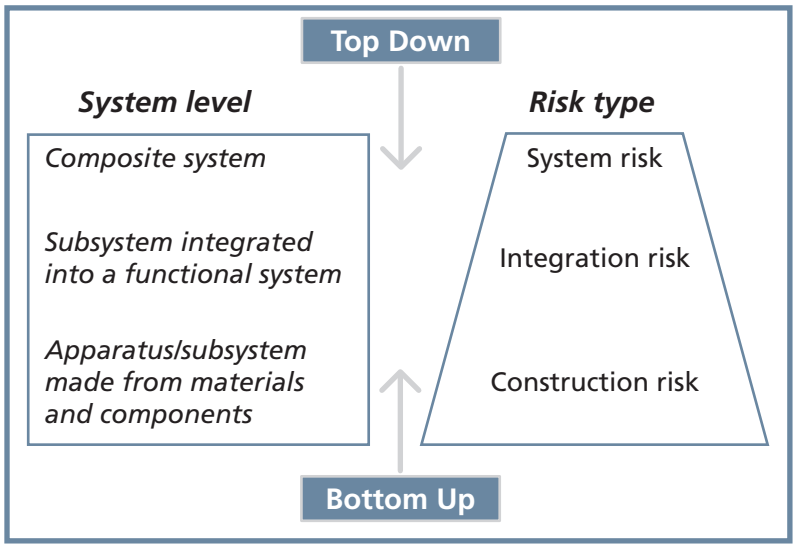


Figure 3:2 Types of Risks at Different System Levels

3.7.1 Level – Apparatus, Subsystems

For the lowest system level, the dangers are very basic and of a fundamental nature.

- Hazards may be made up of dangerous substances (for example toxic, explosive, flammable, oxidising) or they may have a dangerous physical power (electric current), mechanical hazards (sharp edges, moving parts) or something else at a minimum technical level.
- Hazardous conditions may consist of a tense spring, a charged capacitor, a person who is at high altitude or any other direct threat.

Also, some apparatus/components can deliver physical hazards, such as the effects of electromagnetic radiation (radar, laser) and acoustic energy (audible sound) or impulse noise (from firearms), and can therefore constitute hazards.

3.7.2 Level – Subsystems Integrated into Functional Systems

At a slightly higher system level, where the apparatus/subsystems are connected, hazardous conditions can arise as a result of integration and create hazards. Examples of scenarios are weapons that are loaded, a radar station starting its broadcast, a laser meter that starts, helicopter rotor blades starting up and a vessel starting its propellers. When such events start unintentionally, or at the wrong time and with staff exposed, unintentional risks may occur.

3.7.3 Level – Complex Systems

At the higher system level, where complex systems have been given a certain capability, for example an action, there is usually some form of control or management system to direct the effect towards the correct target. Such management systems may be local or the management/control may be conducted from a distance (remote). In both cases, the controls may fail. The local control may be disrupted by a short circuit in the input resonator, control cables may break, a mechanical or electrical breakdown may occur in the joystick etc. Remote operations may fail due to cable breaks, short circuits in the input resonator or radio controls may jam or otherwise become inoperative. As a result, a fully functional weapon system in an uncontrolled manner may be initiated and used against an unintentional target, therefore exposing everyone within the area of impact to mortal danger.

3.8 Design Rules

3.8.1 DesignA's Design Rules

Following an investigation of accidents and deviations that have happened, new knowledge of the risk content and risk characteristics inherent in technical systems normally arises at DesignA, (see *section 3.9.4*). It is important that information on deviations, safety measures and risk reduction measures come to DesignA's attention.

It is DesignA's fundamental responsibility to continuously compile and document acquired knowledge of accident risks in technical systems. Also, the knowledge generated through business intelligence, new standards etc., should be included in this documentation.

When technical systems are used, DesignA works continuously on design changes to reduce any identified risks. Design modifications that could be applied to avoid the discovered risk of an accident when similar technology is used in the future are transformed into a general design requirement (design rule). Also, these design rules are being added as experience grows.

Examples of existing codes include RMM (Rules of Military Ground Operations) *[35]*, RMS (Rules for Naval Operations, prepared by the Armed Forces *[36]*), RML (Rules for Military Aircraft, developed by the Armed Forces *[34]*), H VAS-E (FMV Weapons and Ammunition Safety Manual *[11]*), H FordonSäk (FMV Handbook on Vehicle Safety *[10]*), the Armed Forces and FMV's handbooks on Electrical Safety *[30]* and H ProgSäkE (the Armed Forces Handbook for Software in Safety-Critical Applications *[20]*).

The background to these being developed is that the current technical systems are particularly dangerous and that a large number of hazardous conditions and hazards and possible hazardous events and potential emergencies are known. In several cases, accidents have actually occurred.

Design guidelines specify how known accident risks can be avoided through certain design changes or the requirement of regulations when being constructed. The purpose of a design framework is that, for a proven technology, the design or requirements for design features, in order to prevent/reduce the effects of known accident risks, are specified in an appropriate manner.

Following a review/follow-up of the design work, a checklist of rules to support the work of identifying where there is a risk of an accident occurring is used.

3.8.2 Armed Forces' Design Rules

Under the heading "Military exceptions from limit values", in *section 2.4.1*, the needs of the Armed Forces have been identified for the development of their own application instructions with guidelines, limit values etc., which are defined by the Armed Forces as tolerable for Swedish military personnel.

In the event that such limit values have not been produced, the matter is regarded as a risk that a certain degree of damage may occur and is evaluated according to the current technical system's risk matrix.

> Developed and accepted limit values for military technical systems for different types of stresses from noise, vibration, impulse noise etc., often result in the development of more effective materiel compared to that of risk management during design, demonstrating the need for risk-reducing measures.

3.9 Risk Awareness

3.9.1 Definition

The Armed Forces' are dependent on technical systems that have the intended effect in combat. By necessity, the Armed Forces must accept a certain amount of risk-taking in order to gain access to this combat effect. Conscious risk-taking is part of the Armed Forces' normal activities, especially during combat. However, this does not imply a general negligence in terms of risks, but instead an adopted risk-taking after careful consideration by the commanding officer. The procedure requires that each risk should be known and managed and that operational risks are continuously taken into account.

The organisation, with its employees, must constantly strive for the best level of safety possible by working on the risks. A parallel is drawn with the benefit to civil society's concept of "Safety culture", which is defined as "the collection of characteristics and attitudes in organisations and in individuals which ensures that safety issues receive the attention they need" (IAEA, International Atomic Energy Agency).

System safety activities are also a concern for the Armed Forces' organisation and personnel, and they need to work continuously during regular operations. The quest must be to continually find the hazard risks in technical systems and activities.

A high level of risk awareness, with the necessary stimuli from reviews, deviation reports, improvement suggestions and positive attention from the individuals who are involved in operations, are necessary prerequisites to find all accident risks.

A high level of risk awareness exists when everyone recognises and accepts their responsibility for risk management and the organisation's management of system safety risks, which forms an integral part of regular operations.

A good awareness of risk is characterised by the personnel concerned, their positive commitment and participation. Only through good risk awareness will the prerequisites be available to learn about and effectively deal with the risks of accidents that are not yet detected and the risks of accidents that occur during the service life of the materiel.

3.9.2 Allocation of Responsibility between the Organisation and the Individual

In order for good risk awareness to be developed, an atmosphere in which individuals are not punished or called to account for their inadvertent mistakes is required. Systems must be robust and be able to deal with improper use. If a system error is identified, this should be seen as an advantage, because then it is possible to correct the error before an accident occurs (in a combat situation, the error could also weaken our strength and might lead to losses).

This is the ideal condition that can be difficult to achieve in practice. When one person has caused a deviation, it is a normal human reaction to blame or to try to blame others – instead of just the easiest way of providing a frank and honest account of what has occurred. In particular, an organisation working with complex materiel with great risks must take this knowledge about human nature into account and prepare to deal practically with these types of (systemic) abnormalities. Such a pragmatic adaptation is necessary because the incident information is vital to prevent future errors.

The Armed Forces are governed by rules and regulations. An individual who is guilty of serious and deliberate misconduct should of course not go free from responsibilities. The Armed Forces strives to achieve a fair culture where honesty and sincerity are rewarded. This means that unconscious mistakes and errors should be reported as deviations without the risk of punishment. Such an attitude is currently seen in the Air Force, where positive deviation management procedures have contributed to risk-reducing measures being implemented.

Errors and mistakes are inevitable and safety can only be improved if the organisation can learn from its mistakes, which requires access to this type of information about safety shortcomings.

Faults with equipment or incorrect instructions could cause an accident. Reporting of all types of abnormalities is of vital importance to achieve and maintain good levels of safety and must therefore be encouraged. Disciplinary action or threats, severely compromises the willingness to report.

Man's role in a technical system is not straightforward and must therefore always be taken into consideration during a system's service life. See *H SystSäk E Part 2, section 5.17, Operating and Support Hazard Analysis (O&SHA) – Task 206*.

3.9.3 Deviations, how they are reported

A basic element of creating and maintaining a high level of risk perception is to study how safe the materiel is and what is actually happening during operations. This can be done by following up the total operating time, maintenance reports, incident reports with regard to observations, incidents and accidents and to draw conclusions from the overall information. This may mean that risks and hazards can be identified and appropriate risk-reducing measures can be developed, verified, validated and implemented. This is, in brief, a description of system safety activities during the maintenance phase. Only through these active system safety activities can established risk level requirements be continuously maintained.

Studies of operations for a number of companies have shown that most hazardous events do not result in accidents, only in incidents. But often it was only chance that lead to there not being an accident, as no individual or other object worthy of protection was exposed to the hazardous event. Compare the basic principle for an accident to occur according to the risk model in *figure 3:1*.

Most hazardous events are, by nature, very trivial, such as a broken screw, a broken strap, a flat tyre, which are not usually particularly serious events.

Instead, it seems that these events were due to poor quality, low reliability and not really a shortcoming regarding safety. Despite this, most hazardous events have the potential to cause severe injury = accident. However, most accident risks remain undiscovered. Despite the fact that many of them have been proven to have some form of quality defect that was so insignificant that no one filed a report. Only a negligibly small percentage cause deviations that are perceived as safety-critical.

From this, it is understood that the greatest knowledge bank available to provide support to prevent further accidents is the fact that people have a familiarity with past deviations.

Only a few hazards lead to serious accidents. Therefore, only a negligible fraction of necessary knowledge of system failures could be made available by simply investigating accidents that have already happened.

All incidents and accidents contain important information about the technical system's residual accident risk. All accident risks have the potential to be safety-critical and should therefore be reported as anomalies, irrespective of whether an accident has occurred or not.

Access to *information about certain dangers, where an accident has not occurred*, should be regarded as "*free information*", i.e. up-to-date knowledge has been obtained without the cost of an accident.

The information also has the property of being "fresh" with a "best-before date". This means that information can only be used for its intended purpose if it is reported and is used in time for risk management, before an accident/new accident takes place.

The ability to deal with information on deviations efficiently requires access to a reporting and enforcement system that facilitates the handling of these aspects and allows the generation of constructive, risk-reducing measures.

Such a system is aimed at risk reduction and requires the following:

- Deviations (observations, incidents, accidents and other knowledge of existing defects in materiel/systems etc.) are reported.
- It is easy for everyone to report and record the necessary information (what, where, when, who).
- Experienced staff investigate the deviation (how and why it happened).
- Causes, both direct and indirect, are identified efficiently.
- Where possible, proposals are made for corrective action, to reduce the risk of a recurrence of the deviation (for example amended design, additional or modified instruction, training, protective measures).
- This can be followed up to verify that the improvements have worked, or if similar deviations have occurred again.
- Feedback, to the source of the report and to other users of the materiel, should take place as soon as possible.

3.9.4 Deviation Investigation

So that the study of deviations functions effectively, there must be an organisation with the responsibility of managing the deviation reports following use of the technical systems. Information received and gathered is analysed so that the root causes are identified. The main objective is always to develop corrective measures to eliminate risks and prevent accidents.

Causation is often complex and involves both the design of the materiel, how it has been used, personnel training, what sort of awareness of risk there is for the actual item of equipment and the organisation's ability to create and maintain a risk awareness adapted to the organisation's operations.

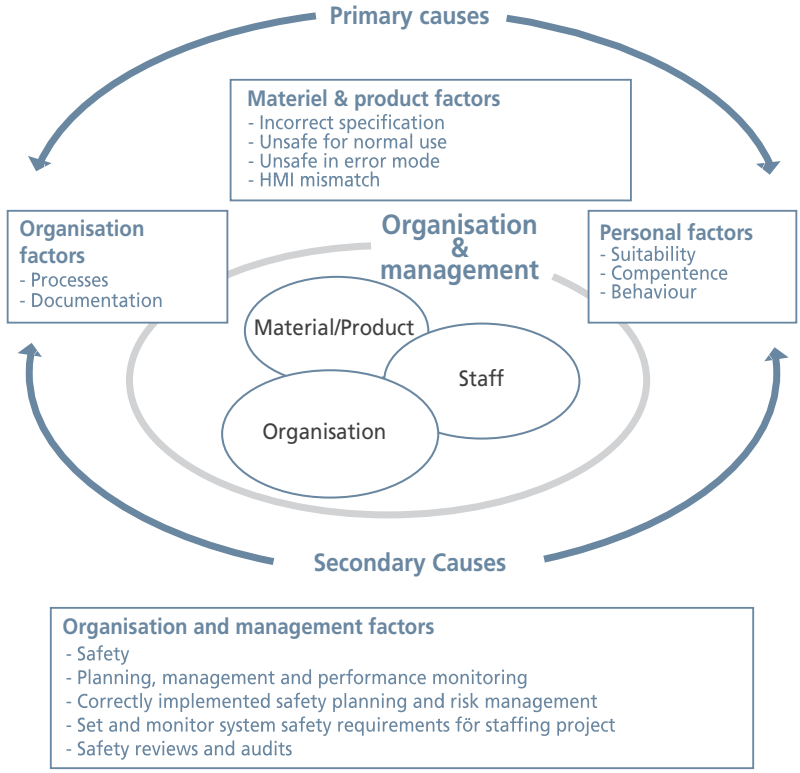


Figure 3:3 Direct and Indirect Causes of Deviations

Relationships between direct and indirect causes are summarised in *figure 3:3*, above. The image shows that all features mentioned in the figure can have an impact on the occurrence of the reported deviation. Therefore, it is essential that the enquiry that proposes corrective actions is also open to propose measures for all areas that may lie behind the reason for the deviation that has occurred (concurrent primary causes and underlying interacting factors).

The goal of the investigation of a deviation: observation, incident or accident, is to clarify the facts about the deviation, not to attribute blame or responsibility. The facts, following analysis with findings, will provide a basis for recommendations so that corrective action can be implemented and accidents can therefore be prevented.

The Armed Forces' HKV should be designated competent resources with the task of organising, managing and monitoring deviation management. HKV should issue rules and procedures for deviation reporting and follow-up.

In the event of a deviation, a deviation investigation of either external actors or the Armed Forces should be made. External actors who can carry out an investigation of deviations in the Armed Forces include (supervisory/regulatory area): the Swedish Work Environment Authority/the Working Environment Act, the Electrical Safety Authority/the Electricity Act, the Police/the Law on the Transportation of Dangerous Goods, the Swedish Civil Contingencies Agency/the Law of Flammable and Explosive goods, the Swedish Radiation Safety Authority/the Radiation Protection Act and the National Board of Accident Investigation, SHK/the Law on the Investigation of Accidents.

The Armed Forces' investigation is carried out at three different levels: unit/contingent, key operators and FMUK (Armed Forces Investigative Commission of Inquiry).

Unit level – An investigation following a deviation will normally be undertaken by the unit where the deviation occurred.

Central operator *[18]* – A study of the deviation which is believed to have or is expected to result in serious injury or failure/breakdown should normally be referred to the central operator. Commander of PROD can, on special occasions and in collaboration with the central operator concerned, participate in or lead investigations that are normally carried out by a military unit.

FMUK – FMUK is an independent investigative group whose task it is to investigate an accident or incident which SHK investigates. Commander of SÄKINSP decides on each individual case whether FMUK is assigned or not. The central operator and personnel director can request from Commander of SÄKINSP that an investigation is conducted by FMUK.

3.9.5 Continuous Improvements

A natural element of good risk awareness is actively working with continuous improvements. The amount of risk in a technical system is not static but often increases with time, partly because of the fact that materiel gets worn, is maintained improperly or inadequately etc., and therefore new risks may arise, and also because people as well as organisations become less vigilant and they become complacent and "blind" or get used to things, especially if no accidents have happened for a long period of time. Vigilance, monitoring and feedback is therefore required at all times to continuously maintain established requirements with regard to risk level.

There are several methods to reduce risks within the system. The following can be regarded as proactive methods (provident and appropriate):

- deviation reporting, investigation and feedback
- safety investigation and review
- system safety activities during both procurement (SSWG-1) and the use of the systems (SSWG-2)
- suggestion activities that include the identification of potential risks.

When an accident has happened this is investigated via a deviation investigation. However, this is a reactive approach (to subsequently prevent recurrence), which means that the damage has already occurred.

4 Risk Management

4.1 Basics

Risk management is a general technique used in many different areas (see *section 2.1*). Some of the general concepts are described in *figure 4:1*, below.

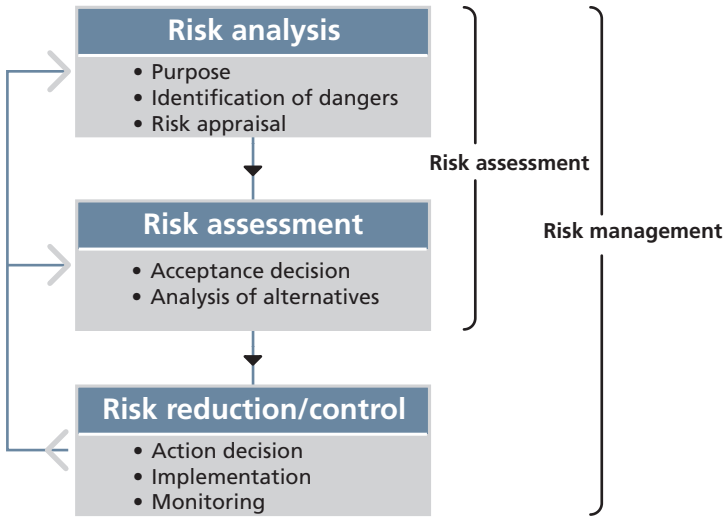


Figure 4:1 General Risk Management Activities (IEC 60300-3-9) [7]

Risk management is, in principle, carried out during two stages of the technical system's service life: during development and use. (*Applied methods for risk management* are described in part 2, Methods.)

4.2 Risk Analysis

4.2.1 Purpose

Risk analysis during the development phase aims to identify and estimate the technical system's accident risks before an accident has occurred. This requires access to authoritative data on the system's behaviour/reaction during future use, both with regard to its good qualities and its bad. Good qualities include, for example, operating data that is reliable and accessible. Bad qualities refer to the system's tendency to "break down", giving rise to different types of hazards and accidents. It is very difficult to identify the data that describes the system's properties, because they relate to the functionality of the system in the future. For the same reason, it is difficult to verify that they are sufficiently accurate once these values have been developed. In the absence of a correct database which describes the system's behaviour in the future, you have to find tools that have the ability to provide an acceptable picture of the technical system's future operating and risk characteristics.

Risk analysis during the time the system is being used aims to identify the risks resulting from changes or modifications. It also includes the basis of consolidated data on reported discrepancies, analysing them to identify possible causes of past events and therefore preventing recurrence.

> Proactive and preventive risk management takes place on the flimsiest of evidence and with incomplete tools, which requires personnel with experience and humility who can perform assessments with a great deal of dynamism.

4.2.2 Identification of Accident Risk

System Risk

The client/person who places the order/user will always have a clear objective with each technical system ordered. The system should be able to deliver a certain capability to the Armed Forces in certain specific operational environments.

At the same time as this capability is defined, there is reason to seek early identification of the associated hazards that this capability can generate, directly or indirectly, and the accidents which might therefore occur. This makes up the accident risks at system level, "systemic risk".

Risk analysis relating to system risks can be carried out most easily by specifying the technical ability of the system and then repeatedly asking the question: "What must never be allowed to happen due to this capability?" (Either as a direct result of a "misdirected" capability or as a secondary effect of the capability.)

In this way, the following systems risks can be identified:

- Crew in danger of drowning if the vessel needs to be abandoned at sea.
- Combat vehicle crew risk their lives if the vehicle overturns in the water and lands on the only exit.
- Submarine crew risk their lives if the submarine cannot float to the surface.
- Aircraft crew risk their lives if the plane crashes.
- Self-combat (any type of weapon effect/disturbance that not only engages the enemy but is also harmful to own units).

Requirements for specific **system safety features** that can protect against identified system risks are identified very early, preferably during the study phase. See *section 6.4, Studies* and *section 6.5.3, Requirements for Systemic Risk*.

Note that MIL-STD-882C includes System Hazard Analysis (SHA) – Task 205, which is about identifying risks that are caused by the overall system design. However, it is not specified in the standard how this should be performed.

System of Systems

A new capability can be created through the use of existing technical systems and products in a new way, possibly along with additionally employed materiel. What is specific is that the intended capability has not been analysed from a system safety point of view and therefore lacks a system safety decision.

On integration of a system/subsystem/product, new accident risks may often arise because new ways of existing hazards may be triggered (new hazardous events, new forms of exposure to hazardous events) and new hazardous conditions are introduced.

Shifting to "higher system levels" often means:

- Accident risks at "lower system levels" remain.
- Accident risks at "higher system levels" arise.

With the development of new systems/functions, identification is needed as a result of the new accident risks arising from new conditions, new triggers, new hazardous conditions and new objects that have entered onto the scene and which may be exposed.

Even when a risk analysis for system of systems is carried out, the purpose is to identify accident risks.

Design Risk

Identifying the primary risks of accidents (that is, the risk of accidents at the lowest technical level) as early as possible is an important part of the design work and something which is always included in the supplier's obligations (and is carried out with the help of the methods described in this handbook). The reason that the supplier is given this responsibility is that the cost of risk-reducing measures which are taken early are relatively low. Considerably more resources are required to address the risk of accidents that are discovered when production has been started or is

completed. Accident risk that is detected even later in the technical system's service life often results in an incident or accident. This may even have caused the loss of human life and, generally speaking, it is very costly to undertake risk-reducing measures on technical systems that are in use.

During design, accident risks caused by specific components/apparatus/technical subsystems are continuously being identified. The designer carries out continuous risk analyses in connection with the choice of materials, components and apparatus and continuously incorporates effective risk-reducing measures as a natural part of the design work.

The risk model shown in *figure 3:1* above, is intended to be supportive when hazards and hazardous conditions are identified. The picture also makes it easier to identify various options in order to eliminate/reduce a particular identified accident risk. Alternatives can be based on:

- Reducing hazards/dangerous physical characteristics, for example by switching to something less dangerous.
- Counteracting/interrupting the mechanism that enables the source of the risk to become "dangerous".
- Slowing down/preventing the triggering of the dangerous characteristics that relate to the hazard.
- A hazard that has been triggered, or a hazardous condition, where an accident may be avoided by preventing exposure, for example by designing and incorporating physical protection for personnel or moving personnel out of the reach of danger.

The onus is on the designer to ensure the requisite function and performance, and also to fulfil requisite requirements in terms of system safety. The designer chooses risk-reducing measures so that all requirements are met at the same time. All this is carried out as economically as possible. The customer specifies the level of risk through the requirements which, in turn, determine how far the designer needs to go with regard to reducing the risks that may arise/may be identified during the design work.

Integration Risk

It is assumed that the subsystems can be developed in accordance with prevailing system safety methods and are provided with properties so that the demands on system safety are fulfilled (see above).

When two different subsystems are designed according to this principle, and are integrated with each other, there is still no guarantee that the results (integration) comply to requirements in terms of risk level. Instead, new accident risks arise out of the conditions so that subsystems do not automatically communicate with each other in a safe manner in all the physical areas that systems can communicate. For example, radio links may interfere with each other, electromagnetic radiation from machines in operation may interfere with functionality, common power supply requires precise knowledge of frequencies, power use, voltages, hydraulic systems which must have the same oils, pressures and connecting devices.

It is natural to expect that a manufacturer/designer will find these accident risks because they are directly due to the design of physical characteristics, and that they might be removed if the design is carried out in an adaptable way. It is therefore the role of the system integrator to take care of and carry out the necessary risk-reducing measures with regard to the risk of integration.

If the parts to be integrated are not all developed with the requirements of being integrated with each other, they may, for example, be made up of COTS parts: the design responsibility for subsystems and for the composite system must therefore be dealt with. Unless the client outsources design responsibility for the integrated system from a single supplier, this remains the task of the client.

Methods

There are several ways, with different purposes, of performing risk identification. The various approaches differ depending on which technical system level the analysis relates to. See *table 4:1*.

Table 4:1 Approaches to Risk Identification

Purpose	Approaches to risk identification
Systemic risk, including system of systems	Identification of overall system functions which, triggered accidentally or otherwise, threaten the system. (These functions usually provide an answer to the question: "What must not happen?")
Design risk	Identification of hazards and hazardous conditions and risk identification when selecting design elements and overall design.
Design risk and integration risk	Theoretical analysis of the functional chains, such as weapons systems, propulsion systems, avionics systems, in order to identify hazards and hazardous conditions. (Examples of weapons systems: sensor – C^2-systems – fire control systems – weapon mountings.)
Design risk and integration risk	Physical tour of the areas where the technical system is installed, space for space, in order to identify hazards and hazardous conditions.

Identification of a Safety Critical Function

There may be a safety critical performance/function inherent in a technical system. This relates to the performance function which, if it does not work, can lead to a dangerous situation that exposes the operator/unit to an elevated accident risk. The engine in a single-engine aircraft is an example of this. Another example is the key fitted to a switch which switches off the current to a rotating radar antenna designed for use by engineers as a precautionary measure prior to conducting maintenance.

There may be times when a new technical system is dependent on "support" (input data, power etc.) for its function, which is safety critical to some extent. The problem can be solved, for example with redundant support functions, i.e. alternative sources which provide support. The responsibility of providing a solution is with the technical system requesting support.

> Hostile action is not a safety risk but part of normal operations and is countered with military conduct, safety measures, tactics and military technology.

Results of Hazard Identification

Results of hazard identification are compiled as a list of identified accident risks, with its reported hazardous condition and hazardous event and relevant exposure. This compilation is done preferably in the Risk Log. A detailed account of this activity and the Risk Log, along with its application, is provided in *appendix 2*. A brief report on the Risk Log is found in *section 4.5*.

4.2.3 Risk Appraisal

Risk appraisal consists of estimating the possible consequences of each identified hazard. In *appendix 1, Risk Appraisal*, a comprehensive description of the appropriate approach is presented. The *results of the risk appraisal activity* is documented in the Risk Log, indicating the estimated values for probability and consequence.

The estimated probability of a certain accident risk relates to the use in accordance with the specified operating profile of a specimen during the intended lifetime of the technical system.

Risk Appraisal of Environmental Risk

Accident risk relating to damage to the external environment may result in consequences that can be restored/rehabilitated or damage which is permanent, for example, completely wiping out a species or permanently destroying a certain physical area.

- Accident risk with repairable consequences can be estimated in monetary terms.
- Accident risk with lasting consequences should always be classified as non-tolerable (i.e. as a red accident risk). Decision on the closure of such an accident risk can only be taken by the Armed Forces.

Risk Appraisal of Financial Risk

Risk of financial loss is considered in this handbook, which may consist of:

- direct damage to or loss of materiel, subsystems, systems
- damage to another person's property
- cost for remediation/sanitation of damage to the external environment caused by the Armed Forces' activities with the technical system in question.

4.3 Risk Evaluation

4.3.1 Determining Requirements Relating to Accident Risk

The basis for the Armed Forces' risk management approach is to specify the maximum permitted value of an accident risk in the technical system. This is done by means of risk matrices: one for personal injury and one for financial damage.

A risk matrix (regarding personal risk or risk of financial loss) is **the highest level of risk acceptable** (= tolerable level of risk) for an individual accident risk.

Characteristics of a Risk Matrix – Aversion Factor

Society regards occasional deaths as undesirable, not tolerable, but actually inevitable. Accidents involving several people usually lead to major reactions in a community and demands for social action and legislative change. Consistent with this, minor wounds, broken bones and some degree of disability are regarded as rather fortunate outcomes of accidents that "could have had a worse outcome".

All this means that, in society, there are different acceptance levels of accidents depending on what type of injury occurs. Minor injuries are accepted as inevitable, but there is an aversion to more serious accidents.

This handbook's examples of risk matrices therefore incorporate an aversion factor. This factor takes into account the view that a major injury is tolerated to a lesser extent than a comparable accident that results in minor injuries.

Evaluation Methods

Evaluation of an individual accident risk can be carried out:

- qualitatively, a verbal description of probability and consequence
- quantitatively, where a numerical value is used to indicate likelihood and impact.

Risk Matrix for Bodily Injury

Below are examples of a risk matrix for personal injury. The matrix is taken from MIL-STD 882C and is also described in the Materiel Management Marine Handbook (HMS) *[24]*.

The matrix includes a description of injury class and probability/frequency.

The matrix is quantitative – if a qualitative risk evaluation is to be carried out, the numerical value is disregarded in *table 4:3* and *table 4:4*.

Note that the risk matrix relates to the use of a single example of the system in relation to the technical system's service life.

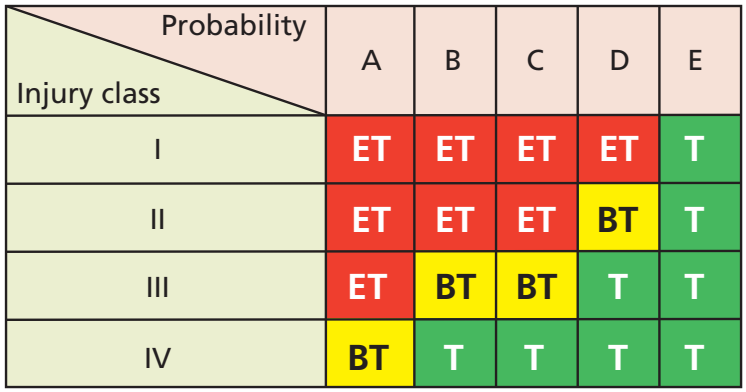


Figure 4:2 Example of a Risk Matrix for the Evaluation of Personal Injury

The concept of risk levels used in *figure 4:2*, above, are:

- ET = Not tolerable
- BT = Limited tolerable
- T = Tolerable.

The injury class categories that relate to an individual are shown in *table 4:2*.

The categorization of probability is shown in *table 4:3* and for frequency in *table 4:4*.

Table 4:3 and *4:4* can be used alternatively. Note, however, that the frequency classes' (A–E) actual values are not consistent in the two tables.

Table 4:2 Categorization of Bodily Injury

Injury class	Description of injury to a person
I	Death
II	Serious injury
III	Less-serious injury
IV	Negligible injury

Table 4:3 Categorization of Accident Probability

	Description of accident probability for one system (one boat/vehicle etc.)	Probability during service life
A	Will probably occur frequently	$>10^{-1}$
B	Will occur several times during a lifetime	$10^{-2} – 10^{-1}$
C	Can occur at any time during a lifetime	$10^{-3} – 10^{-2}$
D	Improbable, but possible that an accident will occur at some point during a lifetime	$10^{-6} – 10^{-3}$
E	Very improbable that an accident will occur at some point during a lifetime	$<10^{-6}$

Table 4:4 Categorization of Accident Frequency

	Description of accident probability, for one system	Frequency
A	Will probably occur frequently	> Once a year
B	Will occur several times during a lifetime	1 time during a period of 1–5 years
C	Can occur any time during a lifetime	1 time during a period of 5–75 years
D	Improbable, but possible that an accident will occur at some point during a lifetime	1 time during a period of 75–1,000 years
E	Very improbable that an accident will occur at some point during a lifetime	< 1 time every 1,000 years

Risk Matrix for Financial Damage

The risk matrix presented below provides examples of financial damage.

The matrix includes a description of damage class and probability/frequency.

The matrix is quantitative – if a qualitative risk evaluation is to be carried out, the numerical value is disregarded in *table 4:3* and *4:4*.

Note that the risk matrix relates to the use of one system during the technical system's service life.

Injury class \ Probability	A	B	C	D	E
I	ET	ET	ET	BT	T
II	ET	ET	BT	T	T
III	ET	BT	T	T	T
IV	BT	T	T	T	T

Figure 4:3 Example of a Risk Matrix for the Evaluation of Financial Damage

Categorization of the probability of financial damage is carried out in the same way as for personal injury, that is, with either *table 4:3* or *4:4*.

Categorization of the damage class for financial damage is carried out in accordance with *table 4:5*.

Table 4:5 Categorization of Financial Damage

Damage class	Description of financial damage (own and others' property damage and remediation costs	Damage in monetary terms (SEK)
I	Approximately the same cost as a total system loss	> 10^9 SEK (> 1 billion)
II	Significant loss	10^7 – 10^9 SEK (10 million - 1 billion)
III	Limited loss	10^5 – 10^7 SEK (100 000 - 10 million)
IV	Slight loss	< 10^5 SEK (< 100,000)

Adjustment of the Damage Class for Financial Risk

To be relevant to a specific technical system (cheaper or more expensive), the risk matrix for financial damage may have to be adapted. It is reasonable that the damage that the technical system can cause is compared to the procurement cost of a single example of the technical system. (Damage class I = total cost of a single example of the technical system).

This means that in the adapted risk matrix for financial damage to the technical system in question, the amounts for each damage class should be changed and based on the total cost of a single example.

An example of the alternative definition of damage classes, which reflect lower values/based on a less costly technical system is as follows:

I	> 10 million
II	100,000 - 10 million
III	1,000 - 100,000
IV	< 1,000

Adaptation is performed when being developed by Tactical-Technical-Financial Objectives (TTEM).

It is also possible to make a difference to the type of property damage and apply different tolerance criteria:

- damage to own system
- damage to property of third parties
- costs associated with repairing damage to the external environment.

Take a closer look at HMS *[24]*.

Use of Qualitative and Quantitative Risk Matrix

A qualitative risk matrix is often used for the first preliminary risk appraisal. As the development of a technical system continues and the understanding of the properties a particular technology has becomes clearer, there is a transfer to a quantitative risk matrix.

A quantitative risk matrix allows a more precise measurement of the exposure's influence on the size of the accident risk.

For really simple technical systems and specific products, and when individual risk sources exist, a qualitative risk matrix may be the only applicable method (in *table 4:3* or, alternatively, *4:4* the third column – the numerical column – can be removed).

An Existing older Risk Matrix or Risk Matrix from this Handbook

If procurement relates to the supplementation of an existing technical system, it is reasonable and appropriate to continue to use the risk matrix that has been used for the original procurement.

General Information about Adjusting the Risk Matrix

This handbook provides examples of risk matrices that can be modified for specific procurements. If the technical system to be procured is considered to be different from a previously acquired technical system in relation to system safety requirements, this should be reflected in the requirements that the risk matrix expresses. Such differentiating criteria may, for example, relate to the following:

- Only a lower tolerable level of risk may be acceptable.
- A higher tolerable level of risk may be acceptable.
- A lot of people will be exposed to the technical system's risks at the same time.

In this respect, the Armed Forces in certain cases may supplement the risk matrix, for example:

- with an additional column for probability, while all probability levels are adjusted
- with an additional row related to the injury class “more deaths”.

It should be noted that the number of risks in a system are not taken into account, which means that the system's size is not given any importance. It is only the level of risk for the specific accident risk, one at a time, which is taken into consideration (identified, appraised and valued).

DesignA can make adjustments in the TTEM to the obtained risk matrix in order to impose upon the supplier to report the closure of the risk in a more controlled manner (= convert one or more green boxes to yellow).

4.3.2 Closure of Risk – Acceptance Decision

For each of a technical system’s accident risks, an acceptance decision is made which determines whether the accident risk can be accepted as is or whether measures must be taken to reduce risk. The acceptance decision is then compared to the value of the accident risk, taken from the technical system’s risk log, with the specified risk value. The comparison is made using the risk matrix.

DesignA will consider and approve the supplier’s risk-management work for all risks, including those that the supplier has classified as “green”.

For accident risks in the yellow area, DesignA will receive a report from the supplier about the risk characteristics, taken/proposed risk-reducing measures, follow-up or whether additional risk-reducing measures will be implemented and then DesignA will decide on the closure of the risk.

Red accident risks, for which it has not been possible to produce sufficient measures to move away from the red area, are notified promptly by DesignA to the Armed Forces. The Armed Forces decides what measures should be taken in response to a red accident risk.

Decision with the Support of the Risk Matrix

Open the document Risk Log. Identify the probability of the four risk elements that relate to the accident risk in question. Read off in the risk matrix each risk part's placing and colour. The colour determines whether the size of the actual sub-accident risk can be tolerated or not. If any of the four risk elements are red (or yellow), the entire accident risk is regarded as not tolerable (or limited tolerable) and risk reduction is needed.

Only when all four markings are located within the green area is the accident risk tolerable.

(See *appendix 1, Risk Appraisal*, for details on individual risk and its risk elements. See *appendix 2, Risk Log*, for details on its use).

Decision-maker

The Armed Forces is responsible for specifying who is entitled to take decisions on various types of risks. During the procurement process, this will be specified in the TTEM as requirements to DesignA. Normally the design requirement is as follows:

The supplier closes the risk after consultation with DesignA.

The supplier informs DesignA of the risk and presents the documentation. DesignA closes the risk.

The supplier informs DesignA of the risk and presents documentation as soon as possible when the risk is discovered.
DesignA informs the Armed Forces of the risk. Only those who have established the Armed Forces' requirements can close the risk.

4.3.3 Analysis of Alternatives

If an accident risk is not tolerable, risk reduction should be carried out. Each risk-reducing measure needs to be prepared from a design point of view. In this regard, it is best to compare several engineering solutions with each other, to find the solution that provides the most impact in relation to the input of resources.

4.4 Risk Reduction/Control

4.4.1 Action Decision

Risk reduction for a technical system that is under development should be conducted as long as it is needed in order to include the established requirements, namely to ensure that the risk is transferred to the green area in the risk matrix.

Compare the text on the *ALARP methodology in H SystSäk E Part 2, section 5.4*. Note the difference that the methodology requires, that all possible/reasonable risk reduction must be made for each individual accident risk, as long as the input resources are reasonably related to the impact/output.

4.4.2 Implementation

The following factors may help to achieve a reduction in risk:

- the conditions for an accident to happen
- the probability for each outcome.

The principle of risk reduction must always be that the accident risks are greater than the requirements specified in TTEM, which must be reduced to the specified requirements level. The risk management work for a technical system must therefore always be based on a risk appraisal. A few suitable tools for this are set out in *appendix 1, Risk Appraisal*.

Risk reduction of accident risks in a technical system can generally be carried out in three different ways:

- a reduction in the presence of a hazardous condition and the likelihood of a hazardous event
- a reduction in the probability of exposure
- a reduction of the consequences of an accident.

Accident risks for a new technical system should be regarded as generally threatening events, each with a variety of outcomes. These scenarios are substantially affected by external factors, such as in its application (how a technique is used in each individual case) and the environment in which the technical system will operate/be used.

To try to identify future accident risks by looking past experiences from previous technical systems is of course possible. But such experiences comprise a collection of special cases, namely accidents that have happened. Each of these accidents were due to certain prevailing external conditions. It is recognized that these conditions ought to be completely unique and hardly apply to another environment and another area of application.

There is therefore a need to find a tool that can provide an overall approach which, at the same time, also makes it possible to vary the input factors in a way that is traceable and documentable.

Of the tools listed in *appendix 1* only Modelling/Simulation has all the necessary qualities needed to provide good quality and well-documented support documentation. Support documentation can easily be produced using the other reported tools as input values for the application of the Modelling/Simulation method.

4.4.3 Monitoring

An accident risk that has been subject to a degree of risk reduction does not necessarily imply that the intended risk level has been reduced. The result of the risk-reducing measure must be verified. The method of verification should be determined at the same time as the risk-reducing measures are prepared and decided. A risk-reducing measure which lacks a method of verification should not be the first choice.

Once the desired risk reduction has been implemented and verified (see *figure 4:1*) a new risk analysis is carried out to ensure that the risk-reducing measures have not led to a risk increase or the introduction of new accident risks.

Thereafter, a new risk evaluation is carried out.

4.5 Risk Log

To develop and deliver complete risk documentation is a mandatory requirement for the supplier. Some of the risk documentation consists of a Risk Log. This handbook demonstrates the Risk Log that meets the Armed Forces' minimum requirements when reporting accident risk and its subcomponents.

When, for example, international cooperation takes place, other documentation may be used whereby the Risk Log should be used for content specification purposes rather than for execution purposes.

When a Risk Log is being kept, work is done on the adjustment of the Risk Log based on the requirements and needs of the technical system. Thereafter, hazards and hazardous conditions are identified, which are then entered into the Risk Log. The Risk Log is continuously supplemented for all risk management activities. Also steps to obtain and verify the reduction of risks and an acceptance decision are entered into the Risk Log.

The Risk Log accompanies the technical system throughout its entire service life. For example, during the maintenance phase the System Safety Working Group, SSWG-2, may be given the assignment of keeping the Risk Log.

During the maintenance phase, the Risk Log is reported for each individual accident risk with an estimation of the risk value before and after any risk-reducing measures are taken. (Detailed instructions regarding how to maintain/keep the Risk Log up to date are described in *appendix 2*.)

The expression “initial risk” is used to indicate the initial estimated size of a certain accident risk. The concept of “residual risk” relates to the size of the risk subsequent to a risk-reducing measure.

5 Description of System Safety Activities

5.1 The Armed Forces' Responsibility for Technical System Safety

Prior to each decision regarding an assignment relating to a technical system, the Armed Forces should identify how responsibilities for the safety of the technical system in question should be allocated in the most appropriate manner. The points below are designed to provide some guidance.

a. Generally speaking, the Armed Forces assumes the entire responsibility for technical system safety. Ordinary operations for the development of a technical system should also include the implementation of the requisite system safety activities. A number of operators are involved in these operations. They have established responsibilities and roles to play.

b. The Armed Forces can, via the allocation of design responsibilities, engage another organization to provide support relating to the safety of a technical system.

c. The Armed Forces is free to hire and appoint any organization to assume responsibility on behalf of the Armed Forces, such as DesignA. For more complex technical systems, a particularly competent technical organization is preferably employed. Design responsibility is retained preferably during the technical system's entire service life.

d. If the Armed Forces makes any modifications to technical systems that a DesignA is responsible for, the responsibility for the safety of the system immediately returns to the Armed Forces.

e. If the Armed Forces does not hire someone else to assume responsibility for technical systems safety, it remains the responsibility of the Armed Forces.

f. If the Armed Forces performs a modification of the technical system covered by DesignA's responsibility, the responsibility for the safety of the system immediately returns to the Armed Forces.

g. For the acquisition of a pure Commercial off the Shelf (COTS) product that is used on a stand-alone basis (i.e. not together with a technical system) and according to the manufacturer's instructions, no special design responsibility is required. Instead, the Armed Forces, as an employer, is responsible for establishing requirements for CE marking and a declaration of conformity that the operating instructions and maintenance instructions are included, and that the obligation to ensure that newly acquired equipment meets the applicable rules before becoming available for use by the Armed Forces' employees *[6]*.

   For civilian ammunition, CE marking is replaced with CIP proof marking.

5.2 Technical Design Responsibility

Technical design responsibility means determining the technical structure and design of the technical system and determining the integration of technical systems/apparatus and components that are subject to a certain allowable configuration (including maintenance solutions) and to ensure that it meets legal requirements, established objectives and other requirements with regard to performance, functionality, information and system safety during the entire service life of the technical system.

Technical design responsibilities, including technical systems management, are normally held by DesignA for all levels of technical systems which DesignA has delivered to the Armed Forces. Technical design responsibility is linked to the type of technical system. See *section 7.7, DesignA's Mandate and Responsibility for Change*.

Industry and suppliers assume product responsibility and may have a technical design responsibility in relation to the procurement organization, but it is always the procuring organization that is responsible for the technical design for the Armed Forces. Design responsibility for military aeronautical products is regulated in the Rules of Military Aviation (RML) *[34]*.

5.3 Requirements and Decisions Regarding System Safety Activities

This section describes the specific requirements and decisions necessary to control system safety activities for the technical system.

The system safety activities during a technical system's entire service life are depicted in *figure 5:1* below.

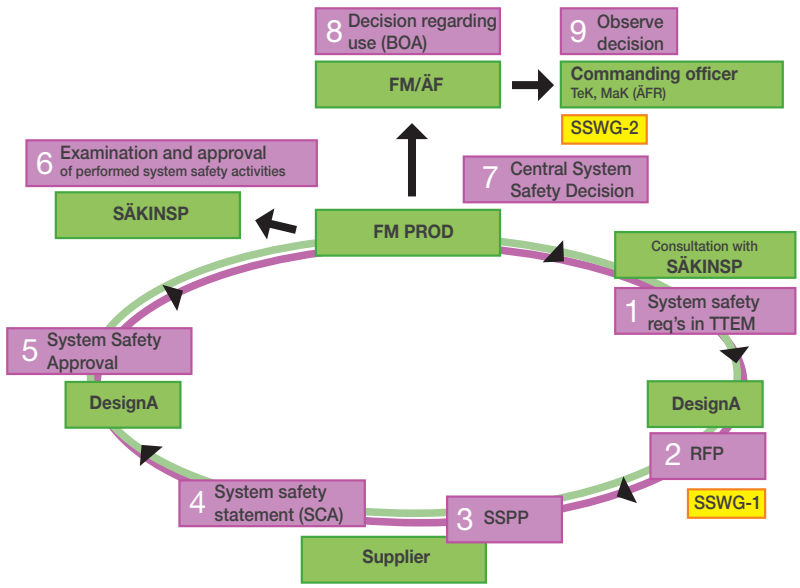


Figure 5:1 System Safety Activities during Service Life

Activities reported in *figure 5:1* (the numbering of the points below correspond to the image numbering):

1. The Owner Representative (ÄF) establishes system safety requirements in the customer order (KB) and TTEM for a certain technical system in consultation with SÄKINSP.
2. DesignA imposes system safety requirements in the Request for Proposal (RFP).
3. The supplier reports intended system safety activities in the tender to DesignA through a preliminary Safety System Program Plan (SSPP).
4. The supplier decides on the Safety Compliance Assessment (SCA) and hands it over to DesignA.
5. For all technical systems submitted to the Armed Forces, and for all integration products, DesignA decides and implements system safety activities and issues a Safety Statement (SS) which is then submitted to the Armed Forces.
6. The ÄF will propose a draft Central Safety Compliance Decision (CSSB) and submit it to the Armed Forces' Safety Inspectorate (SI). The SI then examines the system safety activities and, assuming the activities are judged to be of sufficient quality, provides an opinion on the CSSB.
7. The ÄF determines the CSSB and submits it to the Armed Forces/ÄF.

   ÄFR and the System Safety Working Group (SSWG-2) are the parties with the greatest interest in the risk documentation for the technical system that is handed over by DesignA to the Armed Forces at the following handover times:

   – on presentation of a new technical system
   – on presentation following a modification
   – on presentation following a maintenance task (during a maintenance task the risk documentation is only updated when the maintenance task has resulted in a change in the evaluation of the technical system's risks (hazards and hazardous conditions).

   See also the Armed Forces' routine for the delivery of products from the FMV to the Armed Forces *[9]*.

8. The ÄF makes a BOA (Decision regarding use) and presents it to the commanding officers concerned.
9. The commanding officers ensure that any requirements in the BOA are maintained when the technical system is used and that its configuration is in line with what is specified in the BOA.

   The commanding officer is particularly interested in the Armed Forces' BOA. The commanding officer is responsible for ensuring that the activity is carried out with the right materiel, correctly trained staff, with the proper precautions, in the right environment and in the correct manner. To enable this, the commanding officer requires information as to what the regulations are that apply for a certain technical system and how this can and should be used. All this information can only be obtained from the system safety decision for a specific technical system.

5.4 Determining Requirements

Principles and details when determining requirements are reported together with the description of the Armed Forces' system safety activity. See, in particular, *section 6.5, Procurement*.

5.5 System Safety Decision

System safety activities that have been implemented are documented in the three defined system safety decisions (which, for example, are shown in *figure 5:1* above):

- SCA (supplier)
- SS (DesignA)
- CSSB (ÄF).

These decisions must be firmly grounded. Before any such decision is made, some form of risk analysis and/or the development of a conclusion based on any previous decision is always required. The analyses, conclusions and other considerations must be documented in the decision. If they are more comprehensive, they are summarized in the decision and attached as an annex.

> A system safety decision only approves the configuration and the activity that is reported in the decision. It should be noted that a certain system safety decision approves the reported configuration in the BOA for the reported activity in the decision. Note also that the system safety decision is rarely, or does not have to be, time limited. The need to revoke a system safety decision only arises when it has been shown that the current configuration/use/activity gives rise to greater risks than are tolerable.

On special occasions when DesignA has been given an assignment to issue a specific technical system – an SS, but where the technical system in question does not have an acceptable safety level, the report is instead presented in the form of a **safety message**. (Refer to *H SystSäkE part 2 under safety statement*.)

Sea Trials Command (PTK, see also *H SystSäkE part 2*) contains a specific type of SS which is normally referred to as a safety certificate. The certificate is issued by DesignA and it means that DesignA, after inspecting all the relevant circumstances, has found that the vessel that PTK is to test has an acceptable level of safety.

5.6 Decision and Product Documents for a Technical System

5.6.1 General

Decision and product documents for technical systems should always include:

- a system safety decision
- risk documentation
- a configuration decision.

Confidentiality

Decision and product documents for technical systems should always be open. If a specific assignment has been classified as confidential it has to be documented in a special annex to the ordinary decision/product document for a technical system. The annex is dealt with according to the level of confidentiality.

Details are presented below as to how the decision and product documents can be designed for a new technical system, a changed technical system and for an amended technical system.

5.6.2 New Technical System

System safety activities should be carried out by DesignA for *all new technical systems* that are to be handed over to the Armed Forces. An implemented system safety activity should be documented in risk documentation and there must also be a system safety decision. Determination of the new technical system's size and configuration should be documented with a configuration decision.

A new technical system, as described above, is also understood to be a technical system created by existing materiel by combining subsystems from several technical systems. The purpose may be, for example, to create new capacity (system of systems).

Risk documentation for a new technical system describes the implemented risk work, all identified accident risks, the required documentation for instructions, instructions, handbooks etc., to provide knowledge about the accident risks inherent in the technical system to the operator and how the operator should avoid these risks. The support documentation includes:

- a system safety report (SAR) with analytical results (from analysis activities that have been carried out, such as PHL, PHA, SHA etc.)
- a risk decision (for each risk)
- a Risk Log
- information about the technical system's risks and support for instructions, handbooks etc., with regard to how the risks should be avoided
- any restriction (refers to any restriction in how the technical system is used to temporarily deal with a certain risk).

System safety decision for changes made to technical system:

- a SCA (is carried out when the supplier has participated)
- a SS
- a CSSB.

A CSSB indicates whether a change to the technical system has brought about a new accident risk or increased the risk level. In these cases, the BOA must be updated.

DesignA's configuration decision for a new technical system includes the following:

- a reference to the current SS
- product documentation that establishes the new technical system's size and configuration. This also includes maintenance plans (TO UF) required for the maintenance of the technical system.

5.6.3 Amended Technical System

Amendments to the technical system are defined by its configuration being changed. This occurs when you add a new subsystem, a new component, exchange a specific component for an enhanced/modified function or any other change to the technical system. (See also *section 5.7, Decision Occasions*.)

The system safety activity that has been carried out and which has produced a change to the technical system is documented with risk documentation and a system safety decision. The determination of the scope of the changes made to the technical system, its configuration and the measures that are introduced, are documented with configuration decisions.

Risk documentation for a changed technical system describes the implemented risk work and all identified changes with regard to accident risks (additional, removed, increased, decreased and unchanged) and includes:

- A SAR with regard to changes made to the system parts, including the results of any analyses. (from analysis activities that have been carried out, such as PHL, PHA, SHA etc.) see *H SystSäk E Part 2, section 5.12*, *5.13* and *5.16*.)
- A risk decision for each individual accident risk.
- A Risk Log for each individual accident risk.

System safety decision for changes made to technical system:

- a SCA (is carried out when the supplier has participated)
- a SS
- a CSSB.

A CSSB indicates whether a change to the technical system has brought about a new accident risk or increased the risk level. In these cases, the BOA must be updated.

The configuration decision for changes made to the technical system include, among other things, the following:

- reference to the current statements
- product documentation that establishes the changed technical system's size and configuration
- a technical Order (TO), which is required so that the technical organization, on receipt by the organization/unit, can introduce the change in question to the technical system.

Implementation regulations for the handling, preparation and accountability etc., relating to the implementation of a change to the technical system are regulated by the Armed Forces' and FMV's common Change Management Process *[17]*.

5.6.4 Adjusted Technical System

An adjustment (a minor change) to the technical system is defined as a slight configuration of the system. This means that a risk analysis has been carried out and this has revealed that no new risks have arisen, no existing accident risks been affected by the adjustment and the level of risk has not been increased in terms of any particular accident risk. An example of this may be exchanging a fixed component that has a similar function with a different specification, or any other minor change to any part of the technical system.

A risk analysis that has been carried out on the adjusted technical system should be documented and attached to the TO.

A **configuration decision** is also required if the technical system has been adjusted.

Implementation regulations relating to the handling, preparation and accountability etc., regarding the implementation of a change to the technical system are regulated by the Armed Forces' and FMV's common Change Management Process *[17]*.

5.7 Decision Occasions

The need for a system safety decision or the updating of the existing system safety decision for technical systems, as described above, is analysed when one of the following circumstances has occurred. Guidance on how to implement the analysis and how to handle the different results can be gathered from *figure 5:2*. If the analysis shows that a new/updated decision is required, a decision is taken in accordance with the normal routine.

An analysis is carried out when:

- A deviation report has been submitted to DesignA and a completed investigation reveals considerable, previously unknown, accident risks. DesignA presents a proposal for action on the technical system and/or a proposal for temporary restrictions on its use (restriction).
- SSWG-2 has identified a new accident risk/reassessed the risk level for an existing accident risk which has been documented in the Risk Log (or Risk List).
- A new technical system has been created (for example by using existing products from other technical systems and possibly together with a newly procured product).
- A new technical system has been procured (a number of products have been procured which have been brought together to form one technical system).
- The existing technical system has been given a new configuration (one or several products have been added/changed/removed from the existing technical system).
- The existing technical system, in its present configuration, is intended to be used in a new way (for example to run faster, load more, fire with another type of ammunition).
- The existing technical system, in its present configuration, is to be used in the intended manner but in a new environment.
- The introduction or use of a configuration that has not been approved by DesignA has taken place.

- There has been a change in the regulatory maintenance/or a change is about to happen.
- A change has taken place in the requisite training/or is about to happen.

A review of the considerations when applying system safety methodologies and decision and product documentation in accordance with *section 5.6* is presented in *figure 5:2* below.

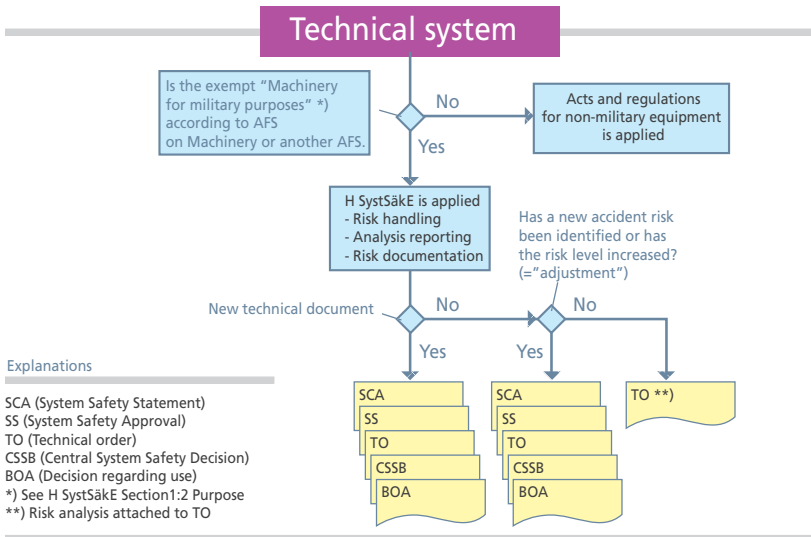


Figure 5:2 Considerations, Decision and Product Documentation for Technical

5.8 Technical System, Structure and Interfaces

The technical system is the basic materiel unit. The concept of a technical system is generally used irrespective of the system level it relates to. A specific technical system can be handed over to the Armed Forces by DesignA. That same system can also be an integration product for inclusion in another technical system (one system or several systems).

There are **interfaces** around all technical systems. These may be other technical systems; a power supply; water, sewage and fuel supplies; repair facilities; air traffic control etc. All system safety activities must be based on the technical system and all of its interfaces, this includes those specified by the Armed Forces as well as those that are implied with consideration to the intended activity etc. See *H SystSäk E Part2, section 5.3, System Safety Requirements in TTEM – S11*.

A **product** is referred to as a technical system that comes from a particular supplier. A product requires a SCA. If a technical system is a COTS product (often a CE marked product), it is assumed that risk-reduction work has been performed in accordance with applicable laws and reported by the manufacturer in the CE marking documentation. For Government Furnished Equipment (GFE) the Armed Forces is responsible for similar activities and support documentation.

Product integration is a product to be integrated in different technical systems. Examples include a radio, laser rangefinder, ammunition, built-in generator and a crypto device. For an integration product, the SS relates to the product's specifications and its actual configuration. The SS later forms a part of the support documentation required to develop the SS for the technical systems in which the integration product forms a part.

Integration is carried out for a technical system that meets the requirements that have been set. In this respect, the integration of parts may include:

- a commercial product
- GFE
- an integration product
- an existing or newly acquired technical system.

The integration is carried out by DesignA or the supplier. On integration normal system safety activities are carried out and DesignA issues a SS.

For a commercial product, as described above, to be integrated into a technical system a *special system safety analysis* is carried out. The objective of the analysis is to examine the characteristics of the commercial product in action, to ensure that the characteristics are not particularly dangerous or can enhance the enemy's combat effects of the technical system. Examples of these characteristics may be that a vehicle has fuel tank near the passenger compartment or contains subsystems which provide safety but which are explosive (such as an air bag/inflatable curtain).

When an integration product is a CE marked COTS product, DesignA analysis this based on demands on the geographical environment/user environment for the technical system in order to identify whether it meets system safety requirements. It is important not to repeat any risk management work that has already been done by the supplier.

Therefore, if possible, the system safety analysis of the integration between technical systems and a COTS product is based on risk analysis work carried out for the COTS product as reported in the CE marking documentation.

5.9 Ammunition

5.9.1 Basics

In the case of explosive materials or pyrotechnic products included in the technical system, DesignA's SS includes a decision from The Swedish Civil Contingencies Agency (MSB) relating to the product's safe transport and storage. See *section 2.4.11*.

Ammunition used for military purposes is a particularly hazardous technical system which, from a system safety point of view, should always be handled in one of the following relevant ways:

- As *ammunition* which is often intended for a particular purpose or a particular weapon or other specified use (see, for example, the anti-tank mine, which is intended to be used independently or with particular launching equipment). Here, ammunition is the integration product. This means that the

ammunition is safe enough for its use in the intended weapon and during the intended use if it is possible for this to be done independently.

- As a stand-alone *transport and storage* item. The object always consists of packaging/transport and storage packaging, with certain specified properties, containing a certain number of ammunition units.

  The requirement on the object is that the packaged ammunition must be sufficiently safe when exposed to mechanical handling in the environment it is intended to be used in.

5.9.2 Safety Statement for Ammunition for Military Purposes

Both these aspects will be covered by a separate SS which DesignA will always provide for each specific military ammunition unit. In addition, a decision from MSB must be included for the approval of the safety of these goods during transport, storage and handling. See *section 2.4.11*.

DesignA should present this SS to the Armed Forces which will produce a CSSB and a BOA for the ammunition in question in its transport and storage packaging.

5.9.3 Integration of the Ammunition with the Technical System

For technical systems, weapons and equivalent, in which military ammunition is to be used, system safety documentation for this technical system will be updated in accordance with the handbook's policy for integration. After that, the Ammunitions List can be updated stating that this weapon, or its equivalent, is approved for firing/use of certain ammunition/or the ammunition is qualified to be fired in certain weapons (and similarly for other types of technical systems where the ammunition is used, see launching equipment for anti-tank mines).

5.9.4 Military Ammunition with IM Features

The technical system ammunition is exposed to such severe stress at high temperatures that an explosion may occur. High temperature may arise, for example, in the case of accidental fire, injury or damage may occur to the Armed Forces' own units and assets that are worthy of protecting. Because it is the characteristics of own weapons that cause/strengthens the effect, this characteristic may be regarded as a system safety deficiency.

The resistance of ammunition to counteract the effects of heat, and several other types of stimuli, is referred to as having Insensitive Munitions (IM) characteristics.

The extent to which military ammunition may cause accidental damage to own units or something else worthy of protection is identified by conducting a threat analysis. A threat analysis is based on the ammunition's intended user environment throughout its entire service life (transport, storage, use, decommissioning) and the stimuli (heat, drops, fire, shrapnel etc.) to which the ammunition can be exposed in this environment. From this threat analysis, the damage that could occur to own units and other things worthy of protection is identified. If the damage is assessed as not tolerable it is possible to demand that the ammunition must have such IM characteristics that the injuries/damage must be prevented/restricted.

In the design, the IM characteristics may, with relatively simple tools, be designed and incorporated into military ammunition and its packaging. If certain ammunition must have IM characteristics, this requirement needs to be specified in the TTEM. See *[4]* and *[44]*.

5.10 Some Technical Systems and Aspects

5.10.1 Training Materiel

Some technical systems/products are solely intended for the purposes of training/exercises in contrast to the live ammunition and equipment used in combat situations. Included here are all types of training equipment, from a blank firing adapter for a hand-held weapon to a simulator for fighter aircraft. A specific system safety analysis needs to be carried out for such equipment to ensure that the equipment's characteristics (handling, interface to the operator, as well as ways to respond to operator action) do not deviate from the characteristics expected during a live engagement with the military equipment in all-important respects that relate to knowledge and skills. By learning how to respond correctly when using the training equipment, so-called negative training can be offset.

5.10.2 Ergonomic Design

The amount of strain technical systems place on the user, both physically and mentally, always needs to be analysed to identify possible risks (musculoskeletal injuries) during predictable conditions of use. Such risks of ill health can be prevented by ensuring the technical system has a good ergonomic design.

5.10.3 System of Systems

System of systems should be regarded as the highest level of technical systems. It may be that the system of systems are nothing more than a large and complex technical system. Typically, only individual requirements for specific skills are specified, despite the fact that the total amount of constituent technical systems facilitates a variety of other capabilities.

However, it is essential to ensure that this capability can be safely exercised. At this system level, as at all other system levels, this is ensured by applying the Armed Forces' system safety methodology.

A new configuration includes technical systems that have already been approved in terms of system safety. This may form the basis for continued system safety activities. Here the focus of system safety activities is to examine the integration between constituent technical systems as they together deliver their intended capabilities.

A similar approach is adopted in international efforts, to prepare for collaboration with technical systems used by foreign units.

5.10.4 Language

Instructions, handbooks and warning labels intended for operators must be designed in English, Swedish or in accordance with special requirements from, for example, the RMS or the RML.

The language of the decision documents (SS, CSSB and the BOA) must always be Swedish.

When purchasing a finished product abroad, obviously not all documentation will be available in Swedish from the supplier. DesignA is responsible for specifying documentation requirements and will ensure that the required documents will be translated into Swedish.

In the event that the instructions, handbooks and warning labels intended for operators are to be translated into Swedish, it is always the supplier of the technical system that is responsible for this translation.

In the Swedish version it should be stated that it is a translation and from which language. The foreign version should be included in the product documentation that comes to DesignA.

The language for technical documentation is specified in the TTEM. If the technical staff who will be maintaining the system have requisite knowledge of technical English, then English may be chosen as the language for technical documentation and the Risk Log. Otherwise, Swedish will be chosen as the language.

In cases where English is chosen as the language for technical documentation, the standards authority will specify the lowest level in terms of the language abilities of technical staff in accordance with the established NATO standard or other recognized standard as specified in the training programme.

5.10.5 Command and Control Systems (C^2) and Weapon Systems

Basics

Different technical systems contain varying amounts of hazards/hazardous conditions. System safety activities are carried out with the aim of identifying and managing prevailing accident risks.

Theoretically, after completing the system safety activities, it may be found that a particular C^2-system has no hazards/hazardous conditions. Is it then "risk free" to integrate this C^2-system with a certain weapons system? The answer is no.

Instructive Approach

The C^2-system's function is to provide management information to an application system. This is normally provided by different weapons systems.

Each weapon system involves a risk that the weapon will be accidentally fired or directed against an unintended target. From a system safety point of view these are inherent hazards in the weapons system. If there is an error in the management data (fire control/tactical command) that can lead to such a risk it should be regarded and treated as a system safety risk inherent in the weapons system. For the C^2-system concerned this is dealt with as a performance requirement with a certain quality measure in terms of reliability and availability of management data.

The above approach means that the C^2-system and the weapons systems only present their own accident risks. The result is that the SS does not require a specification as to which firing units the C^2-system can provide management data for, and that the weapons system is not limited by the different C^2-systems that it can receive management data from.

For a technical system and/or a technical product within the area of C^2-systems which is/are not intended to be integrated into a weapons systems or to be used in the field, *section 5.10.8, Independent Use of Civil Materiel*.

5.10.6 Vehicles System

Within the framework of the vehicles system there are several forms of system construction. This is due to the fact that vehicles are expensive, manufacturers have a market incentive to offer new and adapted technology packed into vehicle types that are adapted to their purpose, while the Armed Forces' needs change rapidly over time. A custom application of the existing regulatory framework facilitates the Armed Forces' activities, at the same time safety requirements are not compromised. *Table 5:1* below, provides a summary of prevailing systems, their construction and an adapted application of standards.

Table 5:1 Application of Standards (Regulations) for Different Alternatives for Vehicle Procurement

Vehicle type	Approval
Special vehicles (including MOTS)	SS + registration inspection + CSSB → BOA
Standard vehicle (COTS)	Manufacturer's declaration/individual approval → BOA (not CSSB)
Standard vehicle (COTS) + civil additions (COTS)	Existing type approval for vehicle + type approval for the addition → BOA (not CSSB)
Standard vehicle (COTS) + military additions	Existing type approval for vehicle + existing BOA + SS for the addition + SS of the integration
	CSSB → BOA (for the addition and integration, i.e. no new system safety work on the vehicle itself other than what is required to system safety analyse the integration)

5.10.7 Expert System

Background

The Armed Forces' operations are characterized by an international commitment with the requirement that it can operate at short notice on a wide variety of arenas. This places particular demands on access to far greater knowledge than before. Skills must be updated and relate to different aspects, such as a combatant's tactics, organization, materiel and combat environment. Knowledge is required to make quick tactical decisions. However, decisions at the minimum technical system level also require access to qualified information, examples include clearing mines and Improvised Explosive Devices (IEDs).

A solution to the need for rapid access to expert and detailed information is the expert system, sometimes referred to as a decision support system. This is a computer program that answers questions from the user by drawing conclusions based on a set of rules and pre-stored facts. Expert systems are usually considered as belonging to the category of software with artificial intelligence. The purpose of expert systems is to mimic the advice from a person who has a lot of experience in this area. Examples of expert systems are programs for disease diagnosis which, based on the patient's symptoms and background (age, gender, occupation, disease, family history etc.), will help the doctor by providing suggestions for possible diseases, with a scale of probability and/or danger.

A future technique for the creation of an expert system is called a neural network. This refers to algorithms for information processing that try to imitate the function of nerve cells and the brain.

Algorithms based on neural networks can often solve problems that are difficult to handle by conventional computer science methods. Examples of applications are: pattern recognition, signal processing, control theory, forecasting, self-organization, problems with constraints and scheduling.

Expert Systems and System Safety

The normal hazards that are inherent in the expert system and which can cause serious personal hazards should be cared for by the manufacturer of the commercial computer equipment which the expert system is "packaged" in. Some other accident risks may not be available as long as the expert system is not physically linked to technical equipment systems.

Expert system errors are limited to information shortcomings, corrupt data, pure misinformation and covert information that goes astray. These shortcomings may give rise to "security" losses, but they may also mislead the operator so that an accident may occur when handling the object that the expert system describes.

The operator can cause an accident when in contact with the object which the expert system describes, by:

- misunderstanding the information
- not applying the information as intended
- not executing the correct grip
- using the wrong tools
- deviating from the correct action and therefore not achieving the intended result in a safe manner.

If, for various reasons (for example, in extreme situations when time is limited), a design is chosen where the expert system is integrated with own technical systems, a number of aspects emerge with regard to managing system safety:

- How to validate the learning-related systems (neural networks)?
- When can fully autonomous operations be applied?
- What is the risk of an accident occurring?
- What restrictions and safety regulations are required to manage identified accident risks?

5.10.8 Independent Use of Civil Materiel

General

H SystSäk E is not applicable for the procurement and independent use of civil materiel outside the technical system.

Civil Standard Materiel

Civil materiel may consist of equipment for the office environment in an organization aimed at promoting peace, a classroom, cafeteria etc. If this materiel is not subject to a law or statute with a military exemption (see *section 1.2*) no system safety activity is required and no system safety decision should be developed.

A decision that the system safety activity in accordance with H SystSäk E will not be implemented and no system safety decisions will be developed, will be made by the ÄF, on initiation of the procurement. This is documented in the procurement decision. The decision will also clarify that the materiel may not be integrated with military technical systems.

In the specific case that the Armed Forces' needs to make a BOA for a civil/standard item of equipment/product, the BOA, with regard to the requirement for CSSB, may be issued on the basis that allowed the marketing of the civil standard item of equipment/product.

If the civil standard item of equipment/product is to be integrated into the technical system, *section 5.6–5.8* above will apply.

5.10.9 Independent Acquisition of Civil Hand-Held Weapons (COTS) and Civil Ammunition (COTS)

General

Civil materiel may consist of civil hand-held weapons (COTS) and civil ammunition (COTS) to be used according to the manufacturer's instructions. Decisions regarding system safety activities in accordance with H SystSäk E not being required for such materiel are made by the ÄF on initiation of the procurement. The decision is documented in the procurement decision. The decision will also clarify that the materiel may not be integrated with military technical systems and it may not be used for military purposes (in combat against human targets).

If the civil hand-held weapons and ammunition are to be integrated into the technical system, *section 5.6–5.8* above, will apply.

Civil Hand-Held Weapons (COTS)

Civil hand-held weapons that is available on the market (COTS) and is marked with a CIP proof mark is thereby authorized to be used according to the manufacturer's instructions. Such weapon does not require a special system safety activity. Any BOA, in respect of the demands on system safety, may be issued on the basis of the documentation that enabled the marketing of the product.

In the event that the TTEM is established for the procurement of COTS weapons, it must be specified that the procurement is for civil weapons (CIP proof marked) for civil use by the Armed Forces and that no specific system safety activity has been implemented and that the weapon is not classified as munitions.

However, it is important that the intended use of the weapon really is mainly regarded as civil. If the weapon is to be used for military purposes (in combat fighting human targets), the Ordinance on International Humanitarian Law for the Monitoring of Arms Projects (Förordningen om folkrättslig granskning av vapenprojekt) *[16]* requires that the weapon must be notified to and approved by the Delegation for International Humanitarian Law Monitoring of Arms Projects.

Civil Ammunition for Hand-Held Weapons (COTS)

Civil ammunition for hand-held weapons available in the market (COTS) and which has a CIP proof mark is therefore approved for handling in Sweden with regard to the law on flammable and explosive goods *[28]*. Such ammunition requires no special system safety activity. Any BOA, in respect of the demands on system safety, may be issued on the basis of the documentation that enabled the marketing of the product.

In the event that the TTEM is established for the acquisition of COTS ammunition, it must be specified that the acquisition relates to civil ammunitions (CIP proof marked) for civil use by the Armed Forces and that no specific system safety activity has been implemented and that the weapon is not classified as munitions.

However, it is important that the intended use of the weapon really is mainly regarded as civil. If the weapon is to be used for military purposes (in combat fighting human targets), the Ordinance on International Humanitarian Law for the Monitoring of Arms Projects *[16]* requires that the weapon must be notified to and approved by the Delegation for International Humanitarian Law Monitoring of Arms Projects.

Under IFTEX *[21]*, COTS munitions (CIP proof marked) to be stored in the Armed Forces' ammunition supplies along with military munitions always require a special military storage code (F code) which governs how military storage is allowed to take place. An F-code can be obtained by applying to the FMV.

5.11 Decision and Product Documents During Military Deployment

5.11.1 Basics

This section is applicable to all types of units and technical systems, regardless of whether the system is employed on land, sea or is airborne.

The section only refers to the provision of support for system safety considerations related to the development of provisions for units which govern the right to implement technical adjustments, temporary repairs, war damage repairs and other measures during an operation.

5.11.2 Technical Adaptation

Technical adaptation of the technical system is carried out in order to increase the chances of success in battle. Appropriate means are partly made up of improving the effectiveness of own technical systems and partly by reducing the effect of the adversary's actions. This improves the possibility of survival for own forces and own personnel.

The requirements on lead time from when a need has been identified for adaptation to its execution is usually short, which means that the regular routine for changing a configuration cannot be applied.

System safety assessment is part of the decision basis for technical adaptation.

Implementation regulations for technical adjustment should, from a system safety point of view, include:

- the right to make a decision
- minimum requirements for risk analysis, including an assessment template (e.g. see *figure 6:1*, however, one box should be red and the others green)
- requirements for decision support (past events/injury/damage/trends, alternative possible actions, the pros and cons of each option)
- minimum requirements for the documentation of implemented action
- minimum documentation requirements for the user
- to whom the report relating to the completed measure for a technical system (some individual systems) should be presented
- when and how decisions are made on the restoration of technical systems
- to whom the report should be sent with information that the technical system (some individual systems) has been restored following technical adjustment.

5.11.3 Temporary Repairs and War Damage Repair

The purpose of temporary repair and war damage repair is to provide temporary help when there is a lack of time or resources to rectify operational or battle damage on a technical system, to facilitate the resolution of an ongoing assignment, to escape a dangerous situation/area or to gain access to an area where the correct repairs can be carried out. Temporary repairs/war damage repairs are always a second choice and should only be used in situations where normal procedures/resources for corrective maintenance cannot be used. The executed repair, as soon as the situation allows, must be replaced by a method of repair with verified methods.

Temporary repairs/war damage repair can be performed by both crew (users) and technical personnel. The complexity of possible repairs differs, however, depending on the equipment and expertise. Only personnel with special training are authorized to carry out temporary repairs.

Temporary repairs are normally carried out only during international operations, and the repairs must be **acceptable** from a system safety point of view.

Battle damage repairs are carried out only during war or warlike conditions. The primary objective of the repairs is to make the technical system usable after battle damage as quickly as possible. The repair work is usually improvised, performed with unorthodox repair methods and typically includes only the minimum necessary measures (repair function and ensure protection). System safety should, if possible, be **taken** into account in the execution of war damage repair.

The result of war damage repair is often that part of the function/protection capacity has been able to be taken back.

Implementation regulations for temporary repairs and war damage repair should, from a system safety point of view, include:

- the right to make a decision
- requirements for decision support (past events/injury/damage/trends, alternative possible actions, the pros and cons of each option)
- minimum requirements for risk analysis, including an assessment template (for example, see *figure 6:1*, however, for war damage repairs, one box should be red and the others green)
- minimum requirements for the documentation of implemented action
- minimum documentation requirements for the user
- to whom the report relating to the completed measure for a technical system (some individual systems) should be presented
- when and how decisions are made on the restoration of technical systems
- to whom the report should be sent that the technical system (some individual systems) has been restored following temporary repairs/war damage repairs.

5.11.4 Other Activities

Activities other than technical adaptation, temporary repairs and war damage repairs which relate to the technical system can be given consideration, in order to increase the chances of success in battle. Examples of this could be quick adaptations made in the form of additions to a technical system.

The requirements on lead time from when a need has been identified for adaptation to its execution is usually short, which means that the regular routine for changing a configuration cannot be applied.

A system safety assessment forms part of the decision basis for such action.

Implementation regulations for "Other Action" should, from a system safety point of view, include:

- the right to make a decision
- requirements for decision support
- minimum requirements for risk analysis, including an assessment template (e.g., see *figure 6:1*), however in the event of other action, one box should be red and the others green)
- minimum requirements for the documentation of implemented action
- minimum documentation requirements for the user
- to whom the report, with regard to the completed action, will be presented
- when and how decisions are made on the restoration/disposal/continued use of technical systems
- to whom the report should be sent with information that the technical system (some individual systems) has been restored/decommissioned etc., following "Other action".

5.12 Quality Control/Design Review

5.12.1 Design Review

Before delivery of the technical system, there is normally some form of quality control. The reason for this is that DesignA must verify that the ordered product complies with technical requirements, including performance, and that the specified operational obligations have been carried out as intended.

It is equally important that documents that provide a report on system safety activities that have been carried out, including their results, are examined in a similar fashion.

The design review is carried out on a number of occasions (see *section 7.3.4, Evaluation of Suppliers*). The activity relates to the examination of documents produced in a systematic way and should always aim to show how and to what extent specified system safety requirements have been met.

A design review can be performed by anyone within a specific project.

5.12.2 Independent Design Review

In addition to a Design Review, there is also the form Independent Review. This form assumes that the person conducting the review is not associated with the project or otherwise engaged by the project ("independent").

An independent review is mainly applied in the following cases:

- When the risks associated with the area of technology can be regarded as major/serious (for example, munitions, avionics systems, strong oxidizing agents and substances that are very hostile to the environment).
- When a technical system is procured based on new technology and the share of unknown accident risks is likely to be relatively high. In this case, possible systemic risks ought to be less well known and difficult to identify.
- When a technical system is procured based on a new application of existing technology and the share of unknown accident risks is likely to be relatively high.

When however procurement is to take place of a technical system in which experience is based on previous procurement, current technology and the Armed Forces' use of similar technical systems, the proportion of unknown risk of accidents is assumed to be relatively low. Overall systemic risk can also be assumed to be known. If more of these conditions apply, the need for an independent review is considered small.

5.12.3 Design Review Report

The results of the review (both of the above types) should always be presented in a report with a separate summary which clearly shows whether the examined documents meet, or do not meet, the demands on system safety.

The report must also contain proposals for measures required in response to the findings of the review. The review report should always be attached to DesignA's SS.

6 The Armed Forces' System Safety Activities

6.1 General – Management

The Supreme Commander (ÖB) has overall responsibility for the technical systems used in the Armed Forces. First of all, the systems must have the requisite characteristics to facilitate implementation during a battle situation, and secondly, the systems accident risks must be so low that they do not cause unintentional injury to a person, damage to property or the external environment.

Requirements for the technical system's safety characteristics are described in Swedish law. Current laws and how they relate to military technical systems are reported in *chapter 2*.

The Armed Forces' Handbook on System Safety, which provides an account of the Armed Forces' system safety methodology, is designed to ensure that these laws are enforced.

To ensure that system safety methodology is applied properly, skills are required by those dealing with system safety issues. The measures implemented by the ÖB (Supreme Commander) to achieve this are specified below.

The Supreme Commander's management measures:

- Maintain and develop the specific methodology that system safety activities are comprised of.
- Designate central operators in the Armed Forces and delegate to them the responsibility for the operational safety process and the system safety process within the Armed Forces.
- Commission C SÄKINSP to come to an agreement regarding completed system safety activities and carry out inspections of the associated work methodologies (processes) and decide on regulations, instructions and handbooks for safety systems in the Armed Forces.

- Agree (usually through coordination agreements) with the supporting authority that this takes on the role of Design Manager (DesignA) for the specific area of technology and complies with the Armed Forces' regulations, instructions and handbooks for system safety and establishes and maintains a design rule book in these areas of technology over the long term.
- Choose, if necessary, a special technical centre in the Armed Forces which is particularly well qualified to also assume the role of Design Manager (DesignA) for a specific area of technology and to establish and maintain a design rule book in this area of technology over the long term.

6.2 Vision

No person (soldier, sailor, officer or civilian) will be injured by the Armed Forces' technical systems.

No property or the external environment will be damaged.

6.3 Management

6.3.1 Implementation of System Safety Activities

An instruction about the Armed Forces' System Safety handbook 2011 *[26]* specifies that for all procurement, modification, renovation and decommissioning of materiel (from 1 January 2011) a decision must be taken as to whether and to what extent the system safety activities should be conducted in accordance with H SystSäkE.

System safety operations are required for each technical system, especially those designed and developed for military use.

It is understood that a technical system also refers to a technical system that has been created through the integration of technical systems, elements from these and/or other products (this includes MOTS and COTS).

System safety requirements apply during a technical system's entire service life.

The scope of system safety activities and their degree of detail are adapted to the technical system's complexity and its estimated accident risks when the technical system is being used.

The ÄF at HKV manages and implements system safety activities during the technical system's entire service life. Control instruments include requirements that relate to the maximum allowable level of individual risk (= tolerable level of risk in the technical system and to continuously ensure that this level is not exceeded.

For technical systems the Armed Forces has in its possession, the ÄF is responsible for following up on risks and proposing and adopting risk-reducing measures. The responsibility for each technical system is distributed to the appropriate organization. The responsibility also includes maintaining the technical system's risk documentation.

The ÄF also allows for the development and maintenance of central system compliance decisions (which form the basis for a Decision Regarding Use (BOA)).

The system safety activities that are generally required at HQ for the materiel system should be analysed by the ÄF at HQ. Furthermore, the ÄF decides on the content, the distribution of responsibilities, delegations, requirement levels etc. Deliberations and decisions can be documented in a System Safety Management Plan (SSMP), which is distributed to those concerned. (See *H SystSäk E Part 2, section 5.1*, the System Safety Programme (SSP) activity that results in the SSMP.)

The system safety activity planned for one or more materiel systems or groups of materiel systems should be appropriately analysed and planned by the ÄF at HQ. The plan is called a SSMP (see above) and provides the basis for the continued control of system safety activities for the technical system in question. The plan may include support for both new procurement and maintenance.

The ÄF aligns system safety activities at DesignA, for instance by specifying demands on system safety requirements when placing an order for a technical system.

The following sections of chapter 6 describe the requirements that can be used by the ÄF when controlling DesignA.

The requirements are numbered according to the following example:

2.641.01, where 2 = H SystSäk E Part 1, 641 = a section number and the last two digits are a serial number within the section.

> The requirement number in bold is a mandatory requirement, the remaining requirements are optional. The Armed Forces can place orders where not all mandatory requirements are applicable.
>
> Optional requirements may be selected by the Armed Forces as deemed appropriate for the technical system in question.

The requirements received by DesignA are detailed in the Armed Forces' order to DesignA (customer order (KB)) or in the Tactical-Technical-Financial Objectives (TTEM). For each requirement presented here, it is specified whether this should be included in the KB or TTEM.

6.3.2 Basic Resources for the Operation of Technical Systems

Basic technical resources such as electricity, power, heating, cooling, ventilation, water and drainage are often necessary to enable the function and operation of a technical system.

For mobile technical systems, these basic resources are found mostly on the platform in question: ship, helicopter or vehicle. Mobile basic resources can also be built into a container designed for field use only, but with lower demands on mobility.

If the Armed Forces requires that the technical system should have a fixed disposition and more qualified protection, this is often satisfied through a fixed installation (building/establishment). In the installation, it is often appropriate to provide basic resources specific to the installation, such as electricity, power, heating, cooling, ventilation, water and drainage. The development of this type of resource is managed through an order from the Armed Forces to The National Fortifications Administration (FORTV), which acts on behalf of DesignA for such installations. Through early consultation with the DesignA in question (for the technical system), it is possible to ensure that, requirements are made so that these basic resources are dimensioned and otherwise have the right properties and interfaces in order to correctly support the technical system in question.

For example, the technical system is a diving chamber – for diving operations (to be procured by the Swedish Defence Materiel Administration (FMV)), which needs to be supplied with different gases in order to function properly. For this, gas systems and compressors are ordered by FORTV.

For submarine operations, a battery charging station is also required (to be procured by the FMV). In order to load and handle batteries in the installation, hoists and electrical connections are needed (overhead cranes and electrical connections are produced by FORTV).

The Armed Forces acquires the technical specifications for the technical system in question from DesignA, so that, in the order to FORTV, the requirements can be correctly specified in terms of the basic resources required. DesignA should also be encouraged to specify whether any basic resource is safety critical and which therefore needs to be rendered safe in a particular way to reduce accident risk to a tolerable level.

System Safe Requirements

2.632.01	Present the technical specification in terms of basic resources for the technical system in question so that the Armed Forces – in its order to FORTV – can order the correct properties for the basic resources for the installation from a technical point of view. (As stated in the KB.) Specify, in particular, if any basic resource is safety-critical and therefore needs to be rendered safe in a particular way.

6.4 Studies

6.4.1 General

When a programme of studies is authorized, the Armed Forces makes demands on the need for certain skills. Often several alternative concepts are developed to facilitate the modelling of a concept that can best be regarded as meeting set requirements. For these concepts an overall system safety analysis is carried out. The aim is to avoid alternatives which produce accident risks which cannot be managed safely and cost-effectively.

Over a period of many years, the Armed Forces has acquired extensive experience of accident risks in technical systems, for instance based on reports of past incidents and accidents.

System safety activities during the study phase are controlled and requirements are established so that lessons are learned from previous technical systems.

When the Armed Forces specifies its requirements, the system safety methodology forms a powerful tool which can transfer and apply previous experiences to new technical systems.

When the requirements are being specified for a new technical system, the tool requires that:

- the previous technical system's list of accident risks is incorporated into the study material
- new accident risks are identified and analysed
- the system risks are identified and proposed countermeasures are developed.

It is preferable to identify hazards and hazardous conditions early on in the study phase and to analyse their nature. To avoid a hazard or a hazardous condition is of great importance, even though access to the probabilities and exposure data are lacking in the early phases.

The risk management work will be extra effective if started early during the study phase. The goal is to create such knowledge of new system solutions in the concept stage, so that a system safety assessment can be produced and rejections can be made of options that are considered difficult to manage or are substandard from a safety point of view.

When the Armed Forces is considering different options as to how a certain capability can be materialized (system design), continuous study reports are produced for the object in question (can be part of the system specification criteria) and a thorough system safety analysis is conducted where different alternative study reports (system specification criteria) are compared. If consistently pursued, this activity leads to a high level of safety and a low cost over the intended lifespan.

6.4.2 Requirements for Study Assignments

The ÄF focuses and guides system safety activities in the implementation of the **study** or development of the **system specification criteria** for a particular function, partly by specifying the conditions and partly by establishing system safety requirements.

Prerequisites for Study/System Specification Criteria

- The technical system in which the object forms a part of as a technical subsystem.
- A function that is implemented through the coordinated extra use of a technical subsystem and products from existing technical systems (based on the principle system of systems).
- In which technical system(s) the object will, in general, form a part of and cooperate with (also during an international effort).
- How the object can be used.
- In which physical environments the object can be used.

System Safe Requirements

2.642.01	Identify the technical system's systemic risks in accordance with the general description in *section 4.2.2*. (As specified in the KB – study assignment.) In the development of this requirement, see *section 4.2*.
2.642.02	Identify and design specific system safety features/ system safety measures that can counteract the identified systemic risks. (As specified in the KB – study assignment). In the development of this requirement, see *section 6.5.3*.
2.642.03	Identify the accident risks in the technical system that has been studied. (As specified in the KB – study assignment.
2.642.04	A risk assessment should be carried out using the attached assessment template. (As specified in the KB – study assignment).

Great/Moderate means the direct damage from the hazard/hazardous condition

Difficult/Easy to manage means the opportunity to design the system so that the hazard causes only minor accident risk.

Figure 6:1 Assessment Template for the Study Phase

When conducting a realizable study, emphasis is directed at achieving functional objectives and, where relevant, choosing between competing alternative designs.

The Risk Log will be produced and include known information about the technical system and its identified accident risks (see *appendix 2*).

> Events or phenomena that were predictable even at the design phase provide experience for the majority of all accidents. Accident risks identified this early can be studied and dealt with more effectively than those that emerge later in the technical system's lifetime.

Ranking: Developed alternatives can be prioritized and ranked from a system safe perspective using the activity "System Safety Evaluation" (SSE)-S10, see *H SystSäk E Part 2, section 5.2*.

6.5 Procurement

6.5.1 General

The Armed Forces makes demands on technical systems in the TTEM. The basics and structure when determining requirements are described in H MÅL *[25]* which refers to H SystSäk E with regard to system safety requirements.

The measures to be undertaken by the Armed Forces as part of the maintenance and use of a certain technical system in order to maintain system safety, and to avoid accidents caused by risks, are regulated by instructions, handbooks, regulations, materiel descriptions and technical orders. The Armed Forces regulates the production of this information in the Customer Order (KB) to DesignA.

6.5.2 Requirements in the Customer Order (KB) relating to DesignA's System Safety Activities

The following operational requirements must be considered for inclusion when the Armed Forces establishes requirements for DesignA's system safety activities. Selected system safety requirements are included in the Armed Forces' KB to DesignA.

System Safety Requirements

2.652.01	Ensure that the supplier conducts system safety activities so that the technical system's accident risks are kept within the established level of risk so as to conform to requirements, at the same time as the requisite capability is provided. (As stated in the KB.)
2.652.02	**Military exemption** (See *section 1.2* and *2.4.1*) Ensure that in the tender the supplier provides a full account that the technical systems comply with Swedish law/regulations applicable to the technical system in question and that they include some kind of exemption for military equipment/military use/activity/equivalent. If the law/regulation provides threshold values for civil operations (equivalent) the supplier must request supplementary formation during the bidding period relating to the Armed Forces' requirements for current threshold values, so that the tender will be based on the right prerequisites. (As stated in the KB.)
2.652.03	Deliver the Safety Statement (SS) with an account of the technical system's scope and interfaces. The SS, in addition to the content as described in *H SystSäk E Part 2, appendix 1*, must also contain the following special sections: xx, yy, zz. Delivery must take place xx weeks before delivery of the technical system. (As stated in the KB.)
2.652.04	Deliver complete risk documentation in accordance with *section 5.6*. Delivery will take place in conjunction with the SS. (As stated in the KB.)
2.652.05	Deliver documentation for the training course which may be required from a system safety point of view. Delivery will take place in conjunction with the SS. (As stated in the KB.)
2.652.06	Deliver orders and instructions for use and maintenance (including support for SäkI). Delivery will take place in conjunction with the SS. (As stated in the KB.)

2.652.07	In designing the current technical system's deviation handling procedures, the Armed Forces' deviation handling system xx should be used. (As stated in the KB.)
2.652.08	The technical system's documentation should be written in Swedish and English. (As stated in the KB.) In the development of this requirement, see also *section 5.10.4* and incorporate the appropriate options for the parts of the documentation in question.
2.652.09	A special review (quality control) should be conducted of subsystem yy/product zz and should be reported with a special review report. (As stated in the KB.) In the development of this requirement, see *section 5.12* and specify the system parts/products in question.

6.5.3 Requirements for Systemic Risk

Accident risks at overall system level (systemic risk) need to be identified and requirements need to be made in terms of the appropriate protective measure which would offset the identified systemic risk.

System risk is based on the system's required capabilities that may be accidentally triggered and therefore cause harm. System risk can often be identified in response to the questions: Given the system capacity, what may this not lead to/cause/what should not happen?

The system safety requirements for the system risk in question must be specified, so that the system is given the ability to counteract this systemic risk. Such capabilities can either be designed to prevent the development of the chain of events the systemic risk consists of, or requirements may be established that a certain "safety device" must be incorporated into (as part of the design) the system's basic configuration. Such a "safety device" should

provide some significant protection features to the system, see *section 4.2.2*, under the section "System risk".

Examples of such built-in safety systems: a fighter aircraft equipped with an ejection seat; transport aircraft equipped with parachutes for the crew; ships equipped with lifeboats; combat vehicles equipped with at least two independent means of escape for the crew; automated weapons systems with time control and manual decisions/partial decisions or stand-alone automated control systems.

System Safety Requirements

2.653.01	Identify systemic risks (accident risk at system level). (As stated in the TTEM.)
2.653.02	Identify appropriate system safety measures to counteract identified systemic risks. (Either by preventing the development of the chain of events that trigger systemic risk or by designing a "safety device" into the system's basic configuration. (As stated in the TTEM.)

In the event that the identification of systemic risk and the requisite countermeasures have been initiated already during the study phase, the work described here should be based on these results (see *section 6.4.2*).

6.5.4 Requirements for Ammunition

Military Munitions

Requirements are always reported here for the procurement of military munitions (see *section 5.9*).

System Safe Requirements

2.654.01	The SS for military munitions relates to the two different properties ammunition has, partly as items of ammunition, intended for a specific type of weapon or weapons, or partly as a stand-alone transport and storage item. (As stated in the KB.)
2.654.02	H SystSäk E and H VAS-E will be applied. (As stated in the KB.) H VAS-E is the FMV's design rules relating to the ammunition's safety characteristics and design rules that comply with the requirements of international law *[16]*. *An equivalent design rulebook or standard may be accepted following the Armed Forces' inspection.*
2.654.03	*The SS for military munitions must include a review report by an independent audit function. (As stated in the KB.)*

Today's review organization at the FMV can be utilized by the Armed Forces. See *section 2.4.11*.

Through an independent review of the ammunition's design etc., the ammunition is checked so that it complies with the design rules under H VAS-E and the Armed Forces' requirements regarding risk level.

Approval of Military Munitions for Storage and Transportation

System Safety Requirements

2.654.04	Obtain approval of acquired military ammunition for the safe transport and storage, from The Swedish Civil Contingencies Agency (MSB). (As stated in the KB.)

Ammunition for Hand-Held Weapons of Civilian Standard Character (COTS)

Ammunition for civilian hand-held weapons that are available on the market (COTS) and is marked with a CIP proof mark, is therefore authorized to be used according to the manufacturer's instructions. Such ammunition does not require a special system safety activity. Any BOA in respect of the demands on system safety may be issued on the basis of the documentation that enabled the marketing of the product.

Requirements reported here can be made for assignments for the procurement of civilian hand-held weapon ammunitions that are available in the market (COTS).

System Safety Requirements

2.654.05	The acquisition will relate to COTS ammunition. Ammunition must be CIP proof marked so no special system safety activity should be performed. The ammunition should not be classified as war munitions. (As specified in the procurement decision.)
2.654.06	A special military storage code (F-code) from IFTEX *[21]* should be obtained on application to the FMV. (As specified in the procurement decision.) An F-code specifies how the storage of the Armed Forces' reserves should be carried out.
2.654.07	Approval of the ammunition must be obtained from the Delegation for International Humanitarian Law Monitoring of Arms Projects *[16]*. (As specified in the procurement decision.) The requirement is only made in the event that the Armed Forces' civil ammunition is intended to be used for military purposes (fighting human targets).

6.5.5 Requirements for Radiation-Emitting Equipment

Operators/passengers may carry radiation-emitting equipment, which may interfere with acquired technical systems. Such equipment may, for example, consist of:

- personal/private equipment such as mobile phones, GPS navigator/receivers
- military equipment with similar characteristics but with a greater effect.

This problem is dealt with most easily and most effectively by specifying which types of equipment this relates to in the TTEM and demanding that these items of equipment are subject to the appropriate system safety analyses and that they are included among the items of equipment that are reported under the SS heading: "The technical system is to be used together with …".

Such additional items of equipment of COTS character are handled in a similar fashion which may be used within the framework of the technical system (such as coffee makers, microwaves, personal computers). It is recommended that requirements are made that specified additional equipment is subject to appropriate system safety analyses and should be included among the products reported under the SS heading: "The technical system is to be used together with …".

System Safety Requirements

2.655.01	The following equipment will be used by the operators in question: xx, yy, zz. Equipment is subject to appropriate system safety analyses and should be included among the products reported under the SS heading: "The technical system is to be used together with …". (As stated in the TTEM.)
2.655.02	The following military equipment should be able to be used by the unit: mm, nn, pp. The equipment is subject to appropriate system safety analyses and should be included among the products reported under the SS heading: "The technical system is to be used together with …". (As stated in the TTEM.)

6.5.6 Requirements for a New Technical System

Prior to the acquisition of a new technical system, a number of general conditions and technical requirements must be specified, these are detailed in the TTEM/TEMU.

General conditions:

- Intended use
  - Required capability – how and what will the technical system be used for, and how it is not supposed to be used, for example, run at speeds of up to 60 km/h, not faster; a maximum load of 20 tons; to be able to carry 12 soldiers with combat equipment. Not intended for loading of general goods.

  - Requirements for endurance and operating profile (correct system safety activity must be based on intended use).
  - Who will the user/operator be? Specific requirements for user interfaces (Human Machine Interface (HMI) requirements) are listed according to the intended command and battle conditions for operators, number of operators and their intended skills.
  - Specific requirements for ergonomic design are specified with regard to the intended use and battle conditions for operators, number of operators. (For example, that the operator must be able to use a certain vehicle wearing combat equipment and a protective mask, that a weapon should be able to be operated with the operator's gloves on, the operator should be able to continue his/her work for at least two hours without a break without any "ergonomic discomfort arising".
  - Geographical environment/application environment.
- Configuration
  - What products are included in the technical system and what products should be included in the technical system.
  - What other technical systems can it be used together with, form part of a technical subsystem and work together with during, for example, an international operation?
- Requirements for a certain safety feature that counteract a systemic risk that has been identified by the Armed Forces.
- Requirements for IM characteristics related to the ammunition.
- Risk level – requirement for the accident risk level which must not be exceeded for a single copy of the system for its intended use (specified in terms of risk matrix).

Systems Safety Requirements

2.656.01	Ammunition must have the following IM features xx, yy, zz. (As stated in the TTEM.) See the Armed Forces' IM Policy or equivalent control document and basics in STANAG 4439 *[44]* and AOP-39 *[4]*.
2.656.02	The technical system's specific risk of injury/accident for an individual must not exceed the tolerable risk level according to the attached risk matrix for personal injury. (As stated in the TTEM.)
2.656.03	The technical system's specific damage/accident risk for financial loss must not exceed the tolerable risk level according to the attached risk matrix for financial damage. (As stated in the TTEM.)

Specific Aspects/Requirements for Certain Military Hand-Held Weapons

For military applications, specially procured hand-held weapons that are of civilian origin are generally CIP proof marked. This means that CIP proof-marked ammunition is automatically certified to be used in this type of weapon, but not for military use against human targets. To make this possible, it is necessary that the Armed Forces secures the approval of each specific type of ammunition to be used against a human target from the Delegation for International Humanitarian Law Monitoring of Arms Projects *[16]*.

On acquisition of specially designed and manufactured hand-held weapons that are for military use and origin, and that are not CIP proof marked, the Armed Forces may still require that DesignA certifies the hand-held weapon for CIP proof-marked ammunition on the market (of specified types and suitable calibre). This ammunition will therefore form a part of DesignA's SS.

Requirements should also be made on DesignA to produce an F-code for the ammunition types in question (see *section 5.10.9* final paragraph) and that DesignA obtains approval for each individual ammunition type from the Delegation for International Humanitarian Law Monitoring of Arms Projects *[16]* (see *section 5.10.9* penultimate paragraph).

6.5.7 Requirements for a New Configuration to Create a Certain Capability

In the event that the capacity is intended to be created through primarily *extra use* or by *reusing* technical subsystems and products that already form a part of/or have formed a part of other technical systems (according to the principle system of systems), the following must be specified in the TTEM/TEMU.

General requirements: Definition of the overall technical system and the identification of constituent technical systems and products – those that will be reused and those to be newly acquired.

System Safe Requirements

Apply most of the technical requirements that can be used for a new technical system *section 6.5.6* and the operational requirements set out in *section 6.5.2*.

6.5.8 Requirements Relating to an Integration Product

When a new technical subsystem/product (regardless of the underlying reason) is to be added to an existing technical system and this new subsystem is small, the following principle of "integration product" is applied, especially if the same product is to be integrated into several different platforms. The principle means that the actual acquisition is handled individually and that the integration is performed for one platform type at a time, through an order to the DesignA in question for the implementation of the actual integration.

The additional subsystem/product may be made up of specially developed materiel that has been purchased or provided GOTS or COTS materiel.

Requirements for the Integration of Product Characteristics

General conditions:

- Intended general use of the integration product
  - Required capability – how and for what the integration product can be used, and how it is not intended to be used (both relate to general use, not platform-specific use).
  - Requirements for endurance (operational profile).
  - Who will the user/operator be, expressed in general terms? Specific requirements for user interfaces (HMI requirements) are listed according to the intended command and battle conditions for operators, number of operators and their intended skills.
  - Geographical environment/application environment.
- Configuration

  Which platforms/other technical systems the integration can be used together with, form a part of a technical subsystem and work together with during, for example, an international operation. It is assumed here, however, that the specific adaptation to the platform is accomplished by using special adaptation equipment for the platform in a special integration order. The integration product is simply "plugged" into the adapted equipment. This product integration will remain identical regardless of the intended platform.

System Safe Requirements

Requirements should be set at a tolerable level of risk (T) to personal and financial injury/damage. Use requirements no. 2.656.02 and 2.656.03. (As stated in the TTEM.)

Requirements for Integration on a Specific Platform

General requirements:

- The requirement to develop adaptation equipment with the capacity to be able to "dock" with the integration product and "take care of" all interfaces between the platform and integration product. The adaptation equipment should be designed to form a part of the technical system the platform forms a part of.
- Specify the intended use of the integration product on the platform in question
  - Required capability – how and with what the integration product can be used, and how it is not intended to be used.
  - Requirements for endurance (operational profile).
  - Who will the user/operator be? Specific requirements for user interface (HMI requirements) are listed according to the intended command and battle conditions for operators, number of operators and their intended skills on the platform type in question.
  - Geographical environment/application environment.
- Configuration

  Within the platform in question, what other technical systems the integration product can be used together with, form part of a technical subsystem and work together with during, for example, an international operation?

System Safe Requirements

Requirements should be set at a tolerable level of risk to personal and financial injury/damage. Use requirements no. 2.656.02 and 2.656.03. (As stated in the TTEM.)

6.5.9 Requirements for Vehicles of Standard Nature (COTS)

Standard vehicles (COTS) which are approved to be included in the Military Vehicle Register (MIFOR) require no special system safety activity. Any decision to use may, with regard to system safety, be issued on the basis that led to the registration in MIFOR.

If such a vehicle is intended to be equipped with military equipment (radio stations, weaponry etc.) system safety activities must be implemented for this equipment, as well as specific system safety activities implemented for integration. (See *section 5.10.6* and requirements according to *6.5.8*.)

The following requirements can be used on assignments for the purchase of civilian vehicles that are sold on the market (COTS).

System Safe Requirements

2.659.01	The procurement relates to COTS vehicles. The vehicle must be approved via a registration inspection or specific approval for inclusion in the MIFOR, so no specific system safety activity is needed. (As specified in the procurement decision/TTEM.)

6.5.10 Ammunition for Hand-Held Weapons of Civilian Standard Character (COTS)

The following requirements can be made on assignments for the purchase of civilian hand-held weapons that are sold on the market (COTS).

System Safe Requirements

2.6510.01	The acquisition will relate to COTS weapons. Ammunition must be CIP proof marked, so no special system safety activity should be performed. The weapon is not classified as munitions. (As specified in the procurement decision/TTEM.)
2.6510.02	Approval of the ammunition must be obtained from the Delegation for International Humanitarian Law Monitoring of Arms Project *[16]*. (As specified in the procurement decision/TTEM.)) The requirement is only made in the event that the weapon is intended to be used by the Armed Forces for military purposes (in combat fighting human targets).

6.5.11 Requirements for Trivial Materiel

Simple products that are used in isolation, such as a bag, sports shoes and which are not subject to law or statute with a military exemption (see *section 1.2*) require no system safety activity. Nor should any system safety decision be developed.

In the specific case that the Armed Forces needs to make a BOA for such a simple product, the BOA, with regard to the Central Safety Compliance Decision (CSSB) requirement, may be issued on the basis that allowed the marketing of the product.

If the product needs to be incorporated into a technical system it will be examined by DesignA if the principle of "Adjusted technical system" *section 5.6.4*, can be applied before the regular system safety activity is initiated.

System Safe Requirements

2.6511.01	The procurement will relate to a COTS product. The product must be CE marked so no special system safety activity should be performed. (As specified in the procurement decision/TTEM.)

6.6 Preparing for Reception

Prior to receipt of delivery from DesignA, the ÄF prepares the supplied technical system for use. Necessary preparations include:

- Instructions for handling and care and the necessary safety regulations are developed and chosen.
- Preparing and deciding on the CSSB, which means that DesignA's SS and other system safety documentation is reviewed (see *section 7.2*).
- Deciding how accidents and incidents should be reported. Ensuring that there are rules, procedures and resources necessary to deal with these reports and that there are rules and procedures on how the required risk-reducing measures should be prepared and taken.
- Deciding on the establishment of the System Safety Working Group (SSWG-2) and specifying the organization, staffing, mission, mandate and resources. Also specifying who the group will report to.

  The SSWG-2 is designated as efficiently as possible:

  – Either according to the principle, one SSWG-2 per technical system/type of unit.
  – Alternatively, a SSWG-2 can be assigned responsibility for a number of (similar) technical systems/subsystems.

6.7 The Armed Forces' Receiving of Materiel Delivery

6.7.1 Safety Statement

The Armed Forces will review and accept the Safety Statement (SS) from DesignA, for instance by comparing it with the order and specified TTEM/TEMU requirements, before it can form the basis for the Armed Forces' CSSB, which forms a necessary partial decision of the Armed Forces' BOA.

6.7.2 Delivery of Materiel

Delivery of materiel by DesignA is of a highly diverse character in terms of scope and complexity. It can relate to anything from a single technical system of an uncomplicated nature to major equipment systems containing many types of technologies and support systems. Therefore, even the scope of the delivery procedure must be varied without any formalities being disregarded. The Owner Representative's Representative (ÄFR) implements a so-called delivery preparation for each specific delivery. Where in agreement with DesignA, the scope of the delivery procedure is determined.

The Armed Forces' list of requirements *[9]* specifies requirements in respect of different kinds of technical systems and delivery varieties. Several of the requirements relate to system safety. A particularly important requirement is that a SSWG-2 is assigned and that complete support documentation will be presented to the SSWG-2 about the technical system's accident risks.

6.8 The SSWG-2

6.8.1 Appointment

The work group for system safety during the maintenance phase, the SSWG-2, is described under the SSWG activity in *H SystSäk E Part 2, section 5.8*.

The SSWG-2 is appointed by the ÄF. A decision regarding the SSWG-2 should, as a minimum, regulate the following:

- chairman
- personnel
- responsibilities and duties
- resources
- work format (stand-alone workgroup or meeting format etc.)
- authorities
- the provision of feedback reports (when, what and to whom)
- from which operators (units, Technical Office (Tek), FMV, FömedC, suppliers etc.) reports are to be received from
- from what other sources (databases etc.) information should be obtained
- to which operators support should be provided.

6.8.2 The Focus of SSWG-2's Work

The SSWG-2 plans its operations based on the prerequisites described above and documents this in its own activities plan (SSPP/SSMP to the SSWG-2 in question):

- The focus of SSWG-2's activities should be to continuously monitor the activities of the technical system from a system safe perspective. The aim is to proactively identify common safety deficiencies and propose appropriate measures to eliminate/reduce them and therefore maintain the specified Tolerable level of risk (T).

- The SSWG-2 seeks all possible information according to the principle of "observing", i.e. without taking administrative responsibility for the final handling etc., of the reports.

During maintenance, system safety activities focus on:

- Making sure that the technical system's accident risks are always at the permissible level of risk. If a certain risk exceeds permitted levels, the SSWG-2 identifies the appropriate measures that may lead to the individual risk of accidents being reduced.
- Risk-reduction measures.
- Reviewing and monitoring incidents and accidents and keeping the technical system's Risk Log/Risk List up to date.
- Keeping SSWG-2's system safety plan continuously up to date. The plan forms a part of SSWG-2's programme explanation and work plan.

When changes in design, environment or intended use are planned, the current system safety analysis (those affected by recent changes) is re-examined to investigate possible effects on the technical system's accident risks (both new risks and those that have been dealt with before).

6.8.3 Deviation Management

When the technical system is created and developed, the technical system's accident risks are identified. However, not all accident risks can be detected (see *section 3.1*). In addition, certain new accident risks arise when being used for the following reasons:

- use other than intended
- less training than intended
- less or other maintenance than intended
- other wear and tear and ageing than expected
- unauthorized modification of the technical system.

These accident risks can make themselves felt through various types of deviations. Some are harmless and others produce accidents. To reduce the risk of accidents it is essential that all deviations are reported and analysed so that risk-reduction measures can be developed and implemented as soon as possible. It is essential that the SSWG-2 informs the operators in question of the circumstances pertaining to the technical systems following delivery and, despite comprehensive system safety activities during development and manufacture, that more unknown accidents risks may still be expected. Therefore, the operator's involvement and attention is important to identify accident risks before they lead to an incident or accident.

6.9 Start-up

To prepare for the start-up of operations, the following are checked:

- system safety-critical training instructions have been applied
- a group for system safety, the SSWG-2, has been organized and works (staffing, information, resources, see *section 6.8*)
- the BOA exists for the technical system that is intended to be used
- there is a routine for handling deviations for the technical system to be put into service
- users and technical personnel are adequately trained for their duties relating to the use of the technical system.

6.10 Operations

Technical systems can be handed over to a unit/school for use and training.

The ÄF can allocate responsibility to follow-up on risks and propose/take risk-reducing measures to the appropriate organization within the Armed Forces. The responsibility also includes maintaining the technical system's risk documentation.

It is prohibited, through local initiatives/decisions, to modify/allow any changes to such materiel. On no account may materiel be interfered with. No materiel may be added to or used in conjunction with the technical system and no parts may be removed, other than that described in the accompanying documentation. The technical system will be used and maintained in accordance with the accompanying documentation and applicable safety regulations.

Proposals for change may be made to the materiel manager of the Armed Forces HQ. During the investigation of the proposal, before any decision regarding introduction, the following, among other things, must be examined:

- costs
- effect
- additional accident risks
- realizability.

See also what is stated in *section 5.11, Decision and Product Documents During Military Deployment*.

6.11 Modification

Modification refers to a change in the technical system that affects DesignA's approved configuration.

Modification is treated as new procurement and requires complete system safety work. This will be carried out for the entire change, including all interfaces to the unchanged parts and functions of the basic system. See also *section 5.6*.

6.12 Disposal

Generally, all risks of accidents associated with disposal must be identified and taken care of. Since the Armed Forces is the owner representative of National Defence Materiel, and military materiel usually has several hidden/integrated hazards, it is very important that the Armed Forces assumes its responsibility of identifying (allowing the identification of) the accident risks inherent in the materiel in question. It is the Armed Forces' responsibility to inform (allow for the education of) the person acquiring or receiving equipment for disposal/scrapping of what these risks are and what characteristics relevant hazards have. See also *H SystSäk E Part 2 section 5.34, Risk Assessment prior to Disposal of System (RADS)*.

On disposal of a product, the Armed Forces must have first carried out a risk analysis before disposal and, based on this, formalize the disposal assignment so that it can be conducted in a safe manner.

Delimitation: The Armed Forces' routines for disposal are not affected here. Only accident risks should be handled in connection with the preparation for disposal.

6.13 Checklist for the Armed Forces' Requirements to DesignA

The checklist is used in the Armed Forces' development of requirements in the KB/TTEM. Requirements in the dark-blue fields are mandatory. The technical system's intended characteristics form the basis for selecting requirements in general.

Table 6:1 System Safety Requirements

Requirement no.	Designation	Applicability for technical system in question			Comments
		Yes	No	N/A	
Requirements for basic resources					
2.632.01	Specify the need for basic resources				
Requirements for studies					
2.642.01	Identify systemic risks				
2.642.02	Identify system safety characteristics/measures to counteract observed systemic risks				
2.642.03	Identify risks in the technical system that have been observed				
2.642.04	Risk assessment should be carried out using the attached assessment template				
Operational requirement in the KB					
2.652.01	Ensure that the supplier carries out the system safety activity				
2.652.02	Military exemption Ensure that the supplier requests supplementation for the Armed Forces' requirements with regard to current thresholds				
2.652.03	Deliver SS The SS must also contain xx, yy, zz				
2.652.04	Deliver complete risk documentation				
2.652.05	Deliver a basis for training				

Requirement no.	Designation	Applicability for technical system in question			Comments
		Yes	No	N/A	
2.652.06	Deliver a basis for regulations and guidelines				
2.652.07	Deviation handling routines apply the Armed Forces' deviation handling system XXXX [name of system				
2.652.08	Language of the system's technical documentation				
2.652.09	Special review				
TTEM requirements - systemic risks					
2.653.01	Identify systemic risks (accident risk at system level)				
2.653.02	System safety measures to prevent systemic risk				
Requirements for military munitions					
2.654.01	The SS for military munitions relate partly to ammunition items and partly as stand-alone transport and storage objects				
2.654.02	H SystSäk E and H VAS-E should be applied				
2.654.03	Review report from an independent review organization				
2.654.04	Approval from MSB regarding safety for transport and storage				
Requirements for civilian ammunition					
2.654.05	COTS munitions to be CIP proof marked				
2.654.06	A storage code (F-code) must be obtained from the FMV				
2.654.07	Approval from the Delegation for International Humanitarian Law Monitoring of Arms Projects, if the Armed Forces intends to use the ammunition for military purposes				

Requirement no.	Designation	Applicability for technical system in question			Comments
		Yes	No	N/A	
Technical requirements in the TTEM – radiation-emitting equipment					
2.655.01	Equipment xx, yy, zz should be covered by the SS				
2.655.02	Military equipment etc., nn, pp should be covered by the SS				
Technical requirements in the TTEM for new technical system					
2.656.01	Ammunition should have IM features xx, yy, zz				
2.656.02	Accident risks for a person according to the attached risk matrix for bodily injury				
2.656.03	Accident risk for financial damage according to the attached risk matrix for financial damage				
Requirements for standard vehicles, in the procurement decision/TTEM					
2.659.01	The vehicle must be approved via registration inspection or special approval				
Requirements for civilian hand-held weapons, in the procurement decision/ TTEM					
2.6510.01	The weapon must be CIP proof marked. The weapon should not be classified as munitions				
2.6510.02	Approval from the Delegation for International Humanitarian Law Monitoring of Arms Projects, if the FM intends to use the ammunition for military purposes				
Requirements for trivial materiel, in the procurement decision/TTEM					
2.6511.01	The product must be CE marked				

7 System Safety Activities – Design Responsibilities

7.1 The Armed Forces' Overall Requirements of DesignA

7.1.1 DesignA's Organization

DesignA must identify at least one officer/member of staff responsible for controlling and managing system safety activities for the materiel/service which it produces when ordered by the Armed Forces. The officer/member of staff signs DesignA's Safety Statement (SS).

7.1.2 Delivery to the Armed Forces

The Armed Forces requires that DesignA (usually in advance of delivery of the technical system) delivers a full description of the implemented system safety activities, with a detailed account of the risks that remain in the technical system.

7.1.3 Involvement in the Armed Forces' System Safety Activities

The Armed Forces expresses its requirements on DesignA's participation in the Armed Forces' system safety activities in a reciprocal coordination agreement or when placing an order for a technical system or if changes are made to the existing technical system. Such participation relates to the production, use, maintenance and disposal of the Armed Forces' products and technical systems, but can also include direct management support.

7.1.4 Long-term Planning of System Safety Activities

It is appropriate that DesignA, in a System Safety Management Plan (SSMP), documents the suggestions and decisions regarding the organization and delegation of work related to DesignA's system safety activities. It is also appropriate in the SSMP to present an analysis report of the coordination agreement with the Armed Forces regarding system safety and the commitments DesignA has made. The SSMP should also comment on decisions taken regarding work methods, templates etc., to be used internally by DesignA. (See *H SystSäk E Part 2, section 5.1*.)

7.2 The Armed Forces' Demands on DesignA when Commissioned with an Assignment

The Armed Forces' system safety requirements in terms of KB and Tactical-Technical-Financial Objectives (TTEM) are cleared of conflicting requirements and formulated so that they are measurable. The requirements are then translated into supplier requirements and outlined in the Request for Proposal (RFP) before being put into in the contract relating to the order. (See *H SystSäk E Part 2, section 5.4*.)

7.3 System Safety Activities

7.3.1 Receipt of the Assignment

For received assignments relating to procurement (where applicable, the study, modification, renovation and decommissioning) of certain technical systems, DesignA carries out system work whereby the need for system safety activities are analysed.

The points below serve as a checklist for this analysis:

- Perform the initial project review with the Project Manager (PL). All of the Armed Forces' system safety requirements are analysed in the documentation relating to the order: the customer order, TTEM and other relevant documents describing the expected performance and the product from a systems

safety perspective (see *section 5.3*). For example, requirements for the special safety design of technical systems (product requirements).

Produce an audit report of the results of the conducted analysis.

- The audit report is communicated to the Armed Forces for possible amendment/supplementation by KB and TTEM.
- Design requirements for both DesignA internally, and for the RFP to suppliers.
- Identify what the technical system consists of and identify a possible break-down into appropriate technical subsystems, and identify possible deliverables.
- Decide for each level of system integration, within the framework of "the entire technical system that has been procured", who will be responsible for this integration and how integration should be verified. (If integration is not ordered from the supplier, all of the integration duties remain the responsibility of DesignA.)

7.3.2 Invitation to Tender – Order

With the production of the RFP, DesignA must always implement the following system safety activities:

- Transform identified system safety requirements in the RFP. Design requirements (technical requirements and operational requirements) to carry out the procurement of each technical system component (based on the Armed Forces' received objectives and requirements).
- Make demands on operations which the supplier must implement (see *H SystSäk E Part 2, section 5.2.4*, for examples of requirements).
- Establish requirements for an independent audit to be performed and assign an organization to this (see *section 7.5*).
- Establish requirements as to which safety reviews must be undertaken and when.

- Specify who has the right to close the risk at a certain level and how this should be reported with DesignA.
- Produce the tender information, where the above-identified requirements are made on the supplier with regard to system safety activities, system safety documentation and system safety characteristics inherent in the technical system.
- Evaluate bids received in terms of the requirements, with a view to identify any deviations.
- Obtain a report on the completed evaluation of bids.

7.3.3 Management of the Project

DesignA manages the project's system safety activities. Possible activities include the following:

- Plan DesignA's system safety activities for the current assignment so that the Armed Forces' established requirements for DesignA's system safety activities are met. Document the planning carried out in DesignA's own SSMP (see *H SystSäk E Part 2, section 5.1*).
- Appoint a System Safety Working Group (SSWG-1) in support of the Project Manager (PL). Exceptions can be made for the simplest procurements where the PL can account for the operations in question.
- Assign special expertise.
- Establish requirements for an independent review to be performed and assign an organization to this (see *section 7.5*).

7.3.4 Evaluation of Suppliers

DesignA controls the supplier's system safety activities by:

- Conducting safety reviews with the supplier.
- Continuously examining the supplier's system safety activities. Establish, if necessary, a record of the observed deviations.
- Continuously review system safety documents that are received from the supplier.
- Establish a detailed report (see *section 5.12* and *7.5*).

7.3.5 Delivery to the Armed Forces

The delivery (of technical systems, services) must be accompanied by commissioned documentation. The following steps should be taken:

- Produce DesignA's SS based on the supplier's Safety Compliance Assessment (SCA), all of the inspection reports produced by DesignA and other system safety activities implemented by DesignA. A summary of DesignA's audit reports is outlined in the SS in the section: "Implemented system safety activities".
- Produce an audit report from an independent auditing organization (internal or external to DesignA) when requested to do so by the Armed Forces or when the technical system consists of or contains ammunition (see *section 6.5.4*).
- Prepare and carry out the handover to the Armed Forces of the product/technical subsystem/technical system that has been procured.

Adaptation

DesignA's system safety activities should be routinely adapted, see *H SystSäk E Part 2, section 3.2*.

The basis for adapting system safety activities for a certain project is the prevalence of accident risks which DesignA feels can arise in the technical system in question during its development, or is of the opinion that it may be inherent in the technical system to be procured, depending on the function intended – technical content, complexity etc. Adaptation of the system safety activities is carried out by adjusting and allocating resources, imposing special requirements on the PL's system safety activities and setting specific requirements for suppliers.

Supplier

DesignA must ensure that the contracted supplier meets the requirements that have been set.

If the supplier (bidder) cannot satisfy all of DesignA's specified requirements, the supplier may submit a tender via a subcontractor.

If no bidder is found that meets all the requirements, DesignA can nevertheless make use of one of them, provided that DesignA ensures that requirements are met.

Miscellaneous

This handbook does not regulate DesignA's internal delegations or work procedures with regard to the implementation of system safety activities. (That is, the handbook *does not control how* the activities are conducted, but rather, *what* DesignA should implement.)

7.4 SSWG-1

7.4.1 Decision Regarding SSWG-1

The system safety working group (SSWG), as support for the procurement project SSWG-1, is described in *H SystSäk E Part 2, section 5.8*.

SSWG-1 is established by DesignA. A decision regarding SSWG-1 should regulate the following:

- chairman
- personnel
- assignments
- resources
- responsibilities
- work forms (contact routes, frequency of meetings, location etc.)
- the provision of feedback reports (when, what and to whom).

7.4.2 Focus of SSWG-1's Work

SSWG-1 plans its operations based on the prerequisites described above and keeps a record of this in its own activity plan (Safety system Programme Plan (SSPP) for the SSWG-1 in question):

- The focus of SSWG-1's activities should be to provide continuous support to the PL's procurement operations with regard to system safety activities. Under current activities with the technical system, SSWG-1 works by focusing on the proactive identification of prevailing safety shortcomings and suggests requisite measures in order to eliminate/reduce these to achieve and maintain an acceptable level of safety.
- Where appropriate, SSWG-1 contributes supplier reports for the project and also provides system safety expertise.
- SSWG-1 monitors the technical system's hazards on a continuous basis during the procurement period to ensure that hazards are within a Tolerable Level of Risk (T). If a certain level of risk exceeds the T SSWG-1 will monitor and ensure that the supplier identifies and proposes appropriate measures that can reduce this to a T.
- SSWG-1 monitors the technical system's Risk Log/Risk List to ensure the supplier continuously updates the information.
- Keeps SSWG-1's SSMP continuously up to date. The plan makes up SSWG-1's programme explanation and work plan.

7.5 Independent Audit

7.5.1 Basics

For the basics regarding auditing and independent auditing, see *section 5.12* and *6.5.4*.

7.5.2 Focus on and Time for Independent Auditing

The purpose of the independent audit is to ensure that the necessary and required standard system safety activities are carried out on:

- all of the technical systems' constituent technical systems and technical subsystems
- overall systemic risks.

Independent auditing is primarily a methods and quality analysis, not a specific risk analysis. The purpose is to ensure that the system safety methodology has been applied correctly and has covered all parts of the technical system.

With regard to the overall systemic risk, the purpose of carrying out an independent review is to ensure that the identification and handling of global risks have been implemented and the resulting systemic risks have been managed in an effective manner.

Independent audits are, in principle, carried out in two separate phases, and therefore with partly different orientations:

- Initially (early phase) as a support for the PL before determining DesignA's internal SSMP.
- In the latter part of the acquisition project (later phase) when it can be shown how the system safety activities have been carried out and results have been received and can be demonstrated.

Early Phase

The following features should be checked:

- The project's current SSMP.
- Does the data from the Armed Forces include a description of possible system hazards and their origin?
- Does the project have its own documented analysis of the possible systemic risks?
- Is the total technical system correctly described?
- Are all of the technical subsystems, directly under the overall technical system level, have been correctly described?

Later Phase

The following features in the technical system should be checked:

- The project's SSMP is implemented.
- The Risk Log is correctly executed, among other things, and that each individual accident risk is resolved (= closed).
- System safety activities for all technical subsystems.
- System safety activities for the interaction between constituent technical subsystems.

Implementation of an Independent Audit

Independent auditing of the required project/product documents are carried out in support of DesignA prior to a decision on the SS.

In order to implement an independent audit it is necessary that the following activities are undertaken and kept up to date:

- Specific members of staff with appropriate skills (expert personnel) are appointed, including an audit leader.
- Routines are developed to identify which material has to be audited, how the audit report will be designed, the chain of command for determining the audit report etc.
- A routine for how the audit should be managed must be developed as a template for the audit report.

7.6 Handover of the Technical System to the Armed Forces

7.6.1 Deliverables

The person responsible for the design of the technical system delivers the following system safety documentation:

- Safety Statement (SS)
- Safety Compliance Assessment (SCA)
- System Safety Report (SAR)
- a report from an independent audit, if required
- the Risk Log, with a risk status for each individual accident risk.

7.7 DesignA's Mandate and Responsibility for Change

DesignA has, on assignment from the Armed Forces, full responsibility to design a technical system in a safe manner. This responsibility must encompass the technical system's entire life. This means that only DesignA, as instructed by the Armed Forces (see *section 5.2, Technical Design Responsibility*) has the right and obligation to amend the technical system's configuration.

Through the SS and the Central Safety Compliance Decision (CSSB) a technical system is defined, with regard to content and how it is used.

- The basis of the decision is described in *section 5.6, Decision and Product Documents for a Technical System*.
- It is DesignA's responsibility, as instructed by the Armed Forces, in a special decision to regulate any legal right ÄFR has to decide on the adjustment of the technical system within DesignA's assigned area of responsibility. The type and extent of such decisions will be governed in the decision. Requirements for feedback to DesignA is also regulated here and how configuration management and documentation should be handled is also outlined.

- Note that in the event that the Armed Forces undertakes to make a change of the technical systems without consultation with DesignA, the previously issued SS which forms the basis for the Decision Regarding Use (BOA) is cancelled and the responsibility for the technical system's system safety returns to the Armed Forces (see *section 5.1*, paragraph *f*).

8 System Safety Operations at Units/ Schools/Centres

8.1 Overall Responsibility

Risk awareness must always characterize the activities relating to the use of technical systems in times of peace, during wars, in combat and during international efforts.

The responsibilities of commanding officers for system safety activities:

- Identify and implement all the local arrangements which make it possible for the military unit to make use of the technical system within the context of BOA and the requirements that have been specified that relate to a specific accident risk.
- Train officers to the required knowledge and skill levels. Special consideration is to be given to knowledge of the technical system in force with regard to the SäkI conditions (the Armed Forces' Safety Instruction for Weapons and Ammunition etc.,) and any restrictions.
- Organize and train staff about the special handling rules necessary for the existing accident risks, which are to be maintained at the required level; and educate staff on how to produce a deviation report.
- Identify and establish contact with the current System Safety Working Group (SSWG-2).
- Ensure that assigned technical systems are not exposed to locally initiated/agreed changes.

8.2 Overall Objectives

Based on the Armed Forces' central objective of a system safety programme, no person (soldier, officer or civilian) will be injured by the technical systems that are operated – it is the commanding officer's responsibility to monitor and manage activities so that this objective is achieved.

8.3 Management

The commanding officer monitors events, as part of their operational responsibilities, to ensure that:

- Only technical systems are used for which a Decision Regarding Use (BOA) is taken.
- Technical systems used in this manner are specified in the BOA.
- Incident reports are written according to established rules.

The following local measures are permitted within the framework of a valid Central Safety Compliance Decision (CSSB) and BOA:

- Use of other approved configurations, such as loading or arming options.
- Maintenance procedures that do not change (by DesignA) the permitted configuration of technical systems.

9 Testing and Experimental Activities

9.1 Background

This section clarifies what applies in terms of protective responsibility when (temporary) personnel are on loan from the Armed Forces to work at the supplier/DesignA or when work is carried out at a common workplace.

9.2 Work Environment Responsibility for Testing and Experimental Activities

9.2.1 Regulations

The following regulations cover the situation where work is done at a common workplace or if the Armed Forces provides personnel to the supplier/DesignA who then carry out tests on behalf of the Armed Forces:

- The Work Environment Act (AML), including chapter 3, section 12, section 7, section 2, section 3 *[5]*.
- The Working Environment Authority's (AV's) Regulations.
- Rules for Naval Operations (RMS-G) *[36]*.
- The Armed Forces' Safety Instruction for Weapons and Ammunition etc., (SäkI G) *[22]*.

9.3 Agreement

An agreement must be written between the Armed Forces and the supplier/DesignA if they borrow/make use of personnel from the Armed Forces or when work is carried out at a common workplace. This agreement may embrace:

- intended activities in general
- which activities the Defence Forces and DesignA's personnel may be instructed to do/participate in
- technical systems, status, risk and safety regulations
- any requirement that DesignA should issue a safety certificate for a technical system and its intended use and operation
- requirements that the Armed Forces' Safety Inspectorate comes to an agreement regarding the safety certificate before beginning operations
- time conditions
- current individuals and their organizational domicile.

NOTE: Safety certificates relate to the ship's technical system. The equivalent for other technical systems is known as a safety statement for testing (see *H SystSäk E Part 2, section 5.31.2*)

9.4 Sea Trials Command

Sea Trials Command (PTK) is governed by the following documents:

- RMS *[36]*.
- The Coordination Agreement between the Armed Forces and the Swedish Defence Materiel Administration (FMV) *[40]*.
- Clarification of requirements for system safety documentation when testing vessels *[23]*.

Details are otherwise shown in the *H SystSäk E Part 2, section 5.31.2* (System Safety Certificate for the technical system for vessels before PTK).

Appendix 1 Risk Appraisal

This appendix aims to provide a detailed description of the operational risk appraisal and provide an in-depth supplement to *section 4.2.3, Risk Appraisal* of the handbook.

Basics of Individual Accident Risk

Risk appraisal begins by identifying the consequences of any known accident risk. Basically, accidents can be considered to have an infinite number of different injury outcomes (consequences). This is evident in studies of a number of regular car accidents that have occurred under comparable conditions. We can note here a wide variation in the number of deaths and injuries of varying severity.

This large variation forms the basis of the challenge which operational risk appraisal will be dealing with – that is, to be able to estimate the impact/consequences to be expected from an identified accident risk and to do this before a larger number of accidents have occurred.

In *table A1:1*, below, examples of some common hazards and hazardous conditions are listed. Against each example of a hazard/hazardous condition is a list of objects that could be used to provide protection as well as the types of accidents that could happen and the expected consequences. The examples demonstrate how an assessment of the worst and most likely or most probable consequence ("outcome as a consequence of the accident") can be made.

If the percentages for the risk elements "worst possible" and "most likely" in *table A1:1* are summarized, it can be seen that for several of the example accidents significant aspects of each incident in terms of the consequences are not taken into account. It can also be seen that death is seldom the most likely result. This means that the risk analyst cannot apply a general method when selecting a certain outcome element.

This therefore results in an incomplete comparison between all of the hazard risks associated with a system, which means that effective risk-reduction work is made more difficult.

Table A1:1 Examples of Commonly used Injury Outcomes

Hazard/hazardous condition	Hazardous event	Exposed	Accident	Injury outcome	
				Worst possible	Most probable
Potential energy of an object or ice on a radio mast	Object or ice falls from the radio mast	Civilians or employees	Object or ice hits a person	Death 1%	Negligible injury 70%
Chlorine gas containers	Chlorine gas emissions	Civilians and employees	People are poisoned	Death 5%	Negligible injury 65%
Kinetic energy in a car and the people in the car	Inattention	Car with driver and passenger	Collision with objects or other cars	Death 5%	Less serious injury 50%
Kinetic energy in an aircraft and its occupants	Loss of radar coverage in the management of air traffic	Aircraft with crew and passengers	Collision with the ground or other aircraft	Death 90%	Death 90%
Own weapon	Mutilation of IFF data (IFF -identification of friend or adversary)	Own plane	Own/allied personnel under fire (friendly fire)	Death 70%	Death 70%

Common ways to evaluate the size of a certain accident risk include trying to evaluate the likelihood that an accident occurs and which results in the worst possible accident outcome, usually death ("worst credible event"), and to evaluate the likelihood that the accident occurs and results in the most likely accident outcome ("most credible event").

Given the wide range of outcomes of accidents, a few standard injury classes need to be defined in order to make the analysis of the entire outcome for a particular accident possible.

The following injury classes will apply to personal injury:

- death
- serious (bodily) injury
- less serious bodily injury
- negligible personal injury.

A similar breakdown is used in the Swedish Rescue Services Agency's "Evaluation of risk" *[48]*.

Below is a comprehensive description of how an accident outcome can be described. *Table A1:1* above, provides the most common examples of "Potential energy of objects or ice on the radio mast". The example is now extended as follows.

In the country there are a considerable number of permanent radio masts. Different objects can come loose and fall from a mast, partly in connection with maintenance work and partly as a result of weathering. Also, the possibility of icing on the masts and their guy lines is well known, and may give rise to a negligible risk to people and property in the vicinity of the mast. The severity of an accident of this type depends on how high the radio mast is and what falls off.

Figure A1:1 Warning Sign

Based on these factors, an evaluation can be made as to how the consequences may be distributed between the four injury classes. Where possible, this type of assessment will be based on available accident statistics from the area in question or the surrounding area.

The mast owner's risk-reducing measures consists of, among other things, an assessment of the risk area and to put up warning signs, as shown in *figure A1:1*. With these additions, an assessment can be made of an accident's entire outcome expressed in terms of the four injury classes. See the example in *table A1:2* below.

Table A1:2 Example of Accident Risk per Injury Class

Distribution of probabilities for a given outcome	Injury class	Risk probability for the injury class in question
In 1 case in 10 it leads to:	Death	1%
In 2 cases in 10 it leads to:	Loss of body function (e.g. amputated leg, loss of vision or hearing)	5%
In 2 cases in 10 it leads to:	Broken bones	24%
In 5 cases in 10 it leads to:	Negligible injury	70%
	Total risk (%)	100%

The examples in *table A1:2* demonstrate the possibility and necessity of evaluating the entire accident's accident outcome for each individual accident – this can be roughly distributed among the previously reported injury classes. (It should again be repeated that these injury classes are only a very rough approximation, but a necessary simplification of reality.)

Below, in *table A1:3* previous examples demonstrate (from *table A1:2*) how the injury outcome can be distributed among the various injury classes.

Table A1:3 has now been fully accounted for; all constituents outcome elements (i.e. 100% are reported). But the figures that appear in Table B1:1 only show one distribution of the assessed injury outcome in terms of risk classes, given that the accident actually occurs. There is no assessment of the likelihood that an accident will actually occur. In order to identify an accident's risk value, an estimate of the probability of the accident itself is also required, in other words, how often it will occur in relation to the service life of the system or some other appropriate interval (e.g. per year, per 100 rounds, per 1,000 flight hours). If it has been assessed that the accident occurs less than once per selected inter-

val, the correct term is accident "probability" of an accident occurring. If an accident occurs more than once during the selected interval, the correct term is accident "frequency". Mathematically, there is no difference when dealing with these terms.

An accident risk value expressed per shot/round may be converted into accident risk per year; in the operational profile, you need to identify how many shots are going to be used each year and then multiply this accordingly.

Table A1:3 Examples of Commonly used Injury Outcomes

Hazard/hazardous condition	Hazardous event	Exposed	Accident	Outcome elements
Potential energy of an object or ice on a radio mast	Potential energy of an object or ice on a radio mast	Civilians or employees	Object or ice hits a person	0.01 dead 0.05 seriously injured 0.24 minor injury 0.7 negligible injury
Chlorine gas containers	Chlorine gas emissions	Civilians or employees	People are poisoned	0.05 dead 0.1 seriously injured 0.2 minor injury 0.65 negligible injury
Kinetic energy in a car and the people in the car	Inattention	Car with driver and passenger	Collision with an object or other car	0.05 dead 0.1 seriously injured 0.5 minor injury 0.35 negligible injury
Kinetic energy in an aircraft and its occupants	Loss of radar coverage in the management of air traffic	Aircraft with crew and passengers	Collision with the ground or other aircraft	0.9 dead 0.1 seriously injured 0.0 minor injury 0.0 negligible injury
Own weapon	Mutilation of IFF data (identification of friend or adversary	Own flight	Own/allied personnel under fire (friendly fire))	0.7 dead 0.1 seriously injured 0.1 minor injury 0.1 negligible injury

Based on the first example in *table A1:1* "Potential energy of an objects or ice on the radio mast", a further extension to describe the relevant parts of this accident is carried out here, this is needed to identify how often such an accident could occur.

The height of the mast has been previously mentioned along with the shape of the object and the ice (size, form etc.). Based on these factors, an evaluation is made with regard to the consequences.

Data is now required which describes how often the hazard is expected to occur (see *table A1:2*), and how often it can be triggered by a "contributing factor" and its "triggers", respectively, and how often a hazardous condition may exist.

The example refers to a fixed radio mast in the countryside. Various objects (which thereby constitute a hazard/hazardous condition) can, throughout the year, come loose from the mast and fall off. People and the property under the mast and its guy lines are therefore exposed.

In addition, objects might become detached from the mast and its guy lines and fall off.

Assumptions about the Accident

Reported figures are very rough assumptions and are designed to provide a base point regarding how the problem can be identified, assessed and calculated (see *section 4.2.1.*):

- Objects break loose from the mast due to weather phenomena or are lost during maintenance, approximately once per year.
- Ice forms on the mast 20 days per year and falls off, on average, every 4 days.
- It is estimated that a person may be found under a mast a total of one day each year.
- It is estimated that the radio mast is not expected to cause significant damage to the external environment.
- Property that is worth protecting is found under the mast for a total of one half day per year.

Calculation for Personal Injury

1 + (20 × 25%) = objects and ice falling six times per year.

As assumed above, a person is exposed for one day per year. The probability of an accident involving injury to a person therefore becomes:

$6/365 \times 1/365 = 5 \times 10^{-5}$, per radio mast and year.

That is, there is an accident every 20,000 years and per radio mast, with the risk of some personal injury.

Note, however, that the example presented does not claim to be numerically representative and intends to highlight the results of a risk analysis regarding the actual risk of injury **before any risk-reducing measures have been taken!**

Estimation of Personal Risk

Relating to an individual accident: "Someone will be exposed to falling objects or ice", the reasoning immediately above means that we can produce a figure as to the likelihood of an accident occurring. According to the above calculation, an accident happens involving some form of injury, each year and for each mast, with a probability of ($p = 5 \times 10^{-5}$).

From *table A1:2*, the estimated distribution as a percentage of the accident's four different standardized injury classes can be seen, i.e. an estimated value of the likelihood of injuries occurring, corresponding to each of the four types of injury being able to occur, given that an accident occurs.

In *table A1:4* below, this shows how an accident with a probability of p = 0.00005 is reported for an injury to a person and per injury category (also called sub-risk) when data in accordance with *table A1:2* is used.

Table A1:4 Examples of Complete Injury Outcomes per Injury Class

Injury class	Assessment of the injury class's share of the total outcome	Probability of a specific injury outcome per injury class, per radio mast and year (= sub-risk).
Death	Occurs in 1 case in 100 = 1%	$5\times10^{-5}\times0.01 = 5\times10^{-7}$
Serious injury	Occurs in 5 cases in 100 = 5%	$5\times10^{-5}\times0.05 = 2.5\times10^{-6}$
Less serious injury	Occurs in 24 cases in 100 = 24%	$5\times10^{-5}\times0.24 = 1.2\times10^{-5}$
Negligible injury	Occurs in 70 cases in 100 = 70%	$5\times10^{-5}\times0.70 = 3.5\times10^{-5}$

Average Use

In order to identify what the risk is of an accident occurring with a given technical system, the environment in which it is used and the intended degree of usage must be specified. When the Armed Forces acquires a technical system it also specifies the intended operational profile. It is in reference to this operating profile that the designer designs the technical system.

If, instead, the Armed Forces for a particular foreign operation uses a technical system designed with an operational profile for defence against invasion (regular training and a time-limited war), the accident risks that may arise during continuous use over a full year are expected to be of a different nature and could possibly occur with a different frequency. In a worst-case scenario this will occur more frequently and with more serious consequences than previously anticipated. The problem is addressed by developing a new system safety decision for its intended use.

Estimation of Environmental Risk

Risk of damage to the external environment may result in repairable damage or damage which totally destroys a species or permanently destroys a certain geographic area. Risks of repairable consequences can be estimated in monetary terms. A hazard risk that is expected to lead to permanent environmental effects always requires, in each case, a special decision from the Armed Forces, see *section 4.2.3*.

Estimate Based on Financial Damage

1 + (20 × 25%) = ice falling six times per year.

As assumed above, valuables are exposed for half a day per year.

The probability of an accident involving injury to a person therefore becomes:

$6/365 \times 0.5/365 = 2 \times 10^{-5}$ per radio mast and year.

That is, there is an accident resulting in the risk of some type of personal injury every 50,000 years and per radio mast.

Note, however, that the example presented, first, does not claim to be numerically representative and, second, intends to highlight the results of a risk analysis regarding the actual risk in terms of financial damage **before any risk-reducing measures have been taken!**

Appraisal of Financial Risk

In this handbook, risk of financial loss is considered to consist of:

- direct damage to or loss of materiel, subsystems and systems
- damage to another person's property
- cost for remediation/sanitation of damage to the external environment that the Armed Forces has caused by its activities with the system in question.

Just as a person-related accident results in all its parts needing to be identified and sorted into different injury classes, the same has to be done for financial damage.

Financial damage classes are defined by first identifying the worst possible outcomes. Then the total outcome space is divided up into four damage classes of equal value (see the example below on how the allocation of values is carried out for the four damage classes).

For example, for objects and ice falling from the radio mast, the worst possible damage could be assessed as ending up in the order of a few hundred thousand Swedish crowns (SEK), whereby the four damage classes could be assigned the following values:

- more than 100,000 SEK ($\geq 10^5$)
- 10,000–100,000 SEK (10^4–10^5)
- 1,000–10,000 SEK (10^3–10^4)
- less than 1,000 SEK ($\leq 10^3$).

For another example, where really serious accidents are expected to occur, the worst possible outcome could end up in the billions (property damage, damages related to a third party and the costs of cleaning up and restoring the environment), the four damage classes could be assigned the following values:

- over 1,000,000,000 SEK ($\geq 10^9$)
- 10,000,000–1,000,000,000 SEK (10^7-10^9)
- 100,000–10,000,000 SEK (10^5-10^7)
- less than 1,000 SEK ($\leq 10^3$).

(Principle: The ratio between two comparable damage classes is always constant.)

These damage classes are used on one axis with the same accident probabilities on the other axis as for personal injuries.

Table A1:5 Examples of Damage Outcomes for Financial Damage

Damage class	Damage in monetary terms (SEK)	Assessment of the damage class's share of the total outcome	Probability of a specific damage outcome per damage class, per radio mast and service life
I	SEK 1,000,000	Occurs in 1 case in 100 = 1%	$2\times10^{-5}\times0.01 = 2\times10^{-7}$ for damage (to an environment)
II	SEK 100,000	Occurs in 5 cases in 100 = 5%	$2\times10^{-5}\times0.05 = 10^{-6}$ for damage (1 in 100,000)
III	SEK10,000	Occurs in 20 cases in 100 = 20%	$2\times10^{-5}\times0,2 = 4\times10^{-6}$ for damage (1 in 10,000)
IV	SEK1,000	Occurs in 740 cases in 10 = 74%	$2\times10^{-5}\times0,74 = 1,5\times10^{-5}$ for damage (1 in 1,000)

It is worth emphasizing that the figures in the above example are assumptions and relate to the situation before risk-reducing measures are taken.

Methods for Risk Appraisal

Empirical Appraisal

Procedure

Empirical data from similar (existing own/existing other's/decommissioned) systems with similar uses are adapted and applied.

Disadvantages

Can be difficult to find data from similar systems, as listed above.

Transformation and adaptation of data is difficult.

Benefits

If accurate and adequate data are available, it is a simple method.

Calculation

Procedure

Based on a detailed knowledge of the system, each individual accident risk is calculated, for instance with the use of fault trees.

Disadvantages

Fault trees are often complex and require extensive knowledge of the detailed components and subsystems' internal relationships, so this method is often cumbersome to implement.

Benefits

This method is often applicable and provides good value for the known technical system, provided that it is relatively small. External factors, such as handling and the environment in which it is used, are incorporated into the fault tree in a clear manner, the estimated probabilities are assigned and this results in a comprehensive figure which relates to the technical system's hazard risk.

The risk-reducing measure reuses all parameters, except for the property that is improved, which together lead to more accurate assessments.

Expert Appraisal

Procedure

A person with very detailed knowledge of the system's characteristics and its use prepares the appraisals and assigns the numerical values.

Disadvantages

It is difficult to find experts with adequate knowledge. It is difficult to repeat the appraisal made when it tends to be relatively dependent on an individual. It is sometimes difficult to ensure aligned documentation when this also tends to be relatively dependent on an individual.

Benefits

A simple and rapid method with good credibility and relevance.

Modelling/Simulation

Procedure

Modelling and simulation means that the current system is illustrated with the use of a model in which different functions are assigned numerical values.

Disadvantages

It can be noted that all assessments are predictions of the future, they are not truths (see *4.2.1*), and that evaluations expressed as figures are still only predictions.

All models (for example in respect of a particular risk) are, by definition, incorrect because they focus on the essential relationships that describe a particular accident. All other factors that surround a possible accident are demarcated. The reason for this is that the model would otherwise be too difficult to manage and assess. But some models are actually correct and offer a good description of real-life situations. However, it is difficult to know which model happens to be correct before the accident occurred.

Benefits

The advantage of modelling and simulation is that you can, in theory, repeat an accident sequence infinitely examining various risk-reducing measures in order to find the measure that gives the best risk reduction at the lowest cost. If a skilled engineer performs the activity early on in the design phase, good quality can be obtained with regard to a risk-reducing effect in relation to the change made. At the same time, there will be a higher quality of both the risk analysis and the assessment of the value of the various risk-reducing measures – and since the simulation is carried out early on in the project, the measure is relatively inexpensive and therefore effective.

Both past experience from previous systems, fault trees and expert appraisals can be used in conjunction with modelling and simulation in order to provide better input data for modelling.

Appendix 2 Risk Log

Background

MIL-STD-882C has considerable shortcomings with regard to instructions as to how the documentation of an accident risk should be carried out and examples of suitable structures for the design of suitable documentation. Nevertheless, the standard requires a full risk analysis. The only guidance in this respect consists of a general reference to U.S. templates from the 1990s.

To support and provide stability to the risk analysis work, H SystSäk E provides a robust tool in the form of a specially designed Risk Log which:

- Constitutes the basis for projects in the design of a project-specific Risk Log.
- Is described in each section below, on the simultaneous presentation of the activity in question.
- Is performed in Excel and is available on H SystSäk E CDR.
- Provides support during the implementation of a system safety activity.
- Connects to the handbook's model for risk management.
- Facilitates a systematic implementation of risk management.
- Facilitates the close monitoring of implemented risk management.

General

The Risk Log is a way to fully document the details of all individual risks. The Risk Log is started when the risk identification of a certain technical system begins. The Risk Log is maintained and updated as long as the technical system is used and maintained. This section presents a simple but comprehensive Risk Log that includes space to record the necessary basic data. Each development project chooses to expand the Risk Log based on the needs that emerge.

The example is based on Excel being used, as this provides advantages as it acts as a calculation aid and can easily be expanded upon, and you can copy and paste information from other applications. It is also possible to use the model with optional help aids, where paper and a pen are the easiest tools to use.

A template for the Risk Log is presented as a file on H SystSäk E CDR.

The Risk Log's basic template contains four tabs. The first tab is for personal injury and financial damage (property and environmental rehabilitation). The second tab is used for accident risks that lead to lasting environmental damage – note that the risk of accidents that lead to lasting environmental damage should always be treated as RED, with the effect that this can only be closed by the Armed Forces (see *section 4.3.2*).

Initially each tab has room for two risks only. The intention is that the user expands the Risk Log, as and when needed, by copying the rows for each new risk.

Below, the management of the Risk Log, with regard to personal injury, is described (the description is also applicable for financial damage and (in some parts) damage to the environment, see *section 4.2.3*).

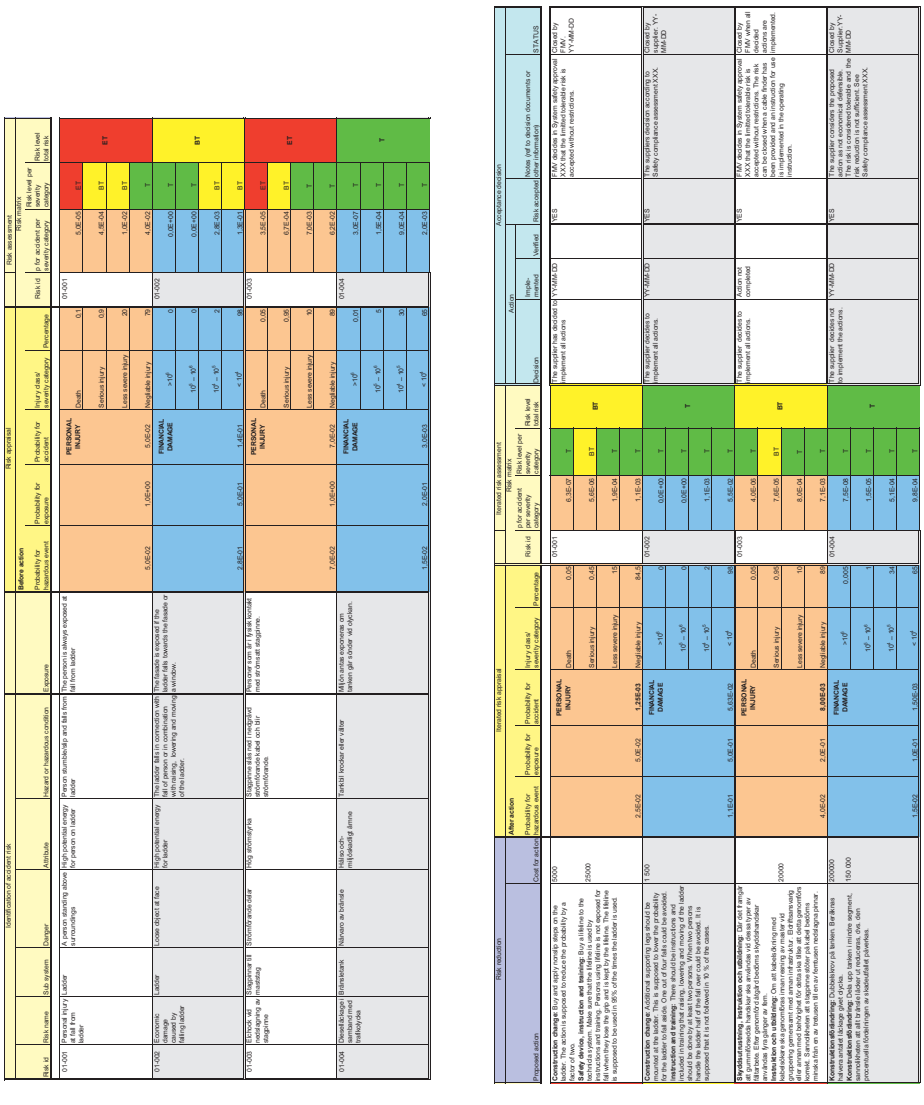
The third tab, "Instructions", includes some simple instructions on how the Risk Log should be handled.

Application

Note that the fourth tab, "Requirements for risk", shows risk matrices, which are also available in the handbook, see *chapter 4*. The values that are there will always be replaced by demands from a Tactical Technical Financial Objective (TTEM) for certain development/procurement projects.

Overview of the Risk Log

Below is highly reduced image of the Risk Log. The aim is to create an understanding among users about its appearance and context. Details are provided below in each of the sections where the intended management is presented in more detail.



Risk Identification

Read *section 4.2.2, Identification of Accident Risk* in part 1.

Study the activities *PHL* (Preliminary Hazard List) and *PHA* (Preliminary Hazard Analysis) as described in part 2.

The risk analysis starts with the identification of risk. Here it is necessary to try to find all the risks that the technical system contains or may give rise to. Start by looking through the dangers by first considering the hazards that exist and then the hazardous conditions that exist. Identify the hazards (dangerous features/properties) that have the potential to cause damage. Define what possible hazardous event could be triggered by the dangerous feature/property or hazardous condition that could occur.

If the danger is in a certain subsystem, it is appropriate to specify it.

Each identified risk is also given a clear identity – a number is an appropriate identifier. Often a two-part number is used, where the first part indicates the subsystem involved and the second part is a serial number within each group. To facilitate communication, each risk should also have a name, which should preferably be short and also describe what the risk is composed of.

Identification of accident risk					
Riskid	Risk name	Sub system	Danger	Attribute	Hazard or hazardous condition
01-001	Personal injury at fall from ladder	Ladder	A person standing above surroundings	High potential energy for person on ladder	Person stumble/slip and falls from ladder
01-002	Economic damage caused by falling ladder	Ladder	Loose object at face	High potential energy for ladder	The ladder falls in connection with fall of person or in combination with raising, lowering and moving of the ladder.

If the model needs to be extended, the “risk identification” cells must be divided up before new columns can be added. When this is done, the top row of cells should be merged again.

Risk Appraisal

Read *section 4.2.3, Risk Appraisal* in part 1.

Study the activities *PHA* and all analytical activities (SSHA, SHA, O&SHA, HHA, EHA, FHA) that are described in part 2.

The risk appraisal means that the magnitude of the risk should be estimated. It is a very difficult task which requires that all possible means and methods are used. Some methods are described in *appendix 1*.

First, the likelihood that a hazardous event will take place is evaluated and then the probability of exposure is evaluated. The probability of accident is then calculated according to the formula used in Excel. The orange-coloured boxes are those which contain a calculation formula.

After this, the accident injury/damage outcome is evaluated. This is done by specifying a percentage distribution between the four different injury/damage outcomes. Note that the sum of the percentage should always be 100.

Risk appraisal				
Before action				
Probability for hazardous event	Probability for exposure	Probability for accident	Injury class/ severity category	Percentage
		PERSONAL INJURY	Death	0,1
			Serious injury	0,9
			Less severe injury	20
5,0E-02	1,0E+00	5,0E-02	Negliable injury	79
		FINANCIAL DAMAGE	$>10^6$	0
			$10^5 – 10^6$	0
			$10^4 – 10^5$	2
2,8E-01	5,0E-01	1,4E-01	$< 10^4$	98

Risk Evaluation

Read *section 4.3, Risk Evaluation*.

The estimated risk value is now compared with the imposed requirements on individual risk.

For the current accident risk, identify the probability of the four risk elements. Read off in the risk matrix, each risk part's position and colour. The colour determines whether the size of the actual sub-accident risk can be tolerated or not. If any of the four risk areas have changed to red (or yellow) the entire accident risk is regarded as not tolerable (or a limited tolerable risk level) and risk reduction is required.

The following applies, depending on the level of risk:

- Red risk level = not tolerable.
  Risk reduction must come down to a green level of risk, if possible.
- Yellow risk level = limited tolerable risk level.
  Risk reduction must come down to a green level of risk, if possible.
- Green risk level = tolerable.
  Risk reduction is not necessary. If it is possible to carry out simple risk reductions, then these should be considered.

	Risk assessment		
	Risk matrix		
Risk id	p for accident per severity category	Risk level per severity category	Risk level total risk
01-001	5,0E-05	ET	ET
	4,5E-04	BT	
	1,0E-02	BT	
	4,0E-02	T	
01-002	0,0E+00	T	BT
	0,0E+00	T	
	2,8E-03	BT	
	1,3E-01	BT	

Risk Reduction

Read *section 4.3.3, Analysis of Alternatives*.

All risk-reduction measures have a price. Some are expensive to implement, others may lead to less-favourable solutions in some respect. Sometimes there can be both a short-term and a long-term solution.

There is always a reason to try to create and consider alternative measures to find the risk-reducing measures that provide the greatest risk reduction at the lowest cost. Sometimes the combination of several measures can provide the most effective end result. A full risk analysis allows for such effectiveness.

Risk reduction	
Proposed action	Cost for action
Construction change: Buy and apply nonslip steps on the ladder. The action is supposed to reduce the probability by a factor of two. **Safety device, instruction and training:** Buy a lifeline to the technicla system. Make sure that the lifeline is used by instructions and training. Persons using lifeline is not exposed for fall when they lose the grip and is kept by the lifeline. The lifeline is supposed to be used in 95% of the times the ladder is used.	5000 25000
Construction change: Additional supporting legs should be mounted at the ladder. This is supposed to lower the probability for the ladder to fall aside. One out of four falls could be avoided. **Instruction and training:** There should be instructions and included in training that raising, lowering and moving of the ladder should be done by at least two persons. When two persons handle the ladder half of the fall over could be avoided. It is supposed that it is not followed in 10 % of the cases.	1 500

Monitoring

Read *section 4.4.3, Monitoring*.

The expected risk reduction of a certain risk-reducing measure must be verified. This can be done by testing, calculation or a combination of both.

A New Risk Appraisal

The renewed risk appraisal is performed to see what the proposed risk-reduction measure leads to and to see improvements in the risk value. All input values can be changed after an action is carried out. Both the likelihood of a hazardous event, the likelihood of exposure and the distribution of damage/injury classes may have been affected. Risk appraisal is performed in the same way as before.

Iterated risk appraisal				
After action				
Probability for hazardous event	Probability for exposure	Probability for accident	Injury class/ severity category	Percentage
		PERSONAL INJURY	Death	0,05
			Serious injury	0,45
			Less severe injury	15
2,5E-02	5,0E-02	**1,25E-03**	Negliable injury	84,5
		FINANCIAL DAMAGE	$>10^6$	0
			$10^5 – 10^6$	0
			$10^4 – 10^5$	2
1,1E-01	5,0E-01	5,63E-02	$< 10^4$	98

Renewed Risk Evaluation

Risk evaluation is now carried out again with the new conditions from the renewed risk appraisal. Now it will show whether the validated risk reduction has led to a sufficient improvement so that risk levels have become green = tolerable. If improvement is not sufficient, additional measures should be considered.

Once the new risk evaluation shows that the verified risk reduction has resulted in sufficient improvement, it is time to decide which actions should be performed.

	Iterated risk assessment		
	Risk matrix		
Risk id	p for accident per severity category	Risk level per severity category	Risk level total risk
01-001	6,3E-07	T	BT
	5,6E-06	BT	
	1,9E-04	T	
	1,1E-03	T	
01-002	0,0E+00	T	T
	0,0E+00	T	
	1,1E-03	T	
	5,5E-02	T	

Acceptance Decision

An acceptance decision means that the risk is considered to be dealt with at present. There is absolutely no restriction on the possibility of bringing up a risk again if new information shows/suggests that the appraisal is not correct.

A green risk is closed by the supplier following communication with DesignA.

A yellow risk is closed/accepted by DesignA following a proposal from the supplier. Then it should also be shown that additional risk reduction is not possible even with a reasonable effort being made.

A red risk may only be closed/accepted by the Armed Forces following a proposal from DesignA. Then it must clearly state that further risk reduction is not possible or what the cost of further risk reduction would be.

Acceptance decision					
Action					
Decision	Imple-mented	Verified	Risk accepted	Notes (ref to decision documents or other information)	STATUS
The supplier has decided to implement all actions	YY-MM-DD		YES	FMV decides in System safety approval XXX that the limitted tolerable risk is accepted without restrictions.	Closed by FMV. YY-MM-DD
The supplier decides to implement all actions.	YY-MM-DD		YES	The suppliers decision according to Safety compliance assessment XXX.	Closed by supplier. YY-MM-DD

Risk Log Environment

The second tab contains the template for the management of environmental risks that can lead to permanent damage. These include large parts of the fields from the normal Risk Log. Risk identification is done in exactly the same way. Risk appraisal is simplified as illustrated below.

Risk appraisal		
Before action		
Probability for hazardous event	Probability for exposure	Probability for accident
		ENVIR.
1,0E-07	1,0E+00	1,0E-07
		ENVIR.
		0,0E+00

The calculation stops here, with the probability of an accident occurring, and this is then followed by a risk reduction, as described above, and then a reappraisal of the risk is carried out.

A risk to the environment is always regarded as a red risk and a red risk can only be closed/accepted by the Armed Forces following a proposal from DesignA.

Appendix 3 Other Safety Forms for Technical Systems

Below are some areas of application (for products/materiel/systems) with special rules/regulations used to guide the implementation of related safety activities. The specified document names etc., are the ones that were current when the handbook was compiled. In the event that a certain reference needs to be applied, it is recommended that you check to see if a later version has been produced.

Area of application	Relates to	Documentation
Ammunition and explosives	The Armed Forces' instruction for the storage and transportation of ammunition and other explosives	IFTEX *[21]*.
Ammunition safety	The safety of munitions	Lag om brandfarliga och explosiva varor (LBE), SFS 2010:1011 (Act on Flammable and Explosive Goods) *[28]*. FMV's Weapons and Ammunition Safety Manual, H VAS-E *[11]*.
Fire and explosion hazard	The Armed Forces' common instructions relating to measures to counter fire and explosion hazards, water pollution and the impact of chemicals on health from flammable goods etc.	BVKF.
Electrical safety	Safety to prevent injury to persons or property through the direct or indirect effects of electrical current	Ellagen (The Electricity Act) *[8]*. Handbok Elsäkerhet i Försvarsmakten. (Handbook on Electrical Safety in the Armed Forces) *[30]*.
Aviation safety for terrestrial systems for air navigation and air combat	The management system's impact on aviation/aircraft	LFS 2008:14. FMV AK Led Flight Safety Process.

Area of application	Relates to	Documentation
Vehicle safety	Vehicle safety	Fordonslagen (2002:547) (The Vehicle Act). Fordonsförordningen (2009:211) (The Vehicle Ordinance). Militärtrafikförordningen (2009:212) (The Military Traffic Ordinance). Vägverket's (the Swedish National Road Administration) Statutes (2003:22). H FordonSäk (FMV's Handbook on Vehicle Safety) *[10]*.
Airworthiness	Safety of flight materiel/aircraft	Regler för militär luftfart, RML (Rules for Military Aviation) *[34]*.
Medical device safety	Medical devices	Lag om medicintekniska produkter (1993:584) (The Medical Devices/Products Act). Förordning om medicintekniska produkter, SFS 1993:876 (The Medical Devices/Products Ordinance).
Program software	Program software in safety-critical applications	FM's Handbook on Program Software in Safety-critical Applications, M7762-000531 H ProgSäkE, 2001 *[20]*.
Seaworthiness	Work environment and safety for ships and their equipment	RMS, the Armed Forces' Rules for Naval Operations *[36]*
Radiation protection	Radioactive materials Materiel that can produce: electromagnetic radiation/fields (radar), laser	The Swedish Radiation Safety Authority's Regulations Related to Ionizing and Non-ionizing Radiation.

Area of application	Relates to	Documentation
Safety of connection equipment	Safety of bridges and ferries etc.	For new bridge equipment, Boverket's (the Swedish National Board of Housing, Building and Planning) 1994 design regulations BKR apply: (released as BFS 1993:58 with amendments BFS 1995:18) which contain regulations and guidelines to the Planning and Building Act 1987:10. For older bridge equipment Vägverket's publication 1991:210 "Buoyancy Classification of Bridges" applies. For ferries the "Armed Forces' Rules for Seaworthiness" apply.
Weapons safety	Safety of weapons materiel	FMV's Weapons and Ammunition Safety Manual H VAS-E *[11]*.

There are further areas of application, however they are not dealt with in the handbook.

Examples include:

- CBRN (chemical, biological, radiologic, nuclear) materiel
- pharmaceuticals
- masts
- lifting devices
- pressure vessels
- work equipment.

Definitions

To facilitate the understanding of the manual, the concepts and acronyms used are provided in the glossary below. Swedish Standard SS 441 05 05, MIL-STD-882C and specialist literature in systems security, has served as the basis for most of these definitions. Note that certain terms have slightly different definitions in various standards. For example, there are differences between Swedish and American military standards.

A number of definitions are specific to the Handbook.

Concept	Explanation
Accident risk	Relates to a risk of harm to a person, property or the external environment. Expressed as a function of the probability of an accident happening and its consequences (the consequences are usually divided into the four injury/damage classes for individuals and the economy). Is distributed, if possible, at sub-risk levels for the four injury/damage classes.
Accident, Mishap	Occurs when someone/something is exposed to a hazardous event or hazardous condition and is therefore injured/damaged (injury/damage to a person, to property or the external environment). An accident is always unplanned, not the result of a hostile act for example. The term “mishap” is used only in the United States.
ALARP	As Low As Reasonably Practicable, as low as practically and reasonably possible (implies a certain risk). A term used in British law – it means that actions to reduce a particular risk should be continued as long as the operation provides an appreciable effect on the risk at a reasonable cost.
Ammunition	Materiel/technical systems intended to produce a harmful effect, smoke or lighting effect, blasting, the laying of mines, mine-clearance and materiel/technical systems which following training replace this. The materiel/technical system may contain explosives or other chemicals.

Concept	Explanation
Approved processes (RML - Rules for Military Aviation)	Every authorization issued is based on an appropriate operational management system. The operational management system includes defining the processes which, among other things, are critical to the quality of the products and services that are delivered. These processes should therefore be approved by the aviation authorities.
Aversion factor	This means that a major injury is tolerated to a lesser extent than with a comparable accident that results in minor injuries.
Barrier	Protective device, such as a sheet metal plate in front of spinning wheels, axles, chains, live tracks, but also in the form of soft parts, which provide a direct, protective function. Even personal protective equipment can be regarded as a part of the barrier.
Battle damage repair	Method of corrective maintenance aimed at quickly restoring technical systems to battle readiness after they have been damaged. Battle damage repairs are carried out only during war or warlike conditions. The repairs should be acceptable from a system safety point of view (see STANAG 2418).
Cause of Failure	The conditions giving rise to a failure.
Central operator	Head of the Armed Forces' command staff, the production manager and operation manager are both central operators.
CIP Convention	The CIP Convention (Permanent International Commission for Firearms Testing) ensures that every civilian firearm, and all civilian ammunition that is sold in the participating countries, is safe for the user. The CIP convention covers 14 countries (Sweden is not a member). The Commission Internationale Permanente pour l'Epreuve des Armes à Feu Portatives.

Concept	Explanation
CIP proof mark	**Civilian firearms** Manufacturers and importers of firearms in a country that is a member of the CIP are required to ask an approved testing agency to perform the testing of any firearm they manufacture or import. Upon completion and approval, the tested weapon parts are provided with a CIP label. **Ammunition** The CIP Convention requires manufacturers and importers of ammunition to be sold to a CIP country to continuously test the ammunition during production in accordance with CIP specifications. Such ammunition is provided with a CIP proof mark.
Civil ammunition	Civilian ammunition that is traded (COTS - Commercial off the Shelf) and is equipped with a CIP proof mark (replaces the CE mark).
Civilian handgun	Civilian small arms (handgun) that is traded (COTS) and is equipped with a CIP proof mark (replaces the CE mark).
Configuration decision	Product documents which specify the scope and configuration of a technical system.
Contributing causes	In order for the damaging effects of a source of a risk to be activated, a certain mechanism is required (see *Trigger*.)
Critical characteristics	A characteristic (tolerance, surface finish, material, manufacture, assembly) of a product, material or process which may result in the failure of a critical item in the event of non-fulfilment of requirements.
Critical defect	Deviation from stipulated requirements regarding a certain characteristic which may lead to an unsafe condition.
Critical fault	A deviation from specified demands in respect of certain characteristics and which can therefore lead to an unsafe condition.
Critical items	A part, assembly, installation or production process with one or several characteristics which results in an unsafe condition in the event of non-fulfilment of requirements.

Concept	Explanation
Customer order *KB*	The ordering of a product or service from the Armed Forces to DesignA. Includes a decision about money and a specification as to what must be delivered, time constraints and more. If the order relates to a technical system (a reference to) Tactical-Technical-Financial Objectives (TTEM)/Technical Financial Objectives for Training Materiel (TEMU) is included.
Danger/Hazard	A condition which is a prerequisite for an accident, includes both a source of risk and a hazardous condition.
Decision document for system safety	Collective term used in the handbook for the following three decision documents: • Safety Compliance Assessment (SCA) • Safety Statement (SS) • Central Safety Compliance Decision (CSSB).
Defect	Deviation from stated requirements regarding a specified characteristic.
Design review	Aimed at examining all technical records in a quality-assured and traceable manner.
Deterministic risk analysis	Deterministic risk analysis is based on the physical risks involved, i.e. that could happen. In this respect, this could either be the worst possible incident which leads to injury or a dimensioning incident (see probabilistic risk analysis).
EASA	The European Air Safety Agency (EASA) via a European Commission (EC) regulation has taken over the European national administrative data for the approval of aircraft equipment for the open European market.
Effect/Damage	The consequence of an accident/incident consists of any injury to a person or damage to property and the external environment.
Environment	Areas in which an organization operates, which includes air, water, land, natural resources, flora, fauna and humans and how they interact.
Expedient repair	Method for non-permanent corrective maintenance of operating damage and/or battle damage involving unconventional repair methods and/or alternative spare materiel supplies. The repair must be acceptable from a system safety aspect.
Expert system	See *Neural networks*.
F-code	Storage code under IFTEX. It forms the basis of how the Armed Forces' ammunitions stores may be kept.

Concept	Explanation
Facility	For certain functions or activities, a prepared area of land, a building or a room, including the requisite installations for the function or activity, such as fortifications, the building of barracks, a base area, links etc. A facility also includes any military fortifications that are required. Facility-bound supplies are also required for the facility.
Fail safe	Characteristic of a unit which prevents defects from becoming critical faults. A fail-safe design is one which ensures that the system moves into a safe state if a fault occurs.
Failure	The discontinuation of a unit's capability to fulfil its required function.
Failure probability density	Failure frequency rating at a given point in time.
Fault effect, Fault consequence	The result which is a direct or indirect consequence of a fault.
Fault mode	One of the possible fault conditions in a unit.
Handling	Handling relates to manufacturing, processing, treatment, packaging, storage, transport, use, disposal, destruction, marketing, maintenance, conveyance and other similar procedures. (The definition comes from the Flammable and Explosive Goods Act.)
Harm	Injury to a person, damage to property or the external environment. The term injury/harm relates to all H SystSäk E possible outcomes.
Hazard severity category	For personal injury: death, serious personal injury, minor personal injury and negligible injury. For financial damage: comparable to total system loss, major loss, limited loss and minor loss. Details can be found in *section 4.2.3*.
Hazardous condition	A physical situation that could lead to an accident occurring.
Hazardous event	An event that occurred by misadventure, that is, without intention, unplanned, and which may result in an accident or incident if someone or something is exposed.
Incident	A hazardous event that does not lead to an accident, as nothing is exposed during a hazardous event.

Concept	Explanation
Incremental development	First the central parts of the system are constructed. This ensures that they function in accordance with the specified requirements. Later additional functions are added and they are inspected in the same way. Once all the required features are in place, the system is ready.
Individual risk	The rate at which an individual is likely to be exposed to a given level of injury/harm caused by specified dangers (Institution of Chemical Engineers – IChemE). It is usually based on an average person in the group.
Interface	Actual environment for certain technical systems. May be made up of other technical systems, power supply (voltage, frequency, current), water, sewage, fuel supplies, repair facilities, air traffic control and more.
Item	A term used to designate a subsystem apparatus, component, part, etc., which may be regarded as separate.
Less serious injury	An injury that a person recovers from following hospital care (e.g. a fracture).
Limited tolerable	A certain level of risk. The Request For Proposal (RFP) specifies who can decide on a risk at this level.
Managing activity	The term often refers to a procurement organisation such as the Armed Forces and DesignA, but may also include suppliers or subcontractors who require an activity of their subcontractor.
Mandatory requirement	A requirement which is of crucial importance to system safety. Comments: If a *mandatory requirement* cannot be met, for example for tactical or cost reasons, non-compliance is permissible if it can be demonstrated that an acceptable level of safety can still be maintained.
Materiel system	Se *Technical system*.
Military accident risk	Risk of injury during a battle caused by deficiencies in materiel design and function. Especially crucial is the advantage the enemy could receive from this in a combat situation.
Military ammunition	Ammunition, regardless of origin, which is intended for use to conduct military operations.
Military materiel (equipment)	Technical systems that have been specifically designed and manufactured (even through integration) to carry out military operations.
Military purpose	Activities aimed at preparing and implementing organized, armed combat.

Concept	Explanation
Negligible damage	An injury which is trivial and minor. Dealt with by using a “plaster and a few days rest”.
Neural networks	Technology for creating expert systems. Refers to algorithms for information processing that try to imitate the function of nerve cells and the brain.
Operational environment	Actual environment for a specific technical system. May be made up of other technical systems, power supply (voltage, frequency, current), water, sewage, chemical conditions, fuel supply, repair facilities, air traffic control, etc.
Operational safety	Armed Forces’ operational safety refers to the Armed Forces’ ability to manage risk in all aspects of its operations so that the constitutional requirements, in terms of the working environment and safety for the Armed Forces’ personnel and requirements with regard to safety for third parties, the external environment and property, are met.
Optional requirement	The selection of optional requirements to be implemented for a technical system adapted by the client based on the complexity of the system (see *Mandatory requirement*).
Owner representative (ÄF)	The ÄF is responsible for the status, privacy, existence and presentation of the supplies before the government. FMV is the ÄF of materiel before delivery to the Armed Forces. The Armed Forces is the ÄF from the time of delivery (and approval) of any supplies to the Armed Forces to the time that the supplies are reported as withdrawn from the Armed Forces’ stock of supplies. This also applies to assets placed in the industry and with the FMV.
Personal safety	The capability of a system to avoid causing unacceptable personal injury.
Proactive	Anticipative and preventive.
Probabilistic risk analysis	Probabilistic risk analysis methods assume that both the probability of accidents will occur, as the consequences arising from them are important for assessing the risk level (see *Deterministic risk analysis*).
Probability of failure	The probability of one or more failures occurring during a specified time period.

Concept	Explanation
Product	The product is understood here to be mainly products that are "sold over the counter"/are commercially available (COTS) and from a safety point of view are designed to comply with product safety and product liability laws and the relevant European Union (EU) directives.
Product safety	Capability of a product to avoid causing personal injury or damage to property or the external environment.
Qualification	Verification of a product's characteristics.
Reactive	The subsequent action taken to try to prevent the repeat of, for example, an accident.
Responsible for design (DesignA)	The person who has this roll with technical design responsibility (see *Technical design responsibility*). Examples of DesignA include: a government agency, a foreign government and the supplier of OPS (PPP Private Public Partnership) contracts with the Armed Forces.
Restriction	Temporary restriction within the technical system's permitted use to temporarily deal with a certain risk and therefore contain the demands on system safety.
Risk	Se *Accident, Mishap*.
Risk acceptance	For all elements of a technical system's accident risks, acceptance decisions are made. The acceptance decision is compared to the value of the accident risk, taken from the technical system's risk log, with the specified risk value.
Risk analysis	Systematic use of available information so as to identify hazards and assess risks to people, property, materiel or the external environment.
Risk log	Documents for the documentation of a technical systems' total risks. Refers to the replacement of previous documents Preliminary Hazard List (PHL), Hazard List and Risk List
Risk matrix	Two-dimensional graph used to illustrate the connection between probability and consequence. Can be graded and provided with borders showing acceptance criteria.
Risk reduction activity	Eliminate hazards. Design intended to eliminate any risk. Introduce protective devices (also referred to as barriers). Introduce active warning devices (such as audio/visual signals). Impose restrictions/training/instructions/warning signs.

Concept	Explanation
Risk source	Something that may lead to personal injury or damage to property, materiel or the external environment.
Safety	Absence of any risk of an accident occurring that could lead to unintentional injury.
Safety analysis	A collective term for those parts of the system safety activities involving both systematic identification of possible hazardous events and their causes and qualitative or quantitative assessment of the risks of a technical system.
Safety certificate	Issued by DesignA and is a form of system safety approval. The safety certificate means that DesignA, after inspecting all the relevant circumstances, has found that the vessel that Sea Trials Command (PTK) is to test has an acceptable level of safety. The safety certificate is sent to the Armed Forces Maritime safety inspection which, on agreement, submits this to the PTK.
Safety defect	A product has a safety defect if it is not as safe as can be reasonably expected.
Safety management	An applied form of quality control defined as all actions intended to influence the safety of an establishment.
Safety message	A report submitted in the special case that design has mandated for a specific technical system that a system safety approval must be issued, but where the technical system in question is found not to have an acceptable safety level.
Security	Absence of relationships involving espionage, sabotage, terrorism and other crimes against national security.
Serious (bodily) injury	Injury with a permanent loss of body function/body part.
Service life	Total time from the creation of a system until its decommissioning.
Single Failure Criterion, Single Event Criterion	Fault or incident which on its own can lead to a hazardous event.
Societal risk	The relationship between frequency and number of people affected by a specified level of damage in a given population exposed to specified risk (IChemE). It therefore calculates the number of people who are covered by an accident.
System	See *Technical system*.

Concept	Explanation
System hazard	Accident risk at overall system level, which is inadvertently caused by the system's required capabilities. Often appears in response to the question: Given system capacity, what may this not lead to/cause/what should not happen?
System of systems	The capability that is created through the use of existing technical systems and products in a new way, possibly along with additionally employed materiel.
System safety	Property of a technical system that does not inadvertently cause damage to a person, property or external environment. (Person: death, physical injury or illness. Property: damage to or loss of property or equipment. External environment: "superficial" damage which can be reconstituted wholly or in part or permanent damage, such as the eradication of a species).
System safety activities	The total amount of work that is carried on for a technical system during the study, development, acquisition/procurement, refurbishment and modification, production, operation (including technical adaptation), maintenance and decommissioning, in order to identify and quantify risks and eliminate them or reduce them in accordance with the requirements that have been established.
System safety decisions	System safety decision: is a general term, which in this handbook includes: • SCA • SS • CSSB.

Concept	Explanation
System safety documentation	With full system safety documentation for a specific technical system it relates to the following. • Documents from the supplier: Risk documentation, including Risk Log, with risk decisions for each risk. System safety report with analytical results (from analysis activities that have been carried out such as PHL, PHA, SHA and others). Safety compliance assessment. • From DesignA: System safety approval (all the above materials from the supplier form part of the documentation). • Within the Armed Forces: CSSB. To link risk documentation and system decisions to a certain technical system requires a decision on the current configuration of the technical system. System security decisions, when used in this handbook, relate to: SCAs, system safety approvals and CSSBs.
System safety requirement	The Armed Forces' demands on DesignA includes both operational obligations and technical requirements in terms of the technical system and its system safety features. See *section 5.3*.
Systematic errors	An error or fault that always occurs at some point when the system has been used which produces the same outcome every time. The reason may be, for example, a logical flaw in the software that provides the same outcome (fault/error) on execution, or the physical failure of a "batch" of components that provide the same outcome when the components are exposed/used (batch = a group of components made in a sequence/with the same machine settings, the same input/raw materials etc).
Systems Office (MaK	Owner Representatives' representative (ÄFR) for all the standard vehicles, COTS products and some other materiel.

Concept	Explanation
Technical adaptation	To temporarily change/adapt a technical system's design and/or function in response to a disturbance, altered threat or changed environment. This also applies when there is a change in operational, tactical or combat technical requirements. Applicable only in direct combat situations (war, crisis, international response). The change is temporary and the materiel needed will be restored to its original state.
Technical design responsibility	Technical design responsibility means determining the technical system's established technical structure and the integration of technical systems/subsystems, equipment and components that are subject to a certain allowable configuration (including maintenance solutions) and to ensure that it meets legal requirements, set objectives and other requirements regarding performance, functionality, information and system safety during the service life of the technical system. Technical design responsibilities, including technical systems management, are normally held by DesignA for all levels of technical systems which DesignA has delivered to the Armed Forces. Technical design responsibility is linked to the type of technical system. Industry and suppliers are responsible for a product and may have a technical design responsibility in relation to the procurement organization, but it is always the procuring organization that is responsible for the technical design.
Technical Office (TeK)	ÄFR for the specific materiel.
Technical order (TO)	Materiel publications issued by the Swedish Defence Materiel Administration (FMV) on behalf of the Armed Forces. Through a TO, the operation, maintenance, care and modification of supplies are governed.
Technical standard order (TSO)	A TSO is issued by the Aviation Authority and is a standard that specifies the minimum attributes of an article.

Concept	Explanation
Technical system	A system is defined by ISO/IEC 15 288 as: "An assembly of interacting elements organized to achieve one or more stated purposes." The system in H SystSäkE always refers to the technical system. The technical system refers to a system that has been created through the integration of technical systems, elements from these and/or other products. Ammunition is always a separate technical system.
Testing	Testing relates to technical verification and validation. Testing, along with a review of the qualification activities, is designed to verify technical demands and expectations, for example to demonstrate that a gun barrel can resist the pressure created by the ammunition intended to be used. Testing may produce far greater risks than regulated safety-approved materiel is allowed to contain (see *Trial/Experiment*.)
The owner representative's representative (ÄFR)	For most technical systems there is an ÄFR, designated in the form of a TeK and a Materiel Office. These act as the owner of the materiel during operation, maintenance and decommissioning. ÄFR is responsible for representing ÄF regarding operational and financial control, monitoring and analysis, configuration mode, modifications and TO operations, as well as technical support and technical development. FMV is the ÄFR for supplies which are mainly procured for and used in FMV's testing operations. For supplies that cannot be clearly assigned to one of the above activities the ÄFR must be regulated for each order.
Tolerable level of risk (T)	A certain level of risk.
Trial/Experiment	An experiment includes: the tactical value of materiel/a system/product, which intends to show that a technical system is tactically useful and can be handled in the manner intended (see *Testing*.)
Trigger	In order for the damaging effects of a source of a risk to be activated a certain mechanism is required. In some cases a trigger may be required to achieve a hazardous event *Contributing causes*).
Validation	Ways of showing that the requirements are correct, namely that the system will function properly in its operational environment if the requirements are fulfilled.

Concept	Explanation
Verification	Confirmation through the drafting and examination of objective evidence that specified requirements have been fulfilled.

Acronyms/Abbreviations

This is a complete list of acronyms and abbreviations that can be found in H SystSäk E.

Acronym/abbreviation	Explanation
ADR	European Agreement Concerning the International Carriage of Dangerous Goods by Road Accord Européen Relatif au Transport International des Marchandises Dangereuses par Route
AE	Architect and Engineering Firm
AFS	Working Environment Authority's Regulations
ALARP	As Low As Reasonably Practicable (relates to a certain type of accident risk)
AML	The Work Environment Act
AOP	Allied Ordnance Publication, NATO
AV	The Swedish Working Environment Authority
BOA	Decision Regarding Use
BT	Limited tolerable risk level
BVKF	The Armed Forces' instruction on measures against fire and explosion hazards, water pollution and chemical health effects from flammable goods etc.
CAA	Civil Aviation Authority, Great Britain
CDRL	Contract Data Requirement List
CE	EC mark of conformity (Communauté Européenne)
CFR	Code of Federal Regulations
CI	Critical Item
CIL	Critical Item List
CIP	Permanent International Commission for Firearms Testing - commonly abbreviated as C.I.P. or CIP (Le Commission Internationale Permanente pour l'Epreuve des Armes à Feu Portatives)
CM	Configuration Management
COSHH	Control of Substances and Hazardous to Health
COTS	Commercial off the Shelf
CSP	Certified Safety Professional

Acronym/abbreviation	Explanation
CSSB	Central Safety Compliance Decision
DAL	Development Assurance Level
Def-Stan	Defence Standard (British standard)
DesignA	Organization responsible for design (including FömedC, FMLOG, FMV, FortV, PPP partner)
DF	Defence Forces
DGA	The French Military Aviation Authority (Délégation Générale pour l'Armement)
DID	Data Item Description, instructions that specify the scope and nature of reports
DLA	Defense Logistics Agency
DoD	Department of Defense (US)
DOD-STD	DOD Standard
DoDI	DOD Instruction
DOT	Department of Transportation
EASA	The European Air Safety Agency
ECP	Engineering Change Proposal
ECPSSR	Engineering Change Proposal System Safety Report
EHA	Environmental Hazard
EHC	Explosive Hazard Classification and Characteristics Data
EOD	Explosive Ordnance Disposal
ESOH	Environmental, Safety and Occupational Health
ET	Non-tolerable risk level
ETA	Event Tree Analysis
EU	European Union
FAA	Federal Aviation Authority
FC	Functional Centre
FHA	Functional Hazard Analysis
FLYGI	Military Flight Safety Inspectorate
FM	The Swedish Armed Forces

Acronym/abbreviation	Explanation
FM ArbO	The Armed Forces' regulations with work procedures for the Armed Forces (FFS 2009:2 with changes FFS 2009:3)
FMEA	Fault Modes and Effects Analysis
FMECA	Fault Modes Effects and Criticality Analysis
FMLOG	Part of Swedish Defence
FMUK	Armed Forces' Commission of Inquiry
FMV	Swedish Defence Materiel Administration
FOI	The Swedish Defence Research Agency
FORTV	The National Fortifications Administration
FRA	The Swedish National Defence Radio Establishment
FRACAS	Failure Reporting, Analysis and Corrective Action
FSD	Defence Standard (in Sweden)
FSI	Armed Forces' Flight Safety Inspector
FTA	Fault Tree Analysis
FömedC	National Defence Medical Centre
G	Generally applicable
GC	Generally applicable for design change
GEIA	Standard institute
GFE	Government Furnished Equipment
GFP	Government Furnished Property
GOTS	Governmental off the Shelf
HAZOP	Hazard and Operability Study
H FordonSäk	Handbook on Vehicle Safety *[10]*
HHA	Health Hazard Assessment
HHAR	Health Hazard Assessment Report
HKV	Headquarters
HMI	Human Machine Interface
H Mål	Handbook for the Armed Forces' development of goals for units, supplies and facilities for the war organization's needs
HRI	Hazard Risk Index
HTM	Half-time Modification

Acronym/abbreviation	Explanation
HTRR	Hazard Tracking and Risk Resolution
H VAS-E	Weapon and Ammunition Safety Manual
IAEA	International Atomic Energy Agency
IChemE	Institution of Chemical Engineers
IEC	International Electrotechnical Commission
IEDs	Improvised Explosive Devices
IFF	Identification of friend or foo
IFTEX	The Armed Forces' instruction for storage and transportation of ammunition and other explosives
ILS	Integrated Logistic Support
IMSC	Integration/Management of Associate Contractors, Subcontractors, and Architect and Engineering Firms
IRS	Interface Requirements Specifications
ISO	International Organization for Standardization
ISSPP	Integrated System Safety Program Plan
JSP	Joint Service Publication
KB	Customer order
LKA	Low-sensitivity ammunition
MA	Managing activity
MaK	Materiel Office
MB	Environmental Code
MCS	Minimal Cut Set
MFI	Navy Vessel Inspection
MIFOR	Military Vehicle Register
MIL-STD	American Military Standard
MOTS	Military off the Shelf
MPD	Materiel Product Declaration
MRAR	Mishap Risk Assessment Report
MS	Materiel System
MSA	Materiel Systems Manager in the Armed Forces HQ
MSB	The Swedish Civil Contingencies Agency
MSI	Materiel System Certificate

Acronym/abbreviation	Explanation
MTC	Materiel Type Certificate
N/A	Not Applicable
NATO	North Atlantic Treaty Organization
NDI	Non-developmental Item
O&SHA	Operating and Support Hazard Analysis
OHHA	Operating and Health Hazard Analysis
OPR	Office of Primary Responsibility
OPS	PPP Private-Public Partnership
OSHA	Occupational Safety and Health Administration
PAL	Product Liability Act
PE	Professional Engineer
PESHE	Programmatic environment, safety, and occupational health evaluation
PHA	Preliminary Hazard Analysis
PHL	Preliminary Hazard List
PHST	Package Storage and Handling Requirements
PL	Project Manager
PM	Program Manager
PPP	PPP, Private–Public Partnership
PRL	Product Manager
PTEMU	Preliminary Technical–Financial–Objectives for Training Materiel
PTK	Sea Trials Command
PTR	Program Trouble Reports
PTTEM	Preliminary Tactical–Technical–Economic Objectives
RADS	Risk Assessment at Disposal of System
REACH	Registration, Evaluation, Authorization and restriction of Chemicals
REMO	Renovation – modification
RENO	Renovation
RFP	Request for Proposal
RML	Rules for Military Aviation

Acronym/abbreviation	Explanation
RML V-5B	Rules for military aviation, Subdivision B – Materiel System Certificate and military type certificate
RML V-5G	Rules for military aviation, Subdivision G – Authorized production organizations
RML V-5J	Rules for military aviation, Subdivision J – Authorized design organizations – level 2
RML V-5JA	Rules for military aviation, Subdivision J – Authorized design organizations – level 3
RML-V-5D	Rules for military aviation, Subdivision D
RML-V-5N	Rules for military aviation, Subdivision N
RMM	Rules for Military Ground Operations
RMS	Rules for naval operations
S	Selectively applicable
SAR	Safety Assessment Report
SCA	Safety Compliance Assessment
SCCSC	Safety Critical Computer Software Components
SCF	Safety Critical Functions
SCG	Storage Compatibility Group
SCN	Specification Change Notices
SDB	Safety data sheet
SDR	System Design Review
SEK	Swedish krona
SEMP	Safety and Environmental Programme Plan
SFS	Swedish Statue Book
SHA	System Hazard Analysis
SHA	System Hazard Analysis
SHK	The National Board of Accident Investigation
SHRI	Software Hazard Risk Index
SI	Safety Instructions
SIL	Safety Integrity Level
SJÖI	Military Maritime Safety Inspectorate
SOW	Statement of Work
SPR	Software Problem Reports

Acronym/abbreviation	Explanation
SR	Safety Review
SRCA	Safety Requirements/Criteria Analysis
SRR	System Requirements Review
SS	Safety Statement
SS	Swedish standard
SS-EN	Swedish Standard European Norm
SSE	System Safety Evaluation
SSHA	Sub System Hazard Analysis
SSI	Safety Significant Item
SSMP	System Safety Management Plan
SSP	System Safety Program
SSPP	System Safety Program Plan
SSPPR	System Safety Program Progress Report
SSPR	System Safety Program Review/Audits
SSPS	System Safety Progress Summary
SSR	Software Specification Review
SSS	System/Segment Specification
SSWG	System Safety Working Group, sometimes called SSWG-1 or SSWG-2
SV	Safety Verification
SäkI	The Armed Forces' safety instruction for weapons and ammunition etc
SäkI G	The Armed Forces' safety instruction for weapons and ammunition etc., – common part
SÄKINSP	The Armed Forces' Security Inspectorate
T	Tolerable risk level
TA	Technical directive
TC	Service Branch Centre
TeK	Technical Office
TEMU	Technical–Financial–Objectives for Training Materiel
TjF	Staff Regulations for FMV
TO	Technical Order

Acronym/abbreviation	Explanation
TO UF	Technical Order Maintenance Plans
TOEM	Tactical–Organizational–Financial Objectives
Tso	Technical standard order
TSR	Test and Safety Regulations)
TTEM	Tactical-Technical-Financial Objectives
UAV	Unmanned Aerial Vehicle
UhF	Handbook maintenance service during peacetime
UK	United Kingdom
UN	United Nations
US	United States
UTEMU	Draft Technical–Financial–Objective for Training Materiel
UTTEM	Draft Tactical–Technical–Financial Objectives
V&V	Verification and Validation
WBS	Work Breakdown Structure
VD	Managing Director
WEEE	Waste Electrical and Electronic Equipment
VFM	Operational System for the Armed Forces
WSESRB	Weapon System Explosive Safety Review Board
VVFS	National Road Administration's code of statutes
ÄF	Owner Representative
ÄFR	Owner Representative's Representative
ÖB	Supreme Commander

References

The specified document names etc., are the ones that were current when the handbook was compiled. In the event that a certain reference needs to be applied, it is recommended that you check to see if a later version has been produced.

Ref no	Title
1	ADR, Myndigheten för samhällsskydd och beredskaps föreskrifter om transport av farligt gods på väg och i terräng; MSBFS 2009:2. MSB (Agency for Civil Contingencies): regulations on the transport of dangerous goods by road and terrain, MSBFS 2009:2. The letter "S" after ADR denotes that the regulations contain the Swedish version of Annex A and Annex B to the European Agreement concerning the International Carriage of Dangerous Goods by Road (ADR), supplemented by provisions that only apply to national shipments in Sweden.)
2	AFS 2001:1, Arbetsmiljöverkets föreskrifter om systematiskt arbetsmiljöarbete. (Swedish Working Environment Authority's instructions on Systematic Environment Work.)
3	An Introduction to System Safety Management and Assurance, UK MOD (Ministry of Defence) 2002.
4	AOP-39, Guidance on the Development, Assessment and Testing of Insensitive Munitions (IM).
5	Arbetsmiljölag, SFS 1977:1160 (The Work Environment Act).
6	CE-märkning och produktsäkerhet, Arbetsmiljöverket, ADI 468. (CE Marking and Product Safety.)
7	Dependability management. Part 3: Application guide, section 9: Risk analysis of technological systems, International Electrotechnical Commission, 1995, IEC 60300-3-9.
8	Ellagen SFS 1997:857. (The Electricity Act.) Including the following regulations: • Starkströmsförordningen SFS 1957:601 (High Voltage Regulation) • Elinstallatörsförordningen, SFS 1990:806 (Electrical Contractors' Ordinance) • Elmaterielförordningen, SFS 1993:1068 (Electrical Equipment Ordinance) • Förordningen om elektromagnetisk kompatibilitet, SFS 1993:1067 (The Ordinance on Electromagnetic Compatibility)

Ref no	Title
9	Fastställande av rutin avseende leveranser av produkter från Försvarets materielverk till Försvarsmakten, fastställd med Försvarsmaktens skrivelse 14 760:900947, 2008-12-19. (Determination of the routine for the supply of products from the Defence Materiel Administration for the Armed Forces.)
10	Handbok Fordonssäkerhet 2000 års utgåva, M7762-000511, H FordonSäk. (FMV's Handbook on Vehicle Safety 2000 edition).
11	FMV's Weapons and Ammunition Safety Manual 2000, M7762-000 212, FMV H VAS-E.
12	Fordonsförordningen, SFS 2009:211. (The Vehicle Ordinance.)
13	Fordonslagen SFS 2002:574. (The Vehicle Act.)
14	Förordning om brandfarliga och explosiva varor (FBE), SFS 2010:1075. (The Flammable and Explosive Goods Ordinance.)
15	Förordning om medicintekniska produkter, SFS 1993:876. (The Medical Devices/Products Ordinance.)
16	Förordning (2007:936) om folkrättslig granskning av vapenprojekt. (Regulation on the international legal review of weapons projects).
17	Försvarsmakten och FMV Ändringsstyrningsprocess. (The Armed Forces' and FMV's Change Management Process.)
18	Försvarsmaktens föreskrifter med arbetsordning för Försvarsmakten FM ArbO), FFS 2009:2. (The Armed Forces' Regulations with Work Procedures for the Armed Forces.)
19	Försvarsmaktens gemensamma riskhanteringsmodell. Fastställd med Försvarsmaktens skrivelse 01 310:900666, 2008-12-12. (The Armed Forces' Joint Risk Management Model.)
20	Armed Forces' Handbook on Software in Safety-Critical Applications, M7762-000531 H ProgSäkE, 2001.
21	Försvarsmaktens instruktion för förvaring och transport av ammunition och övriga explosiva varor, IFTEX. (Armed Forces instructions for the storage and transportation of ammunition and other explosives.)
22	Säkerhetsinstruktion för vapen och ammunition med mera, Gemensam del, SäkI G. (Safety instructions for weapons and ammunition etc., Common part, SäkI G.)
23	Förtydligande av krav på systemsäkerhetsdokumentation vid fartygsutprovning, Försvarsmaktens skrivelse 14 910:75564, 2003-10-17. (Clarification of requirements for system safety documentation when testing vessels.)
24	Handbok Materielförvaltning Sjö (HMS). (Handbook on Materiel Management Marine.)

Ref no	Title
25	Handbok för Försvarsmaktens målsättningsarbete (H Mål), 2006. (Handbook for the Armed Forces' development of goals for units, supplies and facilities for the war organization's needs.)
26	Instruktion om Försvarsmaktens handbok Systemsäkerhet, beslutad med FM HKV 14 910:60223, 2010-06-08. (Instruction on the Armed Forces' Handbook on System Safety.)
27	Handbok för Riskanalys, Statens Räddningsverk 2003, ISBN 91-7253-178-9. (Handbook on Risk Analysis.)
28	Lag om brandfarliga och explosiva varor (LBE), SFS 2010:1011. (The Flammable and Explosive Goods Act.)
29	Lag om medicintekniska produkter, SFS 1993:584. (The Medical Devices/Products Act.)
30	Handbok Elsäkerhet i Försvarsmakten. (Handbook on Electrical Safety in the Armed Forces): • M7739-352015 intended for distribution and application in the Armed Forces and content licensed to SS-EN standard. The version should be applied within the Armed Forces by Armed Forces' personnel. • M7739-355002 is intended for distribution and application outside of the Armed Forces and does not maintain the SS-EN standard.
31	Militärtrafikförordningen SFS 2009:212. (Military Traffic Ordinance.)
32	Nomen F 97 Militärhögskolan BEGREPPSKATALOG. (Nomen F 97 Military Academy CONCEPTS DIRECTORY.)
33	Plan- och bygglagen, SFS 1987:10. (The Planning and Building Act.)
34	Regler för militär luftfart, RML. (Rules for Military Aviation.)
35	Regler för militär markverksamhet, RMM. (Rules for Military Ground Operations.)
36	Regler för militär sjöfart, RMS. (Rules for Naval Operations.)
37	Reliability, Maintainability and Risk. David J Smith Butterworth Heinemann.
38	RTCA/DO-178B, Software Considerations in Airborne Systems and Equipment Certification Requirements.
39	Safety Management Requirements for Defence Systems, UK DEF STAN 00-56.

Ref no	Title
40	Samordningsavtal mellan Försvarsmakten och FMV. Samordningsavtal mellan Försvarsmakten och FOI respektive FORTV med tillkommande överenskommelser om systemsäkerhetsverksamhet. (Coordination Agreement between the Armed Forces and the FMV. Coordination Agreement between the Armed Forces and FOI respectively, FORTV.)
41	Sjölagen, SFS 1994:1009. (The Navigation Act.)
42	Sprängämnesinspektionens föreskrifter (SÄIFS 1997:5) om import och om överföring av explosiva varor med ändringar i SÄIFS 1999:3. (The National (Swedish) Inspectorate of Explosives and Flammables Instructions on the import and transfer of explosives.)
43	STANAG 2418, Procedures for Expedient Repair including Battle Damage Repair.
44	STANAG 4439, Policy for Introduction and Testing for Insensitive Munition (IM).
45	Standard best practices for system safety program development and execution, ISO/GEIA-STD-0010.
46	System Safety Program Requirements, MIL-STD-882C.
47	The Tolerability of Risk from Nuclear Power Stations. UK HMSO 1992.
48	Värdering av risk, Räddningsverket Karlstad 1997, ISBN 91-88890-82-1. (The Evaluation of Risk.)

List of Figures

List of Tables

Project manager
Arne Börtemark, FMV

Subject experts
Arne Börtemark, FMV (Part 1 och 2)
Ragnar Ekholm, FMV (Part 1 och 2)
Pär-Anders Wallentin, Saab Dynamics AB (Part 2)
Lars Lange, FMV (Part 2)

Illustrations and cover
Leif Sundberg, Sörman Information AB
Mats Lundgren, Sörman Information AB

Original text
Mats Lundgren, Sörman Information AB

Digital edition
Mats Lundgren, Sörman Information AB

Cover photographs
Katsuhiko Tokunaga, SAAB
Peter Nilsson, Kockums
Sörman Information AB